SIEMENS

Access Control

SiPass integrated

Reference Guide

MP 2.80

A6V11144326

07.09.2020

Smart Infrastructure

Copyright

Technical specifications and availability subject to change without notice.

Edition: 07.09.2020

Document ID: A6V11144326

Table of Contents

1 Introduction

Congratulations on choosing the SiPass® integrated access control and security solution. SiPass integrated is the leading access control software on the market. This User's Reference Manual provides a number of reference data tables that may assist you when assigning system functions, defining alarm classes, assigning operational modes to points, performing manual commands, creating event tasks and sending system messages.

2 Supported Image Formats

This section lists all of the image file formats that are supported by the SiPass integrated Photo ID and Graphics functionality.

The following table lists graphics file formats that are supported by SiPass integrated. They may be used in any aspect of the SiPass integrated *Graphics* Module, and as background images.

Supported Format	File Extension	Maximum Colors
ASCII TEXT (Version 5)	TXT	N/A
Windows Bitmap	BMP	16.7 million
CALS (Computer-aided Acquisition and Logistics Support)	CAL	2
DCX	DCX	16.7 million
EPS	EPS	16.7 million
GEM IMG	IMG	16
GIF	GIF	256
Halo CUT	CUT	256
ICO (ICON)	ICO	16
IFF (Amiga)	IFF	16.7 million
IOCA	ICA	2
JPEG	JPG	16.7 million
LaserView	LV	2
MacPaint	MAC	2
Microsoft Windows Paint MSP	MSP	2
PCX	PCX	16.7 million
PSD (Photoshop)	PSD	16.7 million
Photo CD	PCD	16.7 million
PICT	PCT	16.7 million
Pixmap	XPM	256
SUN RASTER	RAST, RAS, IM, IM1, IM8, IM24, IM32	16.7 million
TARGA	TGA	16.7 million
TIFF (Tagged Image File Format)	TIF	16.7 million
WMF (Windows Metafile)	WMF	16.7 million
WPG (WordPerfect Metafile)	WPG	256
Xbitmap	XBM, BM	2
AutoCAD (Document Exchange Format)	DXF	N/A

3 System Functions

This section lists of all the System Functions that can be assigned to operator groups from the *Operator Group* dialog.

When assigning operator privileges, you must:

1. Assign the system functions to which that operator has access.
2. Assign the appropriate level of access to that function for the operator to adequately perform their job.

The levels of operator privilege that may be assigned to system functions are shown in the following table.

Assigned Privilege	Meaning	Description
<none>	(none)	The operator is not assigned any access to records relating to system functions. They are prevented from creating, deleting, modifying and viewing specific records or their related attributes.
c	(create)	The operator is assigned full control of the records relating to the system functions. This could include privileges to create, delete, modify and view records and their related attributes only if applicable.
e	(edit)	The operator is allowed to view and modify records relating to specific system functions, but is prevented from creating or deleting such records.
v	(view)	The operator is granted access to retrieve and view records relating to specific system functions, but is prevented from creating, deleting or modifying such records.

The following table lists the system functions that may be assigned to an operator group together with a brief description of each function. The table also lists the privilege levels that may be assigned for each system function.

SystemFunction	Description	Assignable Privilege Level
Access Configuration	Determines whether the operator should be allowed to create, modify, delete and view access groups and levels.	<none>, c, e, v
Additional Preferences	Determines whether the operator can tick and un-tick the following checkbox in the *System Preferences* dialog: **Display Higher Priority** Alarm, in the *General* tab.	<none>, c, e, v
Advanced Reports	Determines whether the operator can view and print advanced reports, including Image Verification and Time and Attendance.	<none>, c, e, v
Alarm Definition	Determines whether the operator should be allowed to create, modify, delete and view alarm classes.	<none>, c, e, v
Alarm Queue	Provides privileges for the Alarm Queue window and *Alarm Display* dialog (to allow operators to acknowledge alarms).	<none> >, c, e, v

SystemFunction	Description	Assignable Privilege Level
Anti-Passback Area	Provides privileges for creating, modifying, deleting and viewing Global Anti-Passback areas.	<none>, c, e, v
ASP Configuration	Provides privileges to launch and see Advanced Security Programming module in SiPass Explorer (with 'v' privilege), and also sets a global privilege limit on all configured Activities.	<none>, c, e, v
ASP Operation	Provides privileges to view and edit runtime values in flag/counter/timer runtime mode	<none>, c, e, v
Audit Trail	Determines whether the operator can or cannot view the Active Audit Trail window.	<none>, c , e, v
Audit Trail Report	Determines whether the operator can generate Audit Trail reports.	<none>, c, e, v
Backup	Provides privileges for the backup component for both the Database and Audit Trail.	<none>, c
Card Reader Configuration	Configures card readers.	<none>, c, e, v
Cardholder	Provides privileges for creating, modifying, deleting and viewing cardholder records.	<none>, c, e, v
CCTV Command Set Configuration	Provides privileges to add, delete, edit, or view CCTV Command Sets.	<none>, c, e, v
CCTV Configuration	Determines whether the operator can configure CCTV components via the SiPass interface.	<none>, c, e, v
CCTV Operation	Determines whether the operator can operate CCTV components via the SiPass interface.	<none>, c, e, v
Components	Provides privileges for the *Components* dialog. The level applied to the **Components** system function will take prece-dence over other system functions; for example, **Points**.	<none>, c, e, v
Credential Profile	Provides privileges to configure Credential Profiles for cards	<none>, c, e, v
Custom Command Configuration	Allows the operator to create additional buttons for the menu bar that can be attached to an executable command.	<none>, c, e, v
Custom Pages	Provides privileges to view or edit custom pages in SiPass Explorer	<none>, c, e, v
Customized Reports	Provides privileges for customized reports in SiPass Explorer. This privilege overwrites any individual report privileges assigned to the operator group.	<none>, c, e, v
Database Report	Provides privileges for the Database Reporting component.	<none>, c
Disable Detailed AT Logging	Provides privileges to disable Detailed Audit Trail Logging. Requires System Preferences and Additional Preferences.	<none>, c
Door Interlocking Configuration	Provides privileges to configure, control and view door interlocking functionality.	<none>, c, e, v
DVR Configuration	Determines whether the operator can configure DVR components via the SiPass interface.	<none>, c, e, v

SystemFunction	Description	Assignable Privilege Level
DVR Operation	Determines whether the operator can operate DVR components via the SiPass interface.	<none>, c, e, v
Elevator Control	Provides privileges for functions contained in the *Elevator Control* Module includ-ing banks, floors, floor groups, and elevators.	<none>, c, e, v
Event Task	Provides privileges for creating, modifying, deleting and viewing event tasks.	<none>, c, e, v
External Alarm Monitoring	Provides privileges for the External Alarm Monitoring function. Please note that to use this feature, you will need access to the Unit Group that the ACCs are a part of.	<none>, c, e, v
External System Configuration	Provides privileges for creating, modifying, deleting and viewing external configuration details for OPC buses, units and points.	<none>, c, e, v
FLN Configuration	Provides privileges for the use of the *Field Level Network (FLN) Configuration* tool built-in to the SiPass integrated application. This includes device settings and firmware download to local devices.	<none>, c
Global Card Management	Provides privileges for the use of the *Global Cardholder Management* dialog. This includes upload, download and full synchronization of cardholder databases across the GCM system.	<none>, c
Graphics	Provides privileges for the *Graphics* Module including site plans, drawings, symbols, and card templates.	<none>, c, e ,v
Guard Tour Configuration	Provides privileges for the configuration of Guards. Tours and Tour Groups.	<none>, c, e ,v
Guard Tour Operation	Provides privileges for the starting, stopping and monitoring of guard tours.	<none>, c, e ,v
Holiday	Provides privileges for creating, modifying, deleting and viewing holidays within SiPass integrated.	<none>, c, e, v
Image Verification	Allows the operator to use the Image Verification feature.	<none>, c
Imaging / Printing	Provides privileges for the *Photo ID and Image Verificiation*, including the privilege to design card templates.	<none>, c
Initialize	Provides privileges for performing Manual Initialization.	<none>, c
Interactive Reports	Provides privileges to launch and see Interactive Reports node in SiPass Explorer, as well as allowing configuration in the Interactive Reports dialog.	none>, c, e, v
Intrusion Area Configuration	Provides privileges for creating, modifying, deleting and viewing Intrusion Areas.	<none>, c, e, v
Intrusion Area Operation	Provides privileges for performing Intrusion related tasks. For example: assigning Isolation privileges and arming or disarming intrusion areas manually.	<none>, c
Log Book	Provides privileges for making log book entries.	<none>, c, e, v

SystemFunction	Description	Assignable Privilege Level
Lookup	Provides privileges for access to the Look Up Table in SiPass Explorer to create items in the current table.	<none>, c, e, v
Manual Control	Provides privileges for sending manual commands from the SiPass integrated Workstation Client.	<none>, c
Message Forwarding Configuration	Provides privileges for creating, modifying, deleting and viewing message forwarding functions.	<none>, c, e, v
Message Queue Operation	Provides privileges for using the features of the Messaging Queue window.	<none>, c, e, v
Mustering Report	Provides privileges for the Mustering Report component.	<none>, c, e, v
Offline Access Configuration	Provides privileges for the Offline Access Configuration component.	<none>, c, e, v
Operator	Provides privileges for creating, modifying, deleting and viewing operator records.	<none>, c, e, v
Operator Group	Provides privileges for creating, modifying, deleting and viewing operator groups and operator privileges.	<none>, c, e, v
Overview	Provides privileges for viewing the Overview window, which displays a summary of system components.	<none>, c, e, v
PIN Assignment	Provides privileges for creating, modifying, deleting or viewing PIN numbers assigned in the *Cardholder* dialog.	<none>, c, e, v
Point	Provides privileges for creating, modifying, deleting and viewing output, input and access points.	<none>, c, e, v
Point Group	Provides privileges for creating, modifying and deleting point groups.	<none>, c, e, v
Predefined Reports	Provides privileges for Predefined reports in SiPass Explorer. This privilege overwrites any individual report privileges assigned to the operator group.	<none>, c, e, v
Printers	Provides privileges for configuring and dedicating specific printers for specific functions in SiPass integrated.	<none>, c
Profile Configuration	Provides privileges for configuring cardholder profiles.	<none>, c, e, v
Profile Viewer	Provides access to the Profile Viewer dialog.	<none>, c
Report Configuration	Provides privileges for the Configure Audit Trail Reporting component.	<none>, c
Restore	Provides privileges for Database and Audit Trail restoration.	<none>, c
See PIN	Provides privileges to view PIN Numbers in the *Cardholder* dialog. If an operator does not have this privilege assigned, the PIN number field will be hidden.	<none>, c, e, v

SystemFunction	Description	Assignable Privilege Level
Service Provider Configuration	Provides privileges for creating, modifying, deleting and viewing service provider details.	<none>, c, e, v
Smart Card Encoding	Provides privileges for creating, modifying, deleting and viewing the Smart Card encoding functionality details.	<none>, c, e, v
System Preferences	Provides privileges for the configuration of System Preferences via the *System Preferences* dialog.	<none>, c , e, v
Time and Attendance	Provides privileges for creating, viewing, modifying and deleting details of the Time and Attendance Interface.	<none>, c, e, v
Time Schedule	Provides privileges for creating, modifying and deleting Time Schedules.	<none>, c, e, v
Virtual Monitor	Provides privileges for viewing live videos for IP and DVR cameras	<none>, , v
Visitor	Provides privileges for creating, viewing, modifying and deleting details of visitors.	<none>, c, e, v
Watchlist	Provides privileges to launch and see Watchlists node in SiPass Explorer, as well as allowing Watchlist data import	<none>, c, e, v
Work Group	Provides privileges for creating, modifying and deleting work groups.	<none>, c, e, v

4 Alarm Class

This section lists all of the possible states and their descriptions for each Alarm Type in the *Alarm Class* dialog.

When creating an alarm class, you can define alarm states. For example, if you were to create an alarm class for output points (in particular, doors with locks), you could create two states for that class. The first state would be a restore (normal) state when the door is locked and the second state would be an alarm state when the door is unlocked. The event that triggers the state (door locked or unlocked) is known as the status.

Type	Status	Description
Access	Daily code	The correct Daily Code was entered at a keypad.
	Low battery detected	A card has been used that has a low HFPU battery and needs to be replaced, as soon as possible.
	Good access with time stamp	A valid card was read at a card reader.
	Access granted to Anti-Passback Area	A cardholder has successfully entered an Anti-Passback area with a valid card.
	Card activates APB area either ON	A card was used to secure an area.
	Card activates APB area either OFF	A card was used to unsecure an area.
	Card activates floor	A card was used at a card reader to secure a floor.
	Card did not activate a floor	A card was used, unsuccessfully, at a card reader to secure a floor.
	Door Time Schedule Active	A door has reverted to normal Time Schedule control after being manipulated by a manual command or Event Task.
	Door Free	The door latch is open and the door frame monitor is disabled.
	Door Secured	The door latch is secured and the door frame monitor is enabled.
	Tamper inactive on reader	The tamper input on a reader interface module is inactive.
	Reader online	A reader has come online.
	Reader timeout	A reader has timed out after a card was badged and PIN entry was expected.
	Badge collision on reader	Not supported.
	Access granted on reader	Access has been granted at an access point.
	Door (Latch) locked	The door latch is secured.
	No Additional Access Mode Set	The reader has been set to **No Additional Access** mode.
	PIN as Card Mode Set	The reader has been set to **PIN as Card** mode.
	Daily Code mode set	The reader has been set to **Daily Code** mode.

Type	Status	Description
	Intrusion Control Enabled	Intrusion Control has been enabled at the reader.
	Duress	A duress alarm has been entered at an access point.
	Soft Anti-passback mode	A cardholder has failed to use their card when leaving an area with soft anti-passback and has tried to re-enter the same area. The cardholder will be allowed access.
	Hard Anti-passback mode	A cardholder has failed to use their card when leaving an area with hard anti-passback and has tried to re-enter the same area. The cardholder will be denied access.
	A card read at a disabled readhead	A card was read at a disabled readhead. (Disabled readhead – refers to a card reader that has been sent a manual **Disable** command).
	Group error	A card, from a group (of cards) that has been disabled, was used at a reader or is invalid for the reader where it was used.
	Alarm void card was read	A void card was read at an access point.
	An invalid facility card was read	An invalid Facility Code on a card was read at an access point. (Each site has a site-specific Facility Code).
	Card number limit	The maximum number of cards supported by the hardware (processor) has been reached.
	An invalid PIN number	An invalid PIN (Personal Identification Number) was entered at an access point.
	Bad daily code	An invalid Daily Code was entered at a keypad that requires a Daily Code to be entered.
	Independent service	The elevator has been placed on independent service. (The elevator operates independ-ently of all other elevators, usually controlled from inside the elevator itself). Typically initiated when being repaired.
	Elevator Alarm	The emergency or alarm button within the elevator has been activated.
	Tamper active on reader	The tamper input on a reader interface module is active.
	Reader offline	A reader has gone offline.
	Checksum error on reader	Not supported.
	Access not granted on reader	Access was denied at an access point.
	Door (Latch) unlocked	The door latch has been unsecured.
	Hard Anti-Pass back Error	A cardholder has failed to use their card when leaving an area with soft anti-passback and has tried to re-enter the same area. The cardholder will be allowed access.

Type	Status	Description
	Soft Anti Pass Back Error	A cardholder has failed to use their card when leaving an area with hard anti-passback and has tried to re-enter the same area. The cardholder will be denied access.
	Access Denied- Intrusion Area Armed	Access has been denied because an intrusion area is still armed.
	Access Denied – Hard Perimeter Violation	An access attempt has been denied, due to an Anti-Passback violation in an area configured with a **Hard** Anti-Passback mode.
	Soft Perimeter Violation	A cardholder has entered a soft Anti-Passback area that they are already within.
	3 Wrong PIN entries	A cardholder has entered 3 Wrong PINs at a reader.
	Timed Re-entry Error	A cardholder has attempted to re-enter an area (set to Timed Re-Entry Anti-Passback mode) before their allocated re-entry time
	Card not yet active	A card was presented at a reader before its system start date has been reached.
	Card Expired	A card was presented at a reader after its system end date has expired.
	Time Schedule Violation	A card was read at a reader outside the normal scheduled time for that card.
	Elevator Offline Denied	The HLI Elevator is offline.
	Elevator Override Denied	The HLI Elevator is in external override.
	Elevator Access Collision	The HLI Elevator is in access collision because another access session is in progress.
	Intrusion Control Disabled	Intrusion Control has been disabled at the reader.
	SALTO Battery Low	A SALTO offline door requires a battery change
	SALTO PPD Connection	A PPD has been connected to a SALTO offline door to update the door
Anti-Passback Area	Capacity Full	The number of cardholders in the area equals the defined maximum
	Capacity Exceeded	The number of cardholders in the area exceeds the defined maximum.
	Capacity Not Full	The number of cardholders in the area does not exceed the defined maximum.
	Four Eyes Access Alarm	The Four Eyes Anti Passback area is in an alarm state. The group alarm conditions are established in the *Area* dialog.
	Four Eyes Access Normal	The Four Eyes Anti Passback area is in a normal state.
	Capacity Empty	There are no cardholders in the area.
	Workgroup Capacity Full	The number of cardholders in the area from a Workgroup has reached the maximum for that Workgroup.

Type	Status	Description
	Workgroup Capacity Exceeded	The number of cardholders in the area from a Workgroup has exceeded the maximum for that Workgroup.
	Workgroup Capacity Not Full	The number of cardholders in the area from a Workgroup has not reached the maximum for that Workgroup.
	Workgroup Capacity Empty	The number of cardholders in the area from a Workgroup is zero.
	Capacity Not Empty	The area is no longer empty.
	Workgroup Capacity Not Empty	The number of cardholders in the area from a Workgroup is no longer zero.
Bus	Normal (bus alive)	The bus is communicating with the server.
	Alarm (bus down)	The bus is not communicating with the server.
Camera	Acknowledged	The communication link between the camera switcher and the monitor has been restored.
	Video Normal	The communication to the camera is operating normally.
	Motion Normal	The camera has acknowledged that there is movement in the area and has raised a normal alarm.
	Video Loss	The communication link between the camera switcher and the monitor has been lost.
	Motion Alarm	The camera has detected movement and has raised an alarm.
Device	Communication Back	The device has re-established communication with the server.
	Communication Lost	The device has lost communication with the server.
Door Interlocking	Interlocking Operational	Door Interlocking is enabled.
	Interlocking Disabled	Door Interlocking is disabled.
	Interlocking Alarm	Door Interlocking is in an alarm state.
Flag	Flag State False	The flag has been set to false
	Flag State True	The flag has been set to true
Floor	Floor security on	The floor has been secured.
	Floor security temp on	The Floor has been temporarily secured.
	Floor security off	The Floor has been unsecured
	Floor emergency stop	The Emergency Stop Button inside the elevator has been activated.
	Floor security temp off	The Floor has been temporarily unsecured.
Group	Normal	The group is in a normal state.
	Alarm	The group is in an alarm state. The group alarm conditions are established in the *Group* dialog.

Type	Status	Description
Image Verification Privilege	Normal	The operator has privileges to allow or deny entry based on visual identification of live and database cardholder images.
	Operator No IV privilege	The operator does not have privileges to allow or deny entry based on visual identification of live and database cardholder images.
Input	Passback	A passback button has been activated.
	Normal	The input is normal.
	Door closed	The door is closed.
	Fire override off	The fire override is disabled.
	Battery OK	The unit's battery output voltage is above 11.5V.
	AC power back	The unit's AC power supply has been restored. The unit will cease to draw power from the battery backup.
	Input closed	The input has been closed.
	Input Enabled	The input has changed state and is now enabled.
	Input Physically Enabled at FLN device	The Fire Override on the device has been enabled physically.
	Input tamper or fault cleared	The input tamper state has been cleared / fixed.
	Sintony Input Sealed	The Sintony input is inactive and the input area could be armed.
	Sintony Input Isolated	Overrides the Sintony Input Unsealed therefore allows the area to be armed and also disables the processing of this input in the intrusion system.
	Alarm	The input is in alarm.
	Tamper	A monitored input or wire has changed state and is either short or open circuit.
	Door held	The door is being held open. (The door has remained open after the latch time has expired).
	Door forced	The door has been forced (opened without gaining valid access).
	Fire override on	The fire override has been enabled.
	Battery failed	The unit's battery voltage has dropped below 11V. The battery circuit will be broken, forcing a loss in communications. However, the database memory is retained.
	Battery low	The unit's battery output voltage has dropped below 11.5V.
	AC power failed	The unit's AC power supply has failed. The battery backup will be switched on automatically.

Type	Status	Description
	Input tamper	The input or wiring has been tampered with.
	Input open	The input is an open circuit.
	Card limit reached	The unit's card limit has been exceeded
	Passback tamper	A supervised passback input has detected a tamper.
	Input Disabled	The input has been disabled.
	Input Faulty	The input is not recognised
	Input Physically disabled at FLN device	The input has been physically disabled by setting jumpers on the device.
	Sintony Input Unsealed	The Sintony input is active and may prevent the area from being armed (depending on the configuration)
Intrusion Area	Intrusion Area Armed	The intrusion area has been armed.
	Normal	An intrusion area that was in an alarm state has now returned to the normal state.
	Arming Action Complete	An attempt to arm a dependant intrusion area was made. However, other areas dependant on this area are still unarmed.
	Intrusion Area Part Armed	The intrusion area has been part armed.
	Intrusion Area Part Armed B	The SPC intrusion area has been part armed B. (SPC only)
	Intrusion Area Disarmed	The intrusion area has been disarmed.
	Alarm	An armed intrusion area has been violated.
	Arming Failed	An attempt to arm an intrusion area has failed.
OPC Point	Normal	The OPC Point is in a normal state.
	Acked Alarm	The OPC Point is in alarm, but the alarm has been acknowledged.
	Unacked Normal	The OPC Point is in a normal state after an alarm, but has not been acknowledged.
	Disabled	The OPC Point is disabled.
	Alarm	The OPC Point is in alarm.
Output	Locked	The output is secure.
	Output Enabled	The output has been enabled.
	Unlocked	The output is not secure.
	The output is not secure.	The output has been disabled.
	Output Open	Output is in an open status
Unit	Communication back	Communication between the unit and the server is active.
	Unit reset	A unit has been reset.
	Unit Tamper inactive	The tamper input on a unit is inactive
	Power Returned	Power has been applied to the unit.

Type	Status	Description
	Memory Warning	The Backup Flash memory is approaching full capacity
	Communication lost	Communications between the unit and the server has been lost.
	Unit Tamper active	The tamper input on a unit is active.
	Memory Full	The memory of the unit has reached maximum capacity
	Power Lost	Power has been lost from the unit.
	Memory Overflow	The backup flash memory is full.
	SALTO System Online	SiPass integrated is connected to the SALTO System
	SALTO System Offline	SiPass integrated is not connected to the SALTO System

5 Operational Modes

Operation modes are selectable only for points, not for devices. They affect how the points operate in relation to cardholders and the system.

Type	Mode	Description
Door Reader	Card Only	A card must be presented at the access point to gain valid access.
	Card and PIN	A card must be presented AND a matching PIN entered at the access point to gain valid access.
	Host Verification – Card only	A card must be presented at the access point to gain valid access; also, verification is required by an operator that the live cardholder image matches the stored database image.
	Host Verification – Card and PIN	A card must be presented AND a matching PIN entered at the access point to gain valid access; also verification is required by an operator that the live cardholder image matches the stored database image.
	View Only – Card only	A card must be presented at the access point to gain valid access; also, a snapshot of the cardholder is taken as they enter and stored in the database.
	View Only – Card and PIN	A card must be presented AND a matching PIN entered at the access point to gain valid access; also, a snapshot of the cardholder is taken as they enter, and stored in the database.
	Double/Single Arming	A card must be presented at the access point by a valid cardholder. A double card badge will arm the area and a single card badge will disarm operation for all assigned intrusion areas.
	Card Only Delayed Reporting	This mode is used for access points for entry or exit from defined Anti-Passback Areas. A card must be presented at the access point to gain valid access or exit from the Area, but cardholder entry will not be recognized in the Audit Trail unless the door monitor registers that the door has opened and closed. This means that Area counts will not increase or decrease unless the door monitor registers the appropriate events.
	Card And PIN Delayed Reporting	This mode is used for access points used for entry or exit from defined Anti-Passback Areas. A card must be presented at the access point AND a valid PIN entered to gain valid access or exit from the Area, but card-holder entry will not be recog-nised in the Audit Trail unless the door monitor registers that the door has opened and closed. This means that Area counts will not increase or decrease unless the door monitor registers the appropriate events.
	Disabled Mode	The access point will be disabled.

Type	Mode	Description
	Card + PIN Arm/Disarm	A card must be presented to gain access at the access point. A single card badge unlocks the door providing access without intrusion. A card badge with a PIN unlocks the door and simultaneously arms/disarms the intrusion area. Press ‘1‘ then select ‘E‘ to arm the area or press ‘0‘ and then ‘E‘ to disarm the intrusion area.
	Arm/Disarm Only	A valid card must be presented at the access point as well as a PIN must be entered in order to arm or disarm the intrusion area. Press ‘1‘and then select ‘E‘ to arm the area; or press ‘0‘ and then ‘E‘ to disarm.
	Programmable Authorization – Card Only	A card must be presented at the access point for an ‘authorization started‘ event to be generated. Access is only granted if an ‘authorization granted‘ event is received.
	Programmable Authorization – Card + PIN	A card + PIN must be presented at the access point for an ‘authorization started’ event to be generated, typically used as a trigger in Advanced Security Programming. Access is only granted if an ‘authorization granted’ event is received.

Type	Mode	Description
	Card and Pin Access/Intrusion	This mode provides the option to secure/unsecure the intrusion areas. In case the cardholder wants to arm/disarm/part-arm the area before a card is presented at the access point, it can be done by selecting a number from the reader keypad: • Press ‘0’ then ‘E’ or ‘#’ to disarm the area • Press ‘1’ then ‘E’ or ‘#’ to arm the area • Press ‘2’ then ‘E’ or ‘#’ to part-arm the area • Press ‘9’ then ‘E’ or ‘#’ OR Press just ‘*’ to cancel the current selection After this, a card badge followed by a valid PIN enables standard access and unlocks the door (while performing the selected arming action). **Note:** • The type of reader installed determines if ‘E’ or ‘#’ is used as the enter key for confirming the option selected by a card-holder. • For the Card+PIN functionality, some card readers provide the option to enter a PIN first followed by a card badge. In this case, the ’E’ or ‘#’ key is not required to be pressed again after the PIN is entered, and the users just present their card (previous pressing of the E or # key for arming selection has no effect on this). However, if the card is badged first after selecting an arming action, the ’E’ or ‘#’ key must be pressed after entering the PIN. **For devices that do not require a button to be pressed after entering the PIN:** Some devices (like DC12, DC22, DC800, GrantaCotagCard and GrantaSwipeCard) do not require a button to be pressed after entering the PIN. For example, when entering a PIN at a BC43 reader connected to such a device, the user does not have 'E' or '#' or 'OK' button to send the PIN. • If the card has been badged, the user can enter the PIN di-rectly (which is automatically processed). • If the card has not been badged, each key is processed individually. In this case, the user can press the respective key to arm/disarm/part-arm the area, badge the card and enter the PIN for authentication. In both the above cases, the PIN is processed automatically after the last key for the PIN is pressed and the applicable action is performed. • Press ‘0’ to disarm the area • Press ‘1’ to arm the area • Press ‘2’ to part-arm the area • Press ‘9’ or ‘A’ or ‘B’ to cancel the current selection

Type	Mode	Description
Input/Output	Passback	The input is in alarm state until the passback button has been pressed and the input delay is activated. Triggering passback unlocks the door latch.
	Passback No Message	The input is in alarm state until the passback button has been pressed and the input delay is activated. No passback message is reported back to the system. The latch is not automatically unlocked. Triggering passback unlocks the door latch.
	Passback No Report – Lock not activated	The input is in alarm state until the passback button has been pressed and the input delay is activated. No passback message is reported back to the system. Triggering passback does not unlock the door latch.
	Passback Report – Lock not activated	The input is in alarm state until the passback button has been pressed and the input delay is activated. Triggering passback does not unlock the door latch.
	Input Disabled	Disables the input point.
	Door Frame Auto Pre-Alarm	A Pre-Alarm will sound before the main Door Held Alarm. The Pre-Alarm will not be registered on the Alarm Queue. If the door is not returned to a normal state within the Pre-Alarm time period, the Door Held Alarm will sound and will be registered in the alarm queue. The Door Held Alarm will auto-matically stop when the door returns to a normal state.
	Door Frame Dual Timer	Defines the input point as a door contact sensor that monitors the open or closed state of the door. The input point will use both the Pre-Alarm Delay and Input Delay times when sending alarms.
	Door Frame Held Only	In case when the door has a reader on the outside but no reader (and no passback) on the inside, this mode holds an open door virtually for the Input Delay time duration set by the user and prevents reporting the event as “door-force”.
	Door Frame Manual Pre-Alarm	A Pre-Alarm will sound before the main Door Held Alarm. The Pre- Alarm will not be registered on the Alarm Queue. If the door is not returned to a normal state within the Pre-Alarm time period, the Door Held Alarm will sound and will be registered in the alarm queue. The Door Held will stop only when the door is returned to a normal state and the alarm has been acknowledged.
	Door Frame Sensor	Defines the input point as a door contact sensor that monitors the open or closed state of the door.
	Alarm/Normal	Both changes to alarm and normal states are reported to the system.

Type	Mode	Description
	Fire Stair	Defines the Input point as a fire stair door contact sensor.
	PIR	PIR mode defines the input point as a PIR detector.
	Normal Only	Only normal states are reported to the system
	Alarm Only	Only alarm states are reported to the system
	Report Disable	Disables alarm reporting from the input point to the server. This will prevent alarms from occurring and appearing in the Audit Trail, but Event Tasks will still be triggered.
	Intrusion Area Entry/Exit	Defines the input type as normal except if the cardholder has isolation privileges, they can override a point (if the point is not sealed).
	Intrusion Area No Seal Check	The input seals are not checked when intrusion area is armed. Defines the input type as normal.
	Intrusion Area Instantaneous	Defines the input type as normal except that when the area is secured, there are no entry or exit delay times.
	Intrusion Area Hand Over	Allows secured areas to be accessed in order for an alarm unit to be switched off.
	Output Delay	Allows access to the area for the time configured in the Delay field.
	Single Pulse	Allows access by unlocking the point, followed by a quick re-lock.
	Toggle	Toggles the access point between the Lock and Unlock state, each time a card is badged at the access point.

6 Manual Override

Manual Commands can be used to manually control specific points, areas, elevators and units at your site. The following table lists the commands that can be used to control each type and a brief description of the action that will be performed.

Type	Command	Description
Access	Allow Access	The door will unlock, remain unlocked for the defined period of time and then relock, as per a normal valid card badge.
	Block Door	The door will remain blocked, unable to be opened.
	Cancel Permanent Action	Any current Permanent Command or Event Task, or Access/Internal Action operating on the point will be cancelled. The next Control State in the Control State Queue will take effect.
	Intrusion Control - Disable	Disable Intrusion Control on the selected access point.
	Intrusion Control – Enable	Enable Intrusion Control on the selected access point.
	Intrusion Control – Restore Config	Restore Intrusion Control to whatever is configured.
	Lock Door	The door latch will be locked until the next **unlock** command is received. The Duration can be set to: • Until time schedule change • Permanents
	Reader Buzzer Off	The Reader buzzer is turned off. Only applies to the Siemens reader range.
	Reader Buzzer On	Reader buzzer is turned on. Only applies to the Siemens reader range.
	Reset Reader Tamper	Resets the reader tamper input. Only applies to the Siemens reader range.
	Restore Access Mode	Returns the access point to the normal access operation mode defined in the Components screen.
	Restore additional access mode	Returns the access point to the normal additional access operation mode defined in the Components screen.
	Restore Dual Custody Config Mode	Restores the Dual Custody mode to what is configured.
	Return to Time Schedule Control	The door latch will return to normal Time Schedule control.
	Set “Daily Code“ additional access mode	Set the additional access for the selected access point to Daily Code.
	Set “No Additional Access“	Set the additional access for the selected access point to No Additional Access.
	Set “PIN as Card” additional access mode	Set the additional access for the selected access point to PIN as Card.

Type	Command	Description
	Set Mode “Card and PIN”	Sets the point’s operation mode to “Card and PIN”.
	Set Mode “Card Only”	Sets the point’s operation mode to “Card Only”.
	Set Mode “D.R. Card and PIN”	Sets the point’s operation mode to “Delayed Reporting Card and PIN”.
	Set Mode “D.R. Card Only”	Sets the point’s operation mode to “Delayed Reporting Card Only”.
	Set Mode “Disabled”	Sets the point’s operation mode to “Disabled”.
	Set Mode “H.V. Card and PIN”	Sets the point’s operation mode to “Host Verification. Card and PIN”.
	Set Mode “H.V. Card Only”	Sets the point’s operation mode to “Host Verification Card Only”.
	Set mode “No Dual Custody”	Disables Dual Custody for the access point.
	Set mode “Programmable Authorization – Card + PIN”	Sets the point’s operation mode to “Programmable Authorization – Card + PIN”.
	Set mode “Programmable Authorization – Card Only”	Sets the point’s operation mode to “Programmable Authorization – Card Only”.
	Set mode “Standard Dual Custody”	Set the access point to Standard Dual Custody Mode.
	Set mode “Supervisory Dual Custody”	Set the access point to Supervisory Dual Custody Mode.
	Set Mode “V.O. Card and PIN”	Sets the point’s operation mode to “View Only. Card and PIN”.
	Set Mode “V.O. Card Only”	Sets the point’s operation mode to “View Only Card Only”.
	Unblock Door	Turns off the block door command. Returns the door to its normal programmed mode of operation.
	Unlock Door	The door latch will be unlocked until the next “lock” command is received.
Input	Cancel Permanent Action	Any current Permanent Command or Event Task, or Access/Internal Action operating on the point will be cancelled. The next Control State in the Control State Queue will take effect.
	Isolate	External intrusion areas will ignore the state of inputs that are isolated, for the purposes of arming. This is only applicable for external intrusion input points.
	Pulse	Sends a pulse command to the selected Input. This is only applicable for Sintony input points of type “Serial Coms Input”
	Return to Time Schedule Control	The input point will return to normal Time Schedule control.
	Secure (Enable)	Enables the input, if it is currently disabled, until the next change in Time Schedule.

Type	Command	Description
	Set state Alarm	Set the input to state Alarm. This is only applicable for Sintony input points of type “Serial Comms Input”
	Set state Normal	Set the input to state Normal. This is only applicable for Sintony input points of type “Serial Comms Input”
	Unsecure (Disable)	Disables the input, if it is currently enabled, until the next change in Time Schedule.
Output	Allow Access	Allows access at an output point. (Operates in the same way as if a cardholder used their card to gain valid access at the same point). The output point will only be activated for the latch time.
	Cancel Permanent Action	Any current Permanent Command or Event Task, or Access/Internal Action operating on the point will be cancelled. The next Control State in the Control State Queue will take effect.
	Fast Pulse	The output point will activate in “fast pulse” mode.
	Return to Time Schedule Control	The output will return to normal Time Schedule control.
	Secure (Lock)	Locks the output (temporarily), if the output is currently unlocked. The Duration can be set to : - Until Time Schedule Change - Permanent Duration time can be specified in the HH:MM:SS format.
	Single Pulse	The output will activate a single pulse.
	Slow Pulse	The output will activate in “slow pulse” mode.
	Toggle Point	The state of the output will be toggled to the reverse state.
	Unsecure (Unlock)	Unlocks the output (temporarily), if the output is currently locked, until the next change in Time Schedule.
APB Area (Anti-Passback Area)	Forgive All cards	Forgives all cardholders currently in the area.
	Forgive Card	Forgives the specified cardholder.
	Override Mode	Overrides the selected area with a specific mode.
	Reset Count	Allows the count for an Anti-Passback area to be reset to zero.
	Restore Mode	Restores the configured Anti-Passback mode.
	Add Card	Adds a card to an Anti-Passback area.
	Remove Card	Removes a card from an Anti-Passback area.
Intrusion	Arm	Arms the selected intrusion area.
	Clear Intrusion Alarms	Clears all alarms in memory for the selected area or specified room.
	Disarm	Disarms the selected intrusion area.
	Isolate Point	Manually isolates a point from an intrusion area, excluding that point from a seal check when the area is armed.

Type	Command	Description
	Part Arm	Arms inputs which are marked as Part Arm.
	Part Arm B	Arms inputs which are marked as Part arm B. (SPC intrusion only)
	Force Arm	Manually force-arms an intrusion area. This action includes isolating input points that may be in the Alarm state, and then arming the area.
	Force Part-arm	Manually part-arms an intrusion area. This action includes isolating input points that may be in the Alarm state, and then part-arming the area.
	Silence All Bells	Reset the Alarm output from the SPC Panel
	Clear Intrusion Alarms	Temporarily Disable the all SPC zones in alarm on the panel.
Elevator	Cancel Permanent Action	Any current Permanent Command Event Task, or Access/Internal Action operating on the point will be cancelled. The next Control State in the Control State Queue will take effect.
	Floor off security (unsecure)	Takes the floor off security, until the next change in Time Sched-ule.
	Floor on security (secure)	Places the floor on security, until the next change in Time Schedule.
	Return to Time Schedule control	The elevator will return to normal Time Schedule control.
Unit	Siren On	Activates the local output, if connected.
	Siren Off	De-activates the local output, if connected.
Door Interlocking	Disable	Disable Door Interlocking.
	Restore	Restore Door Interlocking.
Flag	Set flag to ‘False’	Enables this flag.
	Set flag to ‘True’	Disables this flag.

7 Host event tasks

SiPass integrated allows you to define a host event task that performs a certain task (command) when a specific set of circumstances have been met (trigger). The following tables list the sources that can be used to trigger a host event task, along with a brief description of that source and the commands that can be implemented when the source has been triggered.

7.1 Sources

Source	State (trigger)	Description
ACC Control	Activated	This allows to you create a Host event task which can be triggered by a Hardware event, like a Controller Event Task. If you create an ACC Control Host event task, it will be avail-able to select as a Command in the Controller Event Task dia-log.
Access Point	“Daily Code” mode set	Access Point mode set to Daily Code.
	“No Additional Access” mode set	Access Point mode set to No Additional Access.
	“No Dual Custody” mode set	Access Point mode set to No Dual Custody mode.
	“PIN as Card” mode set	Access Point mode set to Daily Code.
	“Standard Dual Custody” mode set	Access Point mode set to Daily Code.
	“Supervisory Dual Custody” mode set	Access Point mode set to Daily Code.
	Access denied- Hard Perimeter Violation	A cardholder has been denied entry due to hard Anti-Passback area restrictions.
	Access Denied- Intrusion Area Armed	A host event task is triggered when a card is presented at a reader is denied entry because the area to which that reader belongs is currently armed.
	Accessibility Valid Card Presented	A valid card with the accessibility option has been presented at a reader.
	Card Expired	A host event task is triggered when an expired card is pre-sented at a reader.
	Card not yet active	A host event task is triggered when a card that has not yet reached its programmed “Start Date” is presented at a reader.
	Card out of range	A host event task is triggered when a card, with a number out of the range supported by the controller, is badged at a reader
	Card valid	A host event task is generated when a valid card is badged at a reader.
	Door Interlocking in Progress Collision	A conflict in the operation of a door interlocking set has occurred.
	Intrusion Control Disabled	Intrusion Control has been disabled at the access point.

Source	State (trigger)	Description
	Intrusion Control Enabled	Intrusion Control has been enabled at the access point.
	Invalid	A host event task is triggered when a point enters any alarm state, assuming that an alarm class has been configured for the access point.
	Invalid Dual Custody	An Invalid Dual Custody event has occurred.
	No Entry	A host event task is triggered if the access point is set to “De-layed Reporting” mode and a valid card has been badged at a reader, but the door monitor has not registered passage through the door.
	Operator Alarm	A host event task is triggered when the nominated access point goes into alarm.
	Operator Alarm Actioned	A host event task is triggered, when an alarm associated with the nominated access point, is actioned by an operator.
	Operator Alarm Not Actioned	A host event task is triggered when the operator fails to action an alarm associated with the nominated access point before the (re-activation) timeout.
	Operator Alarm Timed out	A host event task is triggered when the operator fails to action the alarm associated with the access point and the alarm time-out.
	Operator Normal	A host event task is triggered when the nominated access point changes to a normal state.
	Operator Restore	A host event task is triggered when the nominated access point attains ‘Restored’ status.
	Operator Waiting for Normal	A host event task is triggered when a restorable alarm at the nominated point has been ac-tioned but has not returned to its normal state.
	PIN Error Disabled	A card has been voided after the cardholder has made three consecutive incorrect PIN entries in the facility.
	Reader Offline	A host event task is triggered when a reader enters the offline state. Only valid for the Siemens reader range.
	Reader Online	A host event task is triggered when a reader enters the online state. Only valid for the Siemens reader range.
	Reader Tamper	A host event task is triggered when a reader enters the tamper state (tamper input activated). Only valid for the Siemens reader range.
	SALTO Battery Low	A SALTO offline door requires a battery change.
	SALTO PPD Connection	A PPD has been connected to a SALTO offline door to update the door.
	SALTO System Offline	SiPass integrated is not connected to the SALTO System.
	SALTO System Online	SiPass integrated is connected to the SALTO System.

Source	State (trigger)	Description
	Self Authorization Granted	Cardholder has self-authorized on a Dual Custody access point.
	Soft Perimeter Violation	An anti-passback violation has occurred at a door under soft anti-passback control.
	Time Schedule Violation	A host event task is triggered when a card is presented at a reader outside the cards pro-grammed time schedule for that reader/door.
	Timed Re-Entry Error	A cardholder has attempted to re-enter an area (set to Timed Re-Entry Anti-Passback mode) before their permitted re-entry time.
	Turnstile in Use-Readers Disabled	A cardholder has been denied access at a turnstile due to the turnstile being already in used by another cardholder.
	Valid	A host event task is triggered when the point is returned to any restore state, assuming an alarm class has been con-figured for the access point.
	Valid Card Presented	A host event task is triggered when a valid card is presented at a reader at a delayed reporting mode reader.
	Void card	A host event task is triggered when a card that is void is swiped at a card reader.
Access Point Group	Same as Access Points with less “States” options	See above
Anti-Passback Area Point	Area Count Reset	An Area count has been reset.
	Area Mode Changed	An Area mode has been changed.
	Capacity Empty	The area is vacant.
	Capacity Exceeded	An event task is triggered when the count for the number of cardholders currently in the anti-passback area is above the specified capacity.
	Capacity Full	An event task is triggered when the count for the number of cardholders currently in the anti-passback area has reached the specified capacity.
	Capacity Not Empty	The area is no longer empty.
	Capacity Not Full	The number of cardholders in the area does not exceed the defined maximum.
	Same as Access Points	See above.
	Workgroup Capacity Empty	The number of cardholders in the area from a Workgroup is zero.
	Workgroup Capacity Exceeded	The number of cardholders in the area from a Workgroup has exceeded the maximum for that Workgroup.
	Workgroup Capacity Full	The number of cardholders in the area from a Workgroup has reached the maximum for that Workgroup.
	Workgroup Capacity Not Empty	The number of cardholders in the area from a Workgroup is no longer zero.

Source	State (trigger)	Description
	Workgroup Capacity Not Full	The number of cardholders in the area from a Workgroup has not reached the maximum for that Workgroup.
Anti-Passback Area Point Group	Same as Access Points	See Above
Apogee Control	Trig. ID	A host event task is triggered when a message is received from the Apogee Control corresponding to the Apogee Trigger ID.
Bus Driver	Bus Driver Alive	A host event task is triggered when the bus driver operating the CCTV interface is restored.
	Bus Driver Down	Driver A host event task is trig-gered when the bus driver operating the CCTV interface goes down
Camera Point	Acknowledged	The link between the camera switcher and the monitor is working.
	Motion Alarm	A motion alarm has been gener-ated by the camera.
	Motion Normal	A motion normal has been generated by the camera.
	Video Loss	A host event task is triggered when the live video feed from a camera has been lost.
	Video Normal	Video feed from the camera is restored.
Camera Point Group	Alarm	A host event task is triggered when a camera point group enters the alarm state.
	Normal	A host event task is triggered when a camera point group returns to the normal state.
Database	Database Synchronization failed	A host based event task is triggered when the database synchronization process has failed.
	Database Synchronization OK	A host based event task is triggered when the database synchronization process has succeeded.
Door Interlocking	Interlocking Alarm	Door Interlocking alarm state.
	Interlocking Disabled	Door Interlocking is disabled.
	Interlocking Operational	Door Interlocking is enabled.
External Point	Acknowledged	An event is triggered when an external point is acknowledged at the originating server.
	Alarm	An event is triggered when an External point (source point or area node) enters an alarm state and that information is sent to SiPass integrated by the exter-nal application.
	Normal	An event is triggered when an External point (source point or area node) enters a normal state and that information is sent to SiPass integrated by the exter-nal application.
Floor Point	Alarm	An alarm state has been reported by the floor.

Source	State (trigger)	Description
	Bank Floor Secure	An event task is triggered when the floor is Secured.
	Bank Floor UnSecure	An event task is triggered when the floor is not secured.
	Card No Access	An event task is triggered when a cardholder badges their card and is not permitted access to that floor.
	Other Floor Point triggers are the same as the Access Points, however, relate to elevator floor access.	See “Access Points” Above for more information.
Floor Point Group	Same as Floor Points	See “Floor Point”
Input Point	Alarm	An event task is triggered when the nominated input point goes into alarm.
	Door Closed	An event task is triggered when the nominated input changes to a normal state as a result of the door being closed.
	Door Forced	An event task is triggered when the nominated input goes into alarm, as a result of a door being forced.
	Door Held	An event task is triggered when the nominated input goes into alarm, as a result of a door being held open longer than the specified time.
	Input Tamper	An event task is triggered when the nominated input point group enters a Tamper state.
	Normal	An event task is triggered when the nominated input point goes into the normal state.
	Operator Alarm	An event task is triggered when the nominated input point goes into alarm.
	Operator Alarm Actioned	An event task is triggered when an alarm, associated with the nominated input point, is actioned by an operator.
	Operator Alarm Not Actioned	An event task is triggered when the operator fails to action an alarm associated with the nominated input point before the (re-activation) timeout.
	Operator Alarm Timed out	An event task is triggered when the operator fails to action the alarm associated with the input point and the alarm times out.
	Operator Normal	An event task is triggered when the nominated input point changes to a normal state.
	Operator Restore	An event task is triggered when the nominated input point attains the ‘Restored’ status.
	Operator Waiting for Normal	An event task is triggered when a restorable alarm at the nominated input point has been actioned, but has not returned to its normal state.
Input Point Group	Same as Input Points	See “Input Point”
Intrusion Area Point	Alarm	An event task is triggered when the nominated area point goes into alarm.

Source	State (trigger)	Description
	Normal	An event task is triggered when the nominated area point goes into the normal operation state.
	Armed	An event task is triggered when an intrusion area is armed.
	Arming Action Complete	An event task is triggered when an attempt to arm a dependant intrusion area is complete. However, other areas, to which the dependant area belongs, are still unarmed.
	Arming failed input X in alarm	An event task is triggered when an arming attempt has failed due to an input point in an alarm state.
	Disarmed	An event task is triggered when an area is unsecured at a Data Entry Terminal.
	Part Armed	An event task is triggered when an intrusion area is part armed.
	Part Armed B	An event task is triggered when an intrusion area is part armed B. (SPC only).
	Normal	An event task is triggered when the nominated area point changes to a normal state.
Intrusion Area Point Group	Same as Intrusion Area Points	See “Intrusion Area Point”
Output Point	Lock	An event task is triggered when the nominated output point is locked. **Note:** Locked Temp does not trigger an event task.
	Operator Alarm	An event task is triggered when the nominated output point goes into alarm.
	Operator Alarm Actioned	An event task is triggered when an alarm, associated with the nominated output point, is actioned by an operator.
	Operator Alarm Not Actioned	An event task is triggered when the operator fails to action an alarm associated with the nominated output point before the (re-activation) timeout.
	Operator Alarm Timed Out	An event task is triggered when the operator fails to action the alarm associated with the nominated output point and the alarm times out.
	Operator Normal	An event task is triggered when the nominated output point changes to a normal state.
	Operator Restore	An event task is triggered when the nominated output point attains ‘Restored’ status.
	Operator waiting for normal	An event task is triggered when a restorable alarm at the nominated output point has been actioned but has not returned to its normal state.
	Unlock	An event task is triggered when the nominated output point has been unlocked. **Note:** Unlocked Temp does not trigger an event task.
Output Point Group	Same as Output Points	See “Output Point”

Source	State (trigger)	Description
Special Date	Set time	An event task is triggered at the nominated date time. Time format = HH:MM:SS
Time Schedule	Start	An event task is triggered at the start of the nominated time schedule.
	Start and Stop	An event task is triggered at both the start and end of the nominated time schedule.
	Stop	An event task is triggered at the end of the nominated time schedule.
Unit	Communication Back	An event task is triggered when communications with the nominated controller has been restored.
	Communication Lost	An event task is triggered when communications with the nominated controller has been restored.
	Incomplete Primary Database	An event task is triggered to reinitialize the ACC when the primary database is incomplete.
	No Primary Database	An event task is triggered to reinitialize the ACC when a primary database cannot be detected.
	Operator Alarm	An event task is triggered when the nominated controller enters an alarm state.
	Operator Alarm Actioned	An event task is triggered when an alarm, associated with the nominated controller, is actioned by an operator.
	Operator Alarm Not Actioned	An event task is triggered when the operator fails to action an alarm associated with the nominated controller before the (re-activation) timeout.
	Operator Alarm Timed out	An event task is triggered when the operator fails to action the alarm associated with the nominated controller and the alarm times out.
	Operator Normal	An event task is triggered when the nominated controller returns to a normal state.
	Operator Restore	An event task is triggered when the nominated controller attains ‘Restored’ status.
	Operator Waiting for Normal	An event task is triggered when a restorable alarm at the nominated controller has been actioned but has not returned to its normal state.
	Reset	An event task is triggered when the nominated controller is reset.
Flag	False	Flag has been set to false.
	True	Flag has been set to true.

7.2 Targets / Commands

Target	Command	Description
ACC Trigger	Set Trigger	An ACC Trigger allows you to trigger a Controller event task from a software event, like a Host event task. This Command activates the trigger selected. Any Controller Event tasks of type “Host Control” will be listed in the Location drop-down menu.
	Clear Trigger	This Command clears the trigger selected, if it is currently activated.
Access Point	Allow Access	Allow access as if a valid card has been presented at the reader. The door lock will re-lock after the defined Latch time.
	Lock Door	Locks the door temporarily until the next change in Time Schedule.
	Unlock Door	Unlocks the door temporarily until the next change in Time Schedule.
	Set Mode “Card Only”	Enables Card Only operation at an access point. Refer to Operational modes page 22 for more information.
	Set Mode “Card and PIN”	Enables Card and PIN operation at an access point. Refer to Operational modes page 22 for more information.
	Set Mode “H. V. Card Only”	Enables Host Verification Card Only operation at an access point. Refer to Operational modes page 22 for more information.
	Set Mode “H. V. Card and PIN”	Enables Host Verification Card and PIN operation at an access point. Refer to Operational modes page 22 for more information.
	Set Mode “V. O. Card Only”	Enables View Only Card Only operation at an access point. Refer to Operational modes page 22 for more information.
	Set Mode “V. O. Card and PIN”	Enables View Only Card and PIN operation at an access point. Refer to Operational modes page 22 for more information.
	Set Mode “D. R. Card Only”	Enables Delayed Reporting Card Only operation at an access point. Refer to Operational modes page 22 for more information.
	Set Mode “D. R. Card and PIN”	Enables Delayed Reporting Card and PIN operation at an access point. Refer to Operational modes page 22 for more information.
	Set Mode “Disabled”	Disables an access point. Refer to Operational modes page 22 for more information.
	Restore Access Mode	Restores the previous access mode at an access point. Refer to Operational modes page 22 for more information.
	Reset Reader Tamper	Resets the reader tamper. Only applies to the Siemens reader range.
	Block Door	Blocks the door and prevents cards from being used to gain access at the door using the selected reader.

Target	Command	Description
	Unblock Door	Returns a blocked door to its normal programmed mode of operation.
	Request Access Mode	Request a current access mode.
	Set mode “No Dual Custody”	Disables Dual Custody for the access point.
	Set mode “Standard Dual Custody”	Sets the access point to Standard Dual Custody Mode.
	Set mode “Supervisory Dual Custody”	Sets the access point to Supervisory Dual Custody Mode.
	Restore Access Mode configuration	Restores the access mode that is stored in the database.
	Set “No Additional Access”	Sets the additional access for the selected access point to No Additional Access.
	Set “PIN as Card” additional access mode	Sets the additional access for the selected access point to PIN as Card.
	Set “Daily Code” additional access mode	Sets the additional access for the selected access point to Daily Code.
	Restore additional access mode	Returns the access point to the normal additional access operation mode defined in the Components screen.
	Unlock Door, Override Door Interlocking	Unlocks the door and ignores any Door Interlocking configuration.
	Allow Access, Override Door Interlocking	Allows access and ignores any Door Interlocking configuration.
	Intrusion Control – Enable	Enable Intrusion Control on the selected access point.
	Intrusion Control – Disable	Disable Intrusion Control on the selected access point.
	Intrusion Control – Restore Config	Restore Intrusion Control to whatever is configured.
	Set mode “Authorization – Card Only”	Enables “Authorization – Card Only” operation at an access point. Refer to Operational modes for more information.
	Set mode “Authorization – Card + PIN”	Enables “Authorization – Card + PIN” operation at an access point. Refer to Operational modes for more information.
Access Point Group	Same as access points	See “Access Point”
Actionable Report	Not applicable	Performs the default actions that were configured for the report that appears in the Report field.
Anti-Passback Area	Forgive	Forgives a single cardholder. Enter the card number of the forgiven cardholder into the **Data** field.
	Forgive all	Forgives all cardholders currently in the area.

Target	Command	Description
	Reset Count	Resets the current count for the anti-passback area to zero.
	Override Mode	Override the selected area with a specific mode.
	Restore Mode	Restores the configured Anti-Passback mode.
CCTV	Switch Camera to Monitor	Switches the selected camera to display on the specified monitor. Refer to the *CCTV User's Guide* for more information.
	Run Pattern	Displays a pre-configured pattern on the specified monitor. Refer to the *CCTV User's Guide* for more information.
	Run Sequence	Displays a pre-configured sequence on the specified monitor. Refer to the *CCTV User's Guide* for more information.
	Run Preset	Displays a pre-configured preset on the specified monitor. Refer to the *CCTV User's Guide* for more information.
	Activate Alarm	Activates a pre-configured alarm on the specified monitor. Refer to the *CCTV User's Guide* for more information.
	Acknowledge Alarm	Displays a pre-configured alarm on the specified monitor. Refer to the *CCTV User's Guide* for more information.
Database	Database Backup: Data	Performs a backup of the SiPass integrated data files.
	Database Backup: Binaries	Performs a backup of the SiPass integrated binary files.
	Database backup: Historical	Performs a backup of the historical data.
	Database Backup: Runtime	Performs a backup of the runtime data.
	Database Backup: Full	Performs a complete SiPass integrated Database backup.
Door Interlocking	Disable	Disable Door Interlocking.
	Restore	Restore Door Interlocking.
DVR	DVR Recording	Records the live image from the selected DVR Camera for between 1 and 600 seconds. Enter the desired recording time into the **Duration** field in seconds.
	DVR Operation	The DVR Client will appear displaying the live image from the selected camera and preset.
	DVR Camera Positioning	Moves the selected DVR Camera to a predefined position.
Floor point	Bank Floor secure	Secures the specified floor.
	Bank Floor unsecure	Unsecures the specified floor.
	Cancel permanent action	Cancels the last command for the elevator floor and returns its operation to the programmed operation.

Target	Command	Description
Floor Point Group	As for Floor Points	See above.
Input Point	Disable	Disables the input, if it is currently enabled, until the next change in Time Schedule.
	Enable	Enables the input, if it is currently disabled, until the next change in Time Schedule.
	Pulse	Sends a pulse command to the selected Input. This is only applicable for Sintony input points of type “Serial Coms Input”
	Set state to Alarm	Set the input to state Alarm.
	Set state to Normal	Set the input to state Normal
Input Point Group	Same as Input Points	See above
Intrusion Area Point	Arm Intrusion Area	Arms the selected intrusion area.
	Disarm Intrusion Area	Disarms the selected intrusion area.
	Isolate Input	Manually isolates a point from an intrusion area, excluding that point from a seal check when the area is armed.
	Part Arm Intrusion Area	Arms inputs which are marked as Part Arm.
	Part Arm B Intrusion Area	Arms inputs which are marked as Part Arm B.(SPC only)
Intrusion Area Point Group	Same as Intrusion Area Points	See above
Message Forwarding	Forward to Pager(s)	Allows a message to be forwarded to one or more pagers if the host event task has been triggered.
	Send to all OPC Clients	Sends details of the trigger to all OPC connections defined in the *Components* dialog.
	Forward to Email(s)	Allows a message to be forwarded to one or more email addresses if the host event task has been triggered.
Output Point	Allow Access	Allows access at an output point. (Operates in the same way as if a cardholder used their card to gain valid access at the same point). The output point will only be activated (unlocked) for the pre-set latch time.
	Lock	Locks the output temporarily (if the output is currently unlocked) until the next change in Time Schedule. Enter the Time into the **Data** field, using the format HH:MM:SS.
	Unlock	Unlocks the output temporarily (if the output is cur-rently locked) until the next change in Time Schedule. Enter the time into the **Data** field, using the format HH:MM:SS.
	Toggle	The state of the output will be toggled to the reverse state.

Target	Command	Description
	Slow Pulse Output	The output will pulse slowly. For example, this could be used for alarms that utilize a pulsed output like strobes or sirens. Enter the time that you want the output to slow pulse into the **Data** field, using the format HH:MM:SS.
	Fast Pulse Output	The output will pulse quickly. For example, this could be used for alarms that utilize a pulsed output like strobes or sirens. Enter the time that you want the output to fast pulse into the **Data** field, using the format HH:MM:SS.
	Single Pulse	The output will emit a single pulse.
	Return to Time Schedule control	The output will return to normal Time Schedule control.
	Cancel Permanent Action	Any current Permanent Command or Event Task, or Access/Internal Action operating on the target will be cancelled. The next Control State in the Control State Queue will take effect.
	Unlock, Override Door Interlocking	Unlocks the output and ignores any Door Interlocking configuration.
	Allow Access, Override Door Interlocking	Allows access and ignores any Door Interlocking configuration.
Output Point Group	Same as Output Points	See above
Reporting	Print	Print the selected report.
	SaveAs	Exports the selected report to a file.
	Email Forwarding	Export the selected report to a file and then email it to selected cardholders.
System	Turn Printer Off	Turns the Audit Trail printer off.
	Turn Printer On	Turns the Audit Trail printer on.
	Turn Printer to Short Log	Sets the Audit Trail messages (printed) to summary form (not all columns are sent to the printer).
	Turn Print to Full Log	Sets the Audit Trail messages (printed) to all columns that can appear in the Audit Trail.
	Check Expired Cards	When cards are presented for verification at an access point, their expiry dates are checked.
	Check Before Start Date Cards	When cards are presented for verification at an access point, their start dates are checked.
	Execute Command	Executes a command. (Typically, this would be used to start an executable (.EXE) or batch command (.BAT) file. Enter the path and filename of the file into the **Data** field. For example, C:\Program Files\myfile.bat

Target	Command	Description
	Shutdown Client	Shuts down a SiPass integrated Client. Enter the Computer Name of the PC, on which the Client to be shutdown is running, into the **Data** field. For example, AUSSecServer103.
Unit	Full Initialization	Performs a full initialization for the selected unit.
	Compact Database	Performs compacted database backup database for the selected unit. This operation maybe required when unit's Backup Flash memory becomes full.
	Establish Dial-up Connection	Initiates a dialup connection with the SiPass integrated Server. The audit trail in the unit will be automatically uploaded upon a successful connection.
Workgroup	Void	Voids the workgroup.
	Unvoid	Removes the void flag from a workgroup.
Flag	False	Set Flag to false
	True	Set Flag to true

8 Controller Event Tasks

SiPass integrated allows you to define a controller event task that performs a certain task (command) when a specific set of circumstances have been met (trigger).

Because controller event tasks are triggered by hardware events, you must select what type of component triggers or responds to the event.

The following table lists the Types and States that can be selected when defining a Trigger for a Controller Event Task.

8.1 Sources

Type	State (trigger)	Description
ACC Event Task	Cleared	Allows the operator to trigger a Controller Event Task as a result of another Controller Event Task. The ACC controller event task selected in the Source field has not been triggered or has been reset.
	Set	The ACC controller event task selected in the Source field has been triggered.
Access Point (logical)	“Daily Code” mode set	Access Point mode set to Daily Code.
	“No Additional Access” mode set	Access Point mode set to No Additional Access.
	“No Dual Custody” mode set	Access Point mode set to No Dual Custody mode.
	“PIN as Card” mode set	Access Point mode set to Daily Code.
	“Standard Dual Custody” mode set	Access Point mode set to Daily Code.
	“Supervisory Dual Custody” mode set	Access Point mode set to Daily Code.
	Disable Intrusion Control	Intrusion Control is disabled on the access point.
	Dual Custody Verification Complete	Dual Custody verification has been completed at the access point.
	Enable Intrusion Control	Intrusion Control has been enabled at the access point.
	Invalid Daily Code	An event task is triggered when an invalid daily code has been entered at an access point.
	Reader Online	An event task is triggered when a reader enters the offline state. Only valid for the Siemens reader range.
	Reader Offline	An event task is triggered when a reader enters the online state. Only valid for the Siemens reader range.
	Reader Tamper	An event task is triggered when a reader enters the tamper state (tamper input activated). Only valid for the Siemens reader range.

Type	State (trigger)	Description
	Reader Tamper OK	An event task is triggered when a reader returns from a tamper state. Only valid for the Siemens reader range.
	Self Authorization Granted	Cardholder has self authorized on at Dual Custody access point.
	Valid Daily Code	An event task is triggered when a valid daily code has been entered at a keypad/reader.
	Waiting Dual Custody Verification	An event task is triggered after the first cardholder has badged a card, signalling that the input point is waiting for the second valid card badge of the config-ured Dual Custody.
Always Set	N/A	This option will set Trigger 1 to be TRUE. This can be used to generate complex event triggers, when used in conjunction with the logical operators and Trigger 2.
Anti Passback Area	Area Count Reset	Area count has been reset.
	Area Mode Changed	Area mode has been changed.
	Capacity Empty	The area is vacant.
	Capacity Exceeded	An event task is triggered when the number of cardholders in the area exceeds the defined maximum.
	Capacity Full	An event task is triggered when the number of cardholders currently in the anti-passback area has reached the programmed capacity.
	Capacity Not Empty	The area is no longer empty.
	Capacity Not Full	The number of cardholders in the area does not exceed the defined maximum.
	Four Eyes Access Alarm	An event task is triggered when an area under four eyes control has been violated.
	Four Eyes Access Normal	An event task is triggered when an area under four eyes control returns to normal.
	Workgroup Capacity Empty	The number of cardholders in the area from a Workgroup is zero.
	Workgroup Capacity Exceeded	The number of cardholders in the area from a Workgroup has exceeded the maximum for that Workgroup.
	Workgroup Capacity Full	The number of cardholders in the area from a Workgroup has reached the maximum for that Workgroup.
	Workgroup Capacity Not Empty	The number of cardholders in the area from a Workgroup is no longer zero.
	Workgroup Capacity Not Full	The number of cardholders in the area from a Workgroup has not reached the maximum for that Workgroup.
Card	Access Denied- Hard perimeter violation	An event task is triggered when an access attempt has been denied, due to an Anti-Passback violation in an area configured with a “Hard” anti-Passback mode.

Type	State (trigger)	Description
	Access Denied-Intrusion area armed	An event task is triggered when an access attempt has been denied, where an intrusion area has not been disarmed first.
	Accessibility Valid Card Presented	A valid card with the accessibility option has been presented at a reader.
	Anti Passback Area Capacity reached	An event task is triggered when an access attempt increases the current count for an Anti-Passback area to a value equal to the programmed capacity.
	APB Area Workgroup Capacity Reached	The maximum number of cardholders from a workgroup has been reached in the area.
	Card Expired	An event task is triggered when the card presented has expired (the card stop date is in the past).
	Card Ignored	A card swipe is ignored, as the Access Point is waiting for Host Verification.
	Card Low Battery	Active card has low battery.
	Card not yet active	An event task is triggered when the card presented has not yet reached its programmed start date.
	Card Revision Mismatch	An event task is triggered when a card, whose Print Revision Number recorded on the card does not match the Print Revision Number stored in the database, has been badged at an access point. The Print Revision Number is updated each time the card is printed. This applies only to Siemens proprietary 52-bit card format.
	Door Interlocking In Progress Collision	An event task is triggered if a card is badged a second time at any door in a Door Interlocking set, while the first door interlocking set timeout is still in progress.
	Duress	An event task is triggered when an access attempt has been made under duress.
	Elevator Access Collision	An event task is triggered when the HLI Elevator is in access collision because another access session is in progress.
	Elevator Offline Denied	An event task is triggered when the HLI Elevator is offline.
	Elevator Override Denied	An event task is triggered when the HLI Elevator is in external override.
	Facility Error	An event task is triggered when a card with an invalid facility code was badged at a reader.
	Group Error	An event task is triggered when a card has been badged, whose access group is not permitted access to this point during the Time Schedule or altogether.
	Host Verification Allow Access	Cardholder has been granted access by an operator via Host Verification.
	Host Verification Deny Access	Cardholder has been denied access by an operator via Host Verification.

Type	State (trigger)	Description
	Host Verify Message	An event task has been triggered when a request for Image Verification has been sent from an access point to SiPass integrated.
	Host Verify Timeout Message	An event task has been triggered when a card has been badged at an image verification access point, and the operator has not responded within the defined Host Verify Timeout.
	Host Verify View Only Message	An event task has been triggered when a view-only image verification event has occurred at an access point.
	No Entry	An event task is triggered if the access point is set to “Delayed Reporting” mode and a valid card has been badged at a reader, but the door monitor has not registered passage through the door.
	Passback Error	An event task has been triggered when a card has been badged out of sequence at an access point configured for Global Anti-Passback.
	PIN Error	An event task has been triggered when an incorrect PIN for that card number has been entered at an access point.
	PIN Error Disabled	An event task has been triggered when a card has been voided after the cardholder has made three consecutive incorrect PIN entries in the facility.
	Point Disabled	An event task has been triggered when an access point has been disabled.
	Soft Anti-Passback error	An event task has been triggered when a soft Anti-Passback error has occurred.
	Soft Perimeter Violation	An event task has been triggered when a Soft perimeter violation has occurred.
	Time Schedule Violation	An event task has been triggered when a card was rejected because it has access to this door but not at the current time
	Timed Re-Entry Error	An event task has been triggered when a cardholder has attempted to re-enter an area (set to Timed Re-Entry Anti-Passback mode) before their permitted re-entry time.
Controller	About to Reset	ACC is about to reset.
	AC Power Fail	An event task has been triggered when a controller event task is triggered when the mains power to the ACC fails.
	AC Power OK	An event task has been triggered when a controller event task is triggered when the mains power to the ACC has been restored.
	Audit Trail Disabled	An event task has been triggered when a controller event task is triggered when Audit Trail reporting from the ACC to the Server is disabled.

Type	State (trigger)	Description
	Audit Trail Enabled	An event task has been triggered when a controller event task is triggered when Audit Trail reporting from the ACC to the Server is enabled.
	Audit Trail Full	An event task has been triggered when a controller event task is triggered when the Audit Trail log on the ACC is full.
	Battery Fail	An event task has been triggered when a controller event task is triggered when the DC backup battery connected to the ACC fails.
	Battery Low	An event task has been triggered when a controller event task is triggered when the DC backup battery connected to the ACC is operating at a critically low level.
	Battery OK	An event task has been triggered when a controller event task is triggered when the DC backup battery connected to the ACC is restored.
	Network Communications Failed	An event task has been triggered when the communications between the SiPass integrated Server and a controller has been lost.
	Network Communications OK	An event task has been triggered when the communications between the SiPass integrated Server and a controller has been restored.
	Tamper Active	An event task has been triggered when the tamper input to the ACC registers an alarm.
	Tamper Normal	An event task has been triggered when the tamper input to the ACC registers returns to a normal state.
	Unit Reset	An event task has been triggered when the ACC has been reset.
Device	Battery Fail	An event task has been triggered when the DC backup battery connected to the selected device fails.
	Battery Low	An event task has been triggered when the DC backup battery connected to the selected device is operating at a critically low level.
	Battery OK	An event task has been triggered when the DC backup battery connected to the selected device is restored.
	Battery Present	An event task has been triggered when the DC backup battery connected to the selected device is recharging.
	Invalid Card Technology selected	An event task has been triggered when a card technology has been selected that is incompatible with the reader connected to a Reader Interface Unit.
	Offline	An event task has been triggered when communications between the device and the ACC are disabled.

Type	State (trigger)	Description
	Online	An event task has been triggered when communications between the device and the ACC are restored.
	Power Fail	An event task is triggered when the power supply to the selected device fails.
	Power OK	An event task is triggered when the power supply to the selected device has been restored.
	Reset	An event task is triggered when the selected device is reset.
Door Interlocking	Door Interlocking Alarm	Door Interlocking alarm state.
	Door Interlocking Disabled	Door Interlocking is disabled.
	Interlocking Operational	Door Interlocking is enabled.
	Floor	An event task is triggered when the selected bank floor is disabled.
	Bank Floor Enabled	An event task is triggered when the selected bank floor is enabled.
	Bank Floor Secure	An event task is triggered when the selected bank floor is secured.
	Bank Floor Unsecure	An event task is triggered when the selected bank floor is unsecured.
Host Control	Cleared	This Type allows a Controller Event Task to be triggered from a Host Event Task. An event task is triggered when the Controller Event Task has not been triggered or has been reset.
	Set	An event task is triggered when the Controller Event Task has been triggered.
Input Point (Device)	Active	An event task is triggered when the input point has been enabled or activated.
	Normal	An event task is triggered when the input point has been restored.
	Open	An event task is triggered when the input point has registered a Tamper event i.e. wires have been cut.
	Short	An event task is triggered when the input point has registered a Tamper event i.e. the device has been shorted.
Input Point (logical)	Door Closed	An event task is triggered when a door monitor has registered that a door has closed.
	Door Forced	An event task is triggered when the door monitor has registered that a door has been forced open.
	Door Held	An event task is triggered when a door monitor has registered that a door has been held open for longer than the Input Delay time.

Type	State (trigger)	Description
	Door Opened	An event task is triggered when a door monitor has registered that a door has been opened for longer than the Input Delay time.
	Door Tamper	An event task is triggered when a device has registered that a supervised door monitor input has been tampered with.
	Input Alarm	An event task is triggered when an input point has entered an alarm state.
	Input Faulty	An event task is triggered when an input point has become faulty.
	Input Isolated	An event task is triggered when an input point has been iso-lated.
	Input Normal	An event task is triggered when an input point has been re-stored to a normal state.
	Input Physically disabled at FLN device	The input has been physically disabled by setting jumpers on the device.
	Input Physically enabled at FLN device	The Fire Override on the device has been disabled physically.
	Input Sealed	An event task is triggered when an input point has been sealed.
	Input Tamper	An event task is triggered when a device has registered that a supervised input point has been tampered with.
	Input tamper or fault cleared	The input tamper state has been cleared / fixed.
	Input Unsealed	Input has failed a seal check when arming an Intrusion Area.
	Pass back Tamper	An event task is triggered when a device has registered that a supervised request-to-exit input has been tampered with.
	Pass back Trigger	An event task is triggered when a passback input has been activated.
Intrusion Area	Alarm	An event task will be triggered when the intrusion area enters an alarm state.
	Armed	An event task will be triggered when the specified intrusion area becomes armed.
	Arming Action Complete	An event task will be triggered when an attempt has been made to arm a dependant area, but not all areas to which it belongs have been armed first.
	Arming Failed – Input X in Alarm	An event task will be triggered when the arming of an intrusion area fails due to an input that is currently in an alarm state.
	Disarmed	An event task will be triggered when the specified area has been disarmed.
	Entry Delay Timer Started	An event task will be triggered when the entry delay timer has started.

Type	State (trigger)	Description
	Exit Delay Timer Started	An event task will be triggered when the exit delay timer has started.
	Normal	An event task will be triggered when the intrusion area enters the normal state.
	Part Armed	Intrusion Area has been Part Armed.
	Part Armed B	Intrusion Area has been Part Armed B. (SPC only)
Keypad	Standard Event	An event task is triggered when the “enter” or “#” key has been pressed at an access point with a keypad.
Output Point	Locked	Output point has been locked.
	Unlocked	Output point has been unlocked.
Reader	Smart Card Event	An event task is triggered when an event task is triggered when a MIFARE smart card has been badged at an access point.
	Standard Card Event	An event task is triggered when a standard access card (non-smart card) has been badged at an access point.
Time Schedule	End	An event task is triggered when the selected Time Schedule ends.
	Start	An event task is triggered when the selected Time Schedule begins.
	Start and end	An event task is triggered when the selected Time Schedule begins, and again when it ends.

8.2 Commands

Controller event tasks allow you to perform a range of hardware-related tasks and trigger host event tasks in response to events.

The following table lists the Types and Commands that can be selected when defining an Effect for a Controller Event Task.

Type	Command	Description
Access Point	Reader LED OFF	Turns the Reader LEDs off. You can also select the colour of the LED you want to affect.
	Reader LED blink	Blinks the specified Reader LED. You can also select the colour of the LED you want to affect.
	Unlock Latch	Unlocks the door latch associated with the specified reader.
	Lock Latch	Locks the latch controlled by the selected reader.
	Allow Access	Allows access at the door con-trolled by the reader.
	Set Mode “Card Only”	Enables Card Only operation at an access point. Refer to Operational modes page 22 for more information.
	Set Mode “Card and PIN”	Enables Card and PIN operation at an access point. Refer to Operational modes page 22 for more information.
	Set Mode “H. V. Card Only”	Enables Host Verification Card Only operation at an access point. Refer to Operational modes page 22 for more information.
	Set Mode H. V. “Card and PIN”	Enables Host Verification Card and PIN operation at an access point. Refer to Operational modes page 22 for more information.
	Set Mode V. O. Card Only	Enables View Only Card Only operation at an access point. Refer to Operational modes page 22 for more information.
	Set Mode V. O. “Card and PIN”	Enables View Only Card and PIN operation at an access point. Refer to Operational modes page 22 for more information.
	Set Mode D. R. “Card Only”	Enables Delayed Reporting Card Only operation at an access point. Refer to Operational modes page 22 for more information.
	Set Mode D. R. “Card and PIN”	Enables Delayed Reporting Card and PIN operation at an access point. Refer to Operational modes page 22 for more information.
	Set Mode “Disabled”	Disables an access point. Refer to Operational modes page 22 for more information.
	Restore Access Mode	Restores the previous access mode at an access point. Refer to Operational modes page 22 for more information.

Type	Command	Description
	Return to Time Schedule Control	Returns the Target point to normal Time Schedule control.
	Cancel Permanent Action	Any current Permanent Command or Event Task, or Access/Internal Action operating on the target will be cancelled. The next Control State in the Control State Queue will take effect.
	Reset Reader Tamper	Resets the reader tamper for the specified reader. Only available for the Siemens reader range.
	Reader Buzzer on	Turns the buzzer for the specified reader ON. Only available for the Siemens reader range.
	Reader Buzzer Off	Turns the buzzer for the specified reader OFF. Only available for the Siemens reader range.
	Block Door	Blocks the door for the associated reader.
	Unblock Door	Unblocks the door for the specified reader, the reader returns to its programmed mode of operation.
	Set mode “No Dual Custody”	Disables Dual Custody for the access point.
	Set mode “Standard Dual Custody”	Set the access point to Standard Dual Custody Mode.
	Set mode “Supervisory Dual Custody”	Set the access point to Supervisory Dual Custody Mode.
	Restore Dual Custody Config Mode	Restores Dual Custody to the configured mode.
	Report Dual Custody Config Mode	Reports the configured Dual Custody mode.
	Set “No Additional Access”	Set the additional access for the selected access point to No Additional Access.
	Set “Daily Code” additional access mode	Set the additional access for the selected access point to Daily Code.
	Set “PIN as Card” additional access mode	Set the additional access for the selected access point to PIN as Card.
	Restore additional access mode	Returns the access point to the normal additional access operation mode defined in the Components screen.
	Unlock Door, Override Door Interlocking	Unlocks the door and ignores any Door Interlocking configuration.
	Allow Access, Override Door Interlocking	Allows access and ignores any Door Interlocking configuration.
	Intrusion Control – Enable	Enable Intrusion Control on the selected access point.
	Intrusion Control – Disable	Disable Intrusion Control on the selected access point.
	Intrusion Control – Restore Config	Restore Intrusion Control to whatever is configured.

Type	Command	Description
	Set mode “Authorization – Card Only”	
	Set mode “Authorization – Card + PIN”	
Anti-Passback Area	Reset Count	Resets the current count for the anti-passback area to zero.
	Override Mode	Override the selected area with a specific mode.
	Restore Mode	Restores the configured Anti-Passback mode.
Controller	Turn Siren On	If a siren has been connected to the ACC, it will be activated.
	Turn Siren Off	If a siren has been connected to the ACC and is currently active, it will be de-activated.
Device	Device Reset	A device has been reset.
	Report all inputs	Reports all inputs on a device.
	Card Format Override	This Controller Event Task is specifically for Legacy Asco RIM devices. For further details regarding this event task, please contact the Technical Support Team.
Door Interlocking	Disable Door Interlocking	Disable Door Interlocking.
	Restore Door Interlocking	Restore Door Interlocking.
Floor	Bank Floor Secure	Secures the specified elevator floor (for all elevators within the same bank).
	Bank Floor Unsecure	Unsecures the specified elevator floor (for all elevators within the same bank).
	Bank Floor Enable	Enables the specified elevator floor (for all elevators within the same bank).
	Bank Floor Disable	Disables the specified elevator floor (for all elevators within the same bank).
	Return to Time Schedule	Returns the programmed access control for the specified floor.
	Cancel Permanent Action	Any current Permanent Command or Event Task, or Access/Internal Action operating on the floor will be cancelled. The next Control State in the Control State Queue will take effect.
Input Point	Disable	Disables the selected input point.
	Enable	Enables the selected input point.
	Return to Time Schedule Control	The output will return to normal Time Schedule control.
	Cancel Permanent Action	Any current Permanent Command or Event Task, or Access/Internal Action operating on the target will be cancelled. The next Control State in the Control State Queue will take effect.

Type	Command	Description
	Pulse	Sends a pulse command to the selected Input. This is only applicable for Sintony input points of type “Serial Coms Input”
	Set state to Alarm	Set the input to state Alarm.
	Set state to Normal	Set the input to state Normal.
Intrusion	Arm intrusion area	Arms the specified intrusion area.
	Disarm intrusion area	Disarms the specified intrusion area.
	Isolate input	Isolates input points in alarm mode and disables them within the specified intrusion area so that it can be armed for intrusion.
	Part Arm Intrusion Area	Arm input points in an Intrusion area.
	Part Arm B Intrusion Area	Arm input points B in an Intrusion area.
	Clear Sintony Intrusion area alarm.	Sends command to Sintony panel to clear the Sintony intrusion area alarm.
Output Point	Unlock	Unsecures the selected output point. Enter the time for which you want the door to be unlocked into the **Duration** field, using the format HH:MM:SS.
	Lock	Secures the selected output point. Enter the time for which you want the door to be locked into the **Duration** field, using the format HH:MM:SS.
	Toggle	Reverses the current status of the output point.
	Slow Pulse	Causes the output point to emit a slow pulse behaviour, depending on the point type. For example, a strobe light attached to a door controller would flash at a relatively slow rate. Enter the time for which you want the output to slow pulse into the **Duration** field, using the format HH:MM:SS.
	Fast Pulse	Causes the output point to emit fast pulse behaviour, depending on the point type. For example, a siren attached to a door controller would sound at rela-tively fast repeated intervals. Enter the time for which you want the output to fast pulse into the **Duration** field, using the format HH:MM:SS.
	Single Pulse	Causes the output point to emit a single pulse, depending on the point type.
	Return to Time Schedule Control	The output will return to normal Time Schedule control.

Type	Command	Description
	Cancel Permanent Action	Any current Permanent Command or Event Task, or Access/Internal Action operating on the target will be cancelled. The next Control State in the Control State Queue will take effect.
	Unlock, Override Door Interlocking	Unlocks the output and ignores any Door Interlocking configuration.
	Allow Access, Override Door Interlocking	Allows access and ignores any Door Interlocking configuration.
Run Host Task	N/A	Select a pre-defined host event task from the **Target** drop-down list. The host event task will be executed when the trigger occurs.

9 ASP Trigger States

The following table lists the Point Types and Properties that can be selected for ASP Trigger State.

Category	Trigger Type	Property	Property Values	Description
Input Point	Condition/Event	Input Logical State	Alarm Normal Tamper Disabled Enabled	Logical state of the input.
		Device Input State	Short Normal Active Open	Physical state of the input.
		Door Frame State	Door Forced Door Closed Door Held Door Tamper Input Disabled Door Opened	Logical state of Doorframe input.
		Input Enabled	True False	Enabled state of input.
		Tamper Logical State	Input Tamper Input Fault Tamer or Fault Cleared	Indicates Tamper or Fault state.
		Intrusion State	Input Alarm Input Normal Input Tamper Input Disables Input Isolated	Input Logical state related to intrusion Zone inputs.
		Physical Enable State	Input Disabled (HW) Input Enabled (HW)	Indicates if Input Physically dis-abled by FLN device.
	Event Only	Passback Triggered	True	COV only event for Passback triggered.
		Input Unsealed	True	COV only event for Input Unsealed.
		Input Sealed	True	COV only event for Input Sealed.
		Passback Denied	True	COV only event for Passback Denied.

Category	Trigger Type	Property	Property Values	Description
	Event/Condition	Input Logical State	Short Circuit Tamper Normal Alarm Open Circuit Tamper Tamper Fault Disabled Unsealed Isolated	SPC Input State
	Event/Condition	Input Logical State	Normal Alarm Unknown State Tamper Disabled in hardware Unsealed	Sintony input state
Output Point	Event/Condition	Dual State	Open Closed	Output state Open/Closed only.
		Aux Output State	Open Closed Slow Pulse Fast Pulse	Auxiliary Output state.
Access Point	Event/Condition	Reader Online State	Online Offline	Communication status of the reader.
		Reader Tamper State	Tamper Tamper Okay	Tamper state of the reader.
		Dual custody state	Dual Custody Complete Wait Dual Custody	Dual Custody state of the reader.
		Access Point Enabled State	False True	Enabled state of the reader.

Category	Trigger Type	Property	Property Values	Description
		Primary Access Mode	Card Only Mode Card & Pin Mode Host Verification Card Only mode Host Verification Card & Pin Mode View Only Card Only Mode View Only Card & Pin Mode Card Only Delayed Reporting Card & Pin Delayed Reporting Disabled Mode Programmable Authorization Card Only Mode Programmable Authorization Card & Pin Mode	The Primary Access mode of the reader.
		Additional Access Mode	No Additional Access Daily Code Pin as Card	The additional access mode of the reader.
		Dual Custody Mode	No Dual Custody Standard Dual Custody Supervisory Dual Custody	The dual custody access mode of the reader.
		Intrusion Control Mode	False True	The Intrusion Control Mode of the reader.
		Green LED State	LED On LED Off Blink LED	The Green LED state of the reader.
		Red LED State	LED On LED Off Blink LED	The Red LED state of the reader.
		Yellow LED State	LED On LED Off Blink LED	The Yellow LED state of the reader.
		Reader Buzzer	Off On	
Access Point	Event/Condition	Door Blocked	False True	Depicts that the door is blocked.
		Exclusion from Interlock	True False	Indicates Door is excluded from Door Interlocking Set.

Category	Trigger Type	Property	Property Values	Description
	Event Only	Invalid Daily Code	True	
		Valid Daily Code	True	Shows Valid Daily Code.
		Self Authorize Access	True	Indicates Self Authorized Access.
Anti-Passback Area	Event/Condition	Area Empty	False True	Indicates whether the APB Area is empty.
		Area Capacity	Capacity Full Capacity Exceeded Capacity Okay	Indicates whether the APB Area's capacity is full or exceeded.
		Four Eyes State	Alarm Normal	Indicates the Four Eyes Alarm state of the APB Area.
		Anti-Passback Mode	Hard Anti-Passback Soft Anti-Passback No Anti-Passback	Indicates the APB Mode of the APB Area.
		User Count	Integer Value	Indicates the number of users that are currently in the APB Area
	Event Only	Area Reset Event	True	All Users in the APB Area have been cleared
Anti-Passback Area Workgroup	Event/Condition	Empty State	False True	Indicates whether the APB Area is empty for the given workgroup.
		Capacity State	Capacity Full Capacity Exceeded Capacity Okay	Indicates whether the APB Area's capacity is full or exceeded for the given workgroup.
Intrusion Zone	Event/Condition	Armed State	Armed Disarmed Exit Delay PartArmed	Indicates the Arming state of the Native Intrusion Area.
		Alarm State	Alarm Normal Entry Delay	Indicates Alarm state of the Native Intrusion Area.
	Event Only	Arming Complete	True	Arming Session of Native Intrusion Area Complete.
		Arming Failed	True	Arming Session of All the Intrusion Areas failed.

Category	Trigger Type	Property	Property Values	Description
	Event/Condition	Armed State	Armed Disarmed ExitDelay PartArmed	Indicates the Arming state of the Sintony Intrusion Area.
		Alarm State	Alarm Normal EntryDelay	Indicates Alarm state of the External Intrusion Area.
		Armed State	Armed Disarmed PartArmed PartArmed B	Indicates the Arming state of the SPC Intrusion Area.
		Room 1 State Room 2 State Room 3 State Room 4 State Room 5 State Room 6 State Room 7 State Room 8 State	Unknown Armed Disarmed	Indicates the Arming state of the Sintony Intrusion Area Room.
Bank Floor	Event Only	Floor Selected	True	Bank Floor Selected
	Event/Condition	Enabled State	False True	Indicates if Bank Floor is Enabled/Disabled for Access.
		Secure State	False True	Indicates Secured/Unsecured state of Bank Floor.
Door Interlock	Event/Condition	Enabled	False True	Indicates the state of door interlock.
		State	Operational Disabled Alarm	Door Interlocking State of Interlocking Set.
		Interlock In Progress	False True	Access is occurring at a Door in the Interlocking Set.
Counter	Event/Condition	Done	False True	Indicates Counter Value is greater than or equal to Preset Value.
Time Schedule	Event/Condition	Time Schedule State	False True	Time schedule gets Off or On respectively
Timer	Event/Condition	Enable	False True	Gets a value indicating whether the the timer is enabled or not.

Category	Trigger Type	Property	Property Values	Description
		Done	False True	Gets the current value of the Timer Done.
		Timing	False True	Gets a value indicating whether the timer is currently running.
	Event Only	Time-out	False True	Timeout Event for a Periodic Timer.
Flag	Event/Condition	Flag State	False True	Indicates flag's current state.
Programmable Authorization Event	Condition Only	Programmable Authorization Status	Requested Host Criteria Passed Host Criteria Failed Host Timeout	Programmable Authorization status
Unit	Event/Condition	Comms ok	False True	Indicates the unit communication
	Event/Condition	Database Usage	0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, 65, 70, 75, 80, 85, 90, 95, 100	Indicates the percentage of Database Memory that has been used. The memory is reported in 5-percentile bands.
	Event/Condition	Runtime Memory Usage	0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, 65, 70, 75, 80, 85, 90, 95, 100	Indicates the percentage of Runtime Application Memory that is in use. The memory is reported in 5-percentile bands.
Access Event	Condition Only	Granted Access Event	Valid card Host verification Access Granted Soft Passback Error Soft Passback Perimeter Volation Programmable Authorization Access Granted	Card Events for Access Granted.

Category	Trigger Type	Property	Property Values	Description
		Denied Access Event	Void Card Pin Error Facility Error Group Error Passback Error Point Disabled Host Verification Timeout Card Revision Error Area Capacity Time Entry Error 3 PIN Void Card Not Yet Active Card Expired Time Period Error Intrusion Zone Lockout Perimeter Violation Access Collision Host Access Denied Elevator Offline Elevator Override Elevator Access Collision Invalid Dual Custody Workgroup Limit Error Door Interlocking Access Collision Programmable Authorization Timeout Programmable Authorization Access Denied	Card Events for Access Denied
		Other Access Event	No Entry User Duress Card Ignored card Presented Accessibility card Presented Host Verification Card Low Battery	Other Card Events
		Any Granted Access Event	True	Indicates that the Access Event was a Valid Access Event
		Any Denied Access Event	True	Indicates that the Access Event was a Invalid Access Event

Category	Trigger Type	Property	Property Values	Description
Venue	Event Only	Booking Offset Type	After End After Start Before End Before Start	After setting up a venue, an ASP activity can be configured to trigger an action before or after every booking start or stop. **Note:** The time for the action to take place before or after the start and stop of the venue booking can be set in minutes.

10 ASP Effect States

The following table lists the Point Types and Properties that can be selected for ASP Effect State.

Category	Effect Type	Property	Property Values	Description
Input Point	Regular Effect	Input Enabled	False True	Enabled state of all the input types except SPC.
		Return to Time Schedule Control	True	Pulse command to return to Time Control Period.
		Set Input	True	Command to set Sintony input.
		Clear Input	True	Command to clear Sintony input.
		Clear Isolate Input	True	Command to clear isolation of SPC Input.
		Isolate Input	True	Command to isolate Sintony/SPC input.
	Stateless Effect	Pulse Input	TrueTrue	Command to pulse Sintony input.
Output Point	Stateless Effect	Toggle Output	True	Toggles the door latch, local, elevator state of the output
	Alternative Effect	Dual State	Open Closed	Output State of Door Latch, Local, Elevator - Open and Closed only
	Regular Effect	Unlock Override Interlock	True	Overrides the door interlock state, setting the state of the Latch output to Unlock.
	Stateless Effect	Door Latch	Allow Access Override Interlock	Overrides the door interlock state setting the state of the Latch output to Allow Access
		Single Pulse Output	True	Unlock the output for a single, short pulse period for Door Latch and Auxiliary.
	Regular Effect	Output Cancel Perm	True	Cancel Permanent Override Command.
		Return to time schedule	True	Return to Time Period Control.
	Stateless Effect	Toggle Auxiliary	True	Toggles the state of the Auxiliary output.
	Alternative Effect	Aux Output State	Open Closed Pulse Fast Pulse	Auxiliary Output state.

Category	Effect Type	Property	Property Values	Description
Access Point	Regular Effect	Primary Access Mode	Card Only Mode Card & Pin Mode Host Verification Card Only mode Host Verification Card & Pin Mode View Only Card Only Mode View Only Card & Pin Mode Card Only Delayed Reporting Card & Pin Delayed Reporting Disabled Mode Programmable Authorization Card Only Mode Programmable Authorization Card & Pin Mode	The Primary Access Mode of the reader.
		Additional Access Mode	No Additional Access Daily Code Pin as Card	The additional access mode of the reader.
		Dual Custody Mode	No Dual Custody Standard Dual Custody Supervisory Dual Custody	The dual custody access mode of the reader.
		Intrusion Control Mode	False True	The Intrusion Control Mode of the reader
	Alternative Effect	Green LED State	LED On LED Off Blink LED	The green state of the reader.
		Red LED State	LED On LED Off Blink LED	The red state of the reader.
		Yellow LED State	LED On LED Off Blink LED	The yellow state of the reader.
		Reader Buzzer	Off On	Switches on/off the Reader Buzzer of the Access Point.
		Door Blocked	False True	Blocks the Door.
	Stateless Effect	Allow Access	True	Allows Access command.

Category	Effect Type	Property	Property Values	Description
		Return to Time Schedule Control	True	Returns to Time Schedule Control.
		Cancel Permanent Override	True	Cancels Permanent Override command.
		Access Unlock Override Interlock	True	Override interlock and unlock door.
		Allow Access Override Interlock	True	Override interlock and allow access.
	Regular Effect	Reset Reader Tamper	True	Command to Reset Reader tamper.
		Interlock Exclusion Command	Include Exclude Exclude and Unsecure Exclude and Allow Access	Perform Door Interlock Exclusion command on door.
		Programmable Authorization Granted	False True	Invoke Grant or Deny External Authorization command.
Anti-Passback Area	Regular Effect	Reset Area	True	Command to clear all users from the APB Area.
		Anti Passback Mode	Hard Anti-Passback Soft Anti-Passback No Anti-Passback	Indicates the APB Mode of the APB Area.
Intrusion Zone	Regular Effect	Force Arm	True	Arm the Native Intrusion Area and automatically isolate unsealed inputs.
		Force Part Arm	True	Part-Arm the Native Intrusion Area and automatically isolate unsealed inputs
		Arm	True	Arm the Intrusion Area.
		Part-Arm	True	Part-Arm the Intrusion Area.
		Disarm	True	Disarm the Intrusion Area.
		Part Arm B	True	Part Arm B the SPC Intrusion Area.

Category	Effect Type	Property	Property Values	Description
		Room 1 State Room 2 State Room 3 State Room 4 State Room 5 State Room 6 State Room 7 State Room 8 State	Unknown Armed Disarmed	Indicates the Arming state of the Sintony Intrusion Area Room.
Bank Floor	Regular Effect	Return to Time Schedule Control	True	Return to Time Period Control
		Cancel Permanent Override	True	Cancel Permanent Override Command.
		Secure State	True False	Shows the secure state of the bank floor.
Door Interlock	Regular Effect	Restore	True	Return Door Interlocking Set to configured Enabled state
		Disable	True	Disable Door Interlocking Set.
Counter	Regular Effect	Counter Value	Integer Value	Sets register containing the current counter value.
		Preset	Integer Value	Sets the preset value of the counter.
	Stateless Effect	Increment	Integer Value	Increments the counter by the specified amount.
		Decrement	Integer Value	Decrements the counter by the specified amount.
Timer	Regular Effect	Reset	True	Rest Timer Value to zero.
		Period Value	Integer Value	Sets the timer timeout/done period
	Alternative Effect	Enable	False True	Gets a value indicating the whether the timer is enabled or not.
Flag	Alternative Effect	Flag State	False True	Set or clears the flag state, or resets the flag state to it’s default state.
	Stateless Effect	Toggle Flag	True	Toggle Flag State.

Issued by
Siemens Switzerland Ltd
Smart Infrastructure
Global Headquarters
Theilerstrasse 1a
CH-6300 Zug
+41 58 724 2424
www.siemens.com/buildingtechnologies

A6V11144326