

Event code reporting for Challenger10 and ChallengerPlus

Copyright ©2025 Aritech, All Rights Reserved.

Trademarks and patents The Challenger name and logo are trademarks of KGS Fire and Security Australia Pty Ltd.

All trademarks are the property of their respective owners.

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



Contact information For contact information, see www.aritech.com.au

Content

CID Reporting Codes	4
CID Codes via RAS / Keypad entry	7
STU serial reporting formats	9
STU serial data.....	9
STU system messages	9
STU channel data.....	10
Decimal to CID Hex cross-reference	11

CID Reporting Codes

The table below lists CID reporting codes for the Challenger system. This table covers system and device events, and is laid out in a similar format to how the control room will receive them. For example, a monitoring control room would see a CID event as:

ACCT MT QXYZ GG CCC

ACCT = 4 digit account number, as determined by the comms path or area. (Not covered in table below)

MT = Message Type, used to identify the CID message to the receiver. (Not covered in table below)

Q = Event qualifier. This is typically either a '1' (new event), or a '3' (restored event). Events capable of sending restoral codes are specified in the table below.

XYZ = Event Code.

GG = Group Number. '00' is used to indicate no group applies, typically for system events.

CCC = Zone or User Number. '000' is used to indicate no zone or user information applies.

Event Code	Group Number	Zone / User Number	Description	Restoral ¹	Min	Max	Type	C10	CH+
102	00	375	Guard failed to check in within required time					Y	Y
120	00	1-128	Duress entered at RAS	Y	1	128	Door / RAS	Y	Y
121	00	1-999	Duress was activated with a wireless pendant	Y	1	999	User	Y	Y
130	1-99	1-999	Input secure alarm	Y	1	999	Input	Y	Y
139	1-99	1-999	Input alarm has unsealed again without being reset	Y	1	999	Input	Y	Y
140	00	421	Area was armed again during area search without testing all required inputs					Y	Y
140	00	422	All inputs failed to be tested during area search	Y				Y	Y
140 ³	1-99	1-999	Input alarm, CID type programmed by input database (default 140)	Y	1	999	Input	Y	Y
143	00	1-128	RAS offline	Y	1	128	Door / RAS	Y	Y
143	00	129-160	DGP offline	Y	1	32	DGP	Y	Y
143	00	554-585	Sub RAS on NAC has gone offline ²	Y	1	32	DGP		Y
143	00	586-617	1st sub DGP on NAC has gone offline ²	Y	1	32	DGP		Y
145	00	1-128	RAS tamper fail / incorrect PIN entered at RAS too many times	Y	1	128	Door / RAS	Y	Y
145	00	129-160	DGP tamper fail	Y	1	32	DGP	Y	Y
145	00	554-585	1st sub RAS on NAC has gone into tamper ²	Y	1	32	DGP		Y
145	00	586-617	1st sub DGP on NAC has gone into tamper ²	Y	1	32	DGP		Y
150	00	361	Camera film is low	Y				Y	Y
150	00	362	Camera film is out	Y				Y	Y
150	00	363	Courier entered the building					Y	Y
150	00	366	Access test was started	Y				Y	Y
150	00	367	Access test failed to test inputs					Y	Y
150	00	368	Access test successfully tested inputs					Y	Y
150	00	369	Secure test was started	Y				Y	Y
150	00	370	Secure test failed to test inputs					Y	Y
150	00	371	Secure test successfully tested inputs					Y	Y
150	00	372	The delay button was pressed and timer started					Y	Y
150	00	373	Alarms were reset automatically					Y	Y

Event Code	Group Number	Zone / User Number	Description	Restoral ¹	Min	Max	Type	C10	CH+
150	00	374	Panel time is changed					Y	Y
150	00	377	Technician is on site	Y				Y	Y
150	00	378	Program mode entered via RAS					Y	Y
300	00	129-160	DGP fuse fail	Y	1	32	DGP	Y	Y
300	00	586-617	1st sub DGP on NAC has gone into fuse fail ²	Y	1	32	DGP		Y
301	00	129-160	DGP mains fail	Y	1	32	DGP	Y	Y
301	00	586-617	1st sub DGP on NAC has gone into mains fail ²	Y	1	32	DGP		Y
302	00	129-160	DGP battery low	Y	1	32	DGP	Y	Y
302	00	586-617	1st sub DGP on NAC has gone into low battery ²	Y	1	32	DGP		Y
303	00	1-16	RAS encryption reset COMMS 1		1	16	RAS	Y	Y
303	00	65-80	RAS encryption reset COMMS 2		65	80	RAS	Y	Y
303	00	129-160	DGP Encryption reset		1	32	DGP	Y	Y
304	00	1-16	RAS dipswitch or address changed		1	16	RAS	Y	Y
304	00	65-80	RAS dipswitch or address changed		65	80	RAS	Y	Y
304	00	129-160	DGP dip switch changed		1	32	DGP	Y	Y
305	00	1-16	RAS CPU restart		1	16	RAS	Y	Y
305	00	65-80	RAS CPU restart		65	80	RAS	Y	Y
305	00	129-160	DGP CPU restarted		1	32	DGP	Y	Y
307	1-99	1-999	Input failed to test with required number of days	Y	1	999	Input	Y	Y
309	00	129-160	DGP battery test fail	Y	1	32	DGP	Y	Y
311	00	129-160	DGP battery missing		1	32	DGP		Y
311	00	586-617	1st sub DGP on NAC has reported a battery missing ²		1	32	DGP		Y
320	00	129-160	DGP siren fail	Y	1	32	DGP	Y	Y
320	00	586-617	1st sub DGP on NAC has gone into siren fail ²	Y	1	32	DGP		Y
330	00	1-128	RAS depolled	Y	1	128	Door / RAS	Y	Y
330	00	129-160	DGP depolled	Y	1	32	DGP	Y	Y
333	00	423-425	Hardware failure with expander	Y	1	3	Expander	Y	Y
339	00	425	Memory expander has been defaulted					Y	Y
343	00	425	Memory expander has been unable to restore all the users from its SD card					Y	Y
344	00	129-160	Radio frequency has been jammed on wireless DGP	Y	1	32	DGP	Y	Y
344	00	586-617	1st sub DGP on NAC has gone into RF jamming fault ²	Y	1	32	DGP		Y
350	00	393-402	Comm path cannot be reached	Y	1	10	Path	Y	Y
351	00	0	Modem line failed during check	Y				Y	Y
351	00	995	UltraSync is no longer using fastest and most secure connection	Y					Y
354	00	423-425	Communication fault with expander (3G/4G)	Y	1	3	Expander	Y	Y
374	1-99	1-999	Input exit alarm	Y	1	999	Input	Y	Y
381	1-99	1-999	Wireless detector was not detected during routine supervision check	Y	1	999	Input	Y	Y
383	1-99	1-999	Input tamper	Y	1	999	Input	Y	Y
384	1-99	1-999	Wireless detector has low battery	Y	1	999	Input	Y	Y
393	1-99	1-999	Wireless detector is dirty	Y	1	999	Input	Y	Y
402	1-99	1-999	Area armed	Y	1	999	User	Y	Y

Event Code	Group Number	Zone / User Number	Description	Restoral ¹	Min	Max	Type	C10	CH+
411	00	0	Request for technician is sent					Y	Y
416	00	393-402	Management software has connected via comm path		1	10	Path	Y	Y
570	00	1-16	RAS isolated	Y	1	16	RAS	Y	Y
570	00	65-80	RAS deisolated		65	80	RAS	Y	Y
570	00	129-160	DGP isolated	Y	1	32	DGP	Y	Y
570	00	554-585	1st sub RAS on NAC has been isolated ²	Y	1	32	DGP		Y
570	00	365	Camera & popup (bandit) screen disabled	Y				Y	Y
570	00	586-617	1st sub DGP on NAC has been isolated ²	Y	1	32	DGP		Y
570	1-99	1-999	Input isolated	Y	1	999	Input	Y	Y
602	00	393-402	Auto test call was sent to comm path		1	10	Path	Y	Y
608	00	260-358	Area has been disarmed outside of its out of hours time zone	Y	1	99	Area	Y	Y
611	1-99	1-999	Input tested successfully during access/secure test		1	999	Input	Y	Y
701	00	1-999	Battery low on wireless pendant	Y	1	999	User	Y	Y
702	00	1-999	Tamper was activated on a wireless pendant	Y	1	999	User	Y	Y
703	00	408	Panel Ethernet link has failed	Y				Y	Y
703	00	423-425	Expander Ethernet link has failed	Y	1	3	Expander		Y
704	00	393-402	Heartbeat failed on comm path	Y	1	10	Path	Y	Y
706	00	410	Ethernet hardware failed to initialise	Y				Y	Y
711	00	393-402	Auto test call failed to report		1	10	Path	Y	Y
712	00	409	Firmware upgrade was started					Y	Y
713	00	409	Firmware upgrade was completed					Y	Y
714	00	1-128	A TS0866, TS0867, or TS0869 will report a door fault when an associated subRAS is offline. ² A NAC door will report a door fault when an associated subDGP/RAS is offline/tamper or an associated input is in tamper. ²	Y	1	128	Door		Y
715	00	1-128	A TS0866, TS0867, or TS0869 will report a reader fault when an associated subRAS is in tamper. ² A NAC door will report a reader fault when an associated reader fails because an associated subRAS/DGP is offline/tamper. ²	Y	1	128	Door		Y
716	00	393-402	History in comm path was deleted		1	10	Path		Y
717	00	129-160	DGP requires a voltage calibration		1	32	DGP		Y
718	00	129-160	DGP is in power supply shutdown due to fault that hasn't restored within 32 hours		1	32	DGP		Y
719	00	1-128	Door alarms isolated (DOTL alarm, Forced door, door input faults, egress input faults, interlock input faults)	Y	1	128	Door		Y

NOTES

1. Restoral events use the same **Event Code** as the event report. Events (E) are sent with a prefix '1', Restores (R) are sent with a prefix '3'
2. In this case, a report will only be generated the first time the event occurs, and the restore will only be sent once all devices with that condition are restored.
For example: If sub-RAS 1 goes offline, then later sub-RAS 2 goes offline, sub-RAS 1 will report the event. The restoral will only be sent when both sub-RAS 1 and 2 are back online.
3. ID code (report ID type) is 140 by default. This should be set by the installer to an appropriate CID code using the Inputs configuration menu or form. See "CID Codes via RAS / Keypad entry" below for more details.

CID Codes via RAS / Keypad entry

For each input that you need to send Ademco Contact ID (CID) event messages to a remote monitoring company, you need to program a report ID type. When selecting report ID types on an LCD RAS, only the Contact ID code and classification are displayed (the sub-classification is not displayed on the RAS).

The table below shows the relationship between the Report Type entered through a RAS Keypad, and the CID details it relates to.

Report Type (RAS)	CID Code	Classification	Sub-classification
1	100	Medical alarm	Medical
2	101	Medical alarm	Personal emergency
3	102	Medical alarm	Fail to check in
4	110	Fire alarm	Fire alarm
5	111	Fire alarm	Smoke
6	112	Fire alarm	Combustion
7	113	Fire alarm	Waterflow
8	114	Fire alarm	Heat
9	115	Fire alarm	Pull station
10	116	Fire alarm	Duct detector
11	117	Fire alarm	Flame detector
12	118	Fire alarm	Near alarm
13	120	Panic alarm	Panic
14	122	Panic alarm	Silent panic
15	123	Panic alarm	Audible panic
16	130	Burglar alarm	Burglary
17	131	Burglar alarm	Perimeter
18	132	Burglar alarm	Interior
19	133	Burglar alarm	24 Hour
20	134	Burglar alarm	Entry/exit
21	135	Burglar alarm	Day/night
22	136	Burglar alarm	Outdoor
23	137	Burglar alarm	Tamper
24	138	Burglar alarm	Near alarm
Not applicable*	139	Burglar alarm	Intrusion verifier
25	140	General alarm	General alarm
26	143	General alarm	Expansion module fail
27	144	General alarm	Sensor tamper
28	145	General alarm	Expansion module tamper
29	150	24-hour alarm	General alarm
30	151	24-hour alarm	Gas detected

Report Type (RAS)	CID Code	Classification	Sub-classification
31	152	24-hour alarm	Refrigeration
32	153	24-hour alarm	Loss of heat
33	154	24-hour alarm	Water leakage
34	155	24-hour alarm	Foil break
35	156	24-hour alarm	Day trouble
36	157	24-hour alarm	Low gas level
37	158	24-hour alarm	High temperature
38	159	24-hour alarm	Low temperature
39	161	24-hour alarm	Air flow loss
40	200	Fire supervisory	Fire supervisory
41	201	Fire supervisory	Low water pressure
42	202	Fire supervisory	Low CO2
43	203	Fire supervisory	Gate valve tamper
44	204	Fire supervisory	Low water level
45	205	Fire supervisory	Pump activated
46	206	Fire supervisory	Pump failure
46 TO 47	700 range	User defined	Note: A CID code that is used for a system event should not be assigned to an input.

NOTES

* CID 139 (Burglar alarm intrusion verifier) indicates that a subsequent multi-break alarm has occurred when using the default ChallengerPlus setting. Multi-break alarms may optionally be reported using the same CID code as with Challenger V8 panels. See "Enable V8 multibreak" MAPROG-TS-CHPLUS ChallengerPlus Programming Manual.

STU serial reporting formats

The hex values in this section are true hexadecimal (base-16), rather than CID hex (0-9, B-F)

STU serial data

Event (hexadecimal)	Message type	Detail
31	First Area Accessed	Users 1 to 255* (see note)
32 to 50	Access Area (1 to 31)	Users 1 to 255* (see note)
51	All Areas Secure	Users 1 to 255* (see note)
52 to 70	Secure Area (1 to 31)	Users 1 to 255* (see note)
6	Input Alarm	Alarm Input No. (1 to 239)
8	Input Alarm	Restore Input No. (1 to 239)
0E	Input Tamper	Alarm Input No. (1 to 239)
10	Input Tamper	Restore Input No. (1 to 239)
16	Input Isolated	Input No. (1 to 239)
18	Input De-Isolated	Input No. (1 to 239)
6	System Message	Alarm (240 to 255) see "STU system messages" below
8	System Message	Restore (240 to 255) see "STU system messages" below

NOTES

* User numbers 255 and above are reported as user 255.

STU system messages

Input point (hexadecimal)	Input	Message
F0	240	RAS Off-line
F1	241	DGP Off-line
F2	242	CPU Restart
F3	243	Mains Fail
F4	244	Low Battery
F5	245	DGP Tamper
F6	246	Siren Tamper
F7	247	Duress Alarm
F8	248	Guard failed to check-in (no restoral)
F9	249	Remote Login (no restoral)
FA	250	Film out
FB	251	Out-of-Hour Opening
FC	252	Service Requested
FD	253	Line Monitor Fail
FE	254	Program Mode Entered
FF	255	Periodic Test

STU channel data

Channel number	Event reported
1	Duress
2	Alarm or Tamper (Inputs)
3	DGP or RAS Off-Line
4	System Tamper (DGP Tamper & Siren Tamper)
5	Mains Fail
6	Low Battery
7	Isolated Inputs
8	Open Close
9	CPU Restart (Panel reset)
10	Film Out

Decimal to CID Hex cross-reference

Contact ID messages typically contain only decimal values, except where a Contact ID Hex sub-format is specified. In Contact ID Hex reporting the CID message's group number and point ID are offset by 2000 and reported in "hex" to a monitoring station (hex format in this instance is based on Ademco Contact ID Protocol (0 to 9 and B to F)).

[illegible]