Gallagher Command Centre

Underwriters' Laboratory Inc. - Canadian Standards and Configuration Requirements

Gallagher Security's product suite has been evaluated and certified by Underwriters Laboratory (UL) to meet Canadian Standards:

- CAN/ULC-S304:2016 - STANDARD FOR CONTROL UNITS, ACCESSORIES AND RECEIVING EQUIPMENT FOR INTRUSION ALARM SYSTEMS
  - Security Level IV
  - Active Communication Channel Security – Level A4
- CAN/ULC 60839-11-1:2022 - ALARM AND ELECTRONIC SECURITY SYSTEMS – PART 11-1: ELECTRONIC ACCESS CONTROL SYSTEMS - SYSTEM AND COMPONENTS REQUIREMENTS (IEC 60839-11-1:2013, MOD)
  - Grade 2

It is the responsibility of the security engineer and installer to adhere to the below installation standards for ULC compliance and certification. The Gallagher Command Centre commissioned system shall also be designed and installed in accordance with:

- CAN-ULC-S301-2018-(REV2 or later) - STANDARD FOR SIGNAL RECEIVING CENTRES CONFIGURATIONS AND OPERATIONS
- CAN-ULC-S302-14-(R2023 or later) - INSTALLATION, INSPECTION AND TESTING OF INTRUSION ALARM SYSTEMS
- CSA 22.1 - Canadian Electrical Code, Part I, Safety Standard for Electrical Installation

A commissioned Gallagher Command Centre system shall meet the above security classifications provided all configuration and product selection is met. This document provides unit compatibility information and specific configuration requirements to ensure the installed system complies with the license requirements and classification applicable to Gallagher Command Centre software and associated hardware.

Power source requirements for a ULC certified system:

1) The control unit shall be powered from a ULC 60839-11-1 / ULC ORD S304 Listed power supply with minimum standby power in accordance with:
   a) ULC S304: Security level IV - 24 hours minimum
   b) ULC 60839-11-1: Grade 2 – Standby power is optional.
2) The AC connection of the power supply must comply with CSA 22.1 - Canadian Electrical Code, Part I and the local municipal electrical authority. An authorised electrical technician is required to make the connection.
3) The supervision of the supply's primary power shall be accomplished by monitoring the AC loss contacts of the power supply.
4) The supervision of the power supply's standby battery source shall be accomplished by monitoring the battery fault and loss contacts of the power supply.

Copyright © Gallagher Group Limited

5) A supervised tamper switch shall be provided to monitor the rear side and entry side of the power supply's enclosure.
6) For either the AC loss or tamper conditions, a resultant status change must occur at a supervised alarm receiving station such as Gallagher Command Centre software and/or a ULC compliant central monitoring station.
7) Should the total equipment power requirement plus power to recharge the battery exceed the rating of a single power supply system, then additional power supplies must be provided. Requirements 1) to 6) must be applied.
8) Mechanical protection such as conduit between the power supply and the security control system's enclosure must securely in place to prevent tampering of the power cables.

The following power supply models have been UL evaluated with Gallagher products:

- Altronix AL400ULX
- Altronix eFlow4NB
- LifeSafety Power FP075
- LifeSafety Power FP0150

Installation requirements for a ULC certified system:

1) Products and systems that are not UL Listed for Burglar Alarm or Access Control cannot be connected in an UL Listed Burglar Alarm or Access Control system.
2) Products and systems listed in the User Guide are not listed as having UL certification unless included in this UL Configuration Requirements section.
3) Any cables providing signalling from outside the enclosure must be supervised using dual end of line resistors, connected as shown in the respective hardware Installation Notes.
4) If a Dual Cabinet is used without either a Gallagher Controller 6000 variant, Gallagher Controller 7000 variant or a Gallagher High Density I/O Interface, then a tamper board or mechanical tamper must be installed to provide anti-tamper protection at the door and rear of the cabinet.
5) All alarm signalling wires shall be a minimum of 22 AWG or larger.
6) All power wires shall be a minimum of 18 AWG or larger.
7) All communication (e.g. PSTN) wires shall be a minimum of 26AWG or larger.
8) The control unit shall be mounted and secured inside the protected area.
9) All knockouts on the Gallagher Dual Cabinet shall be connected to conduit in UL installations.
10) A UL approved Gallagher Security enclosure shall not be mounted over an electrical outlet. The unit shall be flush mounted to prevent access to the back of the enclosure and must be tamper protected and monitored at the front and rear of the enclosure.
11) The two Ethernet connections available on the Controller 6000HS and 6000HS PIV are referred to by Gallagher as "primary" and "secondary" Ethernet connections. This terminology does not infer Supplementary or Secondary (dual) communication circuits as defined in the UL Standard. The second Gallagher Ethernet port provides an alternative Controller communication path only should the first circuit fail.
12) The Watch Dog relay function in the C6000 High Security Controller has not been evaluated by UL**.**
13) The processor temperature monitor (Controller 6000HS and 6000HS PIV) has not been evaluated by UL.
14) HBUS devices have not been evaluated by UL in a 'daisy chain' configuration outside of the secured enclosure.
15) The model C7000 Controller PoE variants are not ULC 60839-11-1 & ULC S304 listed.
16) The model C7000 Controller DC RS485 and all QuickSwitch module variant communication lines are limited to max cable length of 98 feet (30 meters) to be installed in the same room.

Copyright © Gallagher Group Limited

Configuration requirements applicable to ULC S304 installations:

1) A UL compliant Listed power supply must be configured to supply 24 hours of standby power.
   a) Loss of AC power shall generate an alarm and transmitted to a supervised alarm receiving station such as Gallagher Command Centre software and/or a ULC compliant central monitoring station.
   b) Standby power (battery backup) fault shall generate an alarm and transmitted to supervised alarm receiving station such as Gallagher Command Centre software and/or a ULC compliant central monitoring station.
2) Gallagher Command Centre Software configuration requirements:
   a) If configured to partition, acknowledgement signal must be present at all arming terminals.
   b) Refer to the 'Configuring Local Overrides at Card Readers' topic in the Gallagher Command Centre help file, for instructions for arming/disarming alarm zones at a reader. This feature is only available when the system is installed for burglar alarm or burglar alarm and access applications.
   c) The priority of signals must be configured from highest to lowest priority as follows:
      Burglar Alarm
      Burglar-alarm supervision
      Unauthorised card read
      Other signals with Burglar Alarm system signals having the highest priority.
   d) The intruder alarm zone must be configured as fail to arm and must report to a supervised alarm receiving station if failure occurs.
   e) The local user:
      i. Cannot force arm the system unless open zones are to be manually bypassed (isolate/shunt) by the authorised user. Bypassing of the zone must be reported to a supervised alarm receiving station.
      ii. The keypad variants must display an arm/disarmed indicator to the area (Alarm Zone) the user is operating.
      iii. The display keypad variants must allow the user to view the status of the zones (inputs) during arming.
      iv. The entry delay must be configured to be 60 seconds or less and must generate a delay warning annunciation.
      v. The exit delay must be configured to be 45 seconds or less and must generate a delay warning annunciation.
   f) An operator logged into Gallagher Command Centre software:
      i. Must not be allowed to disarm the alarm zone remotely.
      ii. Is allowed to remote arm, but a 10-minute prewarming annunciation (e.g. reader beepers) must operate before the area (alarm zone) becomes armed.
   g) The system must report the identified user's arming/disarming, denied & granted to a supervised alarm receiving station.
   h) All panels must have a "System" alarm zone (must not be set to area [CC] 00) that must report all events to a supervised alarm receiving station during armed and disarmed.
      i. If the system area is armed, then it shall operate the siren.
      ii. If the system area is disarmed, it must not operate the siren.
      iii. All hardware faults including all types of power and communication fault events must report to a supervised alarm receiving station as a silent alarm.
      iv. Mains fail, battery fail, and low battery functions shall be configured to the same "System" alarm zone the control panel is powered from.
      v. Enclosure tamper must report to a supervised alarm receiving station as a trouble/silent alarm.
3) Communication medium to a central monitoring station:
   a) The communication medium between the protected property and the central monitoring station shall be for the exclusive use of the protected property and is not to be shared with other subscribers.
   b) For ULC 60839-11-1, Grade 2 compliance with the PSTN dialler, maximum delay time for signals reaching the monitoring console is 90s.

Copyright © Gallagher Group Limited

c) For ULC 60839-11-1, Grade 2 compliance with the PSTN dialler, the minimum number of required characters for access by memorized information only shall be 5 characters numeric.

d) In the event of unsuccessful communication, the PSTN dialler shall make a minimum of 5 and maximum of 10 attempts. Where the maximum attempts are reached, an indication of the failure shall be made at the premises.

e) In no event shall the time from going off-hook to on-hook exceed 90s per attempt.

f) Periodic test signals must be configured for:

   i. PSTN: 24 hours

   ii. TCP/IP (PSDN): 1 minute

g) If dual path communication is present (i.e. PSTN & TCP/IP) the primary means of communication must report communication failure/loss via the secondary path to the central monitoring station.

h) When multiplex system signals are transmitted directly from the protected systems to the central supervising station and the loss of the channel prevents the receipt of signals from protective circuits beyond the fault, the number of separate signals (i.e. control units) on a single channel is limited to 1000.

i) If the Ethernet (PSDN) communication fails or a compromise attempt is detected the following message will be displayed at the monitoring station:

   Controller '[Name]' Offline

j) For security levels III and IV, a means to communicate via cellular transmission as an alternative and be equipped with 24-hour standby power must be supplied. Otherwise, the customer must provide 24-hour UPS backup across their networking equipment between the controller and the alarm receiving station.

4) The UPS shall comply with the Standard for Uninterruptable Power Supply Equipment, UL 1778, or the Standard for Fire Protective Signaling Devices, UL 1481. In order to perform maintenance and repair service, a means for disconnecting the input to the UPS while maintaining continuity of power to the automation system shall be provided.

The following points are only applicable to the central supervisory (receiving) station:

5) Line transient protection complying with the Standard for Transient Voltage Surge Suppressors, UL 1449, with a maximum marked rating of 330 V.

6) Signal line transient protection complying with the Standard for Protectors for Data Communications and Fire Alarm Circuits, UL 497B, with a maximum marked rating of 50 volts.

7) Communication circuits and network components connected to the telecommunications network shall be protected by secondary protectors for communication circuits. These protectors shall comply with the Standard for Secondary Protectors for Communications Circuits, UL 497A. These protectors shall be used only on the protected side of the telecommunications network.

8) The central supervisory equipment shall be installed in a temperature-controlled environment. A temperature-controlled environment is defined as one that can be maintained between 13 – 35ºC (55 – 95ºF) by the HVAC system. 24 h of standby power shall be provided for the HVAC system. The standby power system for the HVAC system may be supplied by an engine driven generator alone. A standby battery is not required to be used.

9) PoE power source configuration of the 7000 Single Door Controllers is not listed to ULC S304.

10) For the models 7000 Single Door Controllers RS485 versions the communication Port A/B wire leads installer is not permitted to connect cables greater that 98.5 feet (30 meters) long to the product or to specific circuits of the product.

Copyright © Gallagher Group Limited

Configuration requirements applicable to ULC 60839-11-1 installations:

1) The minimum system configuration consists of:
   Model Gallagher Controller 6000 or 7000 variants, Listed (ALVY), (APOU) power supply, reader and lock.
2) For alarm supervision, the access control system shall also comply with the above ULC S304 requirements.
3) The Door open too long pre-warning annunciation device (the reader beeper) shall operate for 10 seconds before alarm is generated at the alarm receiving station.
4) If Card plus PIN function is configured at the door, the user must be disabled after 5 failed access request attempts.

The below table describes optional functions that have been evaluated by UL as pass and meets the specified requirements.

ULC 60839-11-1 Location	Optional Features verified
Table 2, Line 4	When the release time is configurable, several permitted values can be associated to access rights per portal
Table 2, Line 8	Soft anti-passback
Table 2, Line 14	Visitor escorted access
Table 2, Line 15	Supervisor mode
Table 2, Line 16	Dual occupancy
Table 2, Line 18	Singularization
Table 2, Line 19	Elevator control
Table 2, Line 23	When configurable, several permitted open times may be associated with access rights per access point
Table 3, Line 3	Visual and/or audible indication of portal locked status until access is granted
Table 3, Line 5	Visual annunciation is required when access is granted
Table 3, Line 8	Card usage counter
Table 3, Line 43	Visual annunciation, alert and logging are required when dual/multiple occupancy conditions are not respected (minimum number of persons not present)
Table 4, Line 2	The system shall be capable of managing multiple time zones
Table 4, Line 11	System should be capable of assigning access rights to a group of credentials
Table 4, Line 12	System should be capable of changing access rights to a group of credentials in response to emergency conditions
Table 4, Line 16	The system shall use token
Table 4, Line 17	The system shall use memorized information and token
Table 6, Line 2	System-wide free access granting
Table 6, Line 3	Free access granting until further system command, single portal or group of portals
Table 6, Line 4	Scheduled/timed free access granting, single portal or group of portals
Table 6, Line 6	Blocking of portal until further system command, single portal or group of portals
Table 6, Line 7	Scheduled/timed blocking of portal, single portal or group of portals

Products meeting ULC 60839-11-1 Impact and Ingress evaluation:

UL have evaluated the Gallagher Dual Cabinet, reinforced door C200107 to meet the minimum requirements of ULC 60839-11-1 impact rating of IK04 and ingress rating of IP4X. All other products have not been evaluated by UL.

Copyright © Gallagher Group Limited

Product Classification & Technical Specifications:

☑ Mandatory requirement to comply with the associated standard.
☒ Not permitted for use for the associated standard.
✓ Optional. Allowed for use for the associated standard.

Application Software	Version	Models	ULC-S304 Security Level	ULC 60839-11-1 Security Grade
Gallagher Command Centre	vEL9.xx.xxx	C201311	A4	2
Gallagher Controller software	vCR9.10.xxxxxxx	C300100 C300101 C305101 C400020 C400021 C400010 C400011	A4	2

Server and Workstation Hardware	Models	ULC-S304	ULC 60839-11-1
Any ITE60950 compliant computer	Various	✓	✓
Any ITE60950 listed printer	Various	✓	✓

Network Equipment	Models	ULC-S304	ULC 60839-11-1
Any ITE60950 and/or UL62368-1 compliant equipment	Various	✓	✓

DC Power Supply	Models	ULC-S304 Security Level	ULC 60839-11-1 Security Grade
Units shall be connected to a ULC Listed power supply or control panel which can supply a standby power to minimum Security graded numbers of hours utilizing standby batteries. The power supply shall provide an output voltage compatible with the input voltage range of the units being energized under normal and standby conditions	Various	A4 (24 hrs)	2 (optional)

Cabinets	Models	ULC-S304 Security Level	ULC 60839-11-1 Security Grade	ULC 60839-11-1 Environmental Grade/Class
Gallagher Cabinet	C200100	A4	2	Indoor dry
Gallagher Dual Cabinet	C200104	A4	2	Indoor dry
Gallagher Dual Cabinet, reinforced door (UL Evaluated)	C200107	A4	2	Indoor dry

Gallagher Controller hardware installed in C200100 Cabinets	Models	ULC-S304 Security Level	ULC 60839-11-1 Security Grade	ULC 60839-11-1 Environmental Grade/Class
Controller 6000 x* equipment, PCB with protective covers	C3001xx	A4	2	Indoor
Controller 6000 Enhanced x* equipment, PCB with protective covers	C3001xx	A4	2	Indoor
Controller 6000NU x* equipment, PCB with protective covers	C3001xx	A4	2	Indoor
Controller 6000HS High Security x* equipment, PCB with protective covers	C3051xx	A4	2	Indoor
Controller 7000 equipment, PCB with protective covers	C4001xx	A4	2	Indoor
Controller 7000 Single Door variants with mounting plate accessory	C4000xx	A4	2	Indoor
Controller 7000 Single Door Standard variants with mounting plate accessory	C4000xx	A4	2	Indoor

Copyright © Gallagher Group Limited

Gallagher Controller hardware installed in C200104 Dual Cabinets	Models	ULC-S304 Security Level	ULC 60839-11-1 Security Grade	ULC 60839-11-1 Environmental Grade/Class
Controller 6000 x* equipment, PCB with protective covers	C3001xx	A4	2	Indoor
Controller 6000HS x* equipment, PCB with protective covers	C3001xx	A4	2	Indoor
Controller 6000NU x* equipment, PCB with protective covers	C3001xx	A4	2	Indoor
Controller 6000HS PIV x* equipment, PCB with protective covers	C3051xx	A4	2	Indoor
Controller 7000 equipment, PCB with protective covers	C4001xx	A4	2	Indoor
Controller 7000 Single Door variants with mounting plate accessory (DC) Wiegand / RS485	C4000xx	A4	2	Indoor

* x refers to variations incorporating software limits

Gallagher Reader Modules associated with Gallagher 6000 and 7000 Standard variant Controllers	Models	ULC-S304 Security Level	ULC 60839-11-1 Security Grade	ULC 60839-11-1 Environmental Grade/Class
4H Module	C300142	A4	2	Indoor
8H Module	C300182	A4	2	Indoor

Gallagher Devices installed in either C200100 cabinets or C200104 Dual Cabinets	Models	ULC-S304 Security Level	ULC 60839-11-1 Security Grade	ULC 60839-11-1 Environmenta Grade/Class
HBUS 8 In 2 Out Door Module	C300660	A4	2	Indoor
HBUS 8 In Board	C300680	A4	2	Indoor
HBUS 8 In 4 Out Board	C300684	A4	2	Indoor
HBUS 16 In 16 Out Board	C300688	A4	2	Indoor
HBUS 8 Port Hub	C300698	A4	2	Indoor

UL have evaluated the below listed 3rd party cabinets to be compatible with the selected Gallagher products to meet ULC S 304 and ULC 60839-11-1. Refer to the listed manufacturers ULC rated classifications.

Gallagher Product	Model	3rd Party UL compliant Cabinet
Controller 7000 Equipment	C4001xx	• Life Safety Power FPO150-E4M PSU & E4 Enclosure • Altronix Trove M2 PSU & Enclosure Kit
Controller 7000 High Security	C405101	
QuickSwitch ME02	C300700	
QuickSwitch ME52	C300701	
QuickSwitch ME16IN	C300706	
QuickSwitch ME16OUT	C300707	

Copyright © Gallagher Group Limited

Gallagher T Series Readers	Models	ULC-S304 Security Level	ULC 60839-11-1 Security Grade	ULC 60839-11-1 Environmental Grade/Class
Gallagher T Series Readers are UL approved for use with the following control equipment models as follows: Gallagher Controller 6000, 6000NU, 6000 Enhanced, 6000HS High Security, Controller 7000 Standard Gallagher Controller 7000 Single Door DC variants Gallagher 4H Module, Gallagher 8H Module				
T10 MIFARE Reader	C300400 C300401	A4	2	Outdoor
T10 MIFARE Reader, High Security	C305400 C305401	A4	2	Outdoor
T11 MIFARE Reader	C300410 C300411	A4	2	Outdoor
T11 MIFARE Reader, High Security	C305410 C305411	A4	2	Outdoor
T11 Multi Tech Reader	C300430 C300431	A4	2	Outdoor
T11 Multi Tech Reader, High Security	C305430 C305431	A4	2	Outdoor
T12 MIFARE Reader	C300420 C300421	A4	2	Outdoor
T12 Multi Tech Reader	C300440 C300441	A4	2	Outdoor
T15 MIFARE Reader	C300470 C300471	A4	2	Outdoor
T15 MIFARE Reader, High Security	C305470 C305471	A4	2	Outdoor
T15 Multi Tech Reader	C300480 C300481	A4	2	Outdoor
T15 Multi Tech Reader, High Security	C305480 C305481	A4	2	Outdoor
T20 MIFARE Terminal	C300450 C300451	A4	2	Indoor
T20 Multi Tech Terminal	C300460 C300461	A4	2	Indoor
T20 MIFARE Terminal, High Security	C305450 C305451	A4	2	Indoor
T20 Multi Tech Terminal, High Security	C305460 C305461	A4	2	Indoor
T21 MIFARE Reader, High Security	C305500 C305501	A4	2	Indoor
T21 High Security Reader REV1	C305505 C305506	A4	2	Indoor
T21 Multi Tech Reader, High Security	C305510 C305511	A4	2	Indoor
T30 Multi Tech Keypad Reader	C300490 C300491	A4	2	Outdoor
T30 MIFARE Keypad Reader	C300495 C300496	A4	2	Outdoor

HID Readers	Models	ULC-S304	ULC 60839-11-1
HID Reader	5355A	✓	✓
UL has evaluated R10E-R40E and RPK10E-RPK/RP40E Readers for 7000 Controllers using Wiegand protocol.	5365	✓	✓

Copyright © Gallagher Group Limited

Voltage / Current Measurements

The following table lists Gallagher hardware voltage and current limits to meet UL specifications:

Module	Input		Output			
	Voltage	Current	Relay		Vout	
			Voltage	Current	Voltage	Current
Tamper Board	5 Vdc	30 mA	N/A	N/A	N/A	N/A
HBUS 8 In 2 Out Reader Module	13.6±15% Vdc	50 mA (relays off) 135 mA (relays on)	24V DC/AC	3A resistive, 1A inductive	10-16 Vdc	500 mA
HBUS 4 In 2 Out Module, Wiegand	13.6±15% Vdc	50 mA (relays off) 135 mA (relays on)	24V DC/AC	3A resistive, 1A inductive	13.6 Vdc	750 mA
HBUS 8 In Module	13.6±15% Vdc	50 mA	N/A	N/A	N/A	N/A
HBUS 8 In 4 Out Module	13.6±15% Vdc	45 mA (relays off) 200 mA (relays on)	24V DC/AC	3A resistive, 1A inductive	N/A	N/A
HBUS 16 In 16 Out Module	13.6±15% Vdc	73 mA (relays off) 674 mA (relays on)	24V DC/AC	3A resistive, 1A inductive	N/A	N/A
HBUS 8 Port Hub	13.6±15% Vdc	20 mA	N/A	N/A	N/A	N/A
PSTN Dialler	13.6±15% Vdc	300mA	24V DC/AC	3A resistive, 1A inductive	N/A	N/A
QuickSwitch ME02	13.6±15% Vdc	50 mA (relays off) 200 mA (relays on)	24V DC/AC	3A resistive, 1A inductive	Output is off-set from input by 0.5VDC	600 mA per reader port
QuickSwitch ME52	13.6±15% Vdc	50 mA (relays off) 275 mA (relays on)	24V DC/AC	3A resistive, 1A inductive	Output is off-set from input by 0.5VDC	600 mA per reader port
QuickSwitch ME16IN	13.6±15% Vdc	40 mA (relays off) 115 mA (relays on)	24V DC/AC	3A resistive, 1A inductive	N/A	N/A
QuickSwitch ME16OUT	13.6±15% Vdc	30 mA (relays on) 650 mA (relays off)	24V DC/AC	3A resistive, 1A inductive	N/A	N/A

Copyright © Gallagher Group Limited

Module	Input		Output			
	Voltage	Current	RS485 1		RS485 2	
			Voltage	Current	Voltage	Current
6000 Controller 6000NU Controller	13.6 +15% Vdc	1.94 A	9-16 Vdc	750 mA	9-16 Vdc	750 mA
6000HS Controller 6000HS High Security Controller	13.6±15% Vdc	2.0 A	9-16 Vdc	750 mA	9-16 Vdc	750 mA
7000 Standard Controller (C400100)	13.6±15% Vdc	130 mA	VDC Output is offset from input by 0.4VDC	750 mA	VDC Output is offset from input by 0.4VDC	750 mA
Controller 7000 Enhanced (C400101)	13.6±15% Vdc	200 mA	VDC Output is offset from input by 0.4VDC	750 mA	VDC Output is offset from input by 0.4VDC	750 mA
Controller 7000 High Security (C405101)	13.6±15% Vdc	200 mA	VDC Output is offset from input by 0.4VDC	750 mA	VDC Output is offset from input by 0.4VDC	750 mA

Module	Input		Output							
	Voltage	Current	Vout 1		Vout 2		Vout 3		Vout 4	
			Voltage	Current	Voltage	Current	Voltage	Current	Voltage	Current
4H Module	13.6 +15% Vdc	2.09 A	9-16 Vdc	750 mA	9-16 Vdc	750 mA	N/A	N/A	N/A	N/A
8H Module	13.6 +15% Vdc	3.96 A	9-16 Vdc	750 mA	9-16 Vdc	750 mA	9-16 Vdc	750 mA	9-16 Vdc	750 mA

CONTROLLER 7000 SINGLE DOOR

Module	Input		Output				Battery Charge	
	Voltage	Current/ Watts	Lock Output / AUX		Reader Output		Voltage	Current/ Watts
			Voltage	Current/ Watts	Voltage	Current/ Watts		
Controller 7000 Single Door, RS485 (C400010)	13.6±15% Vdc	1.5 Amps	13.6±15% Vdc	1A	13.6±15% Vdc	0.6A	N/A	N/A
Controller 7000 Single Door, Wiegand (C400011)	13.6±15% Vdc	1.5 Amps	13.6±15% Vdc	1A	13.6±15% Vdc	0.6A	N/A	N/A
Controller 7000 Single Door Relay Board (C400910)	13.6±15% Vdc	45 mA	N/A	N/A	N/A	N/A	N/A	N/A

OUTPUTS (Dry)

Model	Voltage	Current
Controller 7000 Single Board Relay Board (C400910)	24 VAC/VDC	3 A (Resistive) (S)
		1 A (Inductive) (S)
Controller 7000 Single Door, RS485 (C400010) Controller 7000 Single Door, Wiegand (C400011)	24 VAC/VDC	3 A (Resistive) (S)
		1 A (Inductive) (S)

(S) = separately energized

Copyright © Gallagher Group Limited

Reader Model	Part No.	9 Volts Supply		16 Volts Supply	
		Normal standby (mA)	Operate (mA)	Normal standby (mA)	Operate (mA)
T10 MIFARE Reader	C300400 (Black) C300401 (White)	73.2	123.2	43.3	70.1
T10 PIV Reader	C305400 (Black) C305401 (White)	82.5	158.2	47.4	72.3
T11 MIFARE Reader	C300410 (Black) C300411 (White)	63.2	110.4	40.5	61.1
T11 Multi Tech Reader	C300430 (Black) C300431 (White)	72.5	127.7	43.9	68.1
T11 High Security MIFARE Reader	C305410 (Black) C305411 (White)	79	125	44.75	77
T11 High Security Multi Tech Reader	C305430 (Black) C305431 (White)	116.6	210.2	99.1	176
T11 High Security Custom Multi Tech Reader	C305830 (Black) C305831 (White)	111.3	200.6	94.3	169.4
T12 MIFARE Reader	C300420 (Black) C300421 (White)	63.2	110.4	40.5	61.1
T12 Multi Tech Reader	C300440 (Black) C300441 (White)	72.5	127.7	43.9	68.1
T15 MIFARE Reader	C300470 (Black) C300471 (White)	70	115	50	77
T15 Multi Tech Reader	C300480 (Black) C300481 (White)	110	168	81	136
T15 MIFARE Reader, High Security	C305470 (Black) C305471 (White)	70	115	50	77
T15 Multi Tech Reader, High Security	C305480 (Black) C305481 (White)	110	168	81	136
T20 MIFARE Terminal	C300450 (Black) C300451 (White)	262	420	168	257
T20 Multi Tech Terminal	C300460 (Black) C300461 (White)	246	450	157	283
T20 MIFARE Terminal, High Security	C305450 (Black) C305451 (White)	262	420	168	257
T20 Multi Tech Terminal, High Security	C305460 (Black) C305461 (White)	246	450	157	283
T21 MIFARE Reader, High Security	C305500 (Black) C305506 (White)	233	357	149	218
T21 PIV Reader REV1	C305505 (Black) C305501 (White)	293	464	200	257
T21 Multi Tech Reader, High Security	C305510 (Black) C305511 (White)	255	464	164	281
T30 Multi Tech Keypad Reader	C300490 (Black) C300491 (White)	165	266	111	173
T30 MIFARE Keypad Reader	C300495 (Black) C300496 (White)	166	267	111	174

Copyright © Gallagher Group Limited

Appendix A:

Configuration required confirming that the central station is notified of system arming.

The UL requirement is to ensure an Alarm Zone cannot be armed should the receiving station (server) be off-line. As a general rule, all Gallagher Controller activity is managed on the Controller and will continue to function should the Controller go off-line. To meet the UL requirement, the Controller must attempt to contact a function which is only server based to verify that the server is present, before allowing the Alarm Zone to set.

The configuration described below operates as follows:

(i) A request to arm is presented to a "pre-arm" Alarm Zone.
(ii) The output status of the pre-arm Alarm Zone is used to initiate a server-based macro.
(iii) When contacted, the macro requests the main Alarm Zone to arm.
(iv) The main Alarm Zone arms.
(v) If the server is not on-line, then the macro cannot be initiated, therefore the main Alarm Zone will not arm.
It must be noted that should an attempt to arm or disarm an Alarm Zone whilst the server is off-line will require an arm/disarm cycle of the Alarm Zone to confirm its exact status once the server is back on-line. This is not applicable should a server go off-line and then return to on-line without any arm/disarm state change requests while the server is off-line.

Prior to configuring for this requirement, a <Controller> is configured "Controller" and an <Alarm Zone> "Controller Default Alarm Zone" is associated. Carry out the following configuration.

1. Create the <Door> or <Remote Arming Terminal> required to arm and disarm the Alarm Zone.
   a. Assign "Controller Default Alarm Zone" as the default Alarm Zone for all events.
   b. For the door <Entry Reader>, ensure that <Double Card Overrides>, <Arm Alarm Zone> is checked.

2. Create an <Output> "Office Alarm Zone Armed".
   a. Assign "Controller Default Alarm Zone" as the default Alarm Zone for all events.
   b. Save and exit.

3. Create an <Output> "Strobe lamp".
   a. Assign "Controller Default Alarm Zone" as the default Alarm Zone for all events.
   b. On the <Advanced tab>, check <Output is pulsed when activated>.
   c. Set the <Pulse Time> to 1 or more seconds.
   d. Save and exit.

4. Create an <Output> "Office Alarm Zone Disarmed".
   a. Assign "Controller Default Alarm Zone" as the default Alarm Zone for all events.
   b. On the <Advanced> tab, change the <Mapping to an input state> to "On is Closed, Off is Open".
   c. Save and exit.

5. Create a <Macro> "Office Armed".
   a. On the <Action Tab>, drag and drop the "Strobe Lamp" into the window.
   b. Select the "Strobe Lamp" within the macro window.
   c. Set the <Override> to <Pulse>.
   d. Save and exit.

Copyright © Gallagher Group Limited

6. Create an <Action Plan> named “Intruder Alarm”.
    a. Select the <Disarmed> tab.
    b. Drag and drop the “Office Armed” macro from the macro window, into the <Cameras, Macros, and External System Items> window.
    c. Set the <Alarm Priority> to <Not an Event>.
    d. Save and exit.

7. Create an <Output> “Office Alarm Zone pre-arm status”.
    a. Assign “Controller Default Alarm Zone” as the default Alarm Zone for all events.
    b. On the <Event Response> tab, change the <Closed/On> Action Plan to “Intruder Alarm”.
    c. Save and exit.

8. Create an <Alarm Zone> “Pre-arm Office Alarm Zone”.
    a. On the <Connections> tab, assign this Alarm Zone to the “Controller”.
    b. On the <Reflect Outputs> tab, drag and drop the Office Alarm Zone pre-arm status output into the <Armed State> window.
    c. Drag and drop the “Office Alarm Zone disarm” output into the <Disarmed State> window.
    d. Save and exit.

9. For the <Door Access Zone> associated with the door required to arm/disarm the Alarm Zone, configure the <Event Response>, <Alarm Zone for All Events> to use the “Pre-arm Office Alarm Zone”.
    a. Save and exit.

10. For a <Remote Arming terminal>, assign the “Pre-arm Office Alarm Zone” to <Alarm Zones>.
    a. Save and exit.

11. Create an <Alarm Zone> “OFFICE ALARM ZONE”
    a. On the <Connections> tab, assign it to the “Controller”.
    b. On the <Push Buttons> tab, drag and drop the “Strobe lamp” output into the <Armed State> window.
    c. Drag and drop the “Office Alarm Zone Disarmed” output into the <Disarmed State> window.
    d. On the <Reflect Outputs> tab, drag and drop the “Office Alarm Zone Armed” output into the Armed State window.
    e. Save and exit.

12. Create a <Cardholder>
    a. Assign the <Cardholder> access to either the “door” or the “Remote Arming terminal”.
    b. Ensure that the <Cardholder> has the ability to override the “Pre-arm Office Alarm Zone” state to either Armed or Disarmed.

Copyright © Gallagher Group Limited