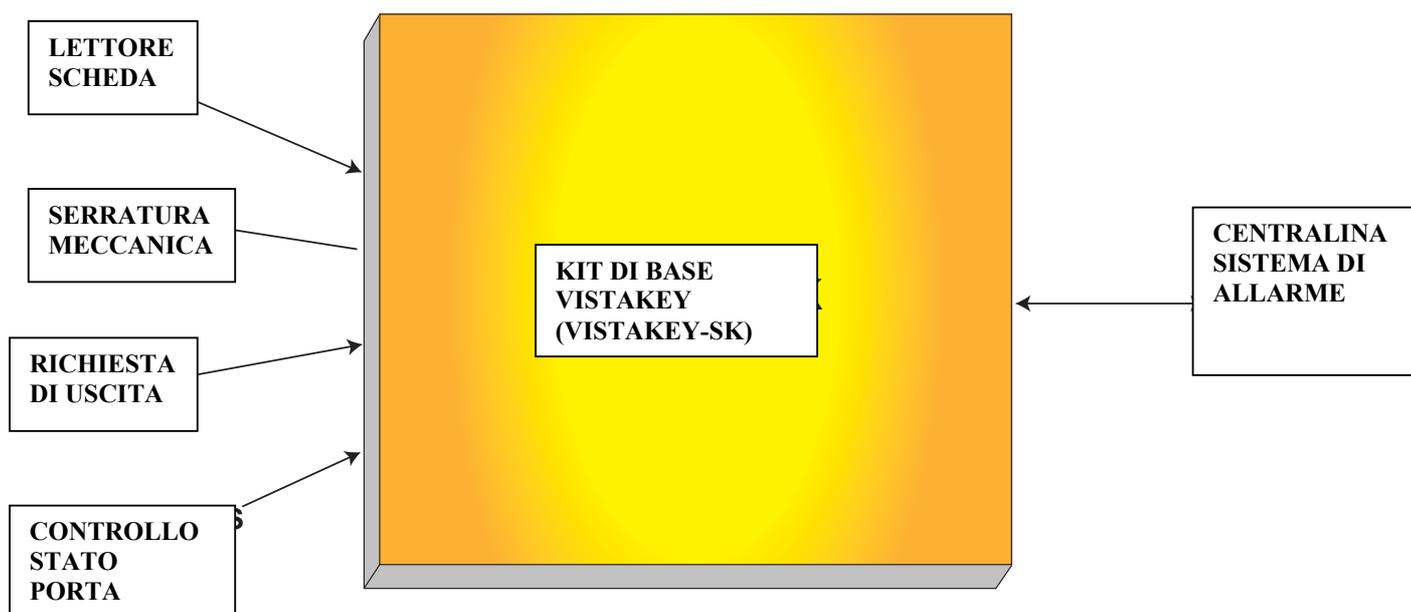


VistaKey-SK-EX

Kit di base controllo accesso singolo

Manuale di installazione e predisposizione



Indice

.....

Descrizione dei simboli.....	vii
Capitolo 1 – Introduzione.....	1-1
Informazioni generali	1-1
Caratteristiche modulo VistaKey.....	1-1
Sistemi di allarme antincendio/antifurto compatibili	1-2
Descrizione kit di base VistaKey (VistaKey-SK)	1-2
Dispositivi esterni	1-2
Procedure di installazione del kit di base VistaKey	1-3
Capitolo 2 – Integrazione del sistema di controllo accesso.....	2-1
Introduzione	2-1
Informazioni generali	2-1
Fase 1 – Planimetria controllo accesso e sistema di sicurezza	2-1
Fase 2 – Definizione privilegi gruppi di accesso	2-2
Fase 3 – Programmazione del sistema	2-3
Punti di accesso	2-4
Descrizione.....	2-4
Applicazione all'esempio corrente	2-4
Modalità di programmazione.....	2-4
Privilegi esclusivi	2-5
Descrizione.....	2-5
Applicazione all'esempio corrente	2-5
Modalità di programmazione.....	2-5
Limiti in modalità inserita	2-6
Descrizione.....	2-6
Applicazione all'esempio corrente	2-6
Modalità di programmazione.....	2-6
Fasce orarie ed eventi temporizzati.....	2-7
Descrizione.....	2-7
Applicazione all'esempio corrente	2-7
Modalità di programmazione.....	2-7
Livelli di autorità codici utente VISTA	2-8
Descrizione.....	2-8
Applicazione all'esempio corrente	2-8
Modalità di programmazione.....	2-9
Abbinamento partizione ai codici utente VISTA	2-10
Descrizione.....	2-10
Applicazione all'esempio corrente	2-10
Modalità di programmazione.....	2-10
Conclusioni	2-13
Capitolo 3 – Installazione - procedura rapida.....	3-1
Informazioni generali	3-1
Installazione del sistema	3-1
Montaggio e collegamento	3-2
Mappatura zone VistaKey per il test.....	3-2
Test iniziale del sistema	4-1

Capitolo 4 – Installazione - procedura dettagliata.....	4-1
Informazioni generali	4-1
Installazione del sistema	4-1
Assemblaggio e montaggio kit di base VistaKey	4-2
Montaggio e collegamento del lettore scheda.....	4-4
Montaggio del lettore	4-4
Collegamento del lettore	4-4
Collegamento uscita logica del modulo VistaKey	4-4
Collegamento zone del modulo VistaKey	4-4
Controllo stato porta	4-5
Richiesta di uscita	4-5
Montaggio e collegamento serratura meccanica/magnetica.....	4-5
Montaggio serratura meccanica/magnetica.....	4-5
Collegamento serratura meccanica/magnetica.....	4-5
Selezione indirizzo modulo VistaKey.....	4-6
Collegamento circuito polling e sistema di alimentazione modulo VistaKey	4-6
Mappatura zone VistaKey per il test.....	4-6
Test iniziale del sistema	4-7
Capitolo 5 – Programmazione.....	5-1
Informazioni generali	5-1
Foglio di programmazione eventi temporizzati	5-2
Foglio di programmazione funzione evento/azione.....	5-7
Mappatura zone VistaKey nelle zone del sistema di allarme	5-10
Impostazione opzioni di programmazione punto di accesso modulo VistaKey	5-14
Impostazione gruppi di accesso.....	5-19
Programmazione funzione evento/azione	5-22
Uscire dalla modalità #93 programmazione modalità menu	5-24
Programmazione eventi temporizzati.....	5-24
Abilitazione gruppi di accesso	5-24
Altre funzioni del sistema	5-24
Uscita momentanea dal punto di accesso.....	5-24
Abilitazione combinatori di accesso	5-27
Comando #73 di abilitazione accesso.....	5-27
Livelli di autorità del sistema di allarme	5-29
Rimozione modulo VistaKey	5-30
Capitolo 6 – Comandi tastiera	6-1
Informazioni generali	6-1
Comandi tastiera aggiuntivi	6-1
Controllo accesso.....	6-2
Comando #73	6-2
Comando #74	6-2
Comando #75	6-3
Comando #79	6-3
Comando #77 controllo dispositivi di uscita.....	6-3
Comando #78 test controllo accesso.....	6-4
Comando #80 controllo parametri	6-5
Funzioni scheda controllo accesso.....	6-5
Registrazione schede.....	6-6
Redazione schede	6-10
Cancellazione automatica.....	6-13
Cancellazione in blocco	6-14
Cancellazione manuale.....	6-15
Uscire dalla modalità programmazione funzioni scheda	6-15

Capitolo 7 – Test del sistema	7-1
Informazioni generali	7-1
Test del sistema	7-1
Rigenerazione azioni temporizzate	7-1
LED e ponticello del modulo VistaKey	7-2
Selezione errata del commutatore di indirizzo	7-2
Cancellazione errori di supervisione dispositivo DSM	7-2
Capitolo 8 – Registro eventi	8-1
Informazioni generali	8-1
Report alla centrale operativa	8-1
Registro eventi della centralina del sistema di allarme	8-2
Capitolo 9 – Modalità capacità ridotta	9-1
Informazioni generali	9-1
Descrizione modalità capacità ridotta (RCM)	9-1
Appendice A – Glossario	A-1
Appendice B – Indice analitico	B-1

Figure

Figura 1-1: Procedure di installazione del modulo VistaKey	1-4
Figura 2-1: Planimetria tipo	2-2
Figura 3-1: Schema elettrico modulo VistaKey	3-4
Figure 4-1: Installazione tipo modulo VistaKey	4-1
Figure 4-2: Installazione della base d'appoggio	4-2
Figure 4-3: Installazione del sistema di alimentazione	4-3
Figure 4-4: Installazione del modulo VistaKey	4-3
Schema connessioni	pagina finale

Tabelle

Tabella 5-1: Codici azione	5-5
Tabella 5-2: Eventi e azioni	5-9

Descrizione dei Simboli

Leggere attentamente la descrizione dei simboli sotto indicati prima di utilizzare il manuale:

UL

Questa nota fornisce informazioni specifiche in caso di installazione del sistema per applicazioni riportate negli elenchi UL.



Questo simbolo segnala informazioni importanti per l'installazione. In caso di inosservanza, il sistema potrebbe non funzionare correttamente.



Questo simbolo segnala condizioni che potrebbero danneggiare o alterare seriamente il funzionamento del sistema e provocare gravi lesioni fisiche. Leggere attentamente.

Enter Zone Num.
(000 = ESCI)

La maggior parte delle opzioni di programmazione del sistema vengono selezionate rispondendo a prompt alfanumerici visualizzati all'interno di una casella sul display della tastiera.

*00

Durante la programmazione del sistema, i campi dati vengono indicati con una "stella" (*) seguita dal codice campo.

CODICE MODELLO: I codici modello indicati all'interno del manuale corrispondono, se non diversamente specificato, a prodotti ADEMCO.

CAPITOLO 1

Introduzione

Contenuto

- ◆ *Informazioni generali*
- ◆ *Caratteristiche modulo VistaKey*
- ◆ *Sistemi di allarme antincendio/antifurto compatibili*
- ◆ *Descrizione kit di base VistaKey (VistaKey-SK)*
- ◆ *Dispositivi esterni*
- ◆ *Procedure di installazione del kit di base VistaKey*

Informazioni generali

VistaKey è un modulo di controllo accesso singolo che permette di controllare l'accesso a locali protetti se collegato ad un sistema di allarme antincendio/antifurto. Per controllare l'accesso da più punti, collegare più moduli VistaKey ad uno stesso sistema di allarme.

Il modulo VistaKey è contenuto nel kit di base VistaKey (VistaKey-SK). Il kit di base VistaKey comprende tutti i componenti necessari per installare la configurazione minima del punto di accesso (ad eccezione delle serrature magnetiche e meccaniche).

Questo manuale di installazione e predisposizione è suddiviso in capitoli disposti secondo la progressione logica delle procedure dettagliate di installazione del modulo VistaKey. Il capitolo 1 riguarda le informazioni generali, le caratteristiche e i problemi di compatibilità. I capitoli successivi forniscono le informazioni sull'integrazione del sistema di controllo accesso, l'installazione (procedura rapida e dettagliata), la programmazione, i comandi tastiera, i test del sistema e la descrizione del registro eventi.

UL

Il modulo VistaKey gestisce tre zone che, nelle installazioni UL, devono essere utilizzate **ESCLUSIVAMENTE** per funzioni di controllo accesso. **NELLE INSTALLAZIONI UL QUESTE ZONE DI INGRESSO NON DEVONO ESSERE UTILIZZATE PER APPLICAZIONI ANTINCENDIO O ANTIFURTO.**



NON utilizzare il modulo VistaKey con una centralina di allarme collegata ad un sistema di controllo accesso PassPoint mediante il modulo VISTA Gateway.

Caratteristiche modulo VistaKey

Le caratteristiche del modulo VistaKey sono:

- Il modulo VistaKey comunica con la centralina del sistema di allarme mediante uno speciale protocollo globale di interrogazione sequenziale del circuito polling del dispositivo Vplex.
- In caso di mancanza alimentazione interna, il modulo VistaKey attiva la funzione di monitoraggio secondario della porta punto di accesso mediante un dispositivo Vplex interno alimentato esclusivamente dal circuito polling. Questo dispositivo viene programmato come nuovo tipo di dispositivo Vplex nella modalità programmazione dispositivo Vplex della

centralina del sistema di allarme. Un'etichetta con il numero di serie è affissa sul modulo VistaKey per l'inserimento manuale del numero di serie.

- Il modulo VistaKey è in grado di gestire massimo 250 titolari di scheda.
- Le opzioni di programmazione del moduli VistaKey vengono programmate mediante software, software residente e memoria non volatile, escludendo la necessità di ponti con piastre a circuito stampato.
- I codici zona punto di accesso (1-15) vengono abbinati utilizzando un semplice interruttore a rotazione con 16 posizioni.
- I moduli VistaKey possono essere facilmente aggiunti o esclusi dal sistema mediante la tastiera del sistema di allarme.
- Grazie al modulo VistaKey, il registro allarmi della centralina del sistema di allarme è potenziato a 512 eventi.
- Gli eventi VistaKey vengono memorizzati nel registro allarmi della centralina del sistema di allarme.
- I moduli VistaKey sono dotati di un'uscita logica con collettore aperto (12mA @ 12VCC).
- In caso di mancanza di collegamento tra il modulo VistaKey e la centralina di allarme per due o più minuti, il modulo VistaKey, pur essendo alimentato, entra automaticamente in modalità capacità ridotta (RCM).

Il modulo VistaKey entra in modalità capacità ridotta per due minuti anche in caso di richiesta di trasferimento dati verso la centralina del sistema di allarme mediante un computer di download collegato direttamente. In modalità capacità ridotta, il modulo VistaKey riconosce e autorizza l'accesso da un punto di accesso alle schede autorizzate (indipendentemente dai parametri di tempo).

Sistemi di allarme antincendio/antifurto compatibili

La tabella sotto indicata elenca i sistemi di allarme con i quali il modulo VistaKey è in grado di interfacciare, il numero massimo di moduli VistaKey (punti di accesso) che possono essere collegati allo stesso sistema di allarme, il livello di revisione minimo del software della centralina richiesto perché il sistema sia compatibile e i codici componente EPROM.

<u>SIST. ALLARME</u>	<u>NUMERO MASSIMO MODULI VistaKey</u>	<u>LIVELLO DI REVISIONE MINIMO DEL SOFTWARE</u>	<u>CODICE COMPONENTE EPROM</u>
VISTA-32FB	4	2.0	WAVIS32FB-12
VISTA-120	8	11.0	WAVIS120-21xx
VISTA-128B	8	2.0	WAVIS128B-12
VISTA-128FB	8	3.0	WAVIS128FB-13
FA1600C	8	7.0	WAVIS150FA-17



Per conoscere il livello di revisione del software della centralina di allarme, entrare in modalità programmazione e digitare #92. La seconda riga del display visualizza il livello di revisione del software (senza punto decimale).

Descrizione kit di base VistaKey (VistaKey-SK)

Il kit di base VistaKey fornisce in un unico e semplice kit di installazione tutti i componenti necessari (ad eccezione della serratura meccanica o magnetica) per l'installazione della

configurazione minima del punto di accesso. Il kit di base VistaKey comprende i componenti sotto indicati:

- Armadietto metallico
- Modulo VistaKey
- Sistema di alimentazione distribuito
- Trasformatore
- Lettore di prossimità
- Soppressore elettrico
- 25 schede di accesso prox ADEMCO
- Base d'appoggio universale
- Attrezzature per l'installazione

Dispositivi esterni

L'elenco sotto indicato riporta alcuni dispositivi esterni che si possono collegare al modulo VistaKey.

<u>DISPOSITIVO</u>	<u>DESCRIZIONE</u>
Lettore scheda*	ADEMCO OP30-FWM oppure un lettore prox con prestazioni equivalenti.
Schede di accesso*	Schede prox ADEMCO in formato 34 bit codificate. Codice componente ADEMCO K3399 (pacchetto da 25 schede).
Richiesta di uscita	Contatto a pulsante o sensore di movimento quale PIR 998ADEMCO.
Controllo stato porta	Contatto quale i contatti magnetici a lamella ADEMCO TUFFFACTS®.
Sistema di alimentazione*	Il sistema di alimentazione interno corrisponde al codice componente ADEMCO SA12040.
Serratura meccanica/magnetica	Serrature meccanica elettrica o magnetica in commercio con tensione di funzionamento 12VCC e corrente massima 1,5A. (N.B.: i chiavistelli elettrici senza scatto non sono compatibili).
Soppressore elettrico*	Qualsiasi soppressore elettrico in commercio quale EL-EDS della EDCO.

- I dispositivi contrassegnati sono inclusi nel kit di base VistaKey.

Procedure di installazione del kit di base VistaKey.

L'installazione del kit di base VistaKey prevede alcune semplici procedure per montare e appendere il sistema e per programmare i punti di accesso mediante la centralina del sistema di allarme. La *figura 1-1: Procedure di installazione del modulo VistaKey* mostra le procedure necessarie.

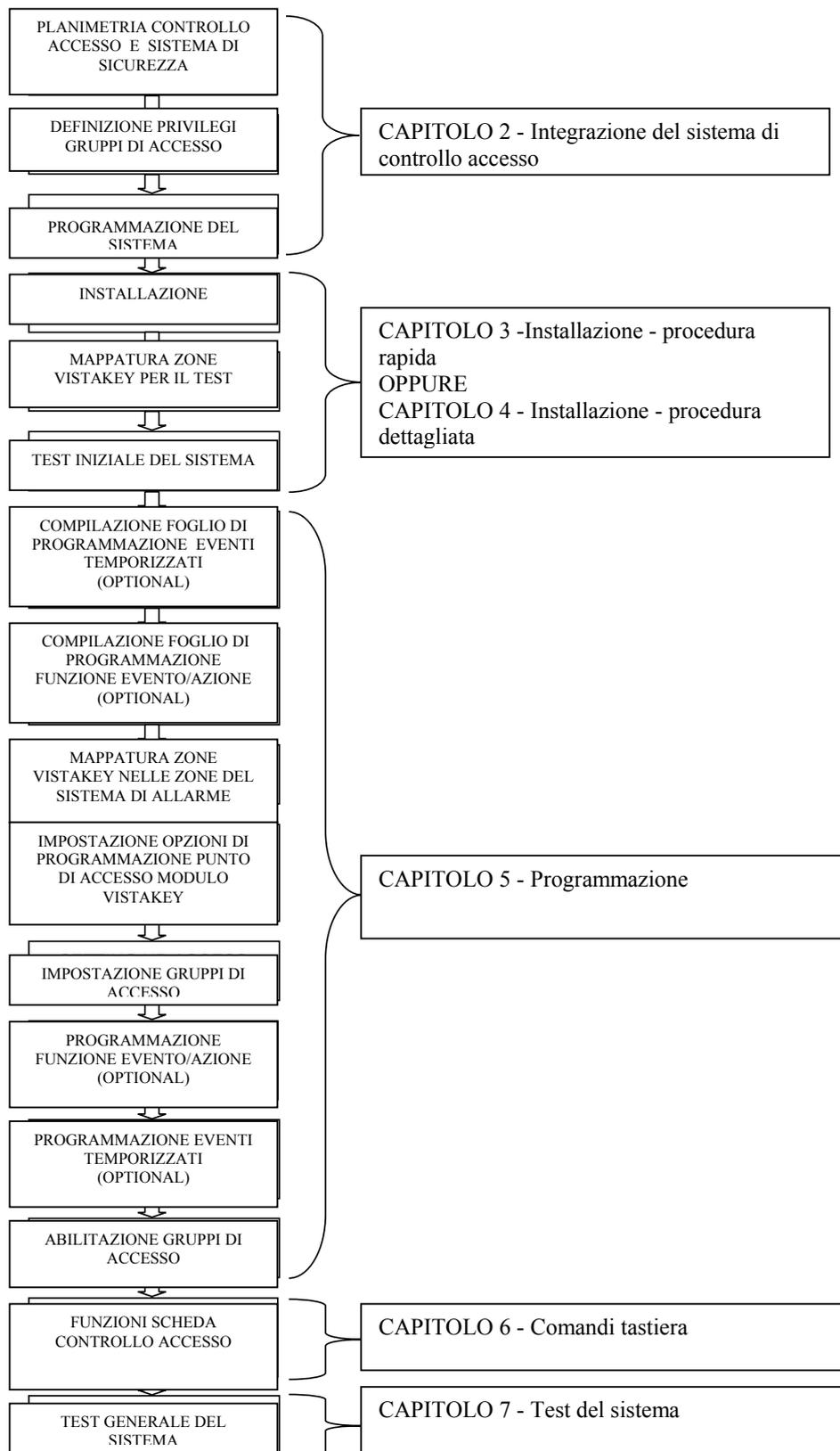


Figura 1-1: Procedure di installazione del modulo VistaKey

Integrazione del sistema di controllo accesso

Contenuto

- ◆ *Introduzione*
- ◆ *Informazioni generali*
- ◆ *Fase 1 – Planimetria controllo accesso e sistema di sicurezza*
- ◆ *Fase 2 – Definizione privilegi gruppi di accesso*
- ◆ *Fase 3 – Programmazione del sistema*
- ◆ *Conclusioni*

Introduzione

L'integrazione del sistema di sicurezza antincendio/antifurto con il controllo accesso richiede la preventiva definizione della posizione dei dispositivi e l'abbinamento dei privilegi. Questo capitolo permette di pianificare e realizzare in modo semplice un sistema di sicurezza che comprende un elaborato sistema di controllo accesso e un tradizionale sistema antifurto. Inoltre, vengono descritti, in modo molto semplice, i concetti e le strategie fondamentali per l'installazione e la configurazione di un sistema antifurto con controllo accesso. Le varie procedure sono rappresentate da un esempio grafico in cui la centralina VISTA è stata integrata con il kit di base VistaKey per il controllo accesso.

Leggere attentamente questo capitolo per definire le priorità da assegnare in fase di installazione e programmazione del sistema.



Informazioni generali

Il modulo di controllo accesso VistaKey è un dispositivo di controllo singolo di facile installazione e configurazione. Questo sistema gestisce un lettore scheda prox con interfaccia Weigand ed utilizza schede prox ADEMCO in formato 34 bit, che, abbinata alla tastiera(e) di controllo VISTA potenziano notevolmente il livello di sicurezza dell'installazione. Come sistema di accesso integrato, il modulo VistaKey offre un controllo completo e versatile dell'ingresso e uscita dipendenti in qualsiasi momento grazie ad una serie di fasce orarie ed eventi temporizzati programmabili. Il sistema è in grado di gestire massimo 250 schede utente suddivise in massimo 8 gruppi di accesso che agiscono su massimo 8 punti di accesso.

Fase 1 – Planimetria controllo accesso e sistema di sicurezza

La prima fase di installazione di un sistema di sicurezza antincendio/antifurto con controllo accesso riguarda la definizione delle reali esigenze di sicurezza del cliente: le condizioni e i privilegi assegnati agli occupanti o agli impiegati in base allo stato, gli abbinamenti e i

parametri di tempo, oltre agli aspetti della sicurezza perimetrale ed interna e ai movimenti degli occupanti nelle 24 ore, 7 giorni su 7, includendo vacanze, ferie e periodi di chiusura dei locali.

L'installazione e predisposizione dei sistemi di sicurezza non è standard. La definizione delle funzioni di controllo accesso necessarie e le modalità di integrazione di queste funzioni nel sistema antincendio/antifurto è, quindi, molto importante. Una serie di rappresentazioni grafiche evidenziano l'importanza di questi concetti e mostrano l'applicazione pratica delle caratteristiche del sistema di sicurezza VISTA.

La planimetria sotto indicata mostra i locali di un tipico edificio adibito a ditta composta da un'area ufficio e da un'area produzione o assemblaggio. La planimetria prevede 3 porte come segue:

- Punto di accesso 1 controllato dal lettore 1 (alla porta 1, partizione 1).
- Punto di accesso 2 controllato dal lettore 2 (alla porta 2, partizione 2).
- Punto di accesso 3 controllato dal lettore 3 (alla porta 3, partizione 3)

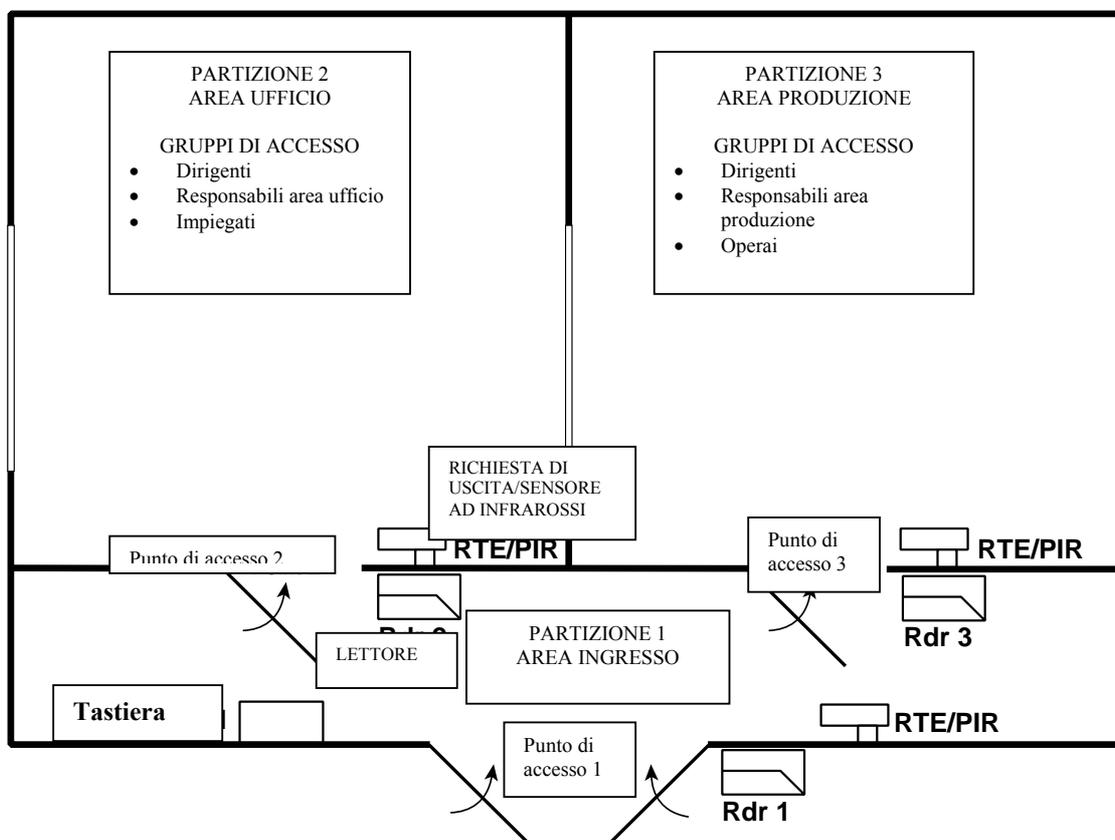


Figura 2-1: Planimetria tipo

La planimetria sopra indicata permette di definire le apparecchiature necessarie per l'installazione del sistema. Nell'esempio sopra indicato le apparecchiature necessarie sono:

- 2 kit di base VistaKey composti ognuno da 1 modulo VistaKey, 25 schede di accesso, 1 lettore prox, 1 sistema di alimentazione e 1 armadietto.
- 1 modulo VistaKey extra da installare all'interno di uno degli armadietti del kit di base.
- 1 centralina VISTA compatibile con il modulo VistaKey (per esempio VISTA-120).

- 1 lettore prox extra.
- 3 dispositivi RTE (richiesta di uscita) quali i sensori di movimento.
- Altre attrezzature ed accessori per la protezione antincendio e antifurto di porte, finestre ed aree interne.

Fase 2 – Definizione privilegi gruppi di accesso

I gruppi di accesso vengono stabiliti tenendo conto delle esigenze di sicurezza dei locali. Una volta chiarite queste esigenze, l'installatore procede alla definizione, in collaborazione con il titolare della ditta o con il direttore, delle caratteristiche di funzionamento che determinano le modalità di raggruppamento degli occupanti i locali. Le caratteristiche di funzionamento devono tenere conto in modo dettagliato dei movimenti del personale all'interno dei locali. Il personale viene suddiviso in gruppi di accesso correlati ai punti di accesso dei locali e a parametri di tempo.

A scopo di esempio, l'elenco sotto indicato mostra i gruppi di accesso con i corrispondenti livelli di autorità delle schede, definiti come i *privilegi di accesso* del titolare della scheda, in base al livello di sicurezza richiesto.

- Dirigenti:
 - a. Accesso a tutti i punti di accesso.
 - b. Inserimento/disinserimento di tutte le partizioni.
 - c. Accesso 24 ore su 24, 7 giorni su 7.
 - d. Disinserimento automatico della partizione mediante inserimento di una scheda valida.
- Responsabili area ufficio:
 - a. Accesso ai punti 1 e 2 negli orari programmati con partizioni inserite o disinserite.
 - b. Disinserimento automatico delle partizioni 1 e 2 mediante inserimento di una scheda valida.
 - c. Accesso al punto 3 e inserimento/disinserimento partizione 3 non autorizzati.
- Impiegati:
 - a. Accesso al punto 1 e inserimento/disinserimento della partizione 1 negli orari programmati.
 - b. Disinserimento automatico della partizione 1 mediante inserimento di una scheda valida.
 - c. Accesso al punto 2 solo a sistema disinserito e negli orari programmati. Inserimento/disinserimento partizione 2 non autorizzato.
 - d. Accesso al punto 3 e inserimento/disinserimento partizione 3 non autorizzati.
- Responsabili area produzione:
 - a. Accesso ai punti 1 e 3 negli orari programmati con partizioni inserite o disinserite.
 - b. Disinserimento automatico delle partizioni 1 e 3 mediante inserimento di una scheda valida.
 - c. Accesso al punto 2 e inserimento/disinserimento della partizione 2 non autorizzato.
- Operai:
 - a. Accesso al punto 1 e inserimento/disinserimento partizione 1 negli orari programmati.
 - b. Disinserimento automatico della partizione 1 mediante inserimento di una scheda valida.
 - c. Accesso al punto 3 solo a sistema disinserito e negli orari programmati. Inserimento/disinserimento partizione 3 non autorizzato.
 - d. Accesso al punto 2 o inserimento/disinserimento partizione 2 non autorizzati.

Fase 3 – Programmazione del sistema

Dopo aver definito i gruppi di accesso, compilare il foglio di programmazione per facilitare la pianificazione del sistema di sicurezza. Il foglio di programmazione sotto indicato è

incompleto ed evidenza di volta in volta i parametri di sicurezza/controllo accesso relativi all'esempio.

Compilare il foglio di programmazione dei gruppi di accesso alla fine del capitolo con i parametri di sicurezza specifici richiesti dal tipo di installazione che si intende realizzare.

Nel foglio di programmazione sotto indicato, sono stati aggiunti i nomi dei gruppi di accesso (colonna 2) e i privilegi (colonna 3) dei gruppi definiti nell'esempio precedente.

GRUPPO DI ACCESSO	CATEGORIA TITOLARI	PRIVILEGI
1	Dirigenti	a. Accesso a tutti i punti di accesso. b. Inserimento/disinserimento di tutte le partizioni. c. Accesso 24 ore su 24, 7 giorni su 7. d. Disinserimento automatico della partizione mediante inserimento di una scheda valida.
2	Responsabili area ufficio	a. Accesso ai punti 1 e 2 negli orari programmati con partizioni inserite o disinserite. b. Disinserimento automatico delle partizioni 1 e 2 mediante inserimento di una scheda valida. c. Accesso al punto 3 e inserimento/disinserimento partizione 3 non autorizzati.
3	Impiegati	a. Accesso al punto 1 e inserimento/disinserimento della partizione 1 negli orari programmati. b. Disinserimento automatico della partizione 1 mediante inserimento di una scheda valida. c. Accesso al punto 2 solo a sistema disinserito e negli orari programmati. Inserimento/disinserimento partizione 2 non autorizzato. d. Accesso al punto 3 e inserimento/disinserimento partizione 3 non autorizzati.
4	Responsabili area produzione	a. Accesso ai punti 1 e 3 negli orari programmati con partizioni inserite o disinserite. b. Disinserimento automatico delle partizioni 1 e 3 mediante inserimento di una scheda valida. c. Accesso al punto 2 e inserimento/disinserimento della partizione 2 non autorizzato.
5	Operai	a. Accesso al punto 1 e inserimento/disinserimento partizione 1 negli orari programmati. b. Disinserimento automatico della partizione 1 mediante/inserimento di una scheda valida. c. Accesso al punto 3 solo a sistema disinserito e negli orari programmati. Inserimento/disinserimento partizione 3 non autorizzato. d. Accesso al punto 2 e inserimento/disinserimento partizione 2 non autorizzati.

Punti di accesso

Descrizione

In questa sezione della fase 3 vengono definiti i punti di accesso (porte) che autorizzano l'accesso ai gruppi mediante inserimento di una scheda valida nel relativo lettore prox.

Applicazione all'esempio corrente

In questa sezione i privilegi del punto(i) di accesso vengono abbinati ad un gruppo. I dirigenti hanno accesso a tutte le porte del sistema, ma gli operai hanno accesso solamente alla porta ingresso principale e alla porta ingresso area produzione (punti 1 e 3).

Modalità di programmazione

I punti di accesso vengono programmati nei menu della modalità di programmazione *93 della centralina VISTA. Fare riferimento al paragrafo *Impostazione gruppi di accesso* del *Capitolo 5: Programmazione* di seguito.

GRUPPI DI ACCESSO	CATEGORIA TITOLARI	PRIVILEGI	PUNTI DI ACCESSO		
			1	2	3
1	Dirigenti	a. Accesso a tutti i punti di accesso. b. Inserimento/disinserimento di tutte le partizioni. c. Accesso 24 ore su 24, 7 giorni su 7. d. Disinserimento automatico della partizione mediante inserimento di una scheda valida.	X	X	X
2	Responsabili area ufficio	a. Accesso ai punti 1 e 2 negli orari programmati con partizioni inserite o disinserite. b. Disinserimento automatico delle partizioni 1 e 2 mediante inserimento di una scheda valida. c. Accesso al punto 3 e inserimento/disinserimento partizione 3 non autorizzati.	X	X	
3	Impiegati	a. Accesso al punto 1 e inserimento/disinserimento della partizione 1 negli orari programmati. b. Disinserimento automatico della partizione 1 mediante inserimento di una scheda valida. c. Accesso al punto 2 solo a sistema disinserito e negli orari programmati. Inserimento/disinserimento partizione 2 non autorizzato. d. Accesso al punto 3 e inserimento/disinserimento partizione 3 non autorizzati.	X	X	
4	Responsabili area produzione	a. Accesso ai punti 1 e 3 negli orari programmati con partizioni inserite o disinserite. b. Disinserimento automatico delle partizioni 1 e 3 con inserimento di una scheda valida. c. Accesso al punto 2 e inserimento/disinserimento della partizione 2 non autorizzato.	X		X

5	Operai	<ul style="list-style-type: none"> a. Accesso al punto 1 e inserimento/disinserimento partizione 1 negli orari programmati. b. Disinserimento automatico della partizione 1 mediante inserimento di una scheda valida. c. Accesso al punto 3 solo a sistema disinserito e negli orari programmati. Inserimento/disinserimento partizione 3 non autorizzato. d. Accesso al punto 2 e inserimento/disinserimento partizione 2 non autorizzati. 	X		X	
---	--------	--	---	--	---	--

Privilegi esclusivi

Descrizione

I privilegi esclusivi permettono al titolare della scheda di accedere a qualsiasi porta del sistema 24 ore su 24, 7 giorni su 7 e di disinserire automaticamente tutte le partizioni inserite mediante inserimento di una scheda valida nel lettore. Il privilegio esclusivo (stato) può essere assegnato ad un utente singolo o ad un gruppo di utenti (come nel sistema tipo descritto).

Applicazione all'esempio corrente

I privilegi esclusivi vengono assegnati al gruppo di accesso dei dirigenti e danno loro la facoltà di accedere a tutte le porte del sistema 24 ore su 24 e di disinserire le partizioni inserite mediante semplice inserimento di una scheda valida nel lettore.

Modalità di programmazione

I privilegi esclusivi vengono abilitati o disabilitati nei menu della modalità di programmazione *93 della centralina VISTA. Fare riferimento al paragrafo *Impostazione gruppi di accesso* del *Capitolo 5: Programmazione* di seguito.

GRUPPI DI ACCESSO	CATEGORIA TITOLARI	PRIVILEGI	PRIVILEGI ESCLUSIVI
1	Dirigenti	<ul style="list-style-type: none"> a. Accesso a tutti i punti di accesso. b. Inserimento/disinserimento di tutte le partizioni. c. Accesso 24 ore su 24, 7 giorni su 7. d. Disinserimento automatico della partizione mediante inserimento di una scheda valida. 	X
2	Responsabili area ufficio	<ul style="list-style-type: none"> a. Accesso ai punti 1 e 2 negli orari programmati con partizioni inserite o disinserite. b. Disinserimento automatico delle partizioni 1 e 2 mediante inserimento di una scheda valida. c. Accesso al punto 3 e inserimento/disinserimento partizione 3 non autorizzati. 	

3	Impiegati	<ul style="list-style-type: none"> a. Accesso al punto 1 e inserimento/disinserimento della partizione 1 negli orari programmati. b. Disinserimento automatico della partizione 1 mediante inserimento di una scheda valida. c. Accesso al punto 2 solo a sistema disinserito e negli orari programmati. Inserimento/disinserimento partizione 2 non autorizzato. d. Accesso al punto 3 e inserimento/disinserimento partizione 3 non autorizzati. 		
4	Responsabili area produzione	<ul style="list-style-type: none"> a. Accesso ai punti 1 e 3 negli orari programmati con partizioni inserite o disinserite. b. Disinserimento automatico delle partizioni 1 e 3 mediante inserimento di una scheda valida. c. Accesso al punto 2 e inserimento/disinserimento della partizione 2 non autorizzato. 		
5	Operai	<ul style="list-style-type: none"> a. Accesso al punto 1 e inserimento/disinserimento partizione 1 negli orari programmati. b. Disinserimento automatico della partizione 1 mediante inserimento di una scheda valida. c. Accesso al punto 3 solo a sistema disinserito e negli orari programmati. Inserimento/disinserimento partizione 3 non autorizzato. d. Accesso al punto 2 o inserimento/disinserimento partizione 2 non autorizzati. 		

Limiti in modalità inserita

Descrizione

Questa funzione permette di limitare (impedire) l'accesso da un punto da parte di un titolare di scheda appartenente ad un gruppo di accesso quando la partizione è inserita. La scheda non deve, però, essere mappata ad un utente VISTA con accesso alla partizione del punto di accesso.

L'impostazione di default prevede la disabilitazione di questa funzione: tutti i titolari di scheda di questo gruppo sono autorizzati ad accedere al punto di accesso abbinato anche se la partizione è inserita. La partizione può, quindi, essere disinserita automaticamente mediante inserimento di una scheda valida.

Applicazione all'esempio corrente

Abilitando la funzione limiti in modalità inserita, gli impiegati non possono accedere al punto 2 e gli operai al punto 3 quando le relative partizioni sono inserite.

Modalità di programmazione

La funzione limiti in modalità inserita può essere abilitata o disabilitata nel menu modalità di programmazione *93 della centralina VISTA. Fare riferimento al paragrafo *Impostazione gruppi di accesso* del *Capitolo 5: Programmazione* di seguito.

GRUPPO DI ACCESSO	CATEGORIA TITOLARI	PRIVILEGI	LIMITI IN MODALITA' INSERITA (partizioni)			
			1	2	3	4
1	Dirigenti	a. Accesso a tutti i punti di accesso. b. Inserimento/disinserimento di tutte le partizioni. c. Accesso 24 ore su 24, 7 giorni su 7. d. Disinserimento automatico della partizione mediante inserimento di una scheda valida.				
2	Responsabili area ufficio	a. Accesso ai punti 1 e 2 negli orari programmati con partizioni inserite o disinserite. b. Disinserimento automatico delle partizioni 1 e 2 mediante inserimento di una scheda valida. c. Accesso al punto 3 e inserimento/disinserimento partizione 3 non autorizzati.				
3	Impiegati	a. Accesso al punto 1 e inserimento/disinserimento della partizione 1 negli orari programmati. b. Disinserimento automatico della partizione 1 mediante inserimento di una scheda valida. c. Accesso al punto 2 solo a sistema disinserito e negli orari programmati. Inserimento/disinserimento partizione 2 non autorizzato. d. Accesso punto 3 e inserimento/disinserimento partizione 3 non autorizzati.		X		
4	Responsabili area produzione	a. Accesso ai punti 1 e 3 negli orari programmati con partizioni inserite o disinserite. b. Disinserimento automatico delle partizioni 1 e 3 mediante inserimento di una scheda valida. c. Accesso al punto 2 e inserimento/disinserimento della partizione 2 non autorizzato.				
5	Operai	a. Accesso al punto 1 e inserimento/disinserimento partizione 1 negli orari programmati. b. Disinserimento automatico della partizione 1 mediante inserimento di una scheda valida. c. Accesso al punto 3 solo a sistema disinserito e negli orari programmati. Inserimento/disinserimento partizione 3 non autorizzato. d. Accesso al punto 2 e inserimento/disinserimento partizione 2 non autorizzati.			X	

Fasce orarie ed eventi temporizzati

Descrizione

Le fasce orarie del sistema di controllo accesso permettono di gestire nel modo più efficiente le risorse e gli eventi del sistema, controllando in modo diretto e preciso l'accesso di un titolare ad un determinato punto di accesso in base all'orario programmato nell'arco della giornata.

Applicazione all'esempio corrente

Le fasce orarie e gli eventi temporizzati permettono di abilitare e disabilitare i gruppi di accesso e quindi di determinare gli orari in cui i titolari di scheda hanno facoltà di accedere ad un punto di accesso. In base al foglio di programmazione sotto indicato, i responsabili area ufficio hanno facoltà di accedere ai punti di accesso 1 e 2 tra le 6.00 (0600) e le 19.00 (1900). Infatti, l'accesso delle categorie di titolari di scheda di questo esempio è soggetto ad una determinata fascia oraria (ad eccezione dei dirigenti).

Modalità di programmazione

Le fasce orarie e gli eventi temporizzati vengono programmati nella *modalità #80 programmazione parametri*. L'azione selezionata è 77 abilitazione gruppo di accesso. L'azione viene abilitata nella fascia oraria e rimane disabilitata negli orari al di fuori della fascia.

GRUPPI DI ACCESSO	CATEGORIA TITOLARI	PRIVILEGI	FASCE ORARIE
1	Dirigenti	a. Accesso a tutti i punti di accesso. b. Inserimento/disinserimento di tutte le partizioni. c. Accesso 24 ore su 24, 7 giorni su 7. d. Disinserimento automatico della partizione mediante inserimento di una scheda valida.	Sempre attiva
2	Responsabili area ufficio	a. Accesso ai punti 1 e 2 negli orari programmati con partizioni inserite o disinserite. b. Disinserimento automatico delle partizioni 1 e 2 mediante inserimento di una scheda valida. c. Accesso al punto 3 e inserimento/disinserimento partizione 3 non autorizzati.	6.00 - 19.00
3	Impiegati	a. Accesso al punto 1 e inserimento/disinserimento della partizione 1 negli orari programmati. b. Disinserimento automatico della partizione 1 mediante inserimento di una scheda valida. c. Accesso al punto 2 solo a sistema disinserito e negli orari programmati. Inserimento/disinserimento partizione 2 non autorizzato. d. Accesso al punto 3 e inserimento/disinserimento partizione 3 non autorizzati.	6.00 - 19.00
4	Responsabili area produzione	a. Accesso ai punti 1 e 3 negli orari programmati con partizioni inserite o disinserite. b. Disinserimento automatico delle partizioni 1 e 3 mediante inserimento di una scheda valida. c. Accesso al punto 2 e inserimento/disinserimento della partizione 2 non autorizzato.	6.00 - 23.59

5	Operai	<p>a. Accesso al punto 1 e inserimento/disinserimento partizione 1 negli orari programmati.</p> <p>b. Disinserimento automatico della partizione 1 mediante inserimento di una scheda valida.</p> <p>c. Accesso al punto 3 solo a sistema disinserito e negli orari programmati. Inserimento/disinserimento partizione 3 non autorizzato.</p> <p>d. Accesso al punto 2 e inserimento/disinserimento partizione 2 non autorizzati.</p>	6.00 - 23.59
---	--------	---	--------------

Livello di autorità codici utente VISTA

Descrizione

In caso di scheda con traccia unica, abbinare il codice utente VISTA alle schede di accesso durante la registrazione. Abilitando la funzione traccia di una scheda, l'autorizzazione o la mancata autorizzazione vengono registrate con codice utente VISTA nel registro eventi o nei report alla centrale (se programmato). Se una scheda mantiene il valore di default 000 come codice utente VISTA in fase di registrazione e la funzione traccia è abilitata, la scheda viene registrata come utente U999 nel registro eventi o nei report alla centrale (se programmato).

I livelli di autorità vengono assegnati ai codici utente, se questi codici sono stati programmati nel sistema di sicurezza VISTA. I comandi tastiera per il controllo accesso da considerare in fase di abbinamento dei livelli di autorità dei codici utente VISTA sono numerosi; per maggiori informazioni sui livelli di autorità e i comandi di controllo accesso fare riferimento al *Capitolo 6: Comandi tastiera*.

Applicazione all'esempio corrente

In questo caso, sono richieste schede con traccia unica. Quindi, ogni scheda registrata nel sistema verrà anche mappata ad un unico codice utente VISTA che deve essere programmato nella centralina VISTA prima della registrazione della scheda.

- **Dirigenti:** Le schede dei dirigenti sono state abbinate ad un codice utente VISTA con livello di autorità "Master." Questo livello di autorità permette ai dirigenti di utilizzare il proprio codice utente VISTA per accedere ai comandi di controllo accesso, controllo dispositivi di uscita e programmazione parametri della tastiera VISTA sotto indicati:

#73, #74, #75, #77 e #80

Il livello di autorità "Master" permette ai dirigenti di registrare le schede, modificare i parametri di accesso delle schede, ecc.

- **Responsabili di area:** Le schede dei responsabili area ufficio e area produzione vengono abbinate ad un codice utente VISTA con livello di autorità "Manager". Questo livello di autorità permette ai responsabili di area di utilizzare i propri codici utente VISTA per accedere ai comandi di controllo acceso della tastiera VISTA sotto indicati:

#73, #74, e #75

Il livello di autorità "Manager" non permette ai responsabili di area di registrare le schede, cancellare le schede oppure modificare i parametri di accesso delle schede. I responsabili di area hanno, però, la facoltà di escludere o mettere in sicurezza dei punti di accesso del sistema utilizzando i propri codici.

- **Impiegati e operai:** Le schede degli operai e degli impiegati vengono abbinate ad un codice utente VISTA con livello di autorità "Operatore B". Questo livello di autorità

permette agli impiegati e agli operai di accedere ai comandi di controllo accesso della tastiera VISTA sotto indicati utilizzando il proprio codice utente VISTA:

#73 e #74

Il livello di autorità "Operatore B" non permette agli impiegati e agli operai di registrare o di cancellare delle schede, di modificare i parametri di accesso delle schede oppure di escludere o mettere in sicurezza dei punti di accesso. I codici utente assegnati a queste categorie permettono di richiedere l'accesso e l'uscita dai punti di accesso delle partizioni autorizzate. Inoltre, il livello di autorità "Operatore B" non permette di escludere le zone di protezione del sistema di sicurezza.

Modalità di programmazione

I livelli di autorità dei codici utente VISTA vengono programmati al momento dell'inserimento dei codici utente nel sistema VISTA. Per ulteriori informazioni fare riferimento al manuale di installazione della centralina VISTA.

GRUPPO DI ACCESSO	CATEGORIA TITOLARI	PRIVILEGI	LIVELLO DI AUTORITÀ UTENTE VISTA
1	Dirigenti	a. Accesso a tutti i punti di accesso. b. Inserimento/disinserimento di tutte le partizioni. c. Accesso 24 ore su 24, 7 giorni su 7. d. Disinserimento automatico della partizione mediante inserimento di una scheda valida.	1 – Master
2	Responsabili area ufficio	a. Accesso ai punti 1 e 2 negli orari programmati con partizioni inserite o disinserite. b. Disinserimento automatico delle partizioni 1 e 2 mediante inserimento di una scheda valida. c. Accesso al punto 3 e inserimento/disinserimento partizione 3 non autorizzati.	2 – Manager
3	Impiegati	a. Accesso al punto 1 e inserimento/disinserimento della partizione 1 negli orari programmati. b. Disinserimento automatico della partizione 1 mediante inserimento di una scheda valida. c. Accesso al punto 2 solo a sistema disinserito e negli orari programmati. Inserimento/disinserimento partizione 2 non autorizzato. d. Accesso punto 3 e inserimento/disinserimento partizione 3 non autorizzati.	4 – Operatore B
4	Responsabili area produzione	a. Accesso ai punti 1 e 3 negli orari programmati con partizioni inserite o disinserite. b. Disinserimento automatico delle partizioni 1 e 3 mediante inserimento di una scheda valida. c. Accesso al punto 2 e inserimento/disinserimento della partizione 2 non autorizzato.	2 – Manager

5	Operai	<p>a. Accesso al punto 1 e inserimento/disinserimento partizione 1 negli orari programmati.</p> <p>b. Disinserimento automatico della partizione 1 mediante inserimento di una scheda valida.</p> <p>c. Accesso al punto 3 solo a sistema disinserito e negli orari programmati. Inserimento/disinserimento partizione 3 non autorizzato.</p> <p>d. Accesso al punto 2 e inserimento/disinserimento partizione 2 non autorizzati.</p>	4 – Operatore B
---	--------	---	-----------------

Abbinamento partizioni ai codice utente VISTA

Descrizione

I codici utente VISTA immessi nella centralina VISTA permettono di accedere a tutte o a nessuna delle tre partizioni del sistema. L'utilizzo in combinazione con la funzione limiti in modalità inserita sopra descritta permette di determinare a quali punti di accesso può accedere un titolare di scheda quando la partizione è inserita.

Applicazione all'esempio corrente

- Il codice utente assegnato ai **dirigenti** permette l'accesso a tutte le partizioni. I privilegi esclusivi vengono assegnati ai dirigenti e, pur ereditando automaticamente (per default) tutti gli elementi per l'inserimento/disinserimento delle partizioni mediante inserimento di una scheda valida nel lettore, è consigliabile programmarli come utenti nel sistema VISTA perché possano eseguire altre funzioni del sistema di sicurezza.
- Il codice utente assegnato ai **responsabili area ufficio** permette l'accesso alle partizioni 1 e 2 a sistema inserito.
- Il codice utente assegnato **agli impiegati**, che normalmente hanno accesso alle partizioni 1 e 2, permette l'accesso solo alla partizione 1 (quando inserita). Il limite in modalità inserita alla partizione 2 è stato precedentemente selezionato per non autorizzare l'accesso degli impiegati alla partizione 2 quando il sistema è inserito.
- Il codice utente assegnato ai **responsabili area produzione** permette l'accesso alle partizioni 1 e 3 quando inserite.
- Il codice utente assegnato agli **operai**, che normalmente hanno accesso alle partizioni 1 e 3, permette l'accesso solo alla partizione 1 (quando inserita). Il limite in modalità inserita alla partizione 3 è stato precedentemente selezionato per non autorizzare l'accesso degli operai alla partizione 3 quando il sistema è inserito.

Modalità di programmazione

Programmazione codici utente. Per ulteriori informazioni fare riferimento al manuale utente della centralina VISTA.

GRUPPO DI ACCESSO	CATEGORIA TITOLARI	PRIVILEGI	CODICI UTENTE VISTA (partizioni)			
			1	2	3	
1	Dirigenti	<p>a. Accesso a tutti i punti di accesso.</p> <p>b. Inserimento/disinserimento di tutte le partizioni.</p> <p>c. Accesso 24 ore su 24, 7 giorni su 7.</p> <p>d. Disinserimento automatico della partizione mediante inserimento di una scheda valida.</p>	X	X	X	

2	Responsabili area ufficio	<p>a. Accesso ai punti 1 e 2 negli orari programmati con partizioni inserite o disinserite.</p> <p>b. Disinserimento automatico delle partizioni 1 e 2 mediante inserimento di una scheda valida.</p> <p>c. Accesso al punto 3 e inserimento/disinserimento partizione 3 non autorizzati.</p>	X	X		
3	Impiegati	<p>a. Accesso al punto 1 e inserimento/disinserimento della partizione 1 negli orari programmati.</p> <p>b. Disinserimento automatico della partizione 1 mediante inserimento di una scheda valida.</p> <p>c. Accesso al punto 2 solo a sistema disinserito e negli orari programmati. Inserimento/disinserimento partizione 2 non autorizzato.</p> <p>d. Accesso al punto 3 e inserimento/disinserimento partizione 3 non autorizzati.</p>	X			
4	Responsabili area produzione	<p>a. Accesso ai punti 1 e 3 negli orari programmati con partizioni inserite o disinserite.</p> <p>b. Disinserimento automatico delle partizioni 1 e 3 mediante inserimento di una scheda valida.</p> <p>c. Accesso al punto 2 e inserimento/disinserimento della partizione 2 non autorizzato.</p>	X		X	
5	Operai	<p>a. Accesso al punto 1 e inserimento/disinserimento partizione 1 negli orari programmati.</p> <p>b. Disinserimento automatico della partizione 1 con inserimento di una scheda valida.</p> <p>c. Accesso al punto 3 solo a sistema disinserito e negli orari programmati. Inserimento/disinserimento partizione 3 non autorizzato.</p> <p>d. Accesso al punto 2 e inserimento/disinserimento partizione 2 non autorizzati.</p>	X			

Una volta completate tutte le voci dell'esempio, il foglio di programmazione appare come indicato nella pagina seguente:

Avvertenze per l'inserimento del sistema di sicurezza:

L'esempio indicato sopra riguarda solamente il controllo accesso e il disinserimento del sistema di sicurezza. Le opzioni che facilitano l'inserimento del sistema di sicurezza sono molteplici:

- Il sistema di sicurezza può essere inserito mediante codice utente di un dirigente(i).
- Il sistema di sicurezza può essere inserito mediante un tasto RF da un dirigente(i).
- Il sistema di sicurezza può essere inserito mediante inserimento nel lettore di un punto di accesso di una scheda di accesso programmata per l'inserimento utilizzando la funzione evento/azione come descritto nel manuale.

Conclusioni

L'esempio descritto in questo capitolo deve essere elaborato e modificato in base alle specifiche esigenze di installazione.

Per facilitare l'installazione iniziale, utilizzare il foglio di programmazione allegato alla fine del capitolo.

Installazione - procedura rapida

Contenuto

- ◆ *Informazioni generali*
- ◆ *Installazione del sistema*
- ◆ *Mappatura zone VistaKey per il test*
- ◆ *Test iniziale del sistema*

Informazioni generali

Questo capitolo fornisce una rapida guida per l'installazione iniziale del modulo VistaKey. Per informazioni più dettagliate, fare riferimento alle procedure del *Capitolo 4 – Installazione - procedura dettagliata*. Le fasi di installazione descritte in questo capitolo sono: installazione del sistema, mappatura zone VistaKey alle zone del sistema di allarme e test iniziale.



Installazione del sistema

Per montare e collegare le apparecchiature necessarie per la creazione di un punto di accesso, seguire le procedure sotto indicate.

Montaggio e collegamento

1. Il modulo VistaKey è dotato di due morsettiere TB1 e TB3 con morsetti a spina. Tenere le viti della morsettiera verso l'esterno della scheda del modulo VistaKey e far scorrere le morsettiere sui piedini della scheda.
2. In caso di montaggio del kit di base del modulo VistaKey, installare la base d'appoggio nell'armadietto, montare l'armadietto ed installare il sistema di alimentazione.
IMPORTANTE: Inserire la rondella in nylon fornita sulla vite di supporto del sistema di alimentazione in basso a destra.
3. Montare il modulo VistaKey, la serratura meccanica o magnetica e il lettore di scheda.
4. Se compatibili, montare il dispositivo di controllo stato porta (DSM) e/o il dispositivo di richiesta di uscita (RTE).
5. Collegare il cavo di interfaccia del lettore di scheda alla morsettiera TB3, *collegando +5V o +12V per ultimo*. Fare riferimento alla *figura 3-1* alla fine del capitolo.
6. Collegare i conduttori principali alla morsettiera TB1 del modulo VistaKey rispettando l'ordine come sotto indicato:
 - a. I conduttori di terra ai morsetti 2, 5 e 9.
 - b. I conduttori dei dispositivi (optional) DSM, RTE, e GP rispettivamente ai morsetti 6, 7 e 8.
 - c. I conduttori della serratura meccanica (o magnetica) al morsetto 10 a relè.
 - d. Il conduttore di alimentazione interna +12V al morsetto 1.

- In caso di installazione del kit di base VistaKey, eseguire il collegamento con il morsetto 7 del sistema di alimentazione.
- e. Il conduttore di alimentazione interna +12V al morsetto 11 a relè N/C (in caso di serratura magnetica), **OPPURE** al morsetto 12 a relè N/O (in caso di serratura meccanica).
In caso di installazione del kit di base VistaKey collegare i morsetti 11 o 12 al morsetto 1 della morsettiera TB1.
 7. Collegare i connettori del circuito polling (-) e (+) (dalla centralina di allarme) rispettivamente ai morsetti 4 e 3.
 8. Selezionare il commutatore di indirizzo sul numero di porta di accesso desiderata (1-15).
 9. Ripetere i punti da 2 a 8 per ogni modulo VistaKey installato.
 10. In caso di installazione del kit di base VistaKey, collegare l'uscita del trasformatore ai morsetti 1 e 2 del sistema di alimentazione.
 11. Collegare il sistema di alimentazione interno al modulo (+12V), utilizzando la spina del trasformatore del kit di base VistaKey. Il lettore emette un bip e il LED rosso rimane acceso. *(Se il LED è giallo e lampeggia, invertire temporaneamente lo stato dell'interruttore del sistema DSM, aprendo la porta se chiusa o chiudendola se aperta fino a completamento del test del punto di accesso come sotto indicato).*

Mappatura zone VistaKey per il test

Mappare le zone del modulo VistaKey nelle zone della centralina del sistema di allarme per preparare il modulo VistaKey e la centralina al test. Per mappare le zone del modulo VistaKey nelle zone del sistema di allarme, seguire le procedure sotto indicate.

- | | |
|---|--------------------------------------|
| 1. Entrare in modalità #93 Programmazione modalità menu del sistema di allarme in base alle procedure descritte nel relativo manuale. Il display visualizza il prompt "Programmazione zona? - 1 = SI' 0 = NO": | PROG ZONE?
1 = SI 0 = NO |
| 2. Premere 1 per programmare la zona. Il display visualizza il prompt "Confermi? - 1 = SI' 0 = NO": | Ins. Per Confer?
1 = SI 0 = NO |
| 3. Premere 1 per confermare. Il display visualizza il prompt "Digitare codice zona? - 000 = per uscire": | DIGITA NR ZONA.?
000 = ESCI |
| 4. Digitare il codice zona a 3 cifre del punto di accesso (es. 100). | |
| 5. Premere [*] due volte. Il display visualizza il prompt "100 risposta zona": | 100 RISPOSTA ZN |
| 6. Digitare il tipo risposta a due cifre, per esempio 01 (Ingresso/Uscita). Premere [*] per confermare. | |
| 7. Tenere premuto [*] fino a quando il display visualizza il prompt "100 tipo ingresso ": | 100 TIPO SENSORE |
| 8. Digitare 11 (DSM) e premere [*] per confermare. Il display visualizza il prompt "100 punto di accesso - (01-15)": | 100 PORTA NR
(01-15) |
| 9. Digitare il codice a due cifre del punto di accesso oggetto del test. Premere [*] per confermare. | |
| 10. Tenere premuto [*] fino a quando il display visualizza il prompt "Digitare codice zona? - 000 = per uscire": | DIGITA NR ZONA.?
000 = ESCI |
| 11. Digitare 000 e premere [*] per confermare. Il display visualizza il prompt "Uscire modalità menu? - 1 = SI' 0 = NO": | USCIRE DAL MENU?
1 = SI' 0 = NO 0 |

12. Premere **1** per uscire dalla modalità menu e digitare **#99** per uscire dalla programmazione.

Test iniziale del sistema



Gli ingressi e le uscite autorizzate dal punto di accesso sono tipi di evento del registro eventi della centralina. Se i valori di default corrispondenti ai "tipo eventi del registro" (campo 1*70 nella centralina di allarme) sono stati modificati e i tipi di evento non sono registrati, non utilizzare le procedure sotto indicate. Per utilizzare questa procedura fare riferimento alla "Modalità di programmazione campi dati" del manuale di installazione e predisposizione del sistema di allarme ed abilitare temporaneamente i tipi di evento nel campo 1*70 per eseguire il test.

Per verificare il funzionamento del modulo VistaKey e delle apparecchiature installate, seguire le procedure sotto indicate:

1. Digitare **Codice installatore + # + 78** su una delle tastiera della centralina di allarme. Il display visualizza il prompt "Modalità test punto di accesso - 0 = per uscire":

MODO TEST ACS 0 = ESCI	<u>0</u>
---------------------------	----------
2. Premere **2**. Il display visualizza il prompt "Modalità test punto di accesso - tutte le schede autorizzate":

MODO TEST ACS ABILITA TUTTE SCH	<u>2</u>
------------------------------------	----------
3. Premere **[★]**. La tastiera emette una serie di bip intermittenti indicando che il sistema è in modalità test e il display visualizza il prompt "Tutte le schede autorizzate - modalità test punto di accesso":

ABILITA TUTTE SCH MODO TEST ACS

4. Inserire una scheda prox ADEMCO nel lettore. Se il sistema è stato installato correttamente, la serratura magnetica o meccanica viene attivata e il LED verde del lettore si accende temporaneamente. In caso di test positivo, avanzare al punto 5. Se la serratura magnetica o meccanica non si attiva e il LED verde non si illumina, procedere come sotto indicato:
 - a. Uscire dalla MODALITA' TEST PUNTO DI ACCESSO digitando **Codice installatore + # + 78 + 0 + ***. La tastiera si tacita e il display visualizza il prompt "Disinserito - pronto all'inserimento":

****DISATTIVATO**** SI PUO INSERIRE
--
 - b. Controllare che tutti i fili siano collegati correttamente e che il sistema sia alimentato dall'esterno.
 - c. Ritornare al punto 1 e ripetere il test.
5. In caso di installazione di più moduli VistaKey per più punti di accesso, ripetere la procedura del punto 4 per ogni punto di accesso.
6. Uscire dalla modalità test punto di accesso digitando **codice installatore + # + 78 + 0 + ***. La tastiera si tacita e il display visualizza il prompt "Disinserito - pronto all'inserimento":

****DISATTIVATO**** SI PUO INSERIRE
--
7. Verificare che i punti di accesso su cui si esegue il test siano registrati nel registro eventi della centralina di allarme seguendo la procedura sotto indicata.
 - a. Visualizzare il registro della centralina di allarme digitando **codice installatore + # + 60** su una tastiera del sistema di allarme. Il display visualizza il prompt "Digitare 0 = recente - 1 = tutti gli eventi":

0= PIU RECENT 1= TUTTI

 - b. Premere **1**. Il display visualizza il prompt "Visualizzazione a sezioni - 0 = NO 1-8 = n. sezione":

EVENTI SETTORI 0=NO 1-8=SETT #

- c. Premere **0**. Il display visualizza il prompt " Registro eventi - tipo CCC UUU":

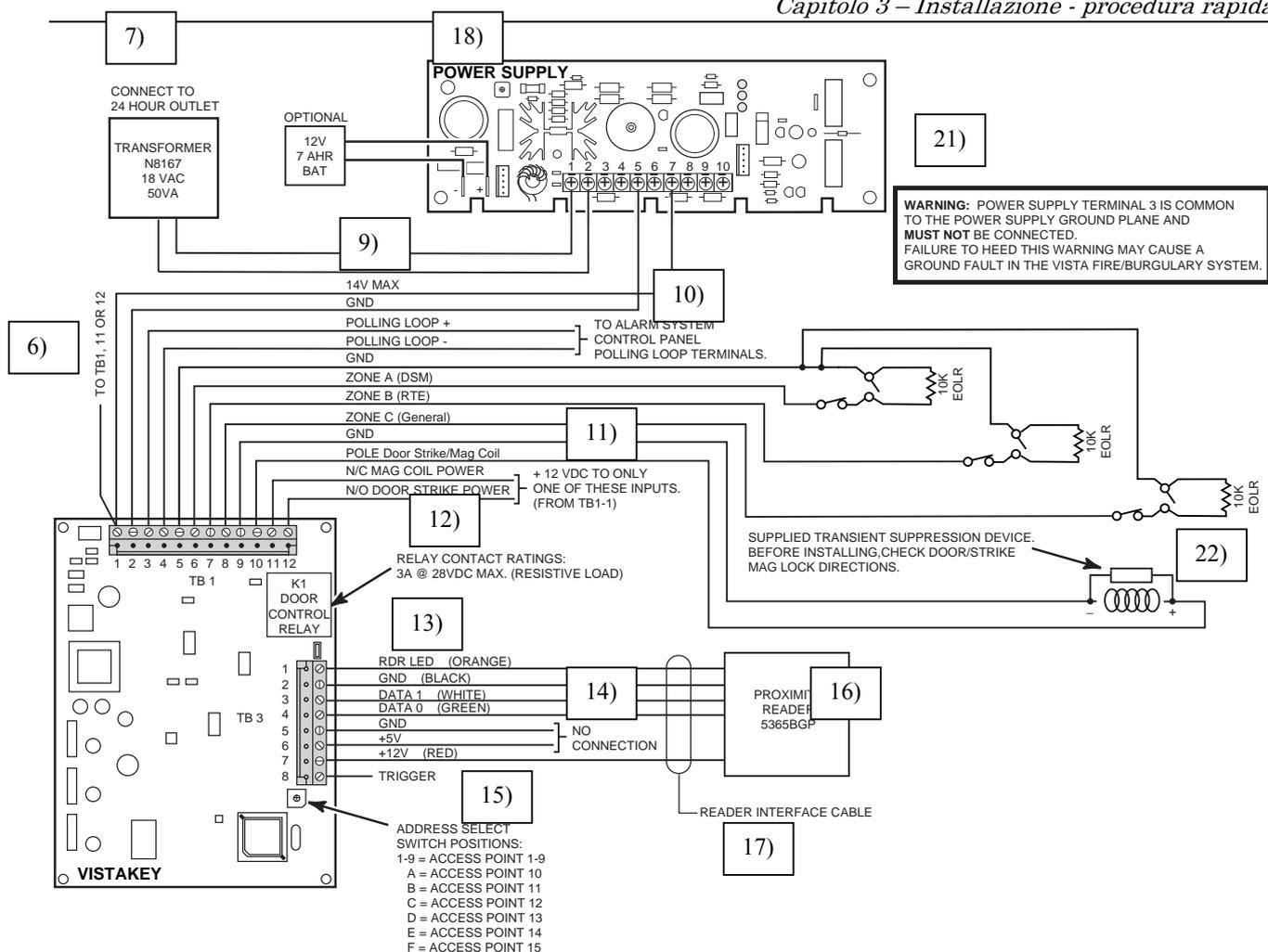
ALARM	ARCHIVIO
TIPO	CCC UUU

- d. Tenere premuto **3** fino a quando il display visualizza il prompt "Tutti gli eventi del registro - tipo CCC UUU":

TUTTI	ARCHIVIO
TIPO	CCC UUU

- e. Premere **8**. Il display visualizza l'evento più recente registrato.
- f. Premere **1** per visualizzare gli eventi precedenti e verificare che tutti i punti di accesso controllati siano nel registro. La prima riga del registro riporta il numero di partizione, la data e l'ora. La seconda riga visualizza "ACS GRT" (accesso autorizzato) oppure "EGR GRT" (uscita autorizzata) seguito dal codice zona a tre cifre e dal codice utente U999, che indica una scheda non abbinata ad un utente. In caso di scheda abbinata ad un utente, il display visualizza il codice utente.
- Se la visualizzazione del punto di accesso è errata (es. i punti di accesso controllati (indirizzi VistaKey) sono 1 e 2, ma il registro visualizza la zona del punto di accesso 1 due volte), controllare il punto di accesso mancante sul commutatore di indirizzo del modulo VistaKey. Se il test su un punto di accesso manca completamente, ricontrollare i collegamenti del sistema.
- g. Premere **[*]** per uscire dalla modalità visualizzazione registro.

L'installazione con procedura rapida è completata e il punto(i) di accesso può essere programmato nella centralina del sistema di allarme seguendo le procedure del *Capitolo 5: Programmazione*.



N.B.:

- Nelle installazioni UL la corrente interna e della serratura magnetica/meccanica deve essere fornita dal kit di base VistaKey.
- In caso di lettore di marca diversa da ADEMCO, controllare la codifica dei colori del lettore che si utilizza.
- L'utilizzo di una batterie optional per il sistema di alimentazione non è approvato per le installazioni UL.

Figura 3-1: Schema elettrico modulo VistaKey

6)
AI MORSETTI 11 O 12 DELLA MORSETTIERA TB1

7)
COLLEGARE ALL'USCITA 24 ORE
TRASFORMATORE N8167 18VAC 50VA

9)
14V MAX
TERRA
CIRCUITO POLLING
CIRCUITO POLLING
TERRA
ZONA A (DSM)
ZONA B (RTE)
ZONA C (GP)
TERRA
POLO bobina serratura meccanica/magnetica
ALIMENTAZIONE BOBINA MAGNETICA N/C

ALIMENTAZIONE SERRATURA MECCANICA N/O

10)
AI MORSETTI DEL CIRCUITO POLLING DELLA CENTRALINA DEL SISTEMA DI ALLARME.

11)
+12V CC SOLO AD UNO DI QUESTI INGRESSI (DAL MORSETTO 1 DELLA MORSETTIERA TB1).

12)
PRESTAZIONI CONTATTO A RELE'
3A @ 28V CC MAX. (CARICO RESISTIVO)

K1 RELE' CONTROLLO PORTA

13)
LED LETTORE (ARANCIONE)
TERRA (NERO)
DATI 1 (BIANCO)
DATI 2 (VERDE)
TERRA
+ 5V
+12V (ROSSO)
USCITA LOGICA

14)
NESSUN COLLEGAMENTO

15)
POSIZIONE COMMUTATORE DI INDIRIZZO
1-9 = PUNTO DI ACCESSO 1-9
A = PUNTO DI ACCESSO 10
B = PUNTO DI ACCESSO 11
C = PUNTO DI ACCESSO 12
D = PUNTO DI ACCESSO 13
E = PUNTO DI ACCESSO 14
F = PUNTO DI ACCESSO 15

16)
LETTORE PROX
5365BGP

17)
CAVO INTERFACCIA LETTORE

18)
SISTEMA DI ALIMENTAZIONE

OPTIONAL
12V 7 AHR BATTERIA

21)
ATTENZIONE: IL MORSETTO 3 DEL SISTEMA DI ALIMENTAZIONE E' COMUNE AL PIANO DI MASSA DEL SISTEMA DI ALIMENTAZIONE E **NON DEVE** ESSERE COLLEGATO.
EVENTUALI INOSSERVANZE POTREBBERO COMPROMETTERE LA MESSA A TERRA DEL SISTEMA ANTINCENDIO/ANTIFURTO VISTA.

Installazione - procedura dettagliata

Contenuto

- ◆ Informazioni generali
- ◆ Installazione del sistema
- ◆ Mappatura zone VistaKey per il test
- ◆ Test iniziale del sistema

Informazioni generali

Questo capitolo fornisce una guida dettagliata per il montaggio e il collegamento del kit di base VistaKey o del modulo VistaKey e dei dispositivi connessi. Le procedure descritte riguardano un solo punto di accesso e devono essere ripetute per ogni punto di accesso installato. La *figura 4-1* mostra un'installazione tipo. Le fasi di installazione descritte in questo capitolo sono: installazione del sistema, mappatura delle zone VistaKey per il test e test iniziale del sistema.



Se sono già state eseguite le procedure del *Capitolo 3 – Installazione - procedura rapida*, saltare questo capitolo e procedere al *Capitolo 5 – Programmazione*.



Installazione del sistema

Per montare e collegare le apparecchiature necessarie per la creazione di un punto di accesso, seguire le procedure sotto indicate.

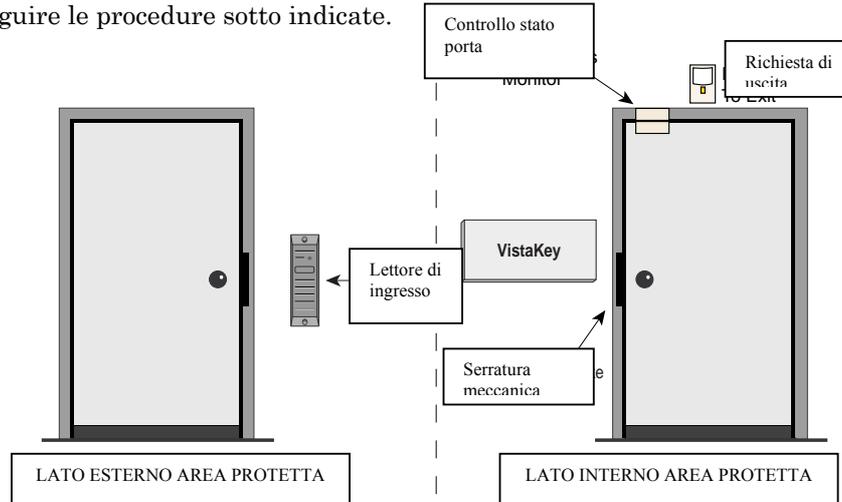


Figura 4-1: Installazione tipo modulo VistaKey

Assemblaggio e montaggio kit di base VistaKey

Per assemblare e montare il kit di base VistaKey, seguire le procedure sotto indicate:

1. Definire la posizione del kit di base VistaKey. Il kit di base deve essere montato all'interno dell'area protetta vicino al meccanismo della serratura meccanica.
2. Rimuovere il coperchio anteriore della centralina del kit di base VistaKey.
3. Montare la base d'appoggio universale (P/N K4555) dell'armadietto del kit di base VistaKey facendo scorrere le alette sul retro della base sulla terza fila di punti di appoggio dell'armadietto. Vedere *figura 4-2*.



Le linguette permettono di fissare la base d'appoggio universale all'interno dell'armadietto. Per fissare maggiormente la base all'armadietto, utilizzare le 2 viti di fermo (incluse) al centro della base.

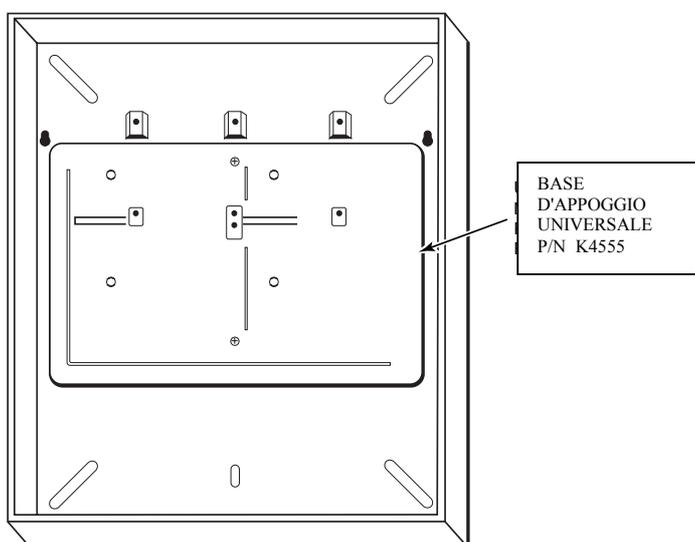


Figura 4-2: Installazione della base d'appoggio

4. Appoggiare l'armadietto sulla parete e contrassegnare i quattro fori di montaggio.
5. Montare l'armadietto sulla parete utilizzando 4 dispositivi di fissaggio (non inclusi).
6. Montare il sistema di alimentazione (P/N SA12040) nell'armadietto del kit di base VistaKey facendolo scorrere nelle fessure sulla parte superiore dell'armadietto. Fissare il sistema di alimentazione utilizzando tre viti, 3 distanziatori neri, e **1 rondella in nylon** (sulla vite in basso a destra). Vedere *figura 4-3*.



La rondella in nylon permette di ridurre i rischi di danni causati da un'errata messa a terra del sistema di allarme antincendio/antifurto. Eventuali danni causati dall'inosservanza di questa precauzione di sicurezza rientrano nella giurisdizione dell'autorità locale competente.

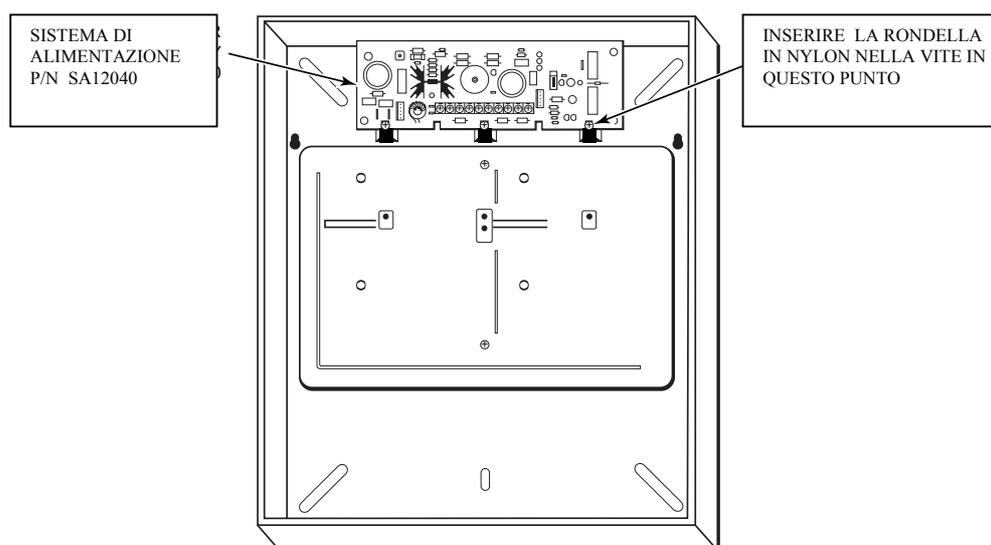


Figura 4-3: Installazione del sistema di alimentazione

7. Rimuovere il frontalino del modulo VistaKey.
8. Il modulo VistaKey è dotato di due morsettiere TB1 e TB3 con morsetti a spina. Tenere le viti della morsettiera verso l'esterno della scheda del modulo VistaKey e far scorrere le morsettiere sui piedini della scheda.
9. Montare il modulo VistaKey nell'armadietto allineando le fessure sul retro del modulo con i piedini della base d'appoggio e quindi far scorrere il modulo VistaKey verso destra. Vedere *la figura 4-4*.

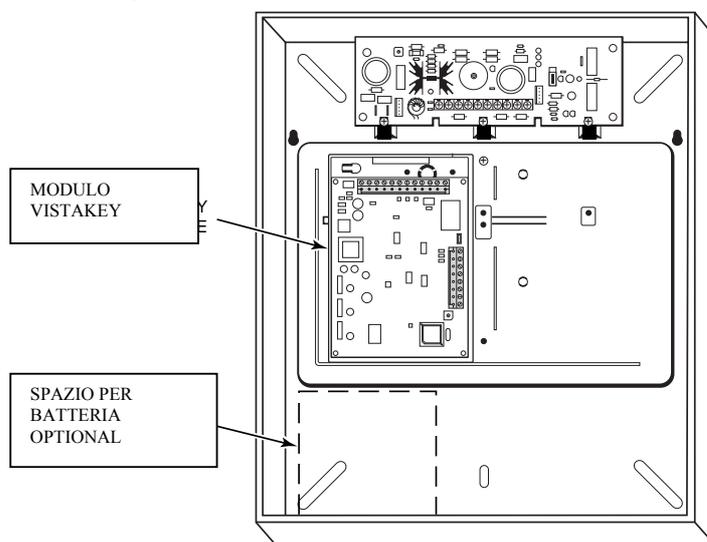


Figura 4-4: Installazione del modulo VistaKey



- Non reinstallare il frontalino del modulo VistaKey in questa fase. Il frontalino deve essere installato in base alle istruzioni indicate di seguito nel manuale.
- Lo spazio a destra nella base d'appoggio può essere utilizzato per un secondo modulo VistaKey.

Montaggio e collegamento del lettore scheda

Il lettore scheda viene montato all'esterno dell'area protetta in un luogo facilmente raggiungibile per far passare la scheda. Per montare e collegare il lettore al modulo VistaKey, seguire le procedure sotto indicate:

Montaggio del lettore

1. In caso di installazione del lettore ADEMCO OP30-FWM, passare al punto 2. In caso di lettore diverso, fare riferimento alla tabella sul retro del lettore per la codifica dei colori dei fili del lettore e delle loro funzioni. Annotare le informazioni nella tabella che segue per facilitarne l'utilizzo al momento del collegamento del lettore al modulo VistaKey.
2. Eseguire due fori sulla parete di montaggio utilizzando il lettore come modello.
3. Fissare il lettore alla parete utilizzando la ferramenta fornita con il lettore.

Collegamento del lettore

Dopo aver montato il lettore, collegarlo al sistema. Fissare i conduttori del lettore ai morsetti corretti della morsettiera TB3 del modulo VistaKey come indicato nella tabella che segue e nello schema connessioni al termine del manuale.

Conduttore lettore	Colore conduttore	n. morsetto morsettiera TB3 del modulo VistaKey
LED verde	Arancione	1
Terra*	Nero	2
DATI 1 (ora)	Bianco	3
DATI 0 (informazioni)	Verde	4
+5VDC†	Rosso †	6
+12VDC†	Rosso †	7

* Il morsetto n. 5 della morsettiera TB3 è anche un morsetto di messa a terra e può essere utilizzato in alternativa al morsetto 2. I morsetti 2 e 5 sono morsetti di terra comuni.
† Collegare a +5VDC OPPURE +12VDC come da istruzioni del manuale del lettore.



I fili del lettore rimasti inutilizzati devono essere isolati l'uno dall'altro e da altri fili o materiali conduttivi.

Collegamento uscita logica del modulo VistaKey

Il modulo VistaKey è dotato di un'uscita logica (morsetto 8 della morsettiera TB3) in grado di ricevere una corrente massima di 15mA con tensione all'origine 12VCC. Si tratta di un'uscita con interruttore digitale a stato solido utilizzata per azionare piccoli carichi quali LED o sirene piezo. Quest'uscita può essere configurata come uscita abbinata ad un punto di accesso o come uscita generica non abbinata per attivare/disattivare dispositivi esterni.

Se si utilizza l'uscita logica del modulo VistaKey, collegare quest'uscita al dispositivo di interfaccia. (Fare riferimento allo schema connessioni alla fine del manuale e alle istruzioni fornite con il dispositivo da collegare all'uscita logica.)

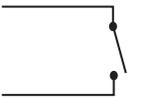
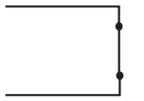
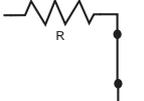
Collegamento zone del modulo VistaKey

Il modulo VistaKey è dotato di 3 ingressi zona. Ogni zona può essere configurata come ingresso controllato (a tre stati) oppure come ingresso non controllato (a due stati). La zona A viene normalmente utilizzata per il dispositivo DSM (controllo stato porta). La zona B può essere configurata come ingresso RTE (richiesta di uscita). La zona C viene utilizzata come ingresso zona generica e può essere utilizzata come ingresso manomissione.

Le zone possono essere configurate in quattro modi:

1. Normalmente aperto
2. Normalmente chiuso
3. Resistore di fine linea (EOLR) normalmente aperto
4. Resistore di fine linea (EOLR) normalmente chiuso

La tabella sotto indicata mostra le diverse opzioni di configurazione degli ingressi zona VistaKey:

	ZONA A DUE STATI (non controllata)		ZONA A TRE STATI (controllata dal resistore EOL*) -Consigliata-	
	Normalmente aperto (N/O)	Normalmente chiuso (N/C)	Normalmente aperto (N/O)	Normalmente chiuso (N/C)
Resistenza zona = 0 (cortocircuito)	Errore	Normale	Errore	Anomalia
Resistenza zona = valore nominale	Non valido	Non valido	Normale	Normale
Resistenza zona = infinito (aperto)	Normale	Errore	Anomalia	Errore
Collegamento sensori (Sensori in stato di pronto)				

* Il valore del resistore EOL è 10KΩ

Controllo stato porta

Il controllo stato porta (DSM) è un dispositivo in grado di segnalare una condizione di aperto di una porta (punto di accesso). Si tratta di un semplice dispositivo quale un contatto magnetico che rimane aperto quando la porta è aperta. Per utilizzare la zona A come controllo stato porta, montare il dispositivo di controllo stato porta in base alle istruzioni allegate al dispositivo DSM. Collegare il DSM al morsetto 6 della morsettiera TB1 nel modulo VistaKey come indicato nello schema connessioni al termine del manuale.

Richiesta di uscita

Il dispositivo di richiesta di uscita (RTE) permette di sbloccare la porta (punto di accesso) e permettere l'uscita dall'area protetta. Solitamente si tratta di un dispositivo ad infrarossi o di un interruttore a contatto istantaneo. Per utilizzare la zona B come richiesta di uscita, montare il dispositivo di richiesta di uscita in base alle istruzioni fornite con il dispositivo. Collegare RTE al morsetto 7 della morsettiera TB1 nel modulo come indicato nello schema connessioni al termine del manuale.

Montaggio e collegamento serratura meccanica/magnetica

La serratura meccanica/magnetica mantiene bloccato un punto di accesso e quindi impedisce ingressi non autorizzati. La serratura meccanica e la serratura magnetica sono alimentate dal sistema di alimentazione mediante il relè del modulo VistaKey.



La serratura meccanica/magnetica **non** deve ricevere corrente dall'uscita alimentazione ausiliaria della centralina del sistema di allarme, ma dal sistema di alimentazione del kit di base VistaKey. Eventuali inosservanze potrebbe danneggiare il sistema di alimentazione della centralina.

Montaggio serratura meccanica/magnetica

Le procedure per il montaggio del dispositivo di chiusura della porta dipendono dal tipo di serratura che si intende installare. Fare riferimento alle istruzioni allegate alla serratura meccanica/magnetica.

Collegamento serratura meccanica/magnetica

Per collegare la serratura meccanica/magnetica, seguire le procedure sotto indicate e fare riferimento allo schema connessioni al termine del manuale.



- Per garantire una protezione transitoria delle serratura magnetica/meccanica e dei contatti a relè, utilizzare un soppressore elettrico quale EL-EDS (prodotto da EDCO e fornito con il kit di base VistaKey). Installare il soppressore sopra i conduttori collegati alla serratura il più vicino possibile al meccanismo.
 - Le serrature meccaniche e magnetiche generano disturbi elettrici. Tenere i fili di collegamento della serratura meccanica/magnetica lontano da altri fili collegati al modulo VistaKey.
-

1. Collegare la bobina della serratura meccanica/magnetica tra il morsetto 9 della morsettiera TB1 (TERRA) e il morsetto 10 della morsettiera TB1 (polo del relè) (serratura meccanica/magnetica).
2. In caso di bobina per serratura magnetica, collegare il sistema di alimentazione al morsetto 11 normalmente chiuso (N/C) della morsettiera TB1, **OPPURE**, in caso di bobina per serratura meccanica, al morsetto 12 normalmente aperto (N/O) della morsettiera TB1 come segue:
In caso di installazione del kit di base VistaKey con sistema di serratura meccanica o magnetica a +12VCC, collegare un ponticello tra il morsetto 1 della morsettiera TB1 e il morsetto 11 o 12.

Selezione indirizzo modulo VistaKey

Abbinare uno dei 15 codici punti di accesso, o codici porta, da 1 a 9, A, B, C, D, E o F, al modulo VistaKey, prima di registrare il modulo nel sistema di allarme.



Uno qualsiasi dei 15 codici punto di accesso può essere abbinato al modulo VistaKey, ma il numero totale di punti di accesso non deve superare il numero di accessi consentito come indicato nel capitolo 1 di questo manuale.

Per selezionare l'indirizzo del modulo VistaKey, regolare il commutatore di indirizzo sulla posizione desiderata utilizzando un giravite a lama dritta piccolo. Per la posizione del commutatore, fare riferimento allo schema connessioni al termine del manuale. In caso di installazione di più moduli VistaKey, l'indirizzo deve essere diverso per ogni modulo.

Collegamento circuito polling e sistema di alimentazione modulo VistaKey

Gli ultimi collegamenti del modulo VistaKey riguardano il circuito polling della centralina e il sistema di alimentazione. Per eseguire questi collegamenti, seguire le procedure sotto indicate e fare riferimento allo schema connessioni al termine del manuale.

1. Collegare il modulo VistaKey alla centralina di allarme mediante il circuito polling + (morsetto 3 della morsettiera TB1) e il circuito polling - (morsetto 4 della morsettiera

2. TB1). Per determinare i punti di connessione e la polarità del collegamento del circuito polling della centralina, fare riferimento al capitolo sul circuito polling nel manuale di installazione e predisposizione della centralina di allarme.
3. Collegare il sistema di alimentazione come sotto indicato:
 In caso di installazione del kit di base VistaKey, collegare il morsetto 1 della morsettiera TB1 nel modulo VistaKey al morsetto 7 del sistema di alimentazione e il morsetto 2 della morsettiera TB1 del modulo VistaKey (TERRA) al morsetto 5 del sistema di alimentazione. Quindi, collegare il trasformatore ai morsetti 1 e 2 del sistema di alimentazione e collegare il connettore primario del trasformatore alla linea di alimentazione principale.
 A conferma del collegamento del sistema di alimentazione, il lettore emette un bip e il LED rosso rimane acceso. *(Se il LED è giallo e lampeggia, invertire temporaneamente lo stato dell'interruttore del sistema DSM, aprendo una porta chiusa o chiudendo una porta aperta fino a completamento del test come descritto sotto)*
3. Reinstallare il frontalino del modulo VistaKey e, in caso di kit di base VistaKey, chiudere lo sportello dell'armadietto.

Mappatura zone VistaKey per il test

Prima di eseguire il test sul modulo VistaKey e sul sistema di allarme, mappare le zone del modulo nelle zone della centralina del sistema di allarme seguendo le procedure sotto indicate:

1. Entrare nella modalità **#93 Programmazione modalità menu** del sistema di allarme in base alle istruzioni del manuale del sistema di allarme. Il display visualizza il prompt "Programmazione zona? - 1 = SI' 0 = NO":

PROG ZONA? 1 = SI' 0 = NO

2. Premere **1** per programmare la zona. Il display visualizza il prompt "Confermi? - 1 = SI' 0 = NO":

INS PER CONFER? 1 = SI' 0 = NO

3. Premere **1** per confermare. Il display visualizza il prompt "Digitare codice zona? - 000 = per uscire":

DIGITA NR ZONA.? 000 = ESCI

4. Digitare il codice zona a tre cifre del punto di accesso (es. 100).

5. Premere **[*]** due volte. Il display visualizza il prompt "100 risposta zona ":

100 RISPOSTA ZN

6. Digitare il tipo risposta a due cifre, per esempio 01 (Ingresso/Uscita). Premere **[*]** per confermare.

7. Tenere premuto **[*]** fino a quando il display visualizza il prompt "100 tipo ingresso ":

100 TIPO SENSORE

8. Digitare **11** (DSM) e premere **[*]** per confermare. Il display visualizza il prompt "100 punto di accesso" - (01-15):

100 PORTA NR (01-15)

9. Digitare il codice punto di accesso a due cifre corrispondente al punto di accesso da controllare. Premere [*] per confermare.
10. Tenere premuto [*] fino a quando il display visualizza il prompt "Digitare codice zona? - 000 = per uscire":

DIGITA NR ZONA?
000 = ESCI

11. Digitare 000 e premere [*] per confermare. Il display visualizza il prompt "Uscire modalità menu? - 1 = SI' 0 = NO":

USCIRE DAL MENU?
1 = SI 0 = NO 0

12. Premere 1 per uscire dalla modalità menu e digitare #99 per uscire dalla programmazione.

Test iniziale del sistema



Gli ingressi e le uscite autorizzate dal punto di accesso sono tipi di evento del registro eventi della centralina. Se i valori di default corrispondenti ai "tipo eventi del registro" (campo 1*70 nella centralina di allarme) sono stati modificati e i tipi di evento non sono registrati, non utilizzare le procedure sotto indicate. Per utilizzare questa procedura fare riferimento alla "Modalità di programmazione campi dati" del manuale di installazione e predisposizione del sistema di allarme ed abilitare temporaneamente i tipi di evento nel campo 1*70 per eseguire il test.

Verificare il funzionamento del modulo VistaKey e delle apparecchiature installate seguendo le procedure sotto indicate.

1. Digitare **Codice installatore + # + 78** su una tastiera del sistema di allarme. Il display visualizza il prompt "Modalità test punto di accesso - 0 = per uscire":

MODO TEST ACS
0 = ESCI 0

2. Premere 2. Il display visualizza il prompt "Modalità test punto di accesso - tutte le schede autorizzate":

MODO TEST ACS
ABILITA TUTTE SCH 2

3. Premere [*]. La tastiera emette una serie di bip intermittenti indicando che il sistema è in modalità test e il display visualizza il prompt "Tutte le schede autorizzate - modalità test punto di accesso":

ABILITA TUTTE SCH
MODO TEST ACS

4. Inserire una scheda prox ADEMCO nel lettore. Se il sistema è stato installato correttamente, la serratura magnetica/meccanica viene attivata e il LED verde del lettore si accende temporaneamente. In caso di test positivo, avanzare al punto 5. Se la serratura magnetica/meccanica non si attiva e il LED verde non si illumina, procedere come sotto indicato:

- a. Uscire dalla MODALITA' TEST PUNTO DI ACCESSO digitando **codice installatore + # + 78 + 0 + ***. La tastiera si tace e il display visualizza il prompt "Disinserito - pronto all'inserimento":

****DISATTIVATO****
SI PUO INSERIRE

- b. Verificare che tutti i cavi siano correttamente collegati e che il sistema sia alimentato dall'esterno.

- c. Ritornare al punto 1 e ripetere il test.
5. In caso di installazione di più moduli VistaKey per più punti di accesso, ripetere la procedura del punto 4 per ogni punto di accesso.
6. Uscire dalla modalità test punto di accesso digitando **codice installatore + # + 78 + 0 + ***. La tastiera si tace e il display visualizza il prompt "Disinserito - pronto all'inserimento":

<p>****DISATTIVATO**** SI PUO INSERIRE</p>
--

7. Verificare che tutti i punti di accesso controllati siano registrati nel registro allarmi della centralina di allarme.
- a. Digitare **codice installatore + # + 60** su una tastiera del sistema di allarme per visualizzare il registro eventi. Il display visualizza il prompt "Digitare 0 = recente - 1 = tutti gli eventi":

<p>0= RECENTI 1= TUTTI</p>

- b. Premere **1**. Il display visualizza il prompt "Visualizzazione a sezioni - 0 = no; 1-8 = n. sezione":

<p>EVENTI SETTORI 0=NO 1-8=SETT #</p>

- c. Premere **0**. Il display visualizza il prompt "Registro eventi - tipo CCC UUU":

<p>ALARM ARCHIVIO TIPO CCC UUU</p>
--

- d. Tenere premuto **3** fino a quando il display visualizza il prompt "Tutti gli eventi del registro - tipo CCC UUU":

<p>TUTTI ARCHIVIO TIPO CCC UUU</p>
--

- e. Premere **8**. Il display visualizza l'evento più recente registrato.
- f. Premere **1** per visualizzare gli eventi precedenti registrati e verificare che tutti i punti di accesso controllati siano registrati. La prima riga del registro riporta il codice partizione, la data e l'ora. La seconda riga del display in modalità test punti di accesso indica "ACS GRT" (accesso autorizzato) oppure "EGR GRT" (uscita autorizzata) seguito dal codice zona a tre cifre e dal codice utente U999, che corrisponde ad una scheda non abbinata ad un utente. In caso di scheda abbinata ad un utente, il display visualizza il codice utente.

Se la visualizzazione del punto di accesso è errata (es. i punti di accesso controllati (indirizzi VistaKey) sono 1 e 2, ma il registro visualizza la zona del punto di accesso 1 due volte), controllare il punto di accesso mancante sul commutatore di indirizzo del modulo VistaKey. Se il test di un punto di accesso manca completamente, ricontrollare i collegamenti del sistema.

- g. Premere [**✳**] per uscire dalla modalità visualizzazione registro.

L'installazione con procedura dettagliata è completata e il punto(i) di accesso può essere programmato nella centralina del sistema di allarme seguendo le procedure indicate nel *Capitolo 5 – Programmazione*.

Programmazione

Contenuto

- ◆ *Informazioni generali*
- ◆ *Foglio di programmazione eventi temporizzati*
- ◆ *Foglio di programmazione funzione evento/azione*
- ◆ *Mappatura zone VistaKey nelle zone sistema di allarme*
- ◆ *Impostazione opzioni di programmazione punto di accesso modulo VistaKey*
- ◆ *Impostazione gruppi di accesso*
- ◆ *Programmazione funzione evento/azione*
- ◆ *Uscire dalla modalità #93 programmazione modalità menu*
- ◆ *Programmazione eventi temporizzati*
- ◆ *Abilitazione gruppi di accesso*
- ◆ *Altre funzioni del sistema*

Informazioni generali

La centralina del sistema di allarme deve essere programmata per interagire con le zone del modulo VistaKey e quindi rendere funzionante l'intero sistema. Questo capitolo fornisce le istruzioni necessarie per impostare la modalità di funzionamento del modulo VistaKey con la centralina del sistema di allarme.

Le procedure di programmazione del modulo VistaKey come parte integrante del sistema di allarme VISTA possono essere suddivise nelle categorie sotto indicate.



- **Foglio di programmazione eventi temporizzati**– Questa sezione fornisce le istruzioni e i codici necessari per compilare il foglio di programmazione eventi temporizzati. Gli eventi temporizzati generano un'azione sulla base di una programmazione oraria e permettono, per esempio, di autorizzare l'ingresso da gruppi di accesso solamente in orario di lavoro. Gli eventi temporizzati sono optional e non sono indispensabili per il funzionamento del sistema in quanto utilizzati solamente per generare una determinata azione in una determinata fascia oraria (programmazione oraria).
- **Foglio di programmazione funzione evento/azione**– Questa sezione fornisce le istruzioni e i codici necessari per la compilazione del foglio di programmazione della funzione evento/azione che permette di generare un'azione al verificarsi di un determinato evento in una determinata fascia oraria. Per esempio, l'accensione di una luce (mediante un relè) in caso di ingresso di un utente (ingresso autorizzato). La funzione evento/azione è optional e non è indispensabile per il funzionamento del sistema in quanto utilizzata solamente per generare una determinata azione al verificarsi di un determinato evento.
- **Mappatura zone VistaKey nelle zone del sistema di allarme**– Le procedure di programmazione delle zone del sistema di allarme permettono di determinare le zone della centralina VISTA selezionate per la ricezione delle informazioni dalle zone del modulo VistaKey. Una zona della centralina VISTA può essere mappata in una zona del modulo VistaKey.
- **Impostazione opzioni di programmazione punti di accesso** – Le procedure di programmazione punti di accesso permettono di determinare i parametri delle zone VistaKey, tra cui il gruppo(i) che ha diritto di accedere da un punto di accesso (porta).
- **Impostazione gruppi di accesso** – Questa sezione permette di determinare le capacità (privilegi) di ogni gruppo di utenti.

- **Programmazione funzione evento/azione** – Questa sezione permette di programmare nel sistema di allarme le informazioni raccolte nel foglio di programmazione funzione evento/azione. La funzione evento/azione genera un'azione al verificarsi di un determinato evento ma non è indispensabile per il funzionamento del sistema in quanto utilizzata solamente per generare una determinata azione al verificarsi di un determinato evento.
- **Programmazione eventi temporizzati**– Questa sezione permette di programmare nel sistema di allarme le informazioni raccolte nel foglio di programmazione eventi temporizzati. Gli eventi temporizzati generano un'azione sulla base di una programmazione oraria, ma sono optional e non sono indispensabili per il funzionamento del sistema in quanto utilizzati solamente per generare una determinata azione in una determinata fascia oraria.
- **Abilitazione gruppi di accesso** – Prima di essere attivati i nuovi gruppi di accesso devono essere abilitati dalla prima fascia oraria valida che viene attivata oppure mediante il comando #77 (abilitazione immediata).



- Il termine *gruppi di accesso* in questo manuale si riferisce ai *gruppi di punti di accesso* e non deve essere confuso con i gruppi di accesso ai quali vengono abbinati i codici utente come descritto nel manuale del sistema di allarme.
- Per ulteriori informazioni sulle procedure di programmazione, fare riferimento al manuale del sistema di allarme.

Foglio di programmazione eventi temporizzati

Il foglio di programmazione degli eventi temporizzati permette di impostare una serie di parametri che attivano terminali di uscita, escludono zone, ecc. sulla base di una programmazione oraria. Massimo 20 eventi possono essere programmati nel sistema ed ogni evento è controllato dalle fasce orarie indicate sopra.

Le azioni che vengono attivate automaticamente ad un determinato orario sono: comandi di relè, comandi inserimento/disinserimento, comandi esclusione zone, condizioni di accesso aperto/chiuso e comandi di controllo accesso.



- I codici azione 60 (PA solo uscita), 66 (PA gruppo solo uscita) o 72 (PA partizione solo uscita) disabilitano il lettore d'ingresso del punto di accesso. Il lettore rimane disabilitato fino a ricevimento di un comando (comando tastiera o evento) che mette in sicurezza il punto di accesso.
- Gli eventi temporizzati descritti in questa parte corrispondono a quelli descritti nel manuale di installazione e predisposizione del sistema di allarme, ad eccezione di alcune azioni che sono state aggiunte. Se esistono già degli eventi temporizzati, verificare che il numero del primo nuovo evento temporizzato sia successivo all'ultimo evento abbinato; in caso contrario, il nuovo evento verrà sovrascritto sui precedenti.
- Allo scadere della fascia oraria che controlla un punto di accesso, il punto di accesso ritorna in modalità protetto.

Compilare il foglio di programmazione eventi temporizzati (alla fine del capitolo) seguendo le procedure sotto indicate:

Per semplificare la comprensione delle procedure di compilazione del foglio di programmazione eventi temporizzati, si suppone di abilitare i gruppi di accesso 1 e 2 dalle 0.00 alle 17.00 (fascia oraria 01) da lunedì a venerdì. Le varie procedure sono supportate da esempi di compilazione del foglio di programmazione.

1. **Digitare il codice azione indicato nella *tabella 5-1: codici azione* corrispondente all'azione desiderata.**

Esempio: Digitare codice azione 77 corrispondente all'abilitazione gruppo di accesso.

N. evento temporiz.	Codice azione	Nome azione	Identificatore azione	Fascia oraria	Tempo di attivazione	Giorni							
						L	M	M	G	V	S	D	V
1	77												
2													

2. Digitare il nome azione indicato nella *tabella 5-1: codici azione* corrispondente al codice azione.

Esempio: Digitare ACS Grp Enbl corrispondente all'abilitazione gruppo di accesso.

N. evento temporiz.	Codice azione	Nome azione	Identificatore azione	Fascia oraria	Tempo di attivazione	Giorni							
						L	M	M	G	V	S	D	V
1	77	ACS Grp Enbl											
2													

3. Digitare l'identificatore dell'azione corrispondente alla descrizione nella *tabella 5-1: codici azione*.

Esempio: Digitare 1 e 2 corrispondente ai gruppi di accesso 1 e 2.

N. evento temporiz.	Codice azione	Nome azione	Identificatore azione	Fascia oraria	Tempo di attivazione	Giorni							
						L	M	M	G	V	S	D	V
1	77	ACS Grp Enbl	1 2										
2													

4. Digitare il codice fascia oraria corrispondente alla fascia oraria (precedentemente programmata) che genera l'azione.

Esempio: se l'orario di inizio della fascia oraria 01 è 08.00 e l'orario di fine 17.00, digitare 01 per la fascia oraria 1.

N. evento temporiz.	Codice azione	Nome azione	Identificatore azione	Fascia oraria	Tempo di attivazione	Giorni							
						L	M	M	G	V	S	D	V
1	77	ACS Grp Enbl	1 2	01									
2													

5. Digitare il tempo di attivazione desiderato per l'azione. I tempi di attivazione validi sono:

1 =All'inizio della fascia oraria

2 =Alla fine della fascia oraria

3 =Solo durante il periodo attivo della fascia oraria (attivo all'inizio della fascia, disattivo alla fine).

4 =All'inizio e alla fine della fascia oraria.

Esempio: Digitare 3 per abilitare il gruppo di accesso per l'intera durata della fascia oraria.

N. evento temporiz.	Codice azione	Nome azione	Identificatore azione	Fascia oraria	Tempo di attivazione	Giorni							
						L	M	M	G	V	S	D	V
1	77	ACS Grp Enbl	1 2	01	3								
2													

6. Selezionare con una X i giorni della settimana in cui l'azione deve essere generata nella fascia oraria specificata. Se si seleziona Vacanza, la selezione dei giorni della settimana non viene considerata (es. l'azione viene generata selezionando Vacanza anche quando la vacanza cade di sabato e sabato non è

selezionato). Per ulteriori informazioni, fare riferimento ai parametri vacanza nel manuale del sistema di allarme.

*Esempio: Digitare **X** sotto L, M, M, G, e V per selezionare da lunedì a venerdì.*

N. evento temporiz.	Codice azione	Nome azione	Identificatore azione	Fascia oraria	Tempo di attivazione	Giorni							
						L	M	M	G	V	S	D	V
1	77	ACS Grp Enbl	1 2	01	3	X	X	X	X	X			
2													

In base all'esempio sopra indicato, i gruppi di accesso 1 e 2 vengono autorizzati all'ingresso nella fascia oraria 08.00 - 17.00 da lunedì a venerdì.

Tabella 5-1: codici azione

CODICE AZIONE	NOME AZIONE	IDENTIFICATORE AZIONE	DESCRIZIONE
Comandi di relè			
I tempi di attivazione validi dei comandi di relè sono 1 (inizio), 2 (fine), 3 (durante).			
L'opzione "durante" permette di controllare il relè solo per un determinato tempo. Per esempio, selezionando "durante" con relè attivo (relay on), il sistema attiva automaticamente il relè all'inizio della fascia oraria e lo disattiva automaticamente alla fine della fascia oraria.			
01	Relay On	n. relè	Relè attivo– Attiva il relè indicato come identificatore
02	Relay Off	n. relè	Relè disattivo– Disattiva il relè indicato come identificatore
03	Relay On 2 sec	n. relè	Relè chiuso per 2 secondi– Chiude per 2 secondi il relè indicato come identificatore
04	Relay xx min	n. relè	Relè chiuso per X minuti – Chiude per X minuti (come da programmazione del campo 1*74) il relè indicato come identificatore
05	Ralay yy sec	n. relè	Relè chiuso per Y secondi – Chiude per Y secondi (come da programmazione del campo 1*75) il relè indicato come identificatore
06	Rly Grp On	n. gruppo relè	Gruppo relè attivo – Attiva il gruppo di relè indicato come identificatore
07	Rly Grp Off	n. gruppo relè	Gruppo relè disattivo – Disattiva il gruppo relè indicato come identificatore
08	Rly Grp 2 sec	n. gruppo relè	Gruppo relè chiuso per 2 secondi– Chiude per 2 secondi tutti i relè del gruppo indicato come identificatore
09	Rly Grp xx min	n. gruppo relè	Gruppo relè chiuso per X minuti– Chiude per X minuti (come da programmazione del campo 1*74) il gruppo di relè indicato come identificatore
10	Rly Grp yy sec	n. gruppo relè	Gruppo relè chiuso per Y secondi– Chiude per Y secondi (come da programmazione del campo 1*75) il gruppo di relè indicato come identificatore
Comandi inserimento/disinserimento			
I tempi di attivazione validi delle funzioni di inserimento e disinserimento automatico sono 1 (inizio), 2 (fine), 3 (durante).			
L'opzione "durante" permette di inserire o disinserire il sistema di allarme solo per un determinato periodo di tempo. Per esempio, selezionando "durante" con la modalità inserimento PARZIALE, il sistema si inserisce automaticamente in modalità PARZIALE all'inizio della fascia oraria e si disinserisce automaticamente alla fine.			
20	Arm STAY	Partizione(i)	Inserimento PARZIALE – Inserisce in modalità PARZIALE la partizione(i) indicata come identificatore
21	Arm AWAY	Partizione(i)	Inserimento TOTALE – Inserisce in modalità TOTALE la partizione(i) indicata come identificatore
22	Disarm	Partizione(i)	Disinserimento – Disinserisce la partizione(i) indicata come identificatore
23	Force Arm STAY	Partizione(i)	Inserimento forzato PARZIALE – Inserisce in modalità PARZIALE la partizione(i) indicata come identificatore escludendo automaticamente le zone aperte
24	Force Arm AWAY	Partizione(i)	Inserimento forzato TOTALE – Inserisce in modalità TOTALE la partizione(i) indicata come identificatore escludendo automaticamente le zone aperte
Comandi di esclusione			
I tempi di attivazione validi dei comandi di esclusione sono 1 (inizio), 2 (fine), 3 (durante). Selezionando 3 (durante) per l'esclusione automatica, il sistema esclude la zona(e) specificata in un determinato elenco zone all'inizio della fascia oraria e le mette in sicurezza al termine della fascia. Se il sistema è selezionato per la messa in sicurezza automatica, l'esclusione zona(e) viene rimossa all'inizio della fascia e ripristinata alla fine.			
30	Bypass Zn list	Elenco zona n.	Esclusione automatica elenco zone – L'elenco zone indicato come identificatore viene automaticamente escluso
31	Unbyps Zn list	Elenco zona n.	Messa in sicurezza automatica elenco zone – L'elenco zone indicato come identificatore viene automaticamente messo in sicurezza

Condizioni di aperto/chiuso

L'unico tempo di attivazione valido di questi comandi è **3** (durante). Selezionando fascia oraria di abilitazione aperto, fascia oraria di abilitazione chiuso e fascia oraria accesso abilitato, la fascia oraria è attiva nelle partizioni indicate come identificatore ad eccezione di quanto sotto indicato:

- Al verificarsi di una funzione evento/azione di disattivazione fascia oraria (partizione non selezionata), la fascia oraria della partizione viene disabilitata solamente se non già legata ad un parametro di tempo che ne prevede l'abilitazione (es. parametri aperto/chiuso, eventi temporizzati, parametri di accesso).
- Se un parametro di tempo (es. parametri aperto/chiuso, eventi temporizzati, parametri di accesso) disabilita una fascia oraria (partizione non selezionata), la fascia oraria della partizione viene disabilitata solamente se non già abilitata da una funzione evento/azione.

40	En Open Wind	Partizione(i)	Fascia oraria di abilitazione partizione aperta – Abilita la fascia oraria di apertura della partizione indicata come identificatore (permette di controllare i report alla centrale operativa - per maggiori informazioni, fare riferimento a casi particolari di report aperto/chiuso nel manuale del sistema di allarme)
----	--------------	---------------	---

Tabella 5-1: codici azione (continua)

CODICE AZIONE	NOME AZIONE	IDENTIFICATORE AZIONE	DESCRIZIONE AZIONE
Condizioni di aperto/chiuso (continua)			
41	En Close Wind	Partizione(i)	Fascia oraria di abilitazione partizione chiusa – Abilita la fascia oraria di chiusura della partizione indicata come identificatore (permette di controllare i report inviati alla centrale operativa - per maggiori informazioni, fare riferimento a casi particolari di report aperto/chiuso nel manuale del sistema di allarme)
42	En Access Wind	Gruppo di accesso	Fascia oraria di abilitazione accesso del gruppo di accesso dell'utente – Abilita la fascia oraria di accesso del gruppo di accesso dell'utente indicato come identificatore (abilita l'utente all'inserimento o disinserimento - per maggiori informazioni, fare riferimento ai limiti dei parametri di accesso nel manuale del sistema di allarme)
50	Off-Normal Reminder	Nessuno	Cicalino anomalia – Tutte le tastiere con zona antincendio in condizione di anomalia emettono una sequenza di bip fino alla conferma da parte dell'utente
Azioni di controllo accesso			
Tutte le azioni di controllo accesso sono attive per la durata della fascia oraria e non prevedono la selezione dell'opzione tempo di attivazione.			
55	AP Grant	Cod. punto di accesso	Punto di accesso autorizzato– Autorizza l'accesso dal punto di accesso indicato come identificatore
56	AP Grant/O	Cod. punto di accesso	Punto di accesso autorizzato con comando manuale– Autorizza l'accesso dal punto di accesso indicato come identificatore con comando manuale
57	AP Protect	Cod. punto di accesso	Punto di accesso protetto – Mette in sicurezza il punto di accesso indicato come identificatore
58	AP Bypass	Cod. punto di accesso	Punto di accesso escluso – Esclude il punto di accesso indicato come identificatore
59	AP Lock	Cod. punto di accesso	Punto di accesso bloccato – Blocca il punto di accesso indicato come identificatore
60	AP Exit Only	Cod. punto di accesso	Punto di accesso solo uscita – Imposta il punto di accesso indicato come identificatore in modalità solo uscita
61	AP Grp Grt	Cod. gruppo	Gruppo punto di accesso autorizzato– Autorizza l'accesso da tutti i punti di accesso del gruppo(i) indicato come identificatore
62	AP Grp Grt/O	Cod. gruppo	Gruppo punto di accesso autorizzato con comando manuale – Autorizza l'accesso da tutti i punti di accesso del gruppi(i) indicato come identificatore mediante comando manuale
63	AP Grp Prot	Cod. gruppo	Gruppo punti di accesso protetto– Mette in sicurezza tutti i punti di accesso del gruppo(i) indicato come identificatore (modalità protetto)
64	AP Grp Bypas	Cod. gruppo	Gruppo punti di accesso escluso– Esclude tutti i punti di accesso del gruppo(i) indicato come identificatore (modalità escluso)
65	AP Grp Lock	Cod. gruppo	Gruppo punti di accesso bloccato– Blocca tutti i punti di accesso del gruppo(i) indicato come identificatore (modalità bloccato)
66	AP Grp Exit O	Cod. gruppo	Gruppo punti di accesso solo uscita– Imposta tutti i punti di accesso del gruppo(i) indicato come identificatore in modalità solo uscita
67	AP Ptn Grt	Cod. partizione	Punti di accesso partizione autorizzati– Autorizza l'accesso da tutti i punti di accesso della partizione(i) indicata come identificatore
68	AP Ptn Grt/O	Cod. partizione	Punti di accesso partizione autorizzati con comando manuale – Autorizza con comando manuale l'accesso da tutti i punti di accesso della partizione(i) indicata come identificatore
69	AP Ptn Prot	Cod. partizione	Punti di accesso partizione protetti – Mette in sicurezza tutti i punti di accesso della partizione(i) indicata come identificatore
70	AP Ptn Bypas	Cod. partizione	Punti di accesso partizione esclusi – Esclude tutti i punti di accesso della

			partizione(i) indicata come identificatore
71	AP Ptn Lock	Cod. partizione	Punti di accesso partizione bloccati – Blocca tutti i punti di accesso della partizione(i) indicata come identificatore
72	AP Ptn Exit O	Cod. partizione	Punti di accesso partizione solo uscita – Imposta tutti i punti di accesso della partizione(i) indicata come identificatore in modalità solo uscita
73	AP Trg On	Cod. punto di accesso	Uscita logica punto di accesso attivata – Attiva l'uscita logica del punto di accesso indicato come identificatore (N.B.: Questo codice azione può essere utilizzato SOLAMENTE con il comando #77 e con la funzione evento/azione. Non può essere utilizzato con eventi temporizzati.)
74	AP Trg Off	Cod. punto di accesso	Uscita logica punto di accesso disattivata – Disattiva l'uscita logica del punto di accesso indicato come identificatore (N.B: Questo codice azione può essere utilizzato SOLAMENTE con il comando #77 e con la funzione evento/azione. Non può essere utilizzato con eventi temporizzati.)
77	ACS Grp Enbl	Cod. gruppo	Gruppo punto di accesso abilitato– Abilita il gruppo(i) di accesso indicato come identificatore (abilita i titolari di un gruppo autorizzando le richieste di accesso valide)
78	ACS Grp Dsbl	Cod. gruppo	Gruppo punto di accesso disabilitato– Disabilita il gruppo(i) di accesso indicato come identificatore

Foglio di programmazione funzione evento/azione

La funzione evento/azione genera azioni che permettono di attivare terminali di uscita, escludere zone, ecc. in base ad eventi che si verificano nel sistema di allarme. 32 diverse funzioni evento/azione possono essere programmate nel sistema

Le azioni programmabili generate automaticamente da (in seguito a) determinati eventi sono: comandi di relè, comandi inserimento/disinserimento, comandi di esclusione zone, condizioni di aperto/chiuso e comandi di controllo accesso.

Compilare il foglio di programmazione funzione evento/azione (alla fine del capitolo) seguendo le procedure sotto indicate:

Per semplificare la comprensione delle procedure di compilazione del foglio di programmazione funzione evento/azione, si suppone di voler accendere una luce (mediante il relè n. 1) con accesso autorizzato dal punto di accesso 1, nella fascia oraria 8.00 - 17.00 (programmata come fascia oraria 1) da lunedì a venerdì. Le varie procedure sono supportate da esempi di compilazione del foglio di programmazione.

1. Digitare il codice evento indicato nella *tabella 5-2: Eventi e azioni* corrispondente all'evento desiderato.

Esempio: digitare il codice evento 22 corrispondente a autorizzazione punto di accesso

Evento	Cod. evento	Nome evento	Identificatore evento	Cod. azione	Azione desiderata	Identificatore azione	Fascia oraria (00= sempre, 01-20 = n. fascia oraria)	Giorni							
								L	M	M	G	V	S	D	V
1	22														
2															

2. Digitare il nome evento indicato nella *tabella 5-2: eventi e azioni* corrispondente al codice evento.

Esempio: digitare AP Grt corrispondente al codice evento 22.

Evento	Cod. evento	Nome evento	Identificatore evento	Cod. azione	Azione desiderata	Identificatore azione	Fascia oraria (00= sempre, 01-20 = n. fascia oraria)	Giorni							
								L	M	M	G	V	S	D	V
1	22	AP Grt													
2															

3. Digitare l'identificatore evento corrispondente alla descrizione della *tabella 5-2: eventi e azioni*.

Esempio: digitare **01** corrispondente al codice punto di accesso.

Evento	Cod. evento	Nome evento	Identificatore evento	Cod. azione	Azione desiderata	Identificatore azione	Fascia oraria (00= sempre, 01-20 = n. fascia oraria)	Giorni							
								L	M	M	G	V	S	D	V
1	22	AP Grt	01												
2															

4. Digitare il codice azione indicato nella *tabella 5-1: codici azione* corrispondente all'azione desiderata.

Esempio: digitare il codice azione. **01** per attivare il relè.

Evento	Cod. evento	Nome evento	Identificatore evento	Cod. azione	Azione desiderata	Identificatore azione	Fascia oraria (00= sempre, 01-20 = n. fascia oraria)	Giorni							
								L	M	M	G	V	S	D	V
1	22	AP Grt	01	01											
2															

5. Digitare il nome azione indicato nella *tabella 5-1: codici azione* corrispondente al codice azione.

Esempio: digitare **Relay On** corrispondente al codice azione 01.

Evento	Cod. evento	Nome evento	Identificatore evento	Cod. azione	Azione desiderata	Identificatore azione	Fascia oraria (00= sempre, 01-20 = n. fascia oraria)	Giorni							
								L	M	M	G	V	S	D	V
1	22	AP Grt	01	01	Relay On										
2															

6. Digitare l'identificatore azione corrispondente alla descrizione della *tabella 5-1: codici azione*.

Esempio: digitare **01** corrispondente al relè n. 1.

Evento	Cod. evento	Nome evento	Identificatore evento	Cod. azione	Azione desiderata	Identificatore azione	Fascia oraria (00= sempre, 01-20 = n. fascia oraria)	Giorni							
								L	M	M	G	V	S	D	V
1	22	AP Grt	01	01	Relay On	01									
2															

7. Digitare il numero fascia oraria corrispondente alla fascia oraria (precedentemente programmata) durante la quale un determinato evento genera l'azione selezionata.

Esempio: se si suppone che l'orario di inizio della fascia oraria 1 è 08.00 e quello di fine 17.00, digitare **01** corrispondente alla fascia oraria 1.

Evento	Cod. evento	Nome evento	Identificatore evento	Cod. azione	Azione desiderata	Identificatore azione	Fascia oraria (00= sempre, 01-20 = n. fascia oraria)	Giorni							
								L	M	M	G	V	S	D	V
1	22	AP Grt	01	01	Relay On	01	01								
2															

8. Selezionare con una **X** i giorni della settimana in cui la funzione evento/azione deve essere generata nella specifica fascia oraria. Se si seleziona Vacanza, la selezione dei giorni della settimana non viene considerata (es. l'azione viene generata selezionando Vacanza anche quando la vacanza cade di sabato e sabato non è selezionato). Per ulteriori informazioni, fare riferimento ai parametri vacanza nel manuale del sistema di allarme.

Esempio: digitare **X** sotto L, M, M, G, e V per selezionare da lunedì a venerdì..

Evento	Cod. evento	Nome evento	Identificatore evento	Cod. azione	Azione desiderata	Identificatore azione	Fascia oraria (00= sempre, 01-20 = n. fascia oraria)	Giorni									
								L	M	M	G	V	S	D	V		
1	22	AP Grt	01	01	Relay On	01	01	X	X	X	X	X					
2																	

In base all'esempio sopra indicato, l'accesso autorizzato dal punto di accesso 1 (evento) attiva il relè n. 1(azione).

9. Ripetere i punti da 1 a 8 per ogni funzione evento/azione desiderata.

Tabella 5-2: eventi e azioni

COD. EVENTO	NOME EVENTO	IDENTIFICATORE EVENTO	DESCRIZIONE EVENTO
Identificatore partizione (Ptn)			
00	None	Nessuno	Non utilizzato
01	Arm Ptn	Partizione(i)	Inserimento partizione – Le partizioni indicate come identificatore sono state inserite
02	Disarm Ptn	Partizione(i)	Disinserimento partizione – Le partizioni indicate come identificatore sono state disinserite
03	Fire Ptn	Partizione(i)	Incendio partizione – Le partizioni indicate come identificatore segnalano un allarme incendio
04	Fire Rst Ptn	Partizione(i)	Ripristino incendio partizione – L'allarme incendio delle partizioni indicate come identificatore è stato ripristinato
05	Burg Ptn	Partizione(i)	Effrazione partizione – Le partizioni indicate come identificatore segnalano un allarme effrazione
06	Burg Rst Ptn	Partizione(i)	Ripristino effrazione partizione – L'allarme effrazione delle partizioni indicate come identificatore è stato ripristinato
07	Alm Ptn	Partizione(i)	Allarme partizione – Le partizioni indicate come identificatore sono in allarme
08	Alm Rst Ptn	Partizione(i)	Ripristino allarme partizione – L'allarme delle partizioni indicate come identificatore è stato ripristinato
09	Dur Ptn	Partizione(i)	Coercizione partizione – Le partizioni indicate come identificatore segnalano un allarme coercizione
10	Dur Rst Ptn	Partizione(i)	Ripristino coercizione partizione – L'allarme coercizione delle partizioni indicate come identificatore è stato ripristinato
11	Trb Ptn	Partizione(i)	Anomalia partizione – Le partizioni indicate come identificatore segnalano un'anomalia
12	Trb Rst Ptn	Partizione(i)	Ripristino anomalia partizione – La condizione di anomalia delle partizioni indicate come identificatore è stata ripristinata
13	Byp Ptn	Partizione(i)	Esclusione partizione – Una zona della partizione(i) indicata come identificatore è stata esclusa
14	Byp Rst Ptn	Partizione(i)	Ripristino esclusione partizione – La zona esclusa della partizione(i) indicata come identificatore è stata messa in sicurezza
15	Late Disarm Ptn	Partizione(i)	Ritardo disinserimento partizione – Le partizioni indicate come identificatore è stata disinserita in ritardo.
16	Early Arm Ptn	Partizione(i)	Inserimento partizione anticipato - Le partizioni indicate come identificatore sono state inserite in anticipo
17	Fail Arm Ptn	Partizione(i)	Errore inserimento partizione - Le partizioni indicate come identificatore non sono state inserite correttamente
Identificatori utente			
18	Arm Usr	Cod. utente VISTA	Inserimento utente – L'utente indicato come identificatore ha inserito la partizione
19	Disarm Usr	Cod. utente VISTA	Disinserimento utente – L'utente indicato come identificatore ha disinserito la partizione
20	Grt Usr	Cod. utente VISTA	Utente autorizzato – L'utente indicato come identificatore è stato autorizzato all'accesso

Identificatori codice scheda			
21	Grant Card	Codice scheda	Scheda autorizzata – L'accesso della scheda con codice identificativo indicato come identificatore è stato autorizzato
Identificatori punto di accesso (PA)			
22	AP Grt	Cod. punto di accesso	Punto di accesso autorizzato – L'accesso dal punto di accesso indicato come identificatore è stato autorizzato
23	AP Deny	Cod. punto di accesso	Punto di accesso non autorizzato – L'accesso dal punto di accesso indicato come identificatore non è stato autorizzato
24	AP Byp	Cod. punto di accesso	Punto di accesso escluso – Il punto di accesso indicato come identificatore è stato escluso
25	None	Nessuno	Non utilizzato
26	AP Lock	Cod. punto di accesso	Punto di accesso bloccato – Il punto di accesso indicato come identificatore è stato bloccato
27	AP Prot	Cod. punto di accesso	Punto di accesso protetto – il punto di accesso indicato come identificatore è stato messo in sicurezza (modalità protetto)
28	None	Nessuno	Non utilizzato
29	AP Grt Ovr	Cod. punto di accesso	Autorizzazione punto di accesso con comando manuale – L'accesso dal punto di accesso indicato come identificatore è stato autorizzato con comando manuale
30	Dur Grt	Cod. punto di accesso	Autorizzazione punto di accesso in coercizione– L'accesso dal punto di accesso indicato come identificatore è stato autorizzato in condizioni di coercizione
31	Prop Opn Alm	Cod. punto di accesso	Allarme anomalia punto di accesso aperto – Il punto di accesso indicato come identificatore segnala un allarme anomalia porta aperta
32	Prop Opn Rst	Cod. punto di accesso	Ripristino allarme anomalia punto di accesso aperto – L'allarme anomalia punto di accesso aperto del punto di accesso indicato come identificatore è stato ripristinato

Tabella 5-2: eventi e azioni (continua)

COD. EVENTO	NOME EVENTO	IDENTIFICATORE EVENTO	DESCRIZIONE EVENTO
Identificatori punto di accesso (PA) (continua)			
33	Force Opn	Cod. punto di accesso	Punto di accesso forzato– Il punto di accesso indicato come identificatore segnala un allarme porta forzata
34	Force Rst	Cod. punto di accesso	Ripristino punto di accesso forzato – L'allarme porta forzata del punto di accesso indicato come identificatore è stato ripristinato
Identificatori codici zona			
35	Fire Zn	Codice zona	Incendio zona– La zona indicata come identificatore segnala un allarme incendio
36	Fire Rst Zn	Codice zona	Ripristino incendio zona– L'allarme incendio della zona indicata come identificatore è stato ripristinato
37	Burg Zn	Codice zona	Effrazione zona– la zona indicata come identificatore segnala un allarme effrazione
38	Burg Rst Zn	Codice zona	Ripristino effrazione zona– L'allarme effrazione della zona indicata come identificatore è stato ripristinato
39	Alm Zn	Codice zona	Allarme zona– La zona indicata come identificatore è in allarme
40	Alm Rst Zn	Codice zona	Ripristino allarme zona– L'allarme della zona indicata come identificatore è stato ripristinato
41	Trb Zn	Codice zona	Anomalia zona– La zona indicata come identificatore segnala un'anomalia
42	Tble Rst Zn	Codice zona	Ripristino anomalia zona– L'anomalia della zona indicata come identificatore è stata ripristinata
43	Byp Zn	Codice zona	Esclusione zona– La zona indicata come identificatore è stata esclusa
44	Byp Rst Zn	Codice zona	Ripristino esclusione zona– La zona indicata come identificatore è stata messa in sicurezza
Identificatori inserimento			

45	Arm Stay Ptn	Partizione(i)	Inserimento parziale partizione – Le partizioni indicate come identificatore sono state inserite in modalità parziale
46	Arm Away Ptn	Partizione(i)	Inserimento totale partizione – Le partizioni indicate come identificatore sono state inserite in modalità totale
47	Arm Inst Ptn	Partizione(i)	Inserimento istantaneo partizione – Le partizioni indicate come identificatore sono state inserite in modalità istantaneo
48	Arm Max Ptn	Partizione(i)	Inserimento massimo partizione – Le partizioni indicate come identificatore sono state inserite in modalità massimo
49	Arm Stay Usr	Cod. utente VISTA	Inserimento parziale utente – L'utente indicato come identificatore ha inserito la partizione in modalità parziale
50	Arm Away Usr	Cod. utente VISTA	Inserimento totale utente – l'utente indicato come identificatore ha inserito la partizione in modalità totale
51	Arm Inst Usr	Cod. utente VISTA	Inserimento istantaneo utente– L'utente indicato come identificatore ha inserito la partizione in modalità istantaneo
52	Arm Max Usr	Cod. utente VISTA	Inserimento massimo utente – l'utente indicato come identificatore ha inserito la partizione in modalità massimo

Mappatura zone VistaKey nelle zone del sistema di allarme

I tipi di zona VistaKey che si possono mappare nelle zone del sistema di allarme sono quattro. La descrizione sotto indicata facilita la comprensione delle procedure di programmazione necessarie.

- **DSM** – Questo tipo zona permette di monitorare lo stato di un punto di accesso (per esempio, aperto, chiuso) mappandolo in una zona. In caso di esclusione punto di accesso, anomalia porta aperta o porta forzata, il sistema DSM risponde in base al tipo risposta zona. Il dispositivo DSM è composto normalmente da un interruttore magnetico installato sulla porta. Lo stato dell'interruttore varia in caso di porta (punto di accesso) aperta.
- **RTE** – Questo tipo zona permette di mappare una zona RTE non abbinata in una zona del sistema di allarme e non viene normalmente utilizzato se la zona RTE svolge la funzione di richiesta di uscita. Il dispositivo RTE può essere un semplice interruttore a contatto istantaneo oppure un più complesso sensore di movimento.
- **GP** – Questo tipo zona permette di mappare la zona GP in una zona del sistema di allarme; funziona come le altre zone della centralina VISTA e, se situata in prossimità del modulo VistaKey, non richiede ulteriori collegamenti al sistema VISTA. Inoltre, permette di controllare le installazioni contro rischi di manomissione al coperchio anteriore dell'armadietto.
- **DSMB** – Il dispositivo DSMB è una zona con tipo di ingresso a circuito seriale polling che permette di mappare il modulo di integrazione sistemi del modulo VistaKey in una zona del sistema di allarme. In caso di mancanza rete locale al modulo VistaKey, lo stato del dispositivo DSM non può essere segnalato alla centralina mediante i normali circuiti a microprocessori del modulo VistaKey. In questo caso il modulo di integrazioni sistemi del dispositivo Vplex, installato sulla scheda del modulo VistaKey e alimentato direttamente dal circuito polling, viene attivato per segnalare lo stato del dispositivo DSM mediante il sistema polling standard del dispositivo Vplex.

Per programmare la centralina VISTA nel modulo VistaKey, entrare nel campo **#93 Programmazione modalità menu** del sistema di allarme in base alle procedure del manuale di installazione del sistema di allarme. Una volta entrati nel campo **#93 Programmazione modalità menu**, il display visualizza il prompt sotto indicato:

PROG ZONA?
1=SI 0=NO

("Programmazione zona? - 1 = SI' 0 = NO") Premere **1** per entrare in modalità programmazione zona. Il display visualizza il prompt sotto indicato.

N.B.: Durante la programmazione, premere [**★**] per visualizzare il prompt successivo. Premere [**#**] per visualizzare il prompt precedente.

INS PER CONFER?
1=SI 0=NO

("Confermi? - 1 = SI' 0 = NO") Questo prompt permette di confermare il numero di serie del dispositivo RF e del dispositivo del circuito polling. In fase di programmazione del modulo VistaKey, questo prompt permette di confermare il numero di serie del dispositivo DSMB ma non è indispensabile.

Premere **1** oppure **0**. Il display visualizza il prompt sotto indicato.

DIGITA NR ZONA?
000 = ESCI 010
Zona 010 selezionata ↑

("Digitare codice zona? - 000= per uscire") Digitare il codice zona a tre cifre della zona VistaKey da programmare. Nell'esempio è stata inserita la zona 010.

Premere [**★**] per confermare. Il sistema si sposta al prompt riassuntivo sotto indicato.

Una volta programmate tutte le zone (DSM, DSMB, RTE, e GP), digitare **000** seguito da [**★**]. Premere **0** più volte fino a quando il display visualizza il prompt "Access Point Pgm" ("Programmazione punto di accesso"). Per programmare il punto(i) di accesso, fare riferimento al paragrafo "Impostazione opzioni di programmazione punto di accesso" di questo capitolo.

010 ZT P RC B IN L
00 _ _ _ _ _

Il display visualizza il prompt riassuntivo della zona programmata. ZT = Tipo zona, P = Partizione, RC = Codice report, B = abbinamento sirena/relè ausiliario di zona, IN = tipo di ingresso dispositivo e L = numero loop del dispositivo al quale il sensore è collegato. Alcuni dispositivi sono in grado di gestire più di una zona grazie a loop singoli. In caso di zona non programmata, il display visualizza il prompt come indicato. Se la programmazione della zona risponde alle esigenze richieste, premere [**#**] per spostarsi al prompt precedente e digitare un nuovo codice zona.

Premere [**★**] per continuare.

010 TIPO ZONA

("010 tipo zona") Selezionare un tipo risposta per la zona DSM^①, RTE^②, GP^③ o DSMB^④. Le opzioni valide sono:

N.B.: Le zone degli ingressi DSM, RTE e GP delle installazioni UL possono essere utilizzate solo per funzioni di controllo accesso.

- | | |
|--------------------------------------|--|
| 00 = Zone non utilizzate | 09 = Incendio senza verifica ^④ |
| 01 = Ingresso/Uscita n.1, Effrazione | 10 = Ritardo interno, effrazione |
| 02 = Ingresso/Uscita n.2, Effrazione | 16 = Incendio con verifica ^④ |
| 03 = Perimetrale, effrazione | 17 = Irrigatori antincendio ^④ |
| 04 = Interno a seguire, effrazione | 18 = Supervisore incendio ^④ |
| 05 = Anomalia giorno/allarme notte | 19 = Anomalia 24 ore |
| 06 = Allarme silenzioso 24 ore | 23 = Nessuna risposta allarme (es. attivazione relè) |
| 07 = Allarme acustico 24 ore | |
| 08 = Ausiliario 24 ore | 29 = Uscita momentanea ^⑤ |

- ① Il tipo zona 01 o 02 permette di impostare il ritardo di ingresso/uscita nelle zone DSM e DSMB. Se il ritardo non è richiesto, selezionare il tipo zona 03.
- ② NON abbinare un tipo risposta alla zona RTE se utilizzata come richiesta di uscita (controllo serratura meccanica o magnetica). Il tipo risposta può essere abbinato solamente nel caso in cui il dispositivo RTE NON è utilizzato come richiesta di uscita essendo una zona non abbinata. Come zona non abbinata, la zona RTE può essere abbinata ad un diverso tipo di risposta per essere utilizzata con un altro tipo zona.
- ③ Nelle installazioni che richiedono la supervisione del coperchio anteriore dell'armadietto, la zona GP deve essere programmata come manomissione (selezionare tipo zona 05).

- ④ Queste zone incendio non possono essere utilizzate nelle installazioni UL.
- ⑤ Per la descrizione completa dell'uscita momentanea, fare riferimento al paragrafo "Uscita momentanea dal punto di accesso" di questo capitolo.

Premere [✱] per confermare e continuare.

010 SETTORE	2
-------------	---

("010 Partizione") Digitare il codice partizione da abbinare a questa zona. Il codice partizione abbinato deve corrispondere al codice partizione abbinato all'area protetta della porta (punto di accesso) che autorizza l'accesso.

Premere [✱] per continuare.

010 CODICE TRAS 1 st 03 2 nd 12	3C
--	----

("010 codice report - 1° 03 2° 12") Digitare il codice report composto da 2 cifre esadecimali, ognuna delle quali a sua volta è composta da due cifre numeriche. Per esempio, se il codice report è "3C", digitare 03 per 3 e 12 per C.

N.B.:

- Digitare 00 per disabilitare l'invio di report eventi di zona. In caso di tipo ingresso DSM, gli eventi sono 423, 46, 427, etc. oltre ai codici report normalmente inviati in base alla selezione del tipo zona. (La lista completa degli eventi di accesso è indicata nel capitolo *Registro eventi* del manuale). In caso di zona GP o RTE non abbinata, i report degli eventi della zona vengono disabilitati. Digitare 00 per escludere la selezione dei combinatori di accesso che potrebbero essere abilitati.
- In caso di codici report di accesso (eventi combinatori di accesso abilitati), il codice report della zona deve essere diverso da zero.
- In caso di abilitazione degli eventi combinatori di accesso, utilizzare il formato report ID Contact.

(Per maggiori informazioni sui codici report e sui formati dei codici report, fare riferimento al capitolo *Comunicazione* nel manuale del sistema di allarme.)

Premere [✱] per continuare.

010 BELL/RLY SEL	0
------------------	---

("010 selezione sirena/relè") Ogni zona può essere abbinata per attivare una o entrambe le uscite sirena e/o il relè ausiliario del sistema. Digitare uno degli abbinamenti sotto indicati:
0=nessuno; 1=sirena 1; 2=sirena 2; 3=sirena 1 e 2; 4=relè ausiliario;
5=sirena 1 e relè aux; 6=sirena 2 e relè aux; 7=sirena 1 e 2 e relè aux.

Premere [✱] per continuare.

010 TIPO SENSORE RF Xmitter	3
--------------------------------	---

("010 tipo di ingresso - trasmettitore RF") Le opzioni valide per questo prompt in fase di programmazione del modulo VistaKey sono: controllo stato porta (DSM), richiesta di uscita (RTE), generico (GP) e dispositivo con circuito seriale polling (DSM secondario [DSMB]). Gli utilizzi di questi tipi ingresso sono:

DSM – Questo tipo ingresso permette di mappare un punto di accesso in una zona. In caso di esclusione punto di accesso, anomalia porta aperta o porta forzata, il sistema DSM risponde in

base al tipo risposta zona. Il dispositivo DSM è composto normalmente da un interruttore magnetico installato nella porta. Lo stato dell'interruttore varia in caso di porta (punto di accesso) aperta.

RTE – Questo tipo ingresso permette di mappare una zona RTE non abbinata in una zona del sistema di allarme. Questo tipo ingresso non viene normalmente utilizzato se la zona RTE viene utilizzata per la funzione richiesta di uscita. Il dispositivo RTE può essere un semplice interruttore a contatto istantaneo oppure un più complesso sensore di movimento.

GP – Questo tipo ingresso permette di mappare la zona GP nella zona del sistema di allarme; funzione come le altre zone della centralina VISTA e, se situato in prossimità del modulo VistaKey, non richiede ulteriori collegamenti al sistema VISTA. Inoltre, permette di controllare le installazioni contro rischi di manomissione al coperchio anteriore dell'armadietto.

CIRCUITO POLLING SERIALE (DSMB) – Il tipo ingresso del circuito polling seriale (per il dispositivo DSMB) permette di mappare il modulo di integrazione sistemi del modulo VistaKey in una zona del sistema di allarme. In caso di mancanza rete locale al modulo VistaKey, lo stato del dispositivo DSM non può essere segnalato alla centralina mediante i normali circuiti a microprocessori del modulo VistaKey. In questo caso il modulo di integrazione sistemi del dispositivo Vplex installato sulla scheda del modulo VistaKey e alimentato direttamente dal circuito polling viene attivato per segnalare lo stato del dispositivo DSM mediante il sistema polling standard del dispositivo Vplex. Le opzioni valide di tipi dispositivi di ingresso sono:

06 = Dispositivo circuito polling seriale (zona VistaKey DSM secondario [VKey DSMB])

N.B.: Per attivare la funzione DSMB, selezionare 06 nell'opzione corrente (TIPO DI INGRESSO) e digitare il codice punto di accesso da 01 a 15 nel prompt successivo (punto di accesso).

11 = Zona DSM VistaKey (VKey DSM)

12 = Zona RTE VistaKey (VKey RTE)

13 = Zona GP VistaKey (VKey GP)

Premere [✱] per continuare.

Premere 11, 12 o 13 per spostare il sistema al prompt "Access Point" ("Punto di accesso"). Premere 06 per spostare il sistema al prompt "Smart Contact" ("Contatto intelligente") oppure al prompt "V-Plex Relay" ("Relè V-Plex").

010 Smart Contact	
1 = SI 0 = NO	0

("010 contatto intelligente - 1 = SI' 0 = NO")
Premere [0] e poi [✱] per continuare.

N.B.: In alcuni sistemi di allarme questo prompt non viene visualizzato.

010 V-PLEX RELAY	
1 = SI 0 = NO	0

("010 relè Vplex - 1 = SI 0 = NO") Premere [0] e poi [✱] per continuare.

010 PORTA NR (01-15)	3
-------------------------	---

("010 punto di accesso - (01-15)") Digitare il codice porta a due cifre (01-15) del modulo VistaKey.

N.B.: L'opzione selezionata deve corrispondere all'indirizzo impostato nel modulo VistaKey per la porta (punto di accesso) da programmare.

Premere [✱] per continuare.

Digitare 11, 12 o 13 come tipo ingresso; il sistema si sposta al prompt riassuntivo. Digitare 06 come tipo ingresso e un codice punto di accesso da 1 a 15 nella procedura sopra; il sistema visualizza il prompt "Input S/N:L" ("Numero di serie ingresso: L") corrispondente alla registrazione del numero di serie del modulo VistaKey.

010 INPUT S/N:L Axxx-xxxx:1

Per registrare il numero di serie del modulo VistaKey (DSMB):

1. Scollegare il modulo VistaKey dal sistema di alimentazione.
2. Attivare la zona DSM fino a quando la tastiera emette due bip e visualizza il numero di serie del modulo VistaKey.
3. Ripristinare la zona DSM e alimentare il modulo.

N.B.: In fase di registrazione, abbinare la zona DSMB del modulo VistaKey al loop 1; il loop 2 deve rimanere inutilizzato.

Premere [✱] per continuare.

010 ZT P RC B IN L 01 2 3C 0 DM 1

Il display visualizza il prompt riassuntivo della zona.

N.B.: Il tipo ingresso corrispondente alla voce IN sul display dipende dall'opzione selezionata nel prompt TIPO INGRESSO indicato sopra: RE (tipo 12 – richiesta di uscita), GP (tipo 13 – generico) oppure DB (tipo 06 – controllo stato porta secondario).

Premere [✱] per confermare la programmazione della zona.

Il sistema di allarme ritorna al prompt "DIGITA NR ZONA." ("DIGITARE CODICE ZONA").

Impostazione opzioni di programmazione punto di accesso modulo VistaKey

Le opzioni del punto di accesso del modulo(i) VistaKey vengono impostate nella modalità programmazione punto di accesso a cui si accede entrando nella funzione #93

Programmazione modalità menu e tenendo premuto il tasto [0] fino a quando il display visualizza il prompt sotto indicato.

Pgm Punto Accesso 1=SI 0=No

("Programmazione punto di accesso - 1 = SI 0 = NO"). Premere 1 oppure 0 per selezionare o saltare la modalità programmazione punto di accesso.

Premere 1 per visualizzare il prompt sotto indicato.

Premere 0 per spostarsi alla modalità programmazione gruppo di accesso.

INS PNT ACS n# 01-15, 00=ESCI	01
----------------------------------	----

("Digitare codice punto di accesso - 01-15, 00 = per uscire") Digitare un numero da **01** a **15** come codice punto di accesso da programmare; oppure **00** per uscire dalla modalità programmazione punto di accesso. Il codice punto di accesso selezionato in questa fase corrisponde alla selezione del commutatore di indirizzo del modulo VistaKey (da 1 a 9 = 01 - 09, A=10, B=11, C=12, D=13, E=14 oppure F=15).

Premere [**✱**] per confermare.

Digitare **00** per terminare la programmazione del punto di accesso. Il sistema si sposta alla programmazione gruppo di accesso.

Digitare un numero da 1 a 15 per visualizzare il prompt sotto indicato

↓ Cod. punto di accesso 01 CONFIG DSM NORM APER	0
---	---

("01 configurazione DSM - normalmente aperto") Digitare la configurazione della zona DSM (zona VistaKey A) ad 1 cifra. La configurazione corrisponde allo stato del dispositivo DSM a porta (punto di accesso) chiuso. Le opzioni valide sono:

- 0 = normalmente aperto
- 1 = normalmente chiuso
- 2 = Resistore di fine linea (EOL) normalmente aperto
- 3 = Resistore di fine linea (EOL) normalmente chiuso

Premere [**✱**] per confermare.

↓ Cod. punto di accesso 01 TEMPO AP PORT 3s	2
---	---

("01 tempo porta aperta - 3 sec.") Il tempo porta aperta corrisponde al tempo in cui la serratura della porta rimane in stato sbloccato (aperto) dopo l'inserimento di una scheda valida nel lettore oppure per attivazione della funzione RTE (se selezionata), a meno che non si verifichi una nuova condizione che blocca la serratura. Digitare la cifra (da 0 a 7) corrispondente alla durata in secondi del relè della serratura meccanica.

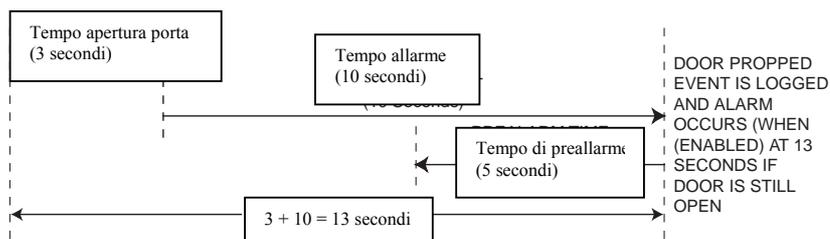
- 0 = 1 sec.
- 1 = 2 sec.
- 2 = 3 sec.
- 3 = 4 sec.
- 4 = 5 sec.
- 5 = 10 sec.
- 6 = 15 sec.
- 7 = 30 sec.

Premere [**✱**] per confermare.

↓ Cod. punto di accesso 01 TEMPO ALLARME 10s	0
--	---

("01 tempo allarme porta - 10 sec.") Digitare il codice ad una cifra del tempo allarme porta. Il conteggio del tempo allarme inizia al termine del tempo apertura porta indicato sopra; quindi, l'intervallo di tempo complessivo prima che venga segnalata la zona aperta corrisponde alla somma del tempo impostato come tempo porta aperta e il tempo impostato in questo prompt (vedere figura sotto). Se il punto di accesso è aperto al termine del tempo allarme impostato, un report di zona aperta (tempo allarme) viene inviato alla centralina VISTA e l'evento viene registrato come anomalia porta aperta.

IL SISTEMA REGISTRA L'EVENTO COME ANOMALIA PORTA APERTA E GENERA UN ALLARME (SE PROGRAMMATO) SE DOPO 13 SECONDI LA PORTA E' ANCORA APERTA
--



Le opzioni valide sono:

- | | |
|-------------|-------------|
| 0 = 10 sec. | 4 = 2 min. |
| 1 = 20 sec. | 5 = 5 min. |
| 2 = 30 sec. | 6 = 10 min. |
| 3 = 1 min. | 7 = 30 min. |

Premere **[*]** per confermare.

↓ Cod. punto di accesso
 01 TEMPO PREALL
 5s 0

("01 tempo di preallarme - 5 sec.") Il tempo di preallarme permette di segnalare all'utente che tiene aperta una porta che, in caso di porta aperta allo scadere del tempo allarme, il sistema rileverà una condizione di zona aperta (risultante in un allarme, se programmato). (Per esempio, come indicato nella figura sopra, se il tempo allarme è impostato a 10 secondi e il tempo di preallarme a 5 secondi, il tempo di preallarme inizia 5 secondi prima che la condizione di allarme [zona aperta] venga segnalata alla centralina VISTA). Il segnale di preallarme viene generato dall'uscita logica del modulo VistaKey e deve essere abilitata nel prompt "PREALARM TRIG" ("SEGNALE DI PREALLARME") di seguito nel capitolo.

Digitare il codice ad una cifra del tempo di preallarme. Le opzioni valide sono:

- | | |
|-------------|-------------|
| 0 = 5 sec. | 4 = 1 min. |
| 1 = 10 sec. | 5 = 2 min. |
| 2 = 15 sec. | 6 = 5 min. |
| 3 = 30 sec. | 7 = 10 min. |

Premere **[*]** per confermare.

↓ Cod. punto di accesso
 01 RICHIUD ON
 INTERV/CHIUSO 0

("01 blocco porta al tempo/chiusura") In caso di installazione di una zona DSM nella porta, il sistema è in grado di determinare se la porta è stata chiusa prima dello scadere del tempo previsto come tempo porta aperta (vedere il prompt "Door Opn Time" - "Tempo porta aperta" - sopra). Selezionando l'opzione "blocco porta al tempo/chiusura", il sistema blocca automaticamente la porta quando si chiude oppure al termine del tempo allarme, indipendentemente dagli eventi precedenti. L'opzione "Tempo/chiusura" impedisce ad un utente successivo di aprire una porta non bloccata. Selezionando "Blocca all'apertura", la serratura meccanica o magnetica si blocca nuovamente non appena la porta viene aperta.

Premere **0** (blocca al termine tempo o alla chiusura della porta, indipendentemente dagli eventi precedenti) oppure **1** (blocca all'apertura della porta).

Premere **[*]** per confermare.

<p>↓ Cod. punto di accesso</p> <p>01 RTE CONFIG NORM APERT 0</p>	<p>("01 configurazione RTE - normalmente aperto") Digitare il codice ad una cifra della configurazione della zona RTE non abbinata (zona VistaKey B). L'opzione selezionata deve corrispondere allo stato del dispositivo RTE (interruttore) quando non attivato (in stato di pronto). Le opzioni valide sono:</p> <ul style="list-style-type: none"> 0 = normalmente aperto 1 = normalmente chiuso 2 = resistore di fine linea (EOL) normalmente aperto 3 = resistore di fine linea (EOL) normalmente chiuso <p>Premere [*] per confermare.</p>
<p>↓ Cod. punto di accesso</p> <p>01 RIATTIVA RTE NON ABILIT 0</p>	<p>("01 azzeramento RTE - non abilitato") Questo prompt permette di estendere il tempo porta aperta ed escludere l'allarme generato in caso di rilevamento di una condizione di aperto. Se abilitato, le successive richieste di uscita (RTE) azzerano il tempo allarme impostato nel prompt precedente "ALARM TIMEOUT" ("TEMPO ALLARME"). Grazie al tempo porta aperta prolungato, il sistema autorizza l'uscita continua di persone senza generare un allarme.</p> <p>N.B.: L'azzeramento RTE può essere applicato solamente se la funzione RTE (Zona VistaKey B) viene abilitata nel prompt successivo. Se la zona VistaKey B viene utilizzata come zona non abbinata, l'opzione selezionata in questo prompt non influisce sul funzionamento del sistema.</p> <p>Premere 1 per azzerare il tempo allarme quando la funzione RTE viene attivata. In caso contrario premere 0.</p>
<p>↓ Cod. punto di accesso</p> <p>01 ABILITA RTE? ABILITAT 1</p>	<p>("01 RTE abilitato? - abilitato") Questo prompt permette di selezionare l'abilitazione (abbinato/utilizzato nel punto di accesso) o la disabilitazione (non abbinato/non utilizzato nel punto di accesso) della funzione RTE. Abilitando la funzione RTE, il modulo VistaKey è in grado di richiedere e/o autorizzare l'accesso mediante questo ingresso zona. Disabilitando la funzione RTE, questa zona non viene abbinata e, quindi, il modulo VistaKey non è in grado di autorizzare l'accesso mediante questa zona.</p> <p>N.B.: Il termine non abbinato significa che la zona VistaKey B non viene utilizzata per la funzioni RTE e quindi può essere utilizzata come le altre zone.</p> <p>Premere 1 per abilitare la funzione RTE. Premere 0 per disabilitare la funzione RTE.</p>

<p>↓ Cod. punto di accesso</p> <div style="border: 1px solid black; padding: 2px;"> <p>01 ELETTR. RTE ABILITAT. 1</p> </div>	<p>("01 serratura meccanica RTE - abilitata") Questo prompt permette di selezionare la risposta della funzione RTE (se abilitata nel prompt precedente): sblocco della serratura meccanica e inizio del tempo di uscita (1) oppure solamente inizio del tempo di uscita (0). L'impostazione tipo è 1. Questa opzione viene selezionata su 0 se la porta può essere sbloccata manualmente dall'interno (es. maniglia funzionante).</p> <p>N.B.: L'azionamento della serratura meccanica mediante RTE può essere applicato solamente se la funzione RTE (zona VistaKey B) è stata abilitata nel prompt precedente. Se la zona VistaKey B viene utilizzata come zona non abbinata, l'opzione selezionata in questo prompt non influisce sul funzionamento del sistema.</p> <p>Premere 0 per escludere lo sblocco della serratura meccanica mediante funzione RTE. Premere 1 per abilitare lo sblocco della serratura meccanica mediante funzione RTE.</p>
<p>↓ Cod. punto di accesso</p> <div style="border: 1px solid black; padding: 2px;"> <p>01 CONFIG GP NORM APERT 0</p> </div>	<p>("01 configurazione GP - normalmente aperto") Digitare il codice ad una cifra della configurazione della zona generica (zone VistaKey C). Questa zona permette di controllare l'armadietto del modulo VistaKey contro eventuali manomissioni. Le opzioni valide sono:</p> <ul style="list-style-type: none"> 0 = normalmente aperto 1 = normalmente chiuso 2 = Resistore di fine linea (EOL) normalmente aperto 3 = Resistore di fine linea (EOL) normalmente chiuso <p>Premere [*] per confermare.</p>
<p>↓ Cod. punto di accesso</p> <div style="border: 1px solid black; padding: 2px;"> <p>01 USC PREALLAR NON ABILITAT 0</p> </div>	<p>("01 uscita logica preallarme - non abilitata") Il prompt uscita logica preallarme permette di abilitare/disabilitare l'uscita logica preallarme. In caso di abilitazione, l'uscita logica viene attivata all'inizio del tempo di preallarme (vedere i prompt precedenti TEMPO DI PREALLARME e TEMPO ALLARME) e disattivata alla chiusura del punto di accesso. Questa uscita può essere utilizzata per l'allarme anomalia porta aperta.</p> <p>Premere 1 per abilitare l'uscita logica preallarme. Premere 0 per disabilitare l'uscita logica preallarme e quindi non abbinare l'uscita.</p>

↓ Cod. punto di accesso	
01 AZIONE USC	
NULLA	0

("01 modalità uscita logica - non utilizzata") Le modalità di funzionamento dell'uscita logica sono: "discreta", "impulso unico" oppure "sequenza". Selezionando "discreta", l'uscita viene attivata con un comando di attivazione e rimane attivata fino al ricevimento di un comando di disattivazione. Per esempio, quando una porta viene aperta e inizia un tempo allarme (porta aperta), l'uscita logica viene attivata e rimane attivata fino a chiusura della porta (ripristino porta aperta). Selezionando l'opzione "unico impulso", l'uscita logica viene attivata una sola volta in seguito ad un comando di attivazione, rimane attivata per un determinato tempo e poi viene disattivata. Selezionando l'opzione "sequenza", l'uscita alterna comandi di attivazione e disattivazione per un determinato tempo di attivazione e disattivazione, e fino a completamento del numero di cicli impostati. Se la selezione conteggio cicli è 0, la sequenza viene terminata da un comando di disattivazione. Selezionare un'opzione da 0 a 3 per determinare la modalità di azione dell'uscita logica.

- 0 = non utilizzata (selezionando 0, il sistema si sposta al prompt successivo GRUPPO DI ACCESSO).
- 1 = discreta (selezionando 1, il sistema si sposta al prompt successivo GRUPPO DI ACCESSO).
- 2 = impulso unico (selezionando 2, il sistema si sposta al prompt "TEMPO ATTIVAZIONE USCITA LOGICA").
- 3 = sequenza (selezionando 3, il sistema si sposta al prompt successivo "CONTEGGIO CICLI").

Premere [✱] per confermare.

↓ Cod. punto di accesso	
01 TRIG RPT CNT	
Continuous	0

("01 conteggio cicli - continuo") Digitare il codice ad una cifra del numero di cicli di attivazione/disattivazione generati dall'uscita logica. Selezionando 0, la sequenza viene terminata da un comando di disattivazione. Le opzioni valide sono:

- 0 = continuo
- 1 = 1 ciclo
- 2 = 2 cicli
- 3 = 3 cicli
- 4 = 4 cicli
- 5 = 5 cicli
- 6 = 10 cicli
- 7 = 25 cicli

Premere [✱] per confermare.

↓ Cod. punto di accesso	
01TRIG OFF TIME	
1s	0

("01 tempo di disattivazione - 1 sec") Digitare il codice ad una cifra del tempo in secondi durante il quale l'uscita logica rimane disattivata in caso di modalità selezionata su "sequenza". Questo tempo corrisponde al tempo di disattivazione (OFF) di una sequenza. Le opzioni valide sono:

- 0 = 1 sec.
- 1 = 2 sec.
- 2 = 3 sec.
- 3 = 4 sec.
- 4 = 5 sec.
- 5 = 10 sec.
- 6 = 15 sec.
- 7 = 30 sec.

Premere [✱] per confermare.

01 TRIG ON TIME 1s	0
-----------------------	---

("01 tempo di attivazione - 1 sec") Digitare il codice ad una cifra del tempo in secondi durante il quale l'uscita logica rimane attivata in caso di modalità selezionata su impulso unico. In caso di modalità selezionata su sequenza, questo tempo corrisponde al tempo di attivazione (ON) di una sequenza ciclica. Le opzioni valide sono:

0 = 1 sec.	4 = 10 sec.
1 = 2 sec.	5 = 30 sec.
2 = 3 sec.	6 = 1 min.
3 = 5 sec.	7 = 2 min.

Premere **[*]** per confermare.

GRP ACS? 1 2 3 4 5 6 7 8 (0-8) x x x x x x x x	
--	--

("Gruppi di accesso? 1 2 3 4 5 6 7 8 - selezionare 0-8") Questo prompt permette di selezionare i gruppi di accesso autorizzati ad accedere o uscire da un determinato punto di accesso quando il rispettivo gruppo di accesso viene abilitato in base ai parametri di programmazione. I titolari di scheda con privilegi esclusivi hanno accesso a tutti i punti di accesso indipendentemente dall'opzione selezionata in questo prompt. I titolari di scheda scaduta non hanno accesso ad alcun punto di accesso, indipendentemente dall'opzione selezionata in questo prompt.

Premere **0** per attivare/disattivare la selezione del punto di accesso; oppure premere i tasti **1-8** per attivare/disattivare la selezione ("x") del numero del gruppo di accesso.

Premere **[*]** per confermare.

CONFIG LET. WEIGAND	0
------------------------	---

("Configurazione lettore - Weigand") Le opzioni valide di questo prompt sono: 0 (Weigand) oppure 1 (orologio/dati). Il lettore ADEMCO è un lettore con configurazione (formato) Weigand.

Premere **0** per selezionare la configurazione Weigand.

Premere **[*]** per confermare.

↓ Cod. punto di accesso 01 MODO LET. Entr.	0
--	---

("Posizione lettore - ingresso") Selezionare la posizione del lettore come INGRESSO o USCITA. Quest'opzione è importante per la selezione degli EVENTI DI INGRESSO e degli EVENTI DI USCITA della funzione evento/azione in fase di programmazione dei gruppi di accesso e permette di determinare le modalità di registrazione e di segnalazione di eventi associati (es. Accesso autorizzato, uscita autorizzata).

Premere **0** oppure **1** per selezionare il lettore come lettore di ingresso (0) oppure come lettore di uscita (1).

Premere **[*]** per confermare.

Il sistema ritorna al prompt "ENTER ACS PT#" ("DIGITARE CODICE PUNTO DI ACCESSO").

Impostazione gruppi di accesso

I gruppi di accesso del modulo VistaKey vengono impostati nella modalità programmazione gruppi di accesso a cui si accede entrando nella funzione **#93 Programmazione modalità**

menu e tenendo premuto il tasto [0] fino a quando il display visualizza il prompt sotto indicato:

PGM GRP ACCESS 1=SI 0=NO	0
-----------------------------	---

("Programmazione gruppi di accesso - 1 = SI' 0 = NO")

Premere **1** oppure **0**.

Selezionare 1 per visualizzare il prompt sotto indicato.

Una volta completata la programmazione dei gruppi di accesso, premere **0**; il sistema d'allarme si sposta alla programmazione della funzione evento/azione.



In fase di abbinamento delle schede ad un nuovo gruppo di accesso, le schede devono essere attivate mediante l'abilitazione del nuovo gruppo di accesso (nel campo #77, programmazione parametri di tempo, ecc.)

GRUPPO ACCESSO 01-08, 00=ESCI	01
----------------------------------	----

("Gruppo di accesso - 01-08, 00 = per uscire") Digitare il codice gruppo da programmare da **01** a **08**, oppure **00** per uscire dalla programmazione gruppi di accesso.

Ogni titolare di scheda deve appartenere ad almeno 1 gruppo di accesso. Il gruppo di accesso attribuisce ai titolari di scheda determinati privilegi concessi a tutti i titolari dello stesso gruppo di accesso. Il titolare di scheda appartenente a più di un punto di accesso, gode di tutti i privilegi dei gruppi di accesso a cui appartiene. I gruppi di accesso determinano il punto(i) di accesso a cui il titolare ha accesso e gli orari in base alla programmazione impostata per il proprio gruppo di accesso.

Premere [*****] per confermare.

Selezionare un numero da 01 a 08 per visualizzare il prompt sotto indicato.

Una volta completata la programmazione dei gruppi di accesso, digitare **00**; il sistema si sposta alla programmazione della funzione evento/azione.

↓ Cod. gruppo di accesso 01 PRIV ESCL? NON ABILIT	0
---	---

("01 privilegi esclusivi? - non abilitati") Premere **1** per abilitare oppure **0** per disabilitare i privilegi esclusivi di un determinato gruppo.

Selezionando l'abilitazione dei privilegi esclusivi, tutti i titolari del gruppo hanno accesso da qualsiasi punto di accesso e hanno la facoltà di disinserire la partizione del punto di accesso (se inserita) in qualsiasi momento, indipendentemente dall'abilitazione del gruppo di accesso del titolare in base a parametri di programmazione o all'abilitazione del gruppo di accesso all'ingresso o all'uscita da qualsiasi punto di accesso. L'unico impedimento posto al diritto di accesso di un titolare con privilegi esclusivi è rappresentato dalla scheda scaduta per utilizzo o per data. In caso di disabilitazione dei privilegi esclusivi, l'ingresso da un determinato punto di accesso viene autorizzato solamente se il punto di accesso è stato programmato per accettare il gruppo di accesso del titolare della scheda (vedere il capitolo *Programmazione punto di accesso*); il gruppo di accesso viene abilitato al momento dell'inserimento della scheda (in base ai parametri, alla funzione evento/azione o in base al selettore dell'azione), digitando il PIN (codice+#73), oppure mediante trasmissione RF; E se la scheda non

è scaduta.

N.B.: I privilegi esclusivi di un gruppo di accesso non sono abilitati in caso di funzionamento del modulo VistaKey in modalità capacità ridotta (RCM). Quando il sistema è in modalità RCM, i privilegi descritto possono essere garantiti solamente se abbinati ad un titolare.

Premere [✱] per confermare.

↓ Cod. gruppo di accesso
01 Tracc?
NON ABILITAT 0

("01 traccia? - non abilitata") Premere **1** (traccia) oppure **0** (nessuna traccia) per determinare se i titolari di scheda del gruppo devono essere tracciati.

Selezionando l'abilitazione della funzione traccia, un determinato gruppo di accesso viene monitorato registrando gli ingressi e le uscite autorizzate o non autorizzate nel registro della centralina e/o inviando un report alla centrale operativa.

Premere [✱] per confermare.

↓ Cod. gruppo di accesso
01 Restr? 1 2 3 4 5 6 7 8
(0-8)

("01 limiti? 1 2 3 4 5 6 7 8 - selezionare 0-8") Premere **0** per attivare/disattivare la selezione della funzione limiti in modalità inserita delle partizioni VISTA; oppure premere i tasti **1-8** (VISTA-128FB) o **1-2** (VISTA-32FB) per attivare/disattivare la selezione ("x") dei codici partizione con funzione limiti in modalità inserita.

N.B.: Se la funzione limiti in modalità inserita della partizione è abilitata e la partizione è inserita, l'accesso del titolare di una scheda dai punti di accesso della partizione non viene autorizzato se sussistono le due condizioni sotto indicate:

1. La funzione limiti in modalità inserita delle partizioni dei gruppi di accesso a cui appartiene il titolare è abilitata e nessun gruppo di accesso ha privilegi esclusivi.
2. Il codice utente VISTA del titolare non è autorizzato all'accesso alla partizione.

Premere [✱] per confermare.

↓ Cod. gruppo di accesso
01 EVENTO ING?
Ness Richies 00

("01 evento di ingresso? - nessuna richiesta") Digitare il codice a due cifre dell'elenco sotto indicato corrispondente all'evento di ingresso con controllo accesso che genera l'azione desiderata. Le opzioni valide e le relative descrizioni sono:

- 00 Nessuna richiesta - l'evento di ingresso non genera nessuna azione.
- 02 Richiesta di accesso (Acs Req) - l'AZIONE DI INGRESSO viene generata dall'inserimento di una scheda nel lettore di ingresso.
- 04 Qualsiasi richiesta (Any Req) - l'AZIONE DI INGRESSO viene generata dall'inserimento di una scheda in un lettore di ingresso o di uscita.
- 05 Accesso autorizzato (Acs Grt) - l'AZIONE DI INGRESSO viene generata quando un lettore di ingresso autorizza l'ingresso.
- 07 Qualsiasi autorizzazione (Any Grt) - l'AZIONE DI INGRESSO viene generata quando un lettore di ingresso autorizza una qualsiasi richiesta.
- 08 Accesso non autorizzato (Acs Deny) - l'AZIONE DI INGRESSO viene generata quando un lettore di ingresso non autorizza un accesso.

10 qualsiasi azione non autorizzata (Any Deny) - l'AZIONE DI INGRESSO viene generata quando un lettore di ingresso non autorizza una qualsiasi richiesta.

N.B.: L'evento di ingresso selezionato è valido solamente quando la scheda inserita appartiene ad un membro di un gruppo di accesso già definito e la scheda viene inserita nel punto di accesso definito nel prompt sotto indicato.

Premere [✱] per confermare.

↓ Cod. gruppo di accesso	
01 PUNTO ACS (01-15)	01

("01 punto di accesso - (01-15)") Digitare il codice punto di accesso da 1 a 15 dell'evento di ingresso descritto sopra.

Premere [✱] per confermare.

↓ Cod. gruppo di accesso	
01 EVENTO ING? NESS.	00

("01 azione di ingresso - nessuna") Digitare il codice a due cifre dell'azione di ingresso desiderata. Le opzioni valide e le relative definizioni sono elencate nella *Tabella 5-1: Codici azione*; oppure digitare 00 corrispondente a "nessuna azione". Le condizioni sotto indicate si riferiscono all'azione di ingresso selezionata:

- L'azione si verifica solamente quando l'evento di ingresso descritto sopra si verifica nel punto di accesso selezionato e la scheda che genera l'evento è abbinata a quel determinato gruppo di accesso.
- Le azioni di inserimento o disinserimento delle partizioni vengono eseguite solamente se l'utente VISTA abbinato alla scheda è anche abbinato alla partizione selezionata.

N.B.: I codici azione 60 (punto di accesso solo uscita), 66 (punto di accesso gruppo solo uscita), oppure 72 (punto di accesso partizione solo uscita) disabilitano il lettore di ingresso del punto di accesso. Il lettore rimane disabilitato fino al ricevimento di un comando (comando tastiera o evento) che mette in sicurezza il punto di accesso.

Premere [✱] per confermare.

In base all'azione di ingresso selezionata, il sistema richiede ulteriori informazioni. Per esempio, selezionando **01** (relè attivo), il sistema richiede il codice relè. Selezionare l'opzione desiderata e premere [✱] per confermare.

↓ Cod. gruppo di accesso	
01 EVENTO USC?	
Ness Richies	00

("01 evento di uscita? nessuna richiesta") Digitare il codice evento di uscita controllo punto di accesso desiderato da 00 a 10. Le opzioni valide e le relative descrizioni sono:

- 00 Nessuna richiesta - l'evento di uscita non genera alcuna azione.
- 03 Richiesta di uscita (Acs Req) - l'AZIONE DI USCITA viene generata dall'inserimento di una scheda nel lettore di uscita.
- 04 Qualsiasi richiesta (Any Req) - l'AZIONE DI USCITA viene generata dall'inserimento di una scheda in un lettore di ingresso o di uscita.
- 06 Uscita autorizzata (Acs Grt) - l'AZIONE DI USCITA viene generata quando un lettore di uscita autorizza un accesso
- 07 Qualsiasi autorizzazione (Any Grt) - l'AZIONE DI USCITA viene generata quando il lettore di uscita autorizza una qualsiasi richiesta.
- 09 Uscita non autorizzata (Acs Deny) - l'AZIONE DI USCITA viene generata quando un lettore di uscita non autorizza un uscita.
- 10 Qualsiasi evento non autorizzato (Any Deny) - l'AZIONE DI USCITA viene generata quando un lettore di uscita non autorizza una qualsiasi richiesta.

N.B.: L'evento di uscita selezionato è valido solamente quando la scheda inserita appartiene ad un membro di un gruppo di accesso già definito e la scheda viene inserita nel punto di accesso definito nel prompt sotto indicato.

Premere **[*]** per confermare.

↓ Cod. gruppo di accesso	
01 PUNTO ACS	
(01-15)	01

("01 punto di accesso - (01-15)") Digitare il codice punto di accesso da 1 a 15 dell'evento di uscita descritto sopra.

Premere **[*]** per confermare.

↓ Cod. gruppo di accesso	
01 AZIONE USC?	
NESS	00

("01 azione di uscita - nessuna") Digitare il codice a due cifre dell'azione di uscita desiderata. Le opzioni valide e la relativa descrizione sono elencate nella *Tabella 5-1: Codici azione* descritta sopra, oppure digitare 00 per "nessuna azione". Le condizioni sotto indicate si riferiscono all'azione di uscita selezionata:

- L'azione si verifica solamente quando l'evento di uscita descritto sopra si verifica nel punto di accesso selezionato e la scheda che genera l'evento è abbinata a quel determinato gruppo di accesso.
- Le azioni di inserimento o disinserimento delle partizioni vengono eseguite solamente se l'utente VISTA abbinato alla scheda è anche abbinato alla partizione selezionata.

N.B.: I codici azione 60 (punto di accesso solo uscita), 66 (punto di accesso gruppo solo uscita) oppure 72 (punto di accesso partizione solo uscita) disabilitano il lettore di ingresso del punto di accesso. Il lettore rimane disabilitato fino al ricevimento di un comando (comando tastiera o evento) che mette in sicurezza il punto di accesso

Premere **[*]** per confermare.

In base all'azione di uscita selezionata, il sistema richiede ulteriori informazioni. Per esempio, selezionando **01** (relè attivo), il sistema

richiede il codice relè. Selezionare l'opzione desiderata e premere [✱] per confermare.

Il programma ritorna al prompt "Access Group" ("Gruppo di accesso") per la programmazione di un altro gruppo di accesso.

N.B.:

- Gli utenti vengono abbinati al gruppo(i) di accesso successivamente nell'ambito del paragrafo *Funzioni scheda controllo accesso del Capitolo 6: Comandi utente*.
- Per attivare i nuovi gruppi di accesso definiti, eseguire le procedure di abilitazione uscendo dalla modalità #93 programmazione modalità menu; fare riferimento al paragrafo successivo *Abilitazione gruppi di accesso* di questo capitolo.

Programmazione funzione evento/azione

La funzione evento/azione permette di generare un'azione al verificarsi di un evento. Per esempio, l'accensione di una luce (mediante relè) quando il sistema autorizza l'accesso (accesso autorizzato).

La funzione evento/azione del modulo VistaKey viene impostata nella programmazione funzione evento/azione a cui si accede entrando nella modalità **#93 Programmazione modalità menu**. Tenere premuto il tasto [0] fino a quando il display visualizza il prompt sotto indicato.

EVENT/AZIONE PGM 1=SI 0=NO	0
-------------------------------	---

("Programmazione funzione evento/azione - 1 = SI' 0 = NO").
Premere **1** oppure **0**.

Selezionare 1 per visualizzare il prompt sotto indicato.

N.B.: Prima di entrare nella programmazione funzione evento/azione, completare le procedure ed il foglio di programmazione del paragrafo *Foglio di programmazione funzione evento/azione* di questo capitolo. Le opzioni da selezionare vengono rilevata dal foglio di programmazione.

Selezionare 0 per spostarsi al prompt uscita programmazione modalità menu.

Event/Azione n# (01-32), 00=ESCI	01
-------------------------------------	----

("Codice funzione evento/azione - (01-32), 00 = per uscire") Digitare il codice evento/azione da programmare da **01** a **32**, in base al foglio di programmazione funzione evento/azione; oppure **00** per uscire dalla programmazione della funzione evento/azione.

Premere [**✱**] per confermare.

Digitare un numero da 01 a 32 per visualizzare il prompt sotto indicato.

Digitare 00 per spostarsi al prompt uscita programmazione.

↓ Cod. evento/azione 01 EVENT ACS?	00
---------------------------------------	----

("01 evento di accesso? - nessuno") Digitare il codice a due cifre dell'evento nella colonna codice evento del foglio di programmazione. Le opzioni valide sono suddivise in 6 diverse categorie e sono:

Identificatori partizione

<u>Cod.</u>	<u>Descrizione</u>	<u>Cod.</u>	<u>Descrizione</u>
00	Nessuno (non utilizzato)	09	Coercizione part.
01	Inserimento part.	10	Ripristino coercizione part.
02	Disinserimento part.	11	Anomalia part.
03	Incendio partizione	12	Ripristino anomalia part.
04	Ripristino incendio part.	13	Esclusione part.
05	Effrazione part.	14	Ripristino esclusione part.
06	Ripristino effrazione part. ritardato part.	15	Disinserimento
07	Allarme part.	16	Inserimento anticipato part.
08	Ripristino allarme part. partizione	17	Errore inserimento

Identificatori utente

<u>Cod.</u>	<u>Descrizione</u>	<u>Cod.</u>	<u>Descrizione</u>
18	Inserimento utente	20	Autorizzazione utente
19	Disinserimento utente		

Identificatori codice scheda

<u>Cod.</u>	<u>Descrizione</u>
21	Scheda autorizzata

Identificatore punto di accesso (PA)

<u>Cod.</u>	<u>Descrizione</u>	<u>Cod.</u>	<u>Descrizione</u>
22	PA autorizzato	30	Autorizzazione coercizione
23	PA non autorizzazione aperta	31	Allarme anomalia porta
24	PA escluso porta	32	Ripristino all. anomalia aperta porta
26	PA bloccato	33	Porta forzata
27	PA protetto	34	Ripristino porta forzata
29	PA autorizzato con comando manuale		

Identificatori codici zona

<u>Cod.</u>	<u>Descrizione</u>	<u>Cod.</u>	<u>Descrizione</u>
35	Incendio zona	40	Ripristino allarme zona
36	Ripristino incendio zona	41	Anomalia zona
37	Effrazione zona	42	Ripristino anomalia zona
38	Ripristino effrazione zona	43	Esclusione zona
39	Allarme zona	44	Ripristino esclusione zona

Identificatori inserimento

<u>Cod.</u>	<u>Descrizione</u>	<u>Cod.</u>	<u>Descrizione</u>
45	Ins. Parziale part.	49	Ins. Parziale utente
46	Ins. Totale part.	50	Ins. Totale utente
47	Ins. Istantaneo part.	51	Ins. Istantaneo utente
48	Ins. Massimo part.	52	Ins. Massimo utente

Premere [✱] per confermare.

In base al codice evento selezionato, il sistema richiede ulteriori informazioni. Per esempio, selezionando **01** (inserimento partizione), il sistema richiede il codice partizione. Selezionare l'opzione desiderata e premere [✱] per confermare.

↓ Cod. evento/azione	
01 AZIONE?	
NULLA	00

("01 azione? - nessuna") Digitare il codice azione del foglio di programmazione, che corrisponde all'azione generata al verificarsi dell'evento entro la fascia oraria e nei giorni selezionati.

Premere [✱] per confermare.

In base all'azione selezionata, il sistema richiede ulteriori informazioni. Selezionare l'opzione desiderata e premere [✱] per confermare.

↓ Cod. evento/azione	
01 FASCIA ORARIA ?	
SEMPRE ATTIVO	00

("01 fascia oraria? - sempre attiva") Digitare il codice a due cifre della fascia oraria definita nel foglio di programmazione (00 = sempre attiva, 01-20 = cod. fascia oraria). Questo codice corrisponde alla fascia oraria entro la quale si verifica l'azione. Selezionando 00 (sempre attiva), l'azione viene generata ogni volta che si verifica l'evento. Negli altri casi, l'azione viene generata solo se l'evento si verifica entro la fascia oraria e nei giorni selezionati.

Premere [✱] per confermare.

GIORNI? LMMGVSDF (0-8)

("Giorni? LMMGVSDV - selezionare 0-8") Premere **0** per attivare/disattivare la selezione di tutti i giorni; oppure premere i tasti **1-8** per attivare/disattivare la selezione ("x") dei singoli giorni (Lunedì = 1, Vacanza = V = 8).

N.B.: Selezionando vacanza, la selezione dei giorni della settimana non viene presa in considerazione (es. l'azione viene generata selezionando Vacanza anche quando la vacanza cade di sabato e sabato non è selezionato).

Premere **[*]** per confermare.

Il sistema ritorna al prompt "Event/Action#" ("codice evento/azione") per la programmazione di altre funzioni evento/azione.

Uscire dalla modalità #93 programmazione modalità menu

USCIRE DAL MENU? 1=SI 0=No	0
-------------------------------	---

("Uscire modalità menu? - 1 = sì 0 = no") Premere **1** per uscire oppure **0** per ritornare al prompt "PROG ZONA.?" ("PROGRAMMAZIONE ZONA?").

Programmazione eventi temporizzati

Gli eventi temporizzati permettono di generare un'azione in base al tempo e vengono programmati nella modalità #80 menu di programmazione parametri del sistema di allarme. Per programmare gli eventi temporizzati, seguire le procedure descritte precedentemente al paragrafo "Foglio di programmazione eventi temporizzati" di questo capitolo e le procedure descritte nel manuale di installazione e predisposizione del sistema di allarme:

1. Determinare le nuove fasce orarie utilizzate dagli eventi temporizzati selezionati.
2. Inserire le informazioni contenute nel foglio di programmazione degli eventi temporizzati alla fine del capitolo.

Abilitazione gruppi di accesso

I nuovi gruppi di accesso inseriti nel sistema devono essere abilitati utilizzando eventi temporizzati oppure mediante il comando #77. Per abilitare il gruppo di accesso mediante eventi temporizzati, completare il foglio di programmazione eventi temporizzati (vedere il paragrafo *Foglio di programmazione eventi temporizzati* di questo capitolo) e fare riferimento al paragrafo precedente *"Programmazione eventi temporizzati"*. Se, invece, si utilizza il comando #77, procedere come sotto indicato:

1. Digitare **codice installatore + #77**.
2. Digitare il codice azione 77 (per abilitare i gruppi di accesso).
3. Digitare il codice gruppo di accesso.
4. Uscire.

Altre funzioni del sistema

I paragrafi sotto indicati contengono informazioni sulla personalizzazione del funzionamento del modulo VistaKey/sistema di allarme ed alcune considerazioni sull'installazione e la programmazione.

Uscita momentanea dal punto di accesso

Il sistema è dotato di una funzione che permette di trasformare momentaneamente (15 secondi) un lettore di ingresso in lettore di uscita. Questa funzione permette all'utente o al

gruppo di accesso di eseguire operazioni quali l'inserimento del sistema mediante inserimento della scheda nel lettore in uscita dai locali. Per utilizzare questa funzione, è necessario collegare un commutatore ad una zona disponibile e programmare il sistema per attivare momentaneamente la funzione di uscita. Seguire le procedure sotto indicate:

1. Collegare il commutatore ad una zona disponibile. Configurare i collegamenti in modo che la zona venga cortocircuitata quando il commutatore viene attivato. Installare il commutatore in una posizione non facilmente accessibile a tutti gli utenti che entrano o escono dall'edificio oppure utilizzare un commutatore a chiave.
2. Per programmare la funzione di uscita momentanea nella centralina VISTA, entrare nella modalità **#93 Programmazione modalità menu** del sistema di allarme in base alle procedure descritte nel manuale del sistema di allarme. Il display visualizza il prompt sotto indicato:

PROG ZONA? 1=SI 0=NO

("Programmazione zona? 1 = SI' 0 = NO") Premere **1** per entrare nella programmazione zona. Il display visualizza il prompt sotto indicato.

N.B.: Premere [**✳**] per visualizzare il prompt successivo in fase di programmazione. Premere [**#**] per visualizzare il prompt precedente.

INS PER CONFER? 1=SI 0=NO

("Confermi? 1=SI' 0 = NO") Questo prompt permette di confermare il numero di serie del dispositivo RF e del dispositivo del circuito polling. In fase di programmazione della funzione uscita momentanea, l'opzione selezionata in questo prompt non influisce sulla programmazione. Premere **1** oppure **0**. Il display visualizza il prompt sotto indicato.

DIGITA NR ZONA.? 000 = ESCI 008

Zona 008 selezionata ↑

("Digitare codice zona? - 000 = PER USCIRE") Digitare il codice zona a tre cifre della zona VistaKey da programmare. L'esempio indica il codice 008.

Premere [**✳**] per confermare. Il sistema si sposta al prompt riassuntivo sotto indicato.

008 ZT P RC B IN L 00 _ _ _ _ _

Il display visualizza il prompt riassuntivo della zona programmata. ZT = tipo zona, P = partizione, RC = codice report, B = abbinamento sirena/relè ausiliario di zona, IN = tipo di ingresso del dispositivo e L = numero loop del dispositivo al quale è collegato il sensore. Alcuni dispositivi sono in grado di gestire più di una zona grazie a loop singoli. In caso di zona non programmata, il display visualizza il prompt come indicato.

Premere [**✳**] per continuare.

008 TIPO ZONA

("008 tipo zona") Premere **29** per la funzione di uscita momentanea.

Premere [**✳**] per confermare e continuare.

008 PORTA NR (01-15) 3	<p>("008 punto di accesso - (01-15)") Digitare il codice porta a due cifre (01-15) del modulo VistaKey. N.B.: L'opzione selezionata in questo prompt deve corrispondere all'indirizzo impostato nel modulo VistaKey come porta (punto di accesso) da programmare. Premere [★] per continuare.</p>
008 Entry or Exit Entry 0	<p>("008 ingresso o uscita - ingresso") Premere sempre 1 per selezionare uscita. Questo prompt è standard e permette di programmare i punti di accesso; non selezionare mai 0 (ingresso) quando si deve programmare la zona di uscita momentanea. Premere [★] per continuare.</p>
008 SETTORE 2	<p>("008 partizione") Digitare il codice partizione al quale è assegnato il punto di accesso. Premere [★] per continuare.</p>
008 CODICE TRAS 1 st 03 2 nd 12 3C	<p>("008 codice report - 1° 03 2° 12") L'opzione selezionate in questo prompt in fase di programmazione della funzione di uscita momentanea non influisce sul funzionamento. Tenere premuto [★] per visualizzare il prompt TIPO SENSORE (TIPO INGRESSO).</p>
008 TIPO SENSORE Hardwire 01	<p>("008 tipo ingresso - zona cablata") Digitare il tipo ingresso zona. In questo esempio, la zona 8 corrisponde alla zona cablata. Premere [★] per continuare.</p>
008 ZT P RC IN L 29 2 80 HW 1	<p>Il display visualizza il prompt riassuntivo della zona. Premere per confermare la programmazione della zona. Il sistema ritorna al prompt "DIGITA NR ZONA." ("DIGITARE COD ZONA"). Digitare "000" e premere [★] per uscire dalla programmazione zone.</p>

3. Uscire dalla modalità #93 programmazione modalità menu.
4. L'azione che deve essere eseguita in caso di uscita può essere abbinata ad un gruppo di accesso o a un titolare di scheda. Per abbinare ad un gruppo di accesso l'azione in caso di uscita, seguire le procedure del punto **a.**, mentre per abbinare l'azione ad un titolare, seguire le procedure del punto **b.**
 - a. Per abbinare ad un gruppo di accesso l'azione in caso di uscita, seguire le procedure del paragrafo precedente "Impostazione gruppi di accesso". Per l'impostazione dei gruppi di accesso, osservare quanto segue:
 - Nel prompt "Exit Event?" (evento di uscita?), digitare 06 corrispondente ad uscita autorizzata.
 - Nel prompt "Access Point?" (punto di accesso?), specificare il punto di accesso che deve autorizzare l'uscita.
 - Nel prompt "Exit Action?" (azione di uscita?), digitare il codice dell'azione di uscita desiderata (per esempio 21 per inserimento totale). La lista dei codici azione è riportata nella *Tabella 5-1: Codici azione*. Le condizioni sotto indicate si riferiscono all'azione di uscita selezionata:

L'azione si verifica solamente se l'evento di uscita sopra indicato si verifica nel punto di acceso selezionato e la scheda che genera l'evento è abbinata al gruppo di accesso programmato.

Le azioni di inserimento e disinserimento delle partizioni vengono eseguite solamente se l'utente VISTA abbinato alla scheda è anche abbinato alla partizione selezionata

Le azioni di accesso autorizzato da un punto di accesso vengono eseguite solamente se la scheda ha accesso a quei punti di accesso.

Le azioni di modifica dello stato (escluso, bloccato, protetto, solo uscita) dei punti di accesso vengono eseguite solamente se l'utente VISTA abbinato alla scheda è abbinato alla partizione a cui appartiene il punto di accesso.

b. Per abbinare l'azione in caso di uscita ad un titolare di scheda, seguire le procedure del paragrafo successivo “Funzioni scheda controllo accesso” nel *Capitolo 6: Comandi tastiera*. Per l'impostazione del titolare della scheda, osservare quanto segue:

- Nel prompt “ACS Event?” (evento di accesso?), digitare 06 corrispondente ad uscita autorizzata.
- Nel prompt “Access Point?” (punto di accesso?), specificare il punto di accesso che deve autorizzare l'uscita.
- Nel prompt “Action?” (azione?), digitare il codice dell'azione di uscita desiderata. (per esempio 21 per inserimento totale). L'elenco dei codici azione è riportato nella *Tabella 5-1: Codici azione*. Se la selezione dell'azione richiede la partizione o altri identificatori, il display visualizza un prompt di richiesta. Le condizioni sotto indicate si riferiscono all'azione di uscita selezionata:

Le azioni di inserimento e disinserimento delle partizioni vengono eseguite solamente se l'utente VISTA abbinato alla scheda è anche abbinato alla partizione selezionata

Le azioni di autorizzazione accesso da un punto di accesso vengono eseguite solamente se la scheda ha accesso a quei punti di accesso.

Le azioni di modifica dello stato (escluso, bloccato, protetto, solo uscita) dei punti di accesso vengono eseguite solamente se l'utente VISTA abbinato alla scheda è abbinato alla partizione a cui è abbinato il punto di accesso.

Il sistema è stato impostato con la funzione uscita momentanea secondo la quale l'azione selezionata viene eseguita quando il gruppo o il titolare esce. Per utilizzare questa funzione, il membro del gruppo di accesso o il titolare devono attivare il commutatore per trasformare il lettore del punto di accesso in lettore di uscita per 15 secondi. Durante questo tempo, l'inserimento della scheda genera l'azione di uscita.

Abilitazione combinatori di accesso

In caso di installazione del modulo VistaKey in un sistema di allarme, i valori di default del sistema vengono impostati in modo che i report delle categorie di eventi sotto indicate non vengano inviati alla centrale operativa:

- Anomalie ACS
- Esclusione ACS
- Sistema ACS (ripristino modulo, test ingresso/uscita)
- Allarmi ACS
- Traccia ACS (Per inviare un report di traccia, il gruppo di accesso o il titolare con funzione traccia devono essere attivati)

N.B.: Per l'elenco degli eventi e dei codici report di ogni categoria, fare riferimento al *Capitolo 8: Registro eventi*.

I valori di default del sistema possono essere modificati e quindi impostati per inviare report di una o di tutte le categorie di eventi. Per modificare i valori di default, entrare in **modalità programmazione campi dati** seguendo le procedure del manuale del sistema di allarme. Il display visualizza:

Programmazione * Prog # Vedi -00	("Modalità programmazione - * inserisci # visualizza - -00")
-------------------------------------	--

Premere ***94**. Il display visualizza:

Programmazione * Prog # Vedi 100	("Modalità programmazione - * inserisci # visualizza - 100")
-------------------------------------	--

Premere ***35**. Il display visualizza:

ACS Dlr Enables 135	("Abilitazione combinatori di accesso") Digitare 6 cifre. Le opzioni valide sono:
------------------------	---

ORDINE DI INSERIMENTO	EVENTO	OPZIONE
1	Traccia ACS	Premere sempre 1 per inviare i report di traccia. Premere 0 per non inviare i report.
2	ANOMALIE ACS	Premere 1 per inviare oppure 0 per non inviare i report anomalia ACS.
3	ESCLUSIONE ACS	Premere 1 per inviare oppure 0 per non inviare i report esclusione ACS.
4	Riservato	Premere 1 oppure 0 . Questo valore ha funzione di segnaposto nella sequenza delle 6 cifre.
5	ACS SISTEMA	Premere 1 per inviare oppure 0 per non inviare i report ACS sistema.
6	ALLARMI ACS	Premere 1 per inviare oppure 0 per non inviare i report allarmi ACS.

La tastiera emette tre bip dopo la digitazione della sesta cifra.

Premere **[*]**. Il display visualizza il prompt sotto indicato.

Digit Indir Prog 1	("Aprire campo di inserimento") Premere #99 . Il display visualizza il prompt sotto indicato.
-----------------------	--

Program Mode * Prog # Vedi -00	("Modalità programmazione - * inserisci # visualizza - -00")
-----------------------------------	--

Premere ancora **#99** per terminare la modalità programmazione campi dati.

Comando #73 di abilitazione accesso

Il comando #73 permette (se programmato) di autorizzare l'ingresso o l'uscita da un punto di accesso della partizione collegato alla tastiera. Il punto di accesso viene automaticamente bloccato allo scadere dell'intervallo di tempo impostato precedentemente come tempo porta aperta. Il funzionamento del comando #73 richiede l'esistenza delle condizioni sotto indicate:

- La tastiera deve essere collegata alla partizione in cui si trova il punto di accesso.
- Se la partizione è inserita e la modalità limiti in modalità inserita è attiva, l'utente deve essere autorizzato per poter disinserire la partizione.
- L'utente deve essere abbinato alla partizione. In caso contrario, l'utente non viene riconosciuto.
- L'utente deve essere abbinato ad una scheda con diritto di accesso al punto specificato.

- L'utente deve essere abilitato all'accesso alla partizione nell'orario in cui viene dato il comando.

Per abilitare questa funzione, entrare nella modalità **#93 Programmazione modalità menu** del sistema di allarme in base alle procedure del relativo manuale. Il display visualizza il prompt sotto indicato:

PROG ZONA? 1=SI 0=NO	("Programmazione zona? 1 = SI' 0 = NO") Premere 1 per entrare in programmazione zona. Il display visualizza il prompt sotto indicato. N.B.: Premere [★] per visualizzare il prompt successivo in fase di programmazione. Premere [#] per visualizzare il prompt precedente.
INS PER CONFER? 1=SI 0=NO	("Confermi? - 1 = SI' 0 = NO") Questo prompt permette di confermare i numeri di serie dei dispositivi RF e del circuito polling. In fase di programmazione della funzione #73, l'opzione selezionata in questo prompt non influisce sulla programmazione. Premere 1 oppure 0 . Il display visualizza il prompt sotto indicato.
DIGITA NR ZONA? 000 = ESCI 025 Zona 025 selezionata ↑	("Digitare codice zona? - 000 = PER USCIRE") Digitare il codice zona a tre cifre della zona da programmare per confermare un comando punto di accesso. L'esempio indica 025. Premere [★] per confermare. Il sistema si sposta al prompt riassuntivo sotto indicato.
025 ZT P RC B IN L 00 _ _ _ _ _	Il display visualizza il prompt riassuntivo della zona programmata. ZT = tipo zona, P = partizione, RC = codice report, B = abbinamento sirena/relè aux della zona, IN = tipo ingresso del dispositivo e L = numero loop del dispositivo a cui è collegato il sensore. Alcuni dispositivi sono in grado di gestire più di una zona grazie a loop singoli. In caso di zona non programmata, il display visualizza il prompt come indicato. Premere [★] per continuare.
025 TIPO ZONA	("025 tipo zona") Premere 27 per il punto di accesso. Premere [★] per confermare e continuare.
025 PORTA NR (01-31) 00	("025 punto di accesso - (01-31)") Digitare il codice porta a due cifre (01-15) del modulo VistaKey. N.B.: L'opzione selezionata in questo prompt deve corrispondere all'indirizzo impostato nel modulo VistaKey per la porta (punto di accesso) da programmare. Premere [★] per continuare.

025 Entrata o Usc Entry 0	("025 ingresso o uscita - ingresso") Premere 0 per selezionare ingresso oppure 1 per selezionare uscita. L'opzione selezionata deve corrispondere (ingresso o uscita) al punto di accesso a cui si accede e determina l'evento che si vuole registrare e segnalare; quindi , selezionare ingresso per un punto di ingresso e uscita per un punto di uscita. Premere [✱] per continuare.
025 SETTORE 1	("025 partizione") Digitare il codice partizione a cui è abbinato il punto di accesso. Premere [✱] per continuare.
025 CODICE TRAS 1 st 01 2 nd 00 10	("025 codice report - 1° 01 2° 00") L'opzione selezionata in questo prompt, in fase di programmazione del comando #73, non altera il funzionamento del sistema. Tenere premuto [✱] per visualizzare il prompt "TIPO SENSORE" (TIPO INGRESSO).
025 TIPO SENSORE None 00	("025 tipo ingresso - nessuno") Digitare il tipo ingresso zona come 09 per selezionare la tastiera. Premere [✱] per continuare.
025 Cons ECP Addr (00-30) 00	("025 indirizzo ECP tastiera - (00-30)") Digitare l'indirizzo ECP della tastiera a due cifre. Premere [✱] per continuare.
025 ZT P RC IN L 27 1 10 CS 1	Il display visualizza il prompt riassuntivo della zona. Premere [✱] per confermare la programmazione dalla zona. Il sistema ritorna al prompt "DIGITA NR ZONA"(DIGITARE COD ZONA). Digitare "000" e premere [✱] per uscire dalla programmazione zone. Uscire dalla modalità #93 programmazione modalità menu.

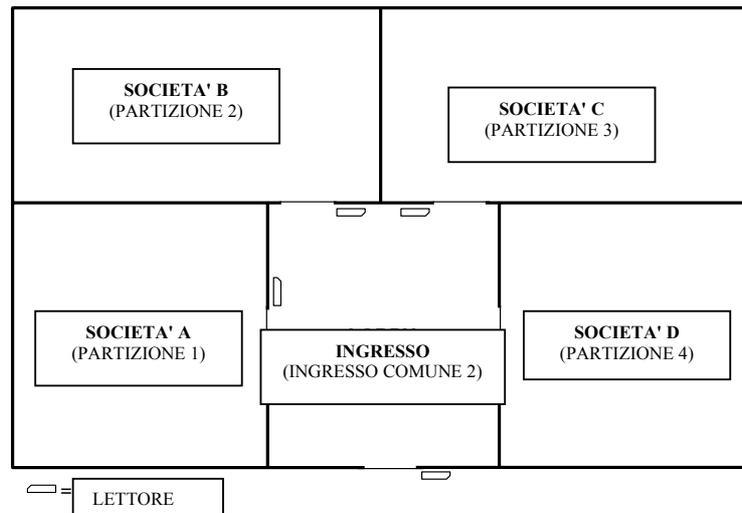
Il sistema è stato programmato in modo che il punto di accesso programmato venga sbloccato dal comando #73 sulla tastiera azionato da un utente autorizzato.

Livelli di autorità del sistema di allarme

La revisione dei livelli di autorità assegnati agli utenti del sistema assume grande importanza quando un modulo VistaKey viene installato in un sistema di allarme. Il livello installatore (livello di autorità 0) e il livello master (livello autorità 1) possono:

- Registrare nuove schede nel sistema
- Inviare i comandi di azione indicati nell'elenco della *Tabella 5-1: Codici azione*

Per esempio, se l'edificio ospita tre diverse società (vedere schema sotto) e ogni società ha un utente con livello master, questo utente è in grado di abbinare anche le schede delle altre società e/o controllare i loro punti di accesso inviando comandi di azione. Conseguentemente, il livello massimo assegnato ad ogni società sarà il livello manager (livello di autorità 2); il livello master deve essere assegnato solamente all'utente responsabile della sicurezza dell'intero edificio.



Rimozione modulo VistaKey

Il modulo VistaKey può essere rimosso (cancellato) dal database del sistema di allarme seguendo la procedura sotto indicata:

1. Entrare in modalità programmazione zona.
2. Spostarsi sui codici zona a cui sono abbinate le zone DSM, DSMB, RTE e GP.
3. Impostare il tipo ingresso zona come "none" (nessuno) oppure impostare il tipo risposta zona come "none" (nessuno) e selezionare l'opzione "SI" (si) nel prompt "Delete Zone?" ("Cancellare zona?"). Questa procedura cancella tutti i parametri di zona.

Foglio di programmazione eventi temporizzati

Cod. evento temporizzato	Cod. azione	Nome azione	Identificatore azione	Fascia oraria	Tempo di attivazione	Giorni							
						L	M	M	G	V	S	D	V
1													
2													
3													
4													
5													
6													
7													
8													
9													
10													
11													
12													
13													
14													
15													
16													
17													
18													
19													
20													

Foglio di programmazione funzione evento/azione

Evento	Cod. evento	Nome evento	Identificatore evento	Cod. azione	Azione desiderata	Identificatore azione	Fascia oraria (00= sempre, 01-20 = cod. fascia oraria)	Giorni									
								L	M	M	G	V	S	D	V		
1																	
2																	
3																	
4																	
5																	
6																	
7																	
8																	
9																	
10																	
11																	
12																	
13																	
14																	
15																	
16																	
17																	
18																	
19																	
20																	
21																	
22																	
23																	
24																	
25																	
26																	
27																	
28																	
29																	
30																	
31																	
32																	

Comandi tastiera

Contenuto

- ◆ Informazioni generali
- ◆ Altri comandi tastiera
- ◆ Comando #77 controllo dispositivi di uscita
- ◆ Comando #78 test controllo accesso
- ◆ Comando #80 controllo parametri
- ◆ Funzioni scheda controllo accesso

Informazioni generali

Installando il modulo VistaKey in un sistema di allarme, l'utente del sistema di allarme dispone di un numero maggiore di comandi ed è in grado di controllare il database delle schede di accesso. Questo capitolo riguarda i comandi tastiera aggiuntivi e le istruzioni per eseguire le funzioni di gestione delle schede di controllo accesso.

Comandi tastiera aggiuntivi

I comandi sotto indicati permettono di controllare i punti di accesso, collaudare il sistema di accesso e/o controllare i titolari delle schede.

Tipo comando	Comando	Descrizione
Controllo accesso	Codice utente + # + 73	Richiesta di ingresso/uscita (accettata solo in caso di partizione utente autorizzata)
	Codice utente + # + 74 + codice punto di accesso + Ingresso o Uscita	Richiesta di ingresso/uscita dal punto di accesso (accettata solo in caso di partizione utente autorizzata)
	Codice utente + # + 75 + codice punto di accesso + comando porta	Modifica dello stato del punto di accesso - attivazione autorizzato/protetto/escluso (accettata solo in caso di partizione utente autorizzata)
	Codice utente + # + 79	Esecuzione funzioni scheda di controllo accesso
Controllo dispositivi di uscita	Codice utente + # + 77	Attivazione di tutte le azioni
Test controllo accesso	Codice utente + # + 78 + comando di autorizzazione	Esecuzione del test di controllo accesso utilizzando le schede del database o tutte le schede
Comandi programmazione parametri	Codice utente + # + 80 + fascia oraria, parametri aperto/chiuso, vacanze, eventi temporizzati o parametri di accesso	Creazione o redazione di fasce orarie, parametri aperto/chiuso, vacanze, eventi temporizzati e/o parametri di accesso

I livelli di autorità utente sotto indicati sono in grado di utilizzare i comandi sopra descritti come segue:

Livello di autorità	Definizione	Comandi						
		#73	#74	#75	#77	#78	#79	#80
	Installatore	X	X	X	X	X	X	X
1	Master	X	X	X	X		X	X
2	Manager	X	X	X				

3	Operatore A	X	X					
4	Operatore B	X	X					
5	Operatore C	X	X					
6	Coercizione	X	X					

Per la descrizione completa dei comandi, fare riferimento ai paragrafi sotto indicati.

Controllo accesso

I comandi di controllo accesso permettono di controllare direttamente i punti di accesso oppure di inserire, rimuovere oppure redigere le schede nel database dei titolari di scheda. I comandi di controllo accesso vengono utilizzati come segue:

Comando #73

Il comando #73 (se programmato sulla tastiera) permette di autorizzare l'ingresso o l'uscita da un punto di accesso della partizione collegata alla tastiera. Il punto di accesso ritorna in modalità bloccato automaticamente allo scadere dell'intervallo di tempo impostato nella programmazione del sistema. Il comando #73 è attivo se sussistono le condizioni sotto indicate:

- La tastiera deve essere collegata alla partizione in cui si trova il punto di accesso.
- L'utente deve essere autorizzato per poter disinserire una partizione inserita e con funzione limiti in modalità inserita attiva.
- L'utente deve essere abilitato all'accesso alla partizione nell'orario in cui viene dato il comando.
- Il codice utente VISTA deve essere assegnato ad una scheda abbinata ad un gruppo di accesso che include il punto e la partizione in cui viene utilizzata la tastiera.
- La richiesta non viene autorizzata se il gruppo di accesso, che permette all'utente di accedere da un punto, è disabilitato.
- Il comando deve essere stato abilitato con la procedura descritta nel *Capitolo 5: Programmazione*.

Digitare il comando #73 come segue:

Codice utente + # + 73

Il punto di accesso rimane sbloccato per il periodo di tempo definito in fase di programmazione del sistema.

Comando #74

Il comando #74 permette di autorizzare l'ingresso o l'uscita da tutti i punti di accesso. Il punto di accesso ritorna automaticamente in modalità bloccato allo scadere dell'intervallo di tempo impostato in fase di programmazione del sistema. Il comando #74 è attivo se sussistono le condizioni sotto indicate.

- L'utente deve essere autorizzato per poter disinserire una partizione inserita e con funzione limiti in modalità inserita attiva.
- Il codice utente VISTA deve essere abbinato alla partizione a cui appartiene la tastiera.
- Il codice utente VISTA deve essere abbinato ad una scheda abbinata ad un gruppo di accesso che include il punto in cui viene richiesto l'accesso.
- Per ottenere l'autorizzazione di accesso, il codice utente VISTA non deve essere necessariamente abbinato alla partizione a cui appartiene il punto di accesso, ma se il codice utente non è abbinato alla partizione, l'accesso non viene autorizzato con partizione inserita e funzione limiti in modalità inserita programmata.

Digitare il comando #74 come segue:

Codice utente + # + 74

Il display visualizza il prompt sotto indicato:

PUNTO ACS	01
00-31	

("Punto di accesso -00-31") Digitare il codice a due cifre (da 01 a 15) del punto di accesso in cui si richiede l'autorizzazione di ingresso o di uscita.

N.B.: In caso di modulo VistaKey, le opzioni da 16 a 31 non sono valide e quindi non generano alcuna azione.

Premere [✱] per confermare. Il display visualizza il prompt sotto indicato:

ENTRATA o USC	0
Entry	

("Ingresso o uscita - ingresso") Digitare **0** per selezionare ingresso oppure **1** per selezionare uscita. Il punto di accesso rimane sbloccato per l'intervallo di tempo impostato in fase di programmazione nei prompt "Door Open Time" ("Tempo porta aperta") e "Relatch" ("Blocco porta").

Comando #75

Il comando #75 permette di modificare lo stato (autorizzato, escluso o protetto) dei punti di accesso. Il comando #75 è attivo se sussistono le condizioni sotto indicate.

- L'utente deve essere autorizzato per poter disinserire una partizione inserita e con funzione limiti in modalità inserita attiva.
- Il livello assegnato all'utente deve essere installatore, master o manager.
- Per mettere in sicurezza o escludere il punto di accesso, l'utente deve essere abbinato alla partizione del punto di accesso.
- Il codice utente VISTA deve essere abbinato alla partizione a cui appartiene la tastiera.
- Il codice utente VISTA deve essere abbinato ad una scheda abbinata ad un gruppo di accesso che include il punto in cui viene richiesto l'accesso.
- Per ottenere l'autorizzazione di accesso, il codice utente VISTA non deve essere necessariamente abbinato alla partizione a cui appartiene il punto di accesso, ma se il codice utente non è abbinato alla partizione, l'accesso viene negato con partizione inserita e funzione limiti in modalità inserita programmata.

Digitare il comando #75 come segue:

Codice utente + # + 75

Il display visualizza il prompt sotto indicato:

PUNTO ACCESS	01
00-31	

("Punto di accesso - 00-31") Digitare il codice a due cifre (da 01 a 15) del punto di accesso di cui si desidera modificare lo stato.

N.B.: In caso di modulo VistaKey, le opzioni da 16 a 31 non sono valide e non generano alcuna azione.

Premere [✱] per confermare. Il display visualizza il prompt sotto indicato:

COMANDO PORT	0
NONE	

("Comando porta - nessuno") Digitare il codice ad una cifra dello stato desiderato. Le opzioni valide sono:

- 0 = NESSUNO – Lo stato del punto di accesso non viene alterato.
- 1 = AUTORIZZATO – Autorizza l'accesso dal punto di accesso che rimane sbloccato per l'intervallo di tempo impostato in fase di

programmazione nei prompt "Door Open Time" ("Tempo apertura porta") e "Relatch" ("Blocco porta").

- 2 = PROTETTO – Il punto di accesso è impostato in modalità normale. Questa opzione permette di mettere in sicurezza (modalità normale) un punto di accesso escluso; l'accesso viene autorizzato solo ai titolari di schede valide.
- 3 = ESCLUSO – Attiva la modalità escluso nel punto di accesso. In modalità escluso, la serratura del punto di accesso rimane sbloccata e gli allarmi per porta forzata o tempo porta aperta scaduto non vengono generati. Inoltre, le richieste di ingresso o di uscita vengono ignorate (la porta rimane sbloccata). Lo stato escluso viene terminato da un comando di messa in sicurezza (vedi sopra) oppure dall'attivazione di una fascia oraria, da un comando di azione oppure da un evento temporizzato.

Premere [✖] per confermare. L'azione selezionata viene attivata.

Comando #79

Il comando #79 permette di inserire, rimuovere oppure redigere delle schede nel database dei titolari del sistema. Per le istruzioni, fare riferimento al paragrafo "Funzioni scheda controllo accesso" in questo capitolo.

Comando #77 controllo dispositivi di uscita

Il comando #77 controllo dispositivi di uscita permette di attivare i terminali di uscita, escludere delle zone, attivare comandi di controllo accesso, ecc. con la supervisione di un operatore in grado di attivare azioni quali comandi di relè, comandi inserimento/disinserimento, comandi esclusione zone, condizioni di accesso aperto/chiuso e comandi di controllo accesso. Il comando #77 è attivo se sussistono le condizioni sotto indicate

- Il livello assegnato all'utente deve essere installatore o master.
- L'utente deve essere autorizzato per poter disinserire una partizione inserita e con funzione limiti in modalità inserita attiva.
- L'utente è in grado di mettere in sicurezza, escludere o bloccare oppure di impostare come solo uscita, solamente il punto di accesso della partizione a cui è abbinato.
- L'utente è in grado di disinserire solo la partizione a cui è abbinato.
- Il codice utente VISTA deve essere abbinato alla partizione a cui appartiene la tastiera.
- Il codice utente VISTA deve essere abbinato ad una scheda abbinata ad un gruppo di accesso che include il punto in cui viene richiesto l'accesso.
- Per ottenere l'autorizzazione di accesso, il codice utente VISTA non deve essere necessariamente abbinato alla partizione a cui appartiene il punto di accesso, ma se il codice utente non è abbinato alla partizione, l'accesso viene negato con partizione inserita e funzione limiti in modalità inserita programmata.

Digitare il comando #77 come segue:

Codice utente + # + 77

Il display visualizza il prompt sotto indicato:

AZIONE ?	01
RELE ON	

("Azione? - relè attivo") Digitare il codice azione a due cifre dell'azione desiderata.

I codici azione corrispondono agli eventi che devono avvenire immediatamente. Ogni azione richiede anche un identificatore, che determina gli effetti dell'azione (relè, gruppo di relè, partizione, elenco zona, gruppo utenti). L'identificatore dell'azione dipende dal tipo di azione selezionata.

La tabella 5-1: Codici azione riporta l'elenco dei "codici azione" (azioni desiderate) utilizzati in fase di programmazione degli eventi azionati da un comando tastiera.

N.B.: I codici azione 60 (PA solo uscita), 66 (PA gruppo solo uscita) oppure 72 (PA partizione solo uscita) disabilitano il lettore di ingresso del punto di accesso. Il lettore rimane disabilitato fino a ricevimento di un comando (comando tastiera o evento) che mette in sicurezza il punto di accesso.

Premere [✱] per confermare.

Il prompt successivo richiede l'identificatore (codice relè, codice partizione, ecc.) dell'azione selezionata. Digitare l'identificatore.

Premere [✱] per confermare. Il display visualizza il prompt sotto indicato:

↓ Codice azione		
01 Sei Sicuro?		0
1=SI 0=NO		

("01 confermi? - 1 = SI' 0 = NO") Premere 1 per confermare l'azione e l'identificatore azione, oppure 0 per cancellarli.

Premere [✱] per continuare. L'azione selezionata (o la cancellazione) viene attivata e il display visualizza il prompt sotto indicato:

ESCI?		
1=SI 0=NO		0

("Uscire? - 1 = SI' 0 = NO") Premere 1 per terminare l'inserimento delle azioni oppure premere 0 per inserire altre azioni.

Premere [✱] per confermare. Selezionare 1 per terminare la programmazione. Selezionare 0 per ritornare al prompt "Action?" ("Azione?").

Comando #78 test controllo accesso

Il comando #78 permette di eseguire il test sui punti di accesso come descritto precedentemente nei capitoli *Installazione - procedura rapida* e *Installazione - procedura dettagliata*.

Comando #80 controllo parametri

Il comando #80 permette di determinare o modificare le fasce orarie del sistema e/o degli eventi temporizzati. Per le istruzioni, fare riferimento alle procedure del paragrafo *Opzioni parametri di programmazione* del manuale del sistema di allarme.

Funzioni scheda controllo accesso

Il comando #79 programmazione funzioni scheda permette di eseguire le funzioni della scheda di controllo accesso: modifica del database della scheda contenuto nel sistema di allarme, registrazione, redazione e/o cancellazione delle schede. Le schede possono essere registrate o cancellate singolarmente o per gruppi. Copiare il foglio di programmazione titolari di scheda al termine del capitolo e compilarlo ogni volta che vengono abbinare nuove schede o vengono abbinare delle schede per la seconda volta.

In fase di registrazione delle schede nel sistema ricordare che:

- Le schede con privilegi esclusivi hanno libero accesso a tutti i punti di accesso, possono disinserire tutte le partizioni del sistema e sono sempre attive indipendentemente dagli eventi temporizzati programmati per il loro gruppo di accesso. La validità della scheda con privilegi esclusivi viene negata solamente in caso di scheda scaduta per utilizzo o per data. Inoltre, le schede con privilegi esclusivi non devono essere mappate ad un gruppo di accesso se non si desidera abbinare alla scheda determinati eventi abbinati al gruppo di accesso.
- Codice utente VISTA: i codici utente VISTA utilizzati per l'abbinamento ad una o più schede, devono essere definiti prima di utilizzare il comando #79 programmazione funzioni scheda. Quando le funzioni della scheda di controllo accesso sono attive, il sistema accetta solamente i codici utente VISTA precedentemente definiti. Per abbinare i codici utente VISTA, fare riferimento alle procedure del manuale del sistema di allarme.
- Campo codice utente VISTA: le schede non mappate a codici utente VISTA validi oppure impostate sui valori di default 000 permettono di accedere e sono in grado di disinserire le partizioni a cui ha accesso il gruppo di accesso della scheda selezionato nella modalità programmazione gruppi di accesso. Per non autorizzare l'accesso di una scheda da una porta a sistema inserito, abilitare la funzione limiti in modalità inserita (vedere il capitolo *Programmazione*).

Le schede mappate ad utenti VISTA validi del sistema hanno sempre accesso ad un punto di accesso e sono sempre in grado di disinserire la partizione a cui ha accesso il gruppo di accesso della scheda selezionato nella modalità programmazione gruppi di accesso. Fare riferimento ai due esempi sotto indicati.

1. Il gruppo di accesso di una scheda viene autorizzato ad accedere da un punto di accesso mediante la modalità programmazione gruppi di accesso. La funzione limiti in modalità inserita della partizione non viene programmata. In breve:

Scheda	Privilegi esclusivi	Codice utente VISTA	Accesso dal punto di accesso con sistema inserito	Disinserimento sistema
001	Si	000	Si	Si
002	Si	*tutti validi	Si	Si
003	No	000	Si	Si
004	No	*Tutti validi	Si	Si

* "Tutti validi": la scheda è abbinata ad un utente VISTA che ha accesso alla partizione a cui è abbinato il punto di accesso.

2. La scheda viene autorizzata all'accesso nella modalità programmazione gruppi di accesso. La funzione limiti in modalità inserita della partizione **viene** programmata. In breve:

Scheda	Privilegi esclusivi	Codice utente VISTA	Accesso dal punto di accesso con sistema inserito	Disinserimento sistema
001	Si	000	Si	Si
002	Si	*tutti validi	Si	Si
003	No	000	No	No
004	No	*tutti validi	Si	Si

* "Tutti validi": la scheda è abbinata ad un "utente VISTA che ha accesso alla partizione.

Per accedere al comando #79 programmazione funzioni scheda, digitare **codice utente + #79**. Il display visualizza il prompt sotto indicato:

PORTA NR	00	("Punto di accesso") Digitare il codice (01-15) del punto di accesso (porta) di cui si desidera modificare i dati della scheda. Premere [*] per confermare.
----------	----	---

Il display visualizza il prompt "Add Card?" ("Registrare scheda?"). Per registrare o redigere una scheda mediante inserimento nel lettore, seguire le procedure del paragrafo sotto indicato "Registrazione schede". Oppure, premere [0] per spostarsi su una diversa opzione. Quando l'opzione selezionata viene visualizzata, rilasciare il tasto [0] e fare riferimento al paragrafo corrispondente in questo capitolo. L'ordine di visualizzazione è:

- Add Card? ("Registrare scheda?")
- Edit Card? ("Redigere scheda?")
- AUTO Delete? ("Cancellare AUTOMATICAMENTE?")
- BLOCK Delete? ("Cancellare IN BLOCCO?")
- MANUAL Delete? ("Cancellare MANUALMENTE ?")
- Quit Card Mode? ("Uscire modalità scheda?")

Inserimento schede nel database

Agg Sch? 1=Si 0=No	0	("Registrare scheda? - 1 = sì 0 = no") Premere 1 per registrare una nuova scheda oppure per redigere una scheda mediante inserimento nel lettore. Premere 0 per spostarsi alla funzione redazione schede. Selezionando 1 il display visualizza il prompt sotto indicato.
-----------------------	---	--

N.B.: Utilizzando questa procedura per la redazione della scheda, il prompt visualizzato dipende dalle opzioni precedentemente selezionate per la scheda da redigere e non corrisponde necessariamente all'esempio indicato.

Ricon Sch. xxx-xx-xxxxxxx		("Inserire scheda") Inserire la scheda nel lettore oppure digitare manualmente il codice (12 cifre) della scheda da registrare o redigere. Dopo aver inserito la scheda, il display visualizza sulla riga in alto il codice ID della scheda VISTA a tre cifre preceduto dal messaggio "SWIPE CARD" ("Inserire scheda") e le 12 cifre con i dati della scheda sulla seconda riga. Se la scheda inserita è già stata registrata, la tastiera emette due bip e continua con la redazione dei dati della scheda esistente. Il significato dei caratteri della seconda riga è:
------------------------------	--	---

- Cifre da 1 a 3 = codice dispositivo a 3 cifre
- Cifre 4 e 5 = codice RCM a due cifre
- Cifre da 6 a 12 = codice ID scheda a 7 cifre

Premere **[*]** per confermare.

N.B.: Se si tratta della prima scheda della sessione di programmazione, il sistema si sposta al prompt successivo. In caso contrario, il sistema esegue una delle due procedure:

- a. Se la voce "in blocco" **non è stata selezionata** sulla prima scheda, il sistema si sposta al prompt successivo.
- b. Se la voce "in blocco" **è stata selezionata** sulla prima scheda, il sistema memorizza il codice scheda e gli altri dati definiti sulla prima scheda e poi si sposta al prompt "ESCI?" ("Uscire?").

↓ Cod. ID scheda VISTA	
001 Priv Escl?	
NON ABILIT	0

("001 privilegi esclusivi? - non abilitati") I titolari di scheda con privilegi esclusivi abilitati sono in grado di accedere a tutti i punti di accesso e di disinserire la partizione del punto di accesso (se inserita) in qualsiasi momento anche se il gruppo di accesso di appartenenza viene abilitato da parametri di programmazione o è abilitato all'ingresso o uscita da qualsiasi punto di accesso. L'unico impedimento all'accesso per un titolare di scheda con privilegi esclusivi è rappresentato dalla scheda scaduta per utilizzi o per data. I titolari di scheda con privilegi esclusivi disabilitati possono accedere da un punto di accesso solo se sussistono le condizioni sotto indicate:

- Il punto di accesso è stato programmato per accettare il gruppo di accesso del titolare.
- Il gruppo di accesso del titolare viene abilitato inserendo la scheda nel lettore (programmazione dei parametri, funzione evento/azione o selettore di azione), digitando il codice PIN (codice + # + 73) oppure mediante trasmissione RF.
- La scheda del titolare non è scaduta.

Digitare **1** per abilitare i privilegi esclusivi oppure **0** per non abilitarli.

N.B.: Se la scheda appartiene ad un gruppo di accesso con privilegi esclusivi, questa funzione può essere ereditata dal gruppo di accesso; in modalità RCM, invece, il sistema accetta solamente i privilegi esclusivi abbinati ad una scheda.

Premere [**✖**] per confermare.

↓ Cod. ID utente VISTA	
001 Tracc?	
NON ABILITAT.	0

("001 traccia? - non abilitata") La funzione traccia permette di monitorare il titolare della scheda registrando gli ingressi/uscite autorizzati e non autorizzati nel registro e inviando (se programmato) un report alla centrale operativa. Una scheda può anche ereditare l'abilitazione traccia dal gruppo di accesso a cui è abbinata. Le schede vengono tracciate se la funzione traccia è abilitata nei gruppi di accesso abbinati.

N.B.: In caso di scheda scaduta (per superamento numero di utilizzi o data di scadenza) e la funzione traccia è abilitata, i tentativi di utilizzo della scheda vengono registrati e inviati (se programmato) come utente U999. Una volta scaduta, la scheda rimane nel database e può essere successivamente riabilitata.

Digitare **1** per attivare la funzione traccia del titolare della scheda oppure **0** per escludere la funzione.

Premere [**✖**] per confermare.

GRP ACS? 1 2 3 4 5 6 7 8
(0-8)

("Gruppo di accesso? 1 2 3 4 5 6 7 8 - selezionare 0-8") I singoli titolari di scheda devono appartenere ad almeno un gruppo di accesso che garantisce determinati privilegi comuni a tutti i titolari appartenenti a quel determinato gruppo di accesso. In caso di appartenenza a più gruppi di accesso, il titolare gode dei privilegi di tutti i gruppi di accesso di appartenenza. I gruppi di accesso determinano anche il punto(i) di accesso da cui ha diritto di accesso il titolare e gli orari in base ai parametri programmati per quel gruppo di accesso.

Premere **0** per attivare/disattivare la selezione di tutti i gruppi di accesso oppure premere i tasti **1-8** per attivare/disattivare la selezione ("x") del codice gruppo di accesso.

Premere **[*]** per confermare.

N.B.: Selezione dei codici. Per esempio, premere 1 per attivare il gruppo 1 e premere ancora 1 per disattivare il gruppo 1.

↓ Cod. ID utente VISTA
001 TERMINI. USO?
USO ILLIMITAT. 00

("01 scadenza per utilizzi - utilizzi illimitati") Questo prompt permette di selezionare la scadenza dei privilegi esclusivi per utilizzo. Digitare 00 per selezionare numero illimitato di utilizzi, oppure digitare un numero da 01 a 14 per selezionare il numero corrispondente di ingressi autorizzati. Le uscite autorizzate non influiscono sul conteggio ai fini della scadenza per utilizzo. Digitando 15 la scheda viene esaurita automaticamente e le richieste di ingresso non vengono autorizzate anche se il titolare gode di privilegi esclusivi. Una volta scaduta, la scheda NON viene cancellata dal database, ma mantiene il proprio codice ID.

N.B.: Se la stessa scheda è impostata con scadenza per superamento numero di utilizzi e anche per superamento data di scadenza ("Expire Month" sotto), l'effettiva scadenza avverrà al verificarsi del primo evento.

Digitare un numero da **00** a **15**.

Premere **[*]** per confermare.

↓ Cod. ID utente VISTA
001 Expire Month
NESS. TERMINE 00

("001 mese di scadenza - nessuna scadenza") Digitare due cifre da **00** a **15** corrispondenti ai parametri di scadenza sotto indicati:

00 = normale (nessuna scadenza)	08 = agosto
01 = gennaio	09 = settembre
02 = febbraio	10 = ottobre
03 = marzo	11 = novembre
04 = aprile	12 = dicembre
05 = maggio	13 = fine giornata
06 = giugno	14 = fine della settimana (domenica)
07 = luglio	15 = fine del mese

N.B.:

- In caso di selezione di mese, fine giornata, fine della settimana e fine del mese, la scheda scade a mezzanotte.
- Se la stessa scheda è impostata con scadenza per superamento numero di utilizzi e anche per superamento data di scadenza

(“Expire Month” sopra), l'effettiva scadenza avverrà al verificarsi del primo evento.

Premere [✱] per confermare.

Selezionare un numero da 01a 12 per visualizzare il prompt “Day of Month” (giorno del mese).

Selezionare 00 oppure un numero da 13 a 15 per spostarsi al prompt “Vista User #” (“Codice utente Vista”).

↓ Cod. ID scheda VISTA 001 Giorno del Mese 00	(“001 giorno del mese”) Digitare il giorno del mese. La scheda scade a mezzanotte del giorno selezionato.
---	---

Premere [✱] per confermare.

↓ Cod. ID scheda VISTA 001 Ut. Vista # 000	(“001 codice utente Vista”) Digitare il codice utente VISTA a tre cifre.
--	--

Il codice utente VISTA permette di autorizzare l'accesso ad una partizione inserita anche se l'accesso alla partizione da parte del gruppo di accesso del titolare della scheda è limitato dalla funzione limiti in modalità inserita. Inoltre, i titolari sono in grado di autorizzare l'ingresso e l'uscita dai punti di accesso abbinati digitando il codice utente VISTA da un dispositivi RF.

N.B.:

- I titolari con codice utente VISTA 000 sono in grado di disinserire ed accedere alle partizioni se la funzione limiti in modalità inserita del gruppo di accesso di appartenenza è disabilitata per quella partizione. Per maggiori informazioni fare riferimento al paragrafo “Impostazione gruppi di accesso ” nel capitolo *Programmazione* di questo manuale.
- Il sistema accetta solamente i codici utente VISTA definiti prima di accedere alla modalità #79 programmazione funzioni scheda.
- I titolari con codice utente VISTA 000 vengono identificati come U999 in caso di selezione della funzione traccia.
- I diritti e privilegi della partizione dell'utente VISTA abbinato devono corrispondere ai diritti e privilegi della partizione abbinati alla scheda e al gruppo di accesso a cui appartiene la scheda.
- Se un codice utente VISTA viene abbinato ad un titolare e successivamente cancellato dal sistema di allarme, il titolare mantiene tutti i diritti e i privilegi ereditati dal codice utente VISTA fino a cancellazione del titolare dal sistema o a scadenza della scheda.

Premere [✱] per confermare.

↓ Cod. ID scheda VISTA 001 EVENT ACS? Ness. Richiest. 00
--

("001 evento di accesso? - nessuna richiesta") Digitare il codice a due cifre dell'evento di controllo accesso desiderato in base all'elenco sotto indicato. Le opzioni valide sono:

00 = nessuna richiesta	06 = uscita autorizzata
02 = richiesta di accesso	07 = qualsiasi autorizzazione
03 = richiesta di uscita	08 = accesso non autorizzato
04 = qualsiasi richiesta	09 = uscita non autorizzata
05 = accesso autorizzato	10 = qualsiasi evento non autorizzato

Premere [✱] per confermare.

N.B.:

- Selezionare 00 "nessuna richiesta" per spostarsi al prompt "Block Entry" ("Registrazione in blocco").
- Per generare un evento di accesso, inserire la scheda nel lettore del punto di accesso definito nel prompt sotto indicato.

↓ Cod. ID scheda VISTA 001 PUNTO ACCESS? (01-15) 00

("001 punto di accesso? - (01-15)") Digitare il codice punto di accesso da 1 a 15 corrispondente all'evento sopra indicato.

Premere [✱] per confermare.

↓ Cod. ID scheda VISTA 001 AZIONE? NULLA 00

("001 azione? - nessuna") Digitare il codice a due cifre dell'azione desiderata. Per le opzioni valide e la relativa descrizione fare riferimento alla *Tabella 5-1: Codici azione* del capitolo *Programmazione* in questo manuale.

N.B.:

- L'azione viene generata quando l'evento di accesso (sopra indicato) viene richiesto mediante inserimento della scheda nel lettore del punto di accesso definito nel prompt sopra indicato.
- Le azioni di inserimento o disinserimento di una partizione vengono eseguite solo se il codice utente VISTA (della scheda) è abbinato alla partizione da inserire o disinserire.
- I codici azione 60 (PA solo uscita), 66 (PA gruppo solo uscita) oppure 72 (PA partizione solo uscita) disabilitano il lettore di ingresso del punto di accesso. Il lettore rimane disabilitato fino a ricevimento di un comando (comando tastiera o evento) che mette in sicurezza il punto di accesso.

Premere [✱] per confermare.

In base all'azione selezionata, il sistema visualizza un prompt di richiesta di ulteriori informazioni. Per esempio, selezionando l'azione **01** (relè attivo), il sistema richiede il codice relè. Selezionare l'opzione desiderata e premere [✱] per confermare.

↓ Cod. ID scheda VISTA
001 Blocco?
1=SI 0=NO
0

("001 aggiungere in blocco - 1 = SI' 0 = NO) Questo prompt permette di registrare più schede con gli stessi dati immessi precedentemente. Se i dati da immettere sono completamente diversi, selezionare "NO" ed inserire i dati singolarmente alternando l'inserimento della scheda nel lettore e l'inserimento dei dati. Oppure, selezionare "SI" (si) per duplicare le informazioni della scheda mediante inserimento della scheda nel lettore. La sequenza per la registrazione in blocco è: inserire scheda, premere [✱], inserire i dati, inserire scheda, premere [✱], inserire scheda, premere [✱],... inserire scheda, premere [✱], uscire. La sequenza per inserire i dati singolarmente è: inserire scheda, premere [✱], inserire dati, inserire scheda, premere [✱], inserire dati ... inserire scheda, premere [✱], inserire dati, uscire.

Digitare **1** per registrare altre schede con informazioni identiche oppure **0** in caso di schede con informazioni diverse.

ESCI?
1=SI 0=NO
0

("Uscire? - 1 = SI' 0 = NO") Digitare **1** oppure **0**.

Selezionare 1 per spostarsi al prompt "Quit Card Mode?" ("Uscire modalità scheda?").

Selezionare 0 per ritornare al prompt "SWIPE CARD" ("Inserire scheda").

Redazione schede

Questa modalità permette di redigere le schede mediante il codice scheda. Per redigere le schede mediante inserimento della scheda oppure mediante inserimento del codice scheda a 12 cifre, fare riferimento alle procedure del paragrafo “Registrazione schede”.

Mod. Sch? 1=SI 0=No

("Redigere scheda - 1 = sì 0 = no) Digitare **1** oppure **0**.

Selezionare 1 per spostarsi al prompt successivo.

Selezionare 0 per spostarsi al prompt “Auto Delete” (“Cancellare automaticamente”).

N.B.: Le schede possono anche essere redatte mediante inserimento nel lettore oppure digitando il codice scheda a 12 cifre. Fare riferimento al paragrafo “Registrazione schede” di questo capitolo.

Sch. n# 1-250 0=ESCI 001

("Codice scheda - 1-250 0 = per uscire") Digitare il codice scheda valido da **001** a **250** oppure **000** per uscire.

Selezionare un numero da 001 a 250 per spostarsi al prompt successivo.

Selezionare 000 per spostarsi al prompt “Quit Card Mode?” (“Uscire modalità scheda?”).

N.B.: In caso di codice scheda non valido, il display visualizza “ERROR” (errore). Un codice scheda non è valido quando non è ancora stato inserito nel sistema.

Premere [**✱**] per confermare.

N.B.: In fase di redazione delle schede, i prompt dipendono dalle opzioni precedentemente selezionate per la scheda che si sta redigendo e non corrispondono necessariamente all'esempio indicato. In caso di scheda non precedentemente definita, il display visualizza un messaggio di errore richiedendo l'inserimento di un codice diverso.

↓ Cod. ID scheda VISTA 001 PRIV. ESCL.? NON ABILIT. 0

("001 privilegi esclusivi? - non abilitati") I titolari di scheda con privilegi esclusivi abilitati sono in grado di accedere a tutti i punti di accesso e di disinserire la partizione del punto di accesso (se inserita) in qualsiasi momento anche se il gruppo di accesso di appartenenza viene abilitato da parametri di programmazione o è abilitato all'ingresso o uscita da qualsiasi punto di accesso. L'unico impedimento all'accesso per i titolari di scheda con privilegi esclusivi è rappresentato dalla scheda scaduta per utilizzi o per data. I titolare di scheda con privilegi esclusivi disabilitati possono accedere da un punto di accesso solo se sussistono le condizioni sotto indicate:

- Il punto di accesso è stato programmato per accettare il gruppo di accesso del titolare.
- Il gruppo di accesso di appartenenza viene abilitato inserendo la scheda nel lettore (programmazione dei parametri, funzione evento/azione o selettore di azione), digitando il codice PIN (codice + # + 73) oppure mediante trasmissione RF.
- La scheda del titolare non è scaduta..

Digitare **1** per abilitare i privilegi esclusivi oppure **0** per non abilitarli.

N.B.: Se la scheda appartiene ad un gruppo di accesso con privilegi esclusivi, questa funzione può essere ereditata dal gruppo di accesso; in modalità RCM, il sistema accetta solamente i privilegi esclusivi abbinati ad una scheda.

Premere **[*]** per confermare.

↓ Cod. ID scheda VISTA	
001 Tracc?	
NON ABILIT.	0

("001 traccia? - non abilitata") La funzione traccia permette di monitorare il titolare di una scheda registrando gli ingressi/uscite autorizzati e non autorizzati nel registro e di inviare (se programmato) un report alla centrale operativa. Una scheda può anche ereditare la funzione traccia dal gruppo di accesso di abbinamento. La scheda viene tracciata se la funzione traccia dei gruppi di accesso abbinati è abilitata.

N.B.: In caso di scheda scaduta (per numero di utilizzi o per superamento data) e la funzione traccia è abilitata, i tentativi di utilizzo della scheda vengono registrati e inviati (se programmato) come utente U999. Una volta scaduta, la scheda rimane nel database e può essere successivamente riabilitata.

Premere **1** per abilitare la funzione traccia titolare oppure **0** per disabilitarla.

Premere **[*]** per confermare.

GRP ACS?	1	2	3	4	5	6	7	8
(0-8)	x	x	x	x	x	x	x	x

("Gruppi di accesso 1 2 3 4 5 6 7 8 - selezionare 1-8") I titolari di scheda devono appartenere ad almeno un gruppo di accesso che garantisce determinati privilegi comuni a tutti i titolari di appartenenza. In caso di appartenenza a più gruppi di accesso, il titolare gode dei privilegi di tutti i gruppi di accesso di appartenenza. I gruppi di accesso determinano anche il punto(i) di accesso da cui il titolare ha diritto di accedere e gli orari in base ai parametri programmati per quel gruppo di accesso.

Premere **0** per attivare/disattivare la selezione di tutti i gruppi di accesso oppure premere i tasti **1-8** per attivare/disattivare la selezione ("x") del codice gruppo di accesso.

Premere **[*]** per confermare.

N.B.: Selezione dei codici. Per esempio, premere **1** per attivare il gruppo 1 e premere ancora **1** per disattivarlo.

↓ Cod. ID scheda VISTA	
001 Termi. Uso?	
USO ILLIMITAT.	00

("001 scadenza per utilizzi - utilizzi illimitati") Questo prompt permette di selezionare la scadenza dei privilegi esclusivi per utilizzo. Digitare 00 per selezionare numero illimitato di utilizzi, oppure digitare un numero da 01 a 14 per selezionare il numero corrispondente di ingressi autorizzati. Le uscite autorizzate non influiscono sul conteggio ai fini della scadenza per utilizzo. Digitando 15 la scheda viene esaurita automaticamente e gli ingressi non vengono autorizzati anche in caso di titolare con privilegi esclusivi. Una volta scaduta una scheda NON viene cancellata dal database, ma mantiene il proprio codice ID.

N.B.: Se la stessa scheda è impostata con scadenza per superamento numero di utilizzi e anche per superamento data di scadenza

- I titolari con codice utente VISTA 000 vengono identificati come U999 se la funzione traccia è stata selezionata.
- I diritti e privilegi della partizione dell'utente VISTA abbinato devono corrispondere ai diritti e privilegi della partizione abbinati alla scheda e al gruppo di accesso a cui appartiene la scheda.
- Se un codice utente VISTA viene abbinato ad un titolare e successivamente cancellato dal sistema di allarme, il titolare mantiene tutti i diritti e i privilegi ereditati dal codice utente VISTA fino a cancellazione dal sistema o fino a scadenza della scheda.

Premere [✱] per confermare.

↓ Cod. ID scheda VISTA
001 Event ACS ?
Nessun Richiesta 00

("001 evento di accesso? - nessuna richiesta") Digitare il codice a due cifre dell'evento di controllo accesso desiderato in base all'elenco sotto indicato. Le opzioni valide sono:

- | | |
|---------------------------|---------------------------------------|
| 00 = nessuna richiesta | 06 = uscita autorizzata |
| 02 = richiesta di accesso | 07 = qualsiasi autorizzazione |
| 03 = richiesta di uscita | 08 = accesso non autorizzato |
| 04 = qualsiasi richiesta | 09 = uscita non autorizzata |
| 05 = accesso autorizzato | 10 = qualsiasi evento non autorizzato |

Premere [✱] per confermare.

N.B.:

- Selezionare 00 “nessuna richiesta” per spostarsi al prompt “Block Entry” (“Registrazione in blocco”).
- L'evento di accesso viene generato quando la scheda viene inserita nel lettore del punto di accesso definito nel prompt sotto indicato.

↓ Cod. ID scheda VISTA
001 PUNTO ACCESS?
(01-15) 00

("001 punto di accesso? - (01-15)") Digitare il codice da 1 a 15 dell'evento sopra indicato.

Premere [✱] per confermare.

↓ Cod. ID scheda VISTA
001 AZIONE?
NULLA 00

("001 azione? - nessuna") Digitare il codice a due cifre dell'azione desiderata. Per le opzioni valide e la relativa descrizione fare riferimento alla *Tabella 5-1: Codici azione* del capitolo *Programmazione* in questo manuale.

N.B.:

- L'azione viene generata quando l'evento di accesso (sopra indicato) viene richiesto mediante inserimento della scheda nel lettore del punto di accesso definito nel prompt sopra indicato.
- Le azioni di inserimento o disinserimento di una partizione vengono eseguite solo se il codice utente VISTA (della scheda) è abbinato alla partizione da inserire o disinserire.
- I codici azione 60 (PA solo uscita), 66 (PA gruppo solo uscita) oppure 72 (PA partizione solo uscita) disabilitano il lettore di ingresso del punto di accesso. Il lettore rimane disabilitato fino a ricevimento di un comando (comando tastiera o evento) che mette in sicurezza il punto di accesso.

Premere [✱] per confermare.

In base all'azione selezionata, il sistema visualizza un prompt di richiesta di ulteriori informazioni. Per esempio, selezionando l'azione **01** (relè attivo), il sistema richiede il codice relè. Selezionare l'opzione desiderata e premere [**✖**] per confermare.

TERMINA SCHEDA? 1=SI 0=NO	0
------------------------------	---

("Uscire? - 1 = SI' 0 = NO") Premere **1** oppure **0**.

Selezionare 1 per spostarsi al prompt "Quit Card Mode?" ("Uscire modalità scheda?").

Selezionare 0 per ritornare al prompt "Exec Priv?" ("Privilegi esclusivi?").

Cancellazione automatica

CANCELLA AUTO? 1=SI 0=No	0
-----------------------------	---

("Cancellare automaticamente? - 1 = sì 0 = no") Premere **1** oppure **0**.

Selezionare 1 per spostarsi al prompt successivo.

Selezionare 0 per spostarsi al prompt "Block Delete?" ("Cancellare in blocco?").

RICON. SCH. xxx-xx-xxxxxxx	
-------------------------------	--

("Inserire scheda") Inserire la scheda nel lettore o digitare il codice scheda da cancellare. Il codice scheda e il codice ID scheda VISTA da cancellare vengono visualizzati. Se il display visualizza zero in corrispondenza del codice scheda e del codice ID scheda VISTA, la scheda non è stata trovata nel database del sistema.

Premere [**✖**] per confermare.

Se il database riconosce la scheda, il sistema si sposta al prompt "Are You Sure?"("Confermi?").

Se il database non riconosce la scheda, il display visualizza il prompt sotto indicato "Card not Found" ("Scheda non riconosciuta").

Card not Found ✖ to continue	
---------------------------------	--

("Scheda non riconosciuta - * per continuare") Premere [**✖**] per continuare. Il sistema si sposta al prompt "ESCI?" (Uscire?).

Sei Sicuro? 1=SI 0=NO	0
--------------------------	---

("Confermi? - 1= SI' 0 = NO") Premere **1** oppure **0**.

Selezionando 1, il sistema indica al database della scheda che la scheda è stata cancellata.

Selezionare 0 per spostarsi al prompt "ESCI?" (Uscire?).

Premere [**✖**] per confermare.

ESCE? 1=SI 0=NO	0
--------------------	---

("Uscire? - 1 = SI' 0 = NO") Premere **1** oppure **0**.

Selezionare 1 per spostarsi al prompt "Quit Card Mode?" ("Uscire modalità scheda?").

Selezionare 0 per ritornare al prompt "Swipe Card" ("Inserire scheda").

Premere [**✖**] per confermare.

Cancellazione in blocco

CANC BLOCCO? 1=SI 0=No	0
---------------------------	---

("Cancellare in blocco - 1 = SI' 0 = NO") Premere **1** oppure **0**.

Selezionare 1 per spostarsi al prompt successivo.

Selezionare 0 per spostarsi al prompt "Manual Delete?" ("Cancellare manualmente").

CANC DA SCH. 1-250 0=Esci	001
------------------------------	-----

("Cancellare dalla scheda - 1-250 0 = per uscire") Digitare il codice a 3 cifre della prima (più bassa) scheda da cancellare. Selezionare 000 per spostarsi al prompt "Quit Card Mode?" ("Uscire modalità scheda?").

Premere **[*]** per confermare.

A Sch. 1-250 0=ESCI	000
------------------------	-----

("Alla scheda - 1-250 0 = per uscire") Digitare il codice a tre cifre dell'ultima scheda (più alta) da cancellare.

N.B.: Se questo numero è inferiore al numero digitato come "Delete from Card" ("Cancellare da scheda") indicato sopra, il sistema non cancella alcuna scheda.

Premere **[*]** per confermare.

Sei Sicuro? 1=SI 0=No	0
--------------------------	---

("Confermi? - 1 = SI' 0 = NO") Premere **1** oppure **0**.

Selezionando 1, il sistema indica al database della scheda che i codici scheda indicati sono stati cancellati dal database e ritorna al prompt "Delete from Card" ("Cancellare da scheda").

Selezionare 0 per ritornare al prompt "Delete from Card" ("Cancellare da scheda") senza indicare al database le schede da cancellare.

Premere **[*]** per confermare.

Cancellazione manuale

Canc. Manuale? 1=SI 0=NO	0
-----------------------------	---

("Cancellare manualmente? - 1 = SI' 0 = NO") Premere **1** oppure **0**.

Selezionare 1 per spostarsi al prompt successivo.

Selezionare 0 per spostarsi al prompt "Quit Card Mode?" ("Uscire modalità scheda?").

Canc Id Sch. N.# (001-250) 0=ESCI	0
--------------------------------------	---

("Cancellare codice ID scheda - (001-250 0 = per uscire") Digitare un numero da **001** a **250** oppure **000** per uscire.

Selezionare un numero da 001 a 250 per spostarsi al prompt successivo.

Selezionare 000 per spostarsi al prompt "Quit Card Mode?" ("Uscire modalità scheda?").

Premere **[*]** per confermare.

Sei Sicuro? 1=SI 0=No	
--------------------------	--

("Confermi? - 1= sì 0 = no) Premere **1** oppure **0**.

Selezionando 1, il sistema indica al database della scheda che la scheda è stata cancellata e il sistema ritorna al prompt "Delete Card ID#" ("Cancellare codice ID scheda").

Selezionare 0 per ritornare al prompt "Delete Card ID#" ("Cancellare codice ID scheda") senza cancellare la scheda dal database.

Premere **[*]** per confermare.

Uscire dalla modalità programmazione funzioni scheda

ESCI 1=SI 0=No

("Uscire modalità scheda? - 1= sì 0 = no") Premere **1** oppure **0**.
Selezionare 1 per uscire dalla programmazione funzioni scheda.
Selezionare 0 per ritornare al prompt "Add Card?" ("Registrare scheda?").

Test del sistema

Contenuto

- ◆ Informazioni generali
- ◆ Test del sistema
- ◆ Rigenerazione azioni temporizzate
- ◆ LED e ponticello del modulo VistaKey
- ◆ Selezione errata del commutatore di indirizzo
- ◆ Cancellazione errori di supervisione dispositivo DSM

Informazioni generali

Questo capitolo tratta il test del sistema, i LED e il ponticello del modulo VistaKey, la selezione errata del commutatore di indirizzo e gli errori di supervisione del dispositivo DSM.

Test del sistema

Le informazioni contenute in questo paragrafo permettono di verificare che i gruppi di accesso definiti autorizzino l'accesso negli intervalli di tempo programmati senza generare allarmi. Se le procedure sotto indicate vengono eseguite con successo, la porzione controllo accesso del sistema è funzionante.

1. Per controllare i gruppi di accesso abilitati e disabilitati da eventi temporizzati, agire sull'orologio in tempo reale della centralina. Per esempio, se il gruppo di accesso è abilitato nella fascia oraria 8.00 - 17.00, impostare l'orologio sulle 7.59 e attendere 1 minuto.
2. Verificare che il gruppo di accesso autorizzi l'accesso mediante inserimento della scheda in quel gruppo.
3. Spostare l'orologio sulle 16.59 e attendere 1 minuto.
4. Verificare che l'accesso (disabilitato) non venga autorizzato mediante inserimento della scheda in quel gruppo.
5. Ripetere i punti da 1 a 4 per ogni punto di accesso.
6. Una volta controllati tutti i gruppi di accesso, riportare l'orologio sull'ora corrente. Se si desidera attivare in modo immediato dei gruppi di accesso controllati da eventi temporizzati, utilizzare il comando #77. Tutti i gruppi di accesso controllati da eventi temporizzati vengono successivamente disabilitati in base ai parametri programmati.

Rigenerazione azioni temporizzate

Durante l'installazione ed il controllo del sistema, le azioni legate a fasce orarie e/o parametri di tempo possono essere rigenerate. In caso di rigenerazione, le azioni legate a fasce orarie definite per il giorno e l'ora corrente vengono attivate secondo le normali modalità. Lo stato delle azioni temporizzate viene rigenerato in seguito agli eventi sotto indicati:

N.B.: La funzione di rigenerazione non prende in considerazione la programmazione dell'intera settimana ai fini della determinazione dello stato degli oggetti di azioni, ma riguarda solamente le fasce orarie del giorno corrente.

- Modifica dei componenti dell'ora/data con il comando tastiera #63. Per eseguire la rigenerazione, modificare ora e/o data.

- Uscita dalla modalità #80 programmazione parametri. La rigenerazione viene eseguita anche se non sono state apportate modifiche alla modalità #80 programmazione parametri.
- Uscita modalità programmazione tastiera. La rigenerazione viene eseguita anche se non sono state apportate modifiche alla modalità programmazione tastiera.
- La centralina rilascia la linea dopo aver raggiunto il conteggio squilli nel tentativo di stabilire un collegamento con il computer di download. La rigenerazione viene eseguita indipendentemente dal successo del collegamento con il computer di download.
- Accensione del sistema.
- Regolazione orologio sull'ora legale.

LED e ponticello del modulo VistaKey

Il modulo VistaKey è dotato di un LED verde, un LED rosso e di un ponticello. Il LED verde indica lo stato del modulo VistaKey, il LED rosso indica lo stato del relè di controllo porta del modulo e il ponticello serve per utilizzi futuri. Per informazioni dettagliate, fare riferimento ai paragrafi sotto indicati.

LED verde

Il LED verde emette una serie intermittente di lampeggi che segnalano lo stato del modulo VistaKey. Ogni sequenza ha un diverso significato come segue:

n. di lampeggi in sequenza	Stato modulo	n. di lampeggi in sequenza	Stato modulo
1	Ripristino (utilizzo futuro)	8	RTE
2	Modalità RCM (utilizzo futuro)	9	Autorizzazione RTE in atto
3	Protetto	10	Allarme porta aperta
4	Escluso	11	Tempo allarme
5	Bloccato	12	Solo uscita
6	Autorizzazione in atto	13	Preallarme
7	Non autorizzazione in atto		

LED rosso

Il LED rosso segnala lo stato del relè di controllo porta del modulo VistaKey. Il LED acceso indica che il relè di controllo porta VistaKey è attivo.

Ponticello

Il ponticello si trova nel modulo VistaKey tra la morsettiera TB3 e il relè di controllo porta K1. Questo ponticello è installato per utilizzi futuri avendo la funzione di cortocircuitare i due spinotti vicino al relè di controllo porta. Se il ponticello viene spostato o rimosso dal modulo, il normale funzionamento del modulo non viene garantito in qualsiasi condizione di funzionamento.

Selezione errata del commutatore di indirizzo

In caso di mancanza rete o di errata selezione del commutatore di indirizzo durante l'utilizzo del sistema, la centralina registra un evento ACLO MOD (mancanza rete modulo). Se viene registrato questo evento ma il sistema è alimentato, verificare che il commutatore di indirizzo del modulo sia selezionato sull'indirizzo corretto.

Cancellazione errori di supervisione dispositivo DSM

In caso di errore nella connessione del circuito polling, il sistema visualizza e registra un messaggio di controllo DSM durante il funzionamento del sistema. Una volta corretto l'errore, il messaggio rimane visualizzato per 1 minuto sul display della tastiera prima di essere cancellato.

C A P I T O L O 8

Registro eventi

Contenuto

- ◆ *Informazioni generali* ◆ *Registro eventi della centralina del sistema di*
- ◆ *Report alla centrale operativa* *allarme*

Informazioni generali

Questo capitolo fornisce le voci del registro eventi che vengono inseriti nel sistema di allarme collegando un modulo VistaKey. L'elenco sotto indicato mostra gli eventi inviati alla centrale operativa (CS) e gli allarmi registrati nella centralina di allarme.

Report alla centrale operativa

L'elenco sotto indicato mostra gli eventi, raggruppati per tipo di evento, che possono essere inviati alla centrale operativa. L'invio dei report viene abilitato mediante l'abilitazione combinatori di accesso (descritta nel capitolo *Programmazione* di questo manuale).

Allarmi accesso

<u>Evento</u>	<u>Codice</u>	<u>Identificatore</u>
Accesso coercizione autorizzato	124	Cod. utente
Uscita coercizione autorizzata	125	Cod. utente
Porta forzata/ripristino	423	Cod. zona DSM

Anomalie accesso

<u>Evento</u>	<u>Codice</u>	<u>Identificatore</u>
Mancanza rete modulo/ripristino*	342	Cod. zona DSM
Anomalia porta aperta/ripristino	426	Cod. zona DSM
Anomalia DSM /ripristino	427	Cod. zona DSM
Anomalia RTE /ripristino	428	Cod. zona DSM

* In caso di mancanza rete o di modifica della selezione del commutatore di indirizzo su una posizione errata, la centralina registra un evento ACLO MOD (mancanza rete modulo) e invia un report di mancanza rete. Se questo evento viene registrato ma il modulo è alimentato, verificare che il commutatore di indirizzo del modulo sia selezionato sull'indirizzo corretto.

Esclusione accesso

<u>Evento</u>	<u>Codice</u>	<u>Identificatore</u>
Accesso escluso/ripristino	577	Cod. zona DSM (Serratura aperta)

Accesso sistema

<u>Evento</u>	<u>Code</u>	<u>Identificatore</u>
Ripristino modulo	339	Cod. zona DSM (All'accensione)
Test ingresso/uscita	607	Cod. zona DSM

Traccia accesso

N.B.: Nei casi sotto indicati, la funzione traccia gruppo di accesso e/o titolare scheda deve essere attiva.

<u>Evento</u>	<u>Codice</u>	<u>Identificatore</u>
Accesso autorizzato	422	Cod. utente
Accesso non autorizzato	421	Cod. utente
Uscita autorizzata	425	Cod. utente
Uscita non autorizzata	424	Cod. utente

N.B.: Gli eventi di chiusura punto di accesso non vengono registrati o segnalati.

Registro eventi della centralina del sistema di allarme

L'elenco sotto indicato contiene gli eventi, suddivisi per categorie, che possono essere registrati nel registro eventi del sistema di allarme.

N.B.: Gli eventi sotto indicati vengono registrati solo se il corrispondente tipo è abilitato nel campo 1*70 della centralina di allarme. Per ulteriori informazioni, fare riferimento al manuale di installazione e predisposizione del sistema di allarme.

Allarme

<u>Evento</u>	<u>Voce registro</u>	<u>Identificatore</u>
Porta forzata	DR FORCE	Cod. zona DSM
Ripristino porta forzata	DRFO RST	Cod. zona DSM

N.B.: Gli eventi sotto indicati vengono registrati solo se la funzione traccia gruppo di accesso o traccia scheda è abilitata.

Accesso autorizzato	ACS GRT	[Cod. zona DSM] U [Cod. utente]
Accesso non autorizzato	ACS DENY	[Cod. zona DSM] U [Cod. utente]
Uscita autorizzata	EGR GRT	[Cod. zona DSM] U [Cod. utente]
Uscita non autorizzata	EGR DENY	[Cod. zona DSM] U [Cod. utente]

Verifiche

<u>Evento</u>	<u>Voce registro</u>	<u>Identificatore</u>
Anomalia porta aperta	DR DROP	Cod. zona DSM
Ripristino anomalia porta aperta	DRPO RST	Cod. zona DSM
Anomalia DSM	DSM TRBL	Cod. zona DSM
Ripristino anomalia DSM	DSM RST	Cod. zona DSM
Anomalia RTE	RTE TRBL	Cod. zona DSM
Ripristino anomalia RTE	RTE RST	Cod. zona DSM
Mancanza rete modulo *	ACLO MOD	Cod. zona DSM
Ripristino mancanza rete modulo		ACRST MOD Cod. zona DSM

* In caso di mancanza rete o di modifica della selezione del commutatore di indirizzo su una posizione errata, la centralina registra un evento ACLO MOD (mancanza rete modulo) e invia un report di mancanza rete. Se questo evento viene registrato ma il sistema è alimentato, verificare che il commutatore di indirizzo del modulo sia selezionato sull'indirizzo corretto.

Esclusione

<u>Evento</u>	<u>Voce registro</u>	<u>Identificatore</u>
Punto di accesso escluso	ACPT BYP	[Cod. zona DSM] U [Cod. utente]
Punto di accesso non escluso	ACPT UNB	[Cod. zona DSM] U [Cod. utente]

Sistema

<u>Evento</u>	<u>Voce registro</u>	<u>Identificatore</u>
Ripristino modulo	RES MOD	Cod. zona DSM

N.B.: Gli eventi di chiusura punto di accesso non vengono registrati o segnalati.

Modalità capacità ridotta

Contenuto

◆ *Informazioni generali*

◆ *Descrizione modalità capacità ridotta (RCM)*

Informazioni generali

Per garantire l'accesso agli utenti in caso di problemi, il modulo VistaKey è dotato della modalità capacità ridotta (RCM) che permette al sistema di funzionare grazie al database delle schede memorizzato nel modulo VistaKey. In caso di mancanza di collegamento tra il modulo VistaKey e la centralina per più di 2 minuti (il modulo VistaKey deve comunque essere alimentato), il modulo entra automaticamente in modalità RCM. Questa modalità viene terminata automaticamente un minuto dopo il ripristino del collegamento.

Inoltre, in caso di richiesta di download da un computer di download collegato direttamente alla centralina, l'intero sistema entra in modalità RCM 2 minuti dopo il collegamento con il computer. La modalità termina 1 minuto dopo la fine del collegamento. In modalità capacità ridotta, il modulo VistaKey riconosce ed autorizza l'accesso dal punto di accesso alle schede autorizzate (indipendentemente dai parametri di tempo).



Il database delle schede viene trasferito dalla centralina al modulo VistaKey 10 minuti dopo l'uscita dalla modalità #79, il download della centralina, l'accensione del modulo VistaKey o a mezzanotte. Quindi, se il sistema entra in modalità RCM mentre si sta lavorando sul database delle schede, le modifiche più recenti potrebbero non essere state trasferite e il modulo funziona sulla base del database esistente prima delle modifiche.

Descrizione modalità capacità ridotta (RCM)

Se il modulo VistaKey è in modalità RCM, la centralina visualizza le zone controllate dal modulo come se fossero in modalità "Check" ("Verifica") e il sistema autorizza l'accesso dai punti controllati dal modulo. Le capacità e i limiti del modulo VistaKey in modalità RCM sono:

- In modalità RCM, la porta/punto di accesso si sposta sulla modalità protetta/normale indipendentemente dallo stato precedente (es. bloccato, escluso o solo uscita.).
- In modalità RCM, il modulo VistaKey non è in grado di autorizzare l'accesso ad una scheda sulla base dei privilegi esclusivi che potrebbero essere normalmente ereditati dall'abbinamento con un gruppo di accesso; l'accesso viene, invece, autorizzato se i privilegi esclusivi sono abbinati alla scheda stessa
- In modalità RCM, i limiti di accesso sulla base di parametri di tempo, la funzione limiti partizione in modalità inserita per un gruppo di accesso e la disabilitazione di gruppi di accesso non vengono considerati.
- In modalità RCM, una scheda del modulo VistaKey è in grado di autorizzare, proteggere o escludere un punto di accesso sulla base delle informazioni contenute nel database della scheda. Quindi, è possibile creare delle schede in grado di autorizzare, proteggere o escludere un punto di accesso quando il modulo VistaKey è in modalità RCM.
- In modalità RCM, una scheda normalmente abilitata per il disinserimento di una partizione del sistema di allarme, non è abilitata per questa operazione.

- La modalità RCM del modulo VistaKey termina 1 minuto dopo il ripristino del collegamento loop.
- Al termine della modalità RCM, la porta/punto di accesso ritorna allo stato precedente (es. bloccato, escluso o solo uscita).

Glossario

- A** **Anomalia** - Condizione per la segnalazione di problemi di linea (cavo o collegamento) di una zona controllata.
- Anomalia porta aperta** – La condizione di aperto di una zona generata quando una porta rimane aperta allo scadere del tempo porta aperta più tempo allarme. Questa condizione si verifica solamente quando la porta è monitorata dal sistema controllo stato porta.
- B** **Bloccato (Punto di accesso)** - Modalità che permette di chiudere la porta del punto di accesso. Le funzioni di controllo accesso dei lettori del punto di accesso vengono disabilitate. In modalità bloccato il punto di accesso non autorizza l'ingresso e l'uscita.
- C** **Codice utente** - Codice identificativo che permette l'accesso al sistema da parte dell'utente. I codici utente vengono inseriti mediante l'interfaccia del sistema.
- Comando manuale** - Opzione di estensione disponibile per alcuni comandi quali autorizzazione punti di accesso, autorizzazione gruppi di accesso, autorizzazione partizioni punti di accesso. Quando l'opzione comando manuale viene utilizzata con un comando di autorizzazione che dipende da un evento temporizzato, il punto di accesso rimane aperto per 30 secondi. Utilizzando il comando come parte integrante di un'autorizzazione inviata mediante un comando tastiera (#77), il sistema visualizza i prompt per la selezione del tempo apertura porta, tempo allarme e tempo preallarme.
- Controllo accesso** - L'accesso da determinate porte viene autorizzato a determinate persone in un determinato momento in base a: 1) cosa presentano, 2) chi sono e/o 3) cosa fanno.
- D** **DSM (Controllo stato porta)** - Zona di un sistema di controllo accesso per il monitoraggio dell'interruttore di modifica della porta. L'interruttore di modifica della porta segnala lo stato della porta (aperta o chiusa) e permette al sistema di determinare se la porta è stata forzata o lasciata aperta oltre il tempo previsto.
- E** **Esclusione (Punto di accesso)** - Quando un punto di accesso si trova in modalità esclusa, il meccanismo di chiusura è sbloccato e il sistema non genera alcun segnale di allarme per porta forzata o tempo porta aperto scaduto. Le richieste di uscita vengono ignorate (la porta è ancora sbloccata). Questa condizione viene anche definita come "libero accesso".
- F** **Funzione evento/Azione** - Opzione programmabile dall'utente per legare determinate funzioni di sistema ad un evento del sistema. L'azione viene eseguita al verificarsi dell'evento del sistema.
- G** **Gruppo di accesso** - Un gruppo di persone che condividono gli stessi privilegi di accesso per quanto riguarda punti di accesso (porte) e tempi abbinati. Il gruppo di accesso determina i privilegi di accesso degli appartenenti. I membri di uno stesso gruppo di accesso godono degli stessi privilegi di accesso.
- L** **Letto** - Dispositivo nel quale l'utente inserisce la propria scheda. I dati vengono letti e trasmessi alla centralina che li elabora e genera la conseguente azione (es. attivazione del relè, ecc.).
- Letto di ingresso** - Dispositivo di entrata installato sul lato ingresso del punto di accesso. Grazie a questo dispositivo il sistema identifica le persone e ne esamina i privilegi di accesso per determinare se possono accedere all'area protetta. Il termine è "letto di ingresso" poiché la maggior parte di dispositivi consistono in un letto di scheda nel quale i titolari devono inserire la propria scheda identificativa.
- Letto di uscita** - Dispositivo di entrata installato sul lato uscita del punto di accesso. Grazie a questo dispositivo il sistema identifica le persone e ne esamina i privilegi di

accesso per determinare se possono accedere all'area protetta. (vedere anche: Lettore di ingresso).

Lettore scheda - Dispositivo mediante il quale il sistema riconosce i titolari di scheda. Il lettore legge la scheda di accesso ed esamina i privilegi di accesso del titolare della scheda per determinare se il titolare della scheda può accedere all'area protetta.

Libero acceso - Vedere esclusione (Punto di accesso)

Livello di accesso - Il tipo di autorizzazioni di accesso abbinata al titolare di una scheda.

M

Meccanismo di controllo porta - L'apparecchiatura installata in un punto di accesso per controllare l'ingresso o l'uscita dei titolari di scheda. Il tipo di meccanismo di controllo porta dipende in parte dal livello di sicurezza che si desidera applicare ai punti di accesso. I tipi di meccanismi disponibili e le modalità di configurazioni degli stessi sono molteplici.

P

Parametri (oppure parametri di tempo) - Serie di intervalli di tempo che determinano il momento di inizio, di fine e di attivazione di eventi o condizioni. Per esempio, i parametri di tempo permettono di definire quando determinati gruppi di accesso hanno accesso ai locali. I parametri di tempo vengono programmati per giorno.

PIR (dispositivi passivi ad infrarossi) - Si tratta solitamente di dispositivi di rilevazione in grado di rilevare i movimenti all'interno di una determinata area e, quindi, di modificare lo stato dei contatti interni. Questi contatti possono essere collegati ad una zona con richiesta di uscita in un sistema di controllo accesso per permettere l'uscita automatizzata nel caso in cui una persona si avvicina ad un punto di accesso dall'interno dell'area protetta.

Privilegi di accesso - I diritti attribuiti ad una persona che determinano le sue capacità di accesso. I privilegi di accesso definiscono quando e dove la persona può avere accesso o uscire da un'area controllata.

Privilegi esclusivi - Opzione concessa ai titolari di scheda che permette di accedere liberamente da tutti i punti di accesso del sistema.

Prossimità - Tecnologia di lettori basata sul collegamento a radio frequenza tra il lettore e la scheda (lettore prox e scheda prox). Le informazioni codificate vengono trasferite dalla scheda al lettore in un unico modello che permette l'identificazione del titolare.

Protetto - Lo stato di un punto di accesso con sistema in modalità normale. Quando un punto di accesso è protetto, solamente i titolari di schede valide possono avere accesso ai locali.

Punto di accesso - L'insieme dei lettori di scheda, delle zone, delle uscite logiche e dei relè di controllo della porta che gestiscono il controllo e il monitoraggio dei meccanismi di controllo di un singolo punto di passaggio.

R

Relè di controllo porta - Il relè di controllo porta è un interruttore elettromeccanico che controlla il passaggio di corrente al meccanismo di bloccaggio della porta. Questo relè fornisce ad un terminale di uscita un contatto a secco a C e, quindi, permette di attivare o disattivare un dispositivo esterno.

Risorsa abbinata - Una risorsa, quale un lettore o un relè, direttamente abbinato ad un punto di accesso. La risorsa abbinata non può più essere controllata o monitorata individualmente. Un relè abbinato, per esempio, viene utilizzato per controllare la porta a cui è abbinato.

RTE (Richiesta di uscita) - Condizione generata da un dispositivo diverso dal lettore di scheda (es. tasto, maniglione antipánico, dispositivi passivi ad infrarossi, tappetini dotati di sensori) che segnala al sistema quando qualcuno sta per uscire dalla zona protetta. L'azione generata può anche corrispondere allo sblocco della porta. Altre definizioni di questa condizione sono: REX, uscita e esclusione.

N.B.: Non confondere questo utilizzo del termine "esclusione" con il significato data da ADEMCO. (Vedere la voce esclusione)

S

Scheda di accesso - Scheda del formato di una carta di credito contenente informazioni codificate per il controllo accesso. Questo sistema utilizza schede di prossimità.

Serratura magnetica - Il meccanismo di bloccaggio è costituito da una grossa lastra metallica fissata alla porta e da una grossa bobina installata nell'intelaiatura della porta. Questi due meccanismi vengono tenuti saldamente attaccati grazie al forte campo magnetico che si crea facendo passare la corrente attraverso la bobina. La porta viene rilasciata (o "sbloccata") interrompendo il passaggio di corrente nella bobina, e quindi, eliminando il campo magnetico.

Serratura meccanica - Dispositivo di bloccaggio elettromeccanico solitamente installato nell'intelaiatura della porta per bloccare e sbloccare la porta elettricamente o elettronicamente. Internamente, il dispositivo è composto da un solenoide al quale viene applicata la corrente in modo che lo stantuffo sposti le leve e liberi il meccanismo di bloccaggio.

Solo uscita - Modalità di configurazione dei punti di accesso. In modalità solo uscita, il punto di accesso accetta solamente le richieste di uscita. I lettori di ingresso vengono ignorati.

Supervisione - Operazione di controllo del corretto funzionamento dei dispositivi, svolta solitamente mediante monitoraggio della tensione o della resistenza. (Vedere anche: Supervisione EOLR e Supervisione mediante relè).

Supervisione EOLR (supervisione mediante resistore di fine linea) - Sistema che permette di rilevare quando un cavo che controlla una zona, per esempio un interruttore di modifica della porta, viene tagliato o circuitato. Il resistore può essere installato nel circuito della zona nel punto protetto in modo che il combinatore possa rilevare l'anomalia della linea, oltre alle condizioni di aperto e normale.

T

Tastiera - Si tratta solitamente di 12 tasti istantanei che permettono di trasmettere un codice al sistema in base ad una specifica sequenza di tasti. La tastiera assomiglia solitamente ad una tastiera telefonica per quanto riguarda la posizione e l'abbinamento dei tasti.

Tempo porta aperta - L'intervallo di tempo in cui il dispositivo di bloccaggio della porta rimane sbloccato (aperto) in seguito all'inserimento di una scheda valida nel lettore o ad una richiesta di uscita, senza che si verifichi una nuova condizione di bloccaggio.

Tempo segnale di preallarme - L'intervallo di tempo, in secondi, che trascorre prima che venga generato un allarme per porta aperta punto di accesso e durante il quale il dispositivo di preallarme è attivato.

Per esempio, se la programmazione della porta prevede un tempo di porta aperta di 30 secondi, il giusto tempo di preallarme è 10 secondi. Dopo 20 secondi dallo sblocco della porta, il sistema segnala per 10 secondi la condizione di porta aperta. Se al termine dei 30 secondi la porta è ancora aperta, il sistema genera un allarme per porta aperta. Il dispositivo di preallarme rimane attivato (in base alla modalità impostata) fino a chiusura della porta e cancellazione dell'allarme per porta aperta.

Terminali di uscita - Dispositivi ausiliari del sistema di controllo accesso che controllano dispositivi esterni quali serrature elettroniche, sirene piezo o spie. Si tratta di uscite di relè (contatti a secco) o di uscite a transistor (collettori elettrici).

Terminale di uscita relè a C - Configurazione composta da un terminale comune, un terminale normalmente aperto e un terminale normalmente chiuso. Se il relè è disattivato, il terminale comune è collegato al terminale normalmente chiuso e non al terminale normalmente aperto. Quando il relè è attivato, il terminale comune è collegato al terminale normalmente aperto e non al terminale normalmente chiuso.

Titolare scheda - Persona che occupa i locali e a cui è stata rilasciata una scheda di accesso o un codice di accesso per la richiesta di utilizzo dei punti di accesso protetti all'interno dei locali.

Transazione - Evento verificatosi all'interno del sistema di controllo accesso che genera un record nel database memorizzato.

U

Uscita logica - Interruttore digitale a stato solido (transistor) che può essere configurato come risorsa abbinata o non abbinata. Questi interruttori permettono di illuminare i LED, attivare le sirene piezo, attivare il relè esterno oppure segnalare un trasmettitore radio a lunga distanza.

V

Vacanza - Voce dei parametri di tempo che selezionano i giorni della settimana lavorativa in cui non devono essere applicati i parametri "normali". Per esempio, il Giorno del Ringraziamento viene considerato una vacanza.

A P P E N D I C E B

Indice analitico



Abbinamento partizione ai codici utente VISTA.2–10	Eventi temporizzati - foglio di programmazione 5–33
Abbinamento partizioni - codici utente VISTA2–10	Eventi temporizzati - programmazione 5–25
Abilitazione combinatori.....5–28	Foglio di programmazione - eventi temporizzati 5–33
Abilitazione combinatori di accesso5–28	Foglio di programmazione - funzione
Abilitazione gruppi di accesso5–26	evento/azione 5–34
Abilitazione RTE5–17	Foglio di programmazione - gruppi di accesso 2–14
Alimentazione - collegamento4–6	Foglio di programmazione - titolari scheda 6–18
Assemblaggio e montaggio.....4–2	Foglio di programmazione gruppi di accesso.. 2–14
Azioni di accesso..... 5–25, 5–28	Foglio di programmazione titolari scheda 6–18
Azioni di ingresso5–22	Funzione evento/azione - compilazione foglio di programmazione 5–7
Azioni di uscita 5–22, 5–28	Funzione evento/azione - foglio di programmazione 5–34
Cancellazione in blocco delle schede6–16	Funzione evento/azione - programmazione 5–23
Cancellazione manuale schede.....6–16	Funzioni scheda 6–5
Cancellazione schede6–15	GP 5–11
Caratteristiche modulo VistaKey.....1–1	Gruppi di accesso - abilitazione 5–26
Circuito polling - collegamento.....4–6	Gruppi di accesso - programmazione 5–20
Comandi - #73 abilitazione accesso 5–29	Inserimento schede nel database 6–7
Comandi - #78.....6–5	Installazione - procedura dettagliata 4–1
Comandi - Test6–5	Installazione - procedura rapida 3–1
Comandi controllo accesso6–2	Installazione del sistema 3–1, 4–1
Comandi tastiera.....6–1	Installazione tipo 4–1
Comandi tastiera - controllo accesso.....6–2	Integrazione del sistema di controllo accesso... 2–1
Comandi tastiera - controllo dispositivi di uscita6–4	Lettole scheda - montaggio e collegamento 4–4
Comandi tastiera - parametri di controllo.....6–5	Limiti in modalità inserita..... 2–6, 5–21
Comando #736–2	Livelli di autorità..... 5–31
Comando #73 abilitazione.....5–29	Livelli di autorità codici utente VISTA..... 2–8
Comando #746–2	Livelli utente - comandi validi..... 6–1
Comando #756–3	Modalità capacità ridotta..... 1–2, 9–1
Comando #776–4	Montaggio e collegamento del sistema..... 3–1
Comando #796–4, 6–5	Planimetria controllo accesso e sistema di allarme 2–1
Comando #806–5	Ponticello..... 7–2
Componenti.....1–2	Privilegi esclusivi..... 2–5, 5–20, 6–7, 6–11
Controllo dispositivi di uscita - comandi tastiera6–4	Programmazione..... 5–1
Controllo stato porta4–5	Programmazione - eventi temporizzati 5–25
Definizione privilegi gruppi di accesso2–3	Programmazione - funzione evento/azione 5–23
Descrizione LED.....7–2	Programmazione - funzioni scheda 6–5
Descrizione LED rosso7–2	Programmazione - gruppi di accesso 5–20
Descrizione LED verde7–2	Programmazione - opzioni punti di accesso ... 5–15
Descrizione RCM.....9–1	Programmazione - schede 6–5
Dispositivi esterni1–3	Programmazione - uscire dalla modalità 5–25
DSM 4–5, 5–10	Programmazione - zone..... 5–11
DSMB.....5–11	Programmazione zona 5–11
Esempio - definizione privilegi gruppi di accesso2–3	Punti di accesso - opzioni di programmazione 5–15
Esempio - planimetria controllo accesso/sistema di sicurezza2–1	Punti di accesso - uscita momentanea 5–26
Esempio - programmazione del sistema2–3	RCM..... 1–2, 9–1
Eventi di accesso 5–24, 5–28	Redazione schede..... 6–11
Eventi di ingresso.....5–21	Registro allarmi - allarmi 8–2
Eventi di uscita..... 5–22, 5–28	Registro allarmi - esclusione..... 8–2
Eventi temporizzati - compilazione foglio di programmazione.....5–2	Registro allarmi - sistema..... 8–2
	Registro allarmi - verifica 8–2

Registro allarmi della centralina	8-2
Registro eventi.....	8-1
Registro eventi - report alla centrale operativa	8-1
Report - accesso sistema	8-1
Report - allarmi accesso.....	8-1
Report - anomalia accesso.....	8-1
Report - centrale operativa	8-1
Report - esclusione accesso	8-1
Report - traccia accesso.....	8-2
Report alla centrale operativa	8-1
Richiesta di uscita	4-5
Rigenerazione azioni temporizzate	7-1
Rimozione modulo VistaKey.....	5-32
RTE	4-5, 5-10
Schede - cancellazione.....	6-15
Schede - cancellazione in blocco	6-16
Schede - cancellazione manuale	6-16
Schede - redazione.....	6-11
Schede - registrazione	6-7
Schede - uscire dalla programmazione	6-17
Schema elettrico - figura 3-1	3-4
Selezione indirizzo.....	4-6
Serratura magnetica - montaggio e collegamento	4-5
Sistemi compatibili.....	1-2
Tabella - codici azione	5-5
Tabella - eventi e azioni.....	5-9
Tabella codici azione	5-5
Tabella eventi e azioni	5-9
Tempo allarme	5-15
Tempo di preallarme	5-16
Tempo porta aperta.....	5-15
Test - mappatura zone per il test	3-2, 4-7
Test - test del sistema	7-1
Test - test iniziale del sistema.....	3-3, 4-8
Test del sistema.....	7-1
Tipo ingresso zona.....	5-13
Tipo zona.....	5-11
Traccia.....	5-21, 6-8, 6-12
Uscire dalla modalità programmazione scheda .	6-17
Uscita - momentanea	5-26
Uscita logica - collegamento	4-4
Uscita momentanea dal punto di accesso	5-26
Zone - collegamento.....	4-4
Zone - mappatura alle zone del sistema di allarme	5-10

GARANZIA ADEMCO LIMITATA

Alarm Device Manufacturing Company (ADEMCO), una Sezione della Pittway Corporation, e le sue divisioni, società controllate e filiali ("Rivenditore"), 165 Eileen Way, Syosset, New York 11791, certifica che i propri prodotti sono conformi agli schemi e ai dati tecnici presentati, garantendoli da difetti di materiale e di fabbricazione in normali condizioni di utilizzo e manutenzione per un periodo di due anni a decorrere dalla data impressa sul timbro di controllo del prodotto oppure, in mancanza di timbro ADEMCO, per un periodo di un anno a decorrere dalla data dell'acquisto originario, se non diversamente indicato sul manuale di Installazione o sul catalogo. In questo caso faranno fede i limiti indicati su tale documentazione. Tale garanzia consiste nella riparazione o sostituzione da parte del rivenditore e a proprio giudizio di tutti i componenti non conformi ai dati tecnici del Rivenditore o con difetti di fabbricazione e di materiale, in condizioni normali di utilizzo e di manutenzione. Le riparazioni e sostituzioni in garanzia non prevedono l'addebito per l'utente dei componenti, della manodopera e del trasporto. La garanzia o altro decade se il prodotto è alterato o riparato in modo non corretto o se la manutenzione è stata eseguita da personale diverso da quello del Servizio Assistenza ADEMCO. Per usufruire della garanzia, restituire il prodotto, con trasporto prepagato, a ADEMCO Factory Service, 165 Eileen Zay, Syosset, New York 11791.

NON ESISTONO GARANZIE, ESPLICITE O LEGALI, DI COMMERCIALIZZABILITÀ O IDONEITÀ A PARTICOLARI UTILIZZI O ALTRO CHE ESTENDONO OLTRE QUESTO TERMINE. IN NESSUN CASO IL RIVENDITORE E' RESPONSABILE VERSO TERZI PER DANNI INDIRETTI O INCIDENTALI DOVUTI ALLA VIOLAZIONE DI QUESTA O DI ALTRE GARANZIE, ESPRESSE O LEGALI, O PER QUALSIASI ALTRA RESPONSABILITÀ, ANCHE SE LA PERDITA O IL DANNO E' CAUSATO DA NEGLIGENZA O ERRORE DEL RIVENDITORE.

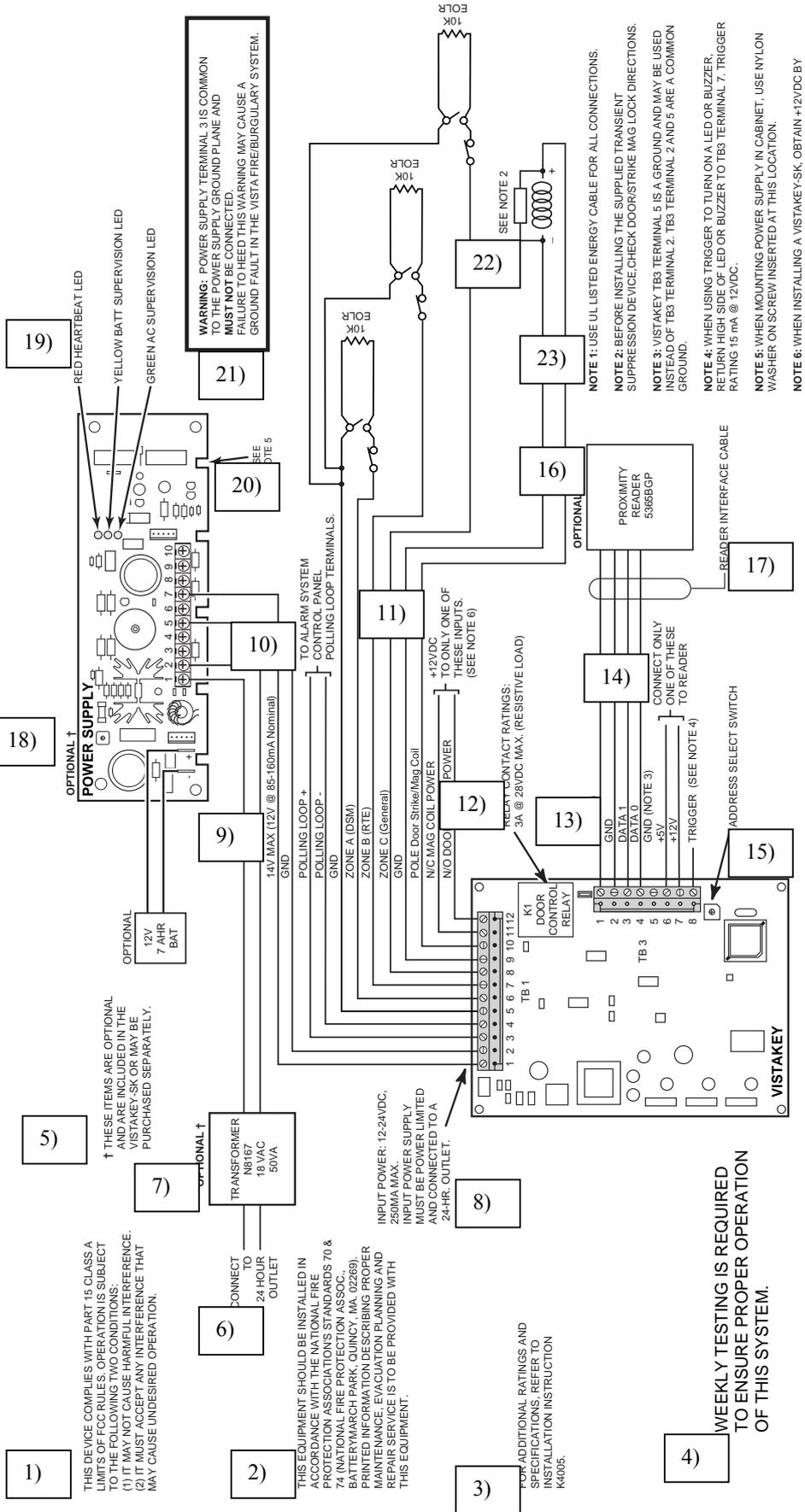
Il rivenditore non garantisce che il prodotto non possa essere manomesso o eluso o che il prodotto eviti lesioni personali o perdita di mobili in seguito ad eventi quali l'effrazione, il furto, l'incendio o altro; o che il prodotto fornisca un'adeguata prevenzione e una protezione certa. Il compratore è consapevole del fatto che un allarme correttamente installato e curato riduce solamente il rischio di effrazione, furto, incendio o di altri eventi che si verificano senza che il sistema generi un allarme. L'assicurazione o la garanzia non evitano il verificarsi di queste situazioni e le conseguenti lesioni personali o perdite materiali. CONSEQUENTEMENTE, IL RIVENDITORE NON E' RESPONSABILE PER LESIONI PERSONALI, DANNI MATERIALI O ALTRE PERDITE, CHE SI ASSUME SIANO STATE CAUSATE DA UN ERRATO FUNZIONAMENTO DEL PRODOTTO. COMUNQUE, QUALORA IL RIVENDITORE FOSSE RITENUTO RESPONSABILE, DIRETTAMENTE O INDIRETTAMENTE, PER PERDITE O DANNI VERIFICATISI NEL PERIODO DI GARANZIA LIMITATA O ALTRO, INDIPENDENTEMENTE DALLA CAUSA O DALL'ORIGINE, LA RESPONSABILITÀ DEL RIVENDITORE E' LIMITATA AL PREZZO DI ACQUISTO DEL PRODOTTO, SOLA ED UNICA AZIONE CONTRO IL RIVENDITORE. Questa garanzia sostituisce ogni precedente garanzia ed è l'unica garanzia fornita dal Rivenditore su questo prodotto. Ampliamenti e modifiche, scritti o verbali, degli obblighi in capo alla Garanzia Limitata non sono autorizzati.

ADEMCO
GROUP

165 Eileen Way, Syosset, New York 11791
Copyright © 2000 PITTWAY CORPORATION



K4005 01/00



SCHEMA CONNESSIONI

SCHEMA CONNESSIONI

- 1)
QUESTO DISPOSITIVO E' CONFORME ALLA SEZIONE 15 LIMITI DI CLASSE A DELLE NORME FCC. IL FUNZIONAMENTO DEL SISTEMA E' SOGGETTO ALLE SEGUENTI CONDIZIONI:
 - (1) IL DISPOSITIVO NON DEVE ESSERE CAUSA DI INTERFERENZE DANNOSE.
 - (2) IL DISPOSITIVO DEVE ESSERE IN GRADO DI SOPPORTARE QUALSIASI TIPO DI INTERFERENZA COMPRESSE QUELLE CHE POSSONO CAUSARE UN FUNZIONAMENTO ANOMALO.

- 2)
QUESTO IMPIANTO DEVE ESSERE INSTALLATO IN BASE ALLE NORME 70 E 74 DELLA NATIONAL FIRE PROTECTION ASSOCIATION (NATIONAL FIRE PROTECTION ASSOCIATION, BATTERYMARCH PARK, QUINCY, MA. 02269). LE ISTRUZIONI PER LA CORRETTA INSTALLAZIONE, I PIANI DI EVACUAZIONE E LE INFORMAZIONI RELATIVE ALLA MANUTENZIONE DEVONO ESSERE FORNITE CON IL PRODOTTO.

- 3)
PER ULTERIORI PRESTAZIONI E DATI TECNICI, FARE RIFERIMENTO AL MANUALE DI INSTALLAZIONE K4005.

- 4)
E' NECESSARIO EFFETTUARE CONTROLLI SETTIMANALI PER GARANTIRE IL CORRETTO FUNZIONAMENTO DEL SISTEMA.

- 5)
QUESTI ARTICOLI SONO OPTIONAL E SONO INCLUSI NEL KIT DI BASE VISTAKEY O POSSONO ESSERE ACQUISTATI SEPARATAMENTE.

- 6)
COLLEGARE ALL'USCITA 24 ORE

- 7)
OPTIONAL. TRASFORMATORE N8167 18VAC 50VA

- 8)
INGRESSO ALIMENTAZIONE: 12-24 V CC, 250MA MAX.
L'INGRESSO SISTEMA DI ALIMENTAZIONE DEVE ESSERE A CORRENTE LIMITATA E COLLEGATO AD UN USCITA 24 ORE.

- 9)
14V MAX. (12V@ 85-160Ma Nominale)
TERRA
CIRCUITO POLLING
CIRCUITO POLLING
TERRA
ZONA A (DSM)
ZONA B (RTE)
ZONA C (generico)
TERRA
POLO bobina serratura meccanica/magnetica
ALIMENTAZIONE BOBINA MAGNETICA N/C
ALIMENTAZIONE SERRATURA MECCANICA N/O

- 10)
AI MORSETTI DEL CIRCUITO POLLING DELLA CENTRALINA DEL SISTEMA DI ALLARME.

- 11)
+12V CC SOLO AD UNO DI QUESTI INGRESSI (VEDERE NOTA 6).

- 12)
PRESTAZIONI CONTATTO DI RELE'
3A @ 28V CC MAX. (CARICO RESISTIVO)

K1 RELE' CONTROLLO PORTA

- 13)
LED LETTORE
TERRA
DATI 1

ADEMCO
GROUP

165 Eileen Way, Syosset, New York 11791
Copyright © 2000 PITTWAY CORPORATION



K4005 01/00

DATI 2
TERRA (NOTA 3) *5V
+12V
USCITA LOGICA (VEDERE NOTA 4)

14)
COLLEGARNE SOLO UNO AL LETTORE

15)
COMMUTATORE DI INDIRIZZO

16)
OPTIONAL
LETTORE PROX
5365BGP

17)
CAVO INTERFACCIA LETTORE

18)
OPTIONAL
SISTEMA DI ALIMENTAZIONE

OPTIONAL
12V 7 AHR BATTERIA

19)
LED ROSSO INTERMITTENTE
LED GIALLO DI CONTROLLO BATTERIA
LED VERDE CONTROLLO ALIMENTAZIONE

20)
VEDERE NOTA 5

21)
ATTENZIONE: IL MORSETTO 3 DEL SISTEMA DI ALIMENTAZIONE E' COMUNE AL PIANO DI MASSA DEL SISTEMA DI ALIMENTAZIONE E **NON DEVE** ESSERE COLLEGATO.
EVENTUALI INOSSERVANZE POTREBBERO CAUSARE PROBLEMI DI MESSA A TERRA NEL SISTEMA ANTINCENDIO/ANTIFURTO VISTA.

22)
VEDERE NOTA 2

23)
NOTA 1: UTILIZZARE CAVI DI COLLEGAMENTO RIPORTATI NEGLI ELENCHI UL.

NOTA 2: PRIMA DI INSTALLARE IL SOPPRESSORE DI TRANSIENTI FORNITO, CONTROLLARE LA POLARITA' DELLA SERRATURA MECCANICA/MAGNETICA

NOTA 3: IL MORSETTO 5 DELLA MORSETTIERA TB3 DEL MODULO VISTAKEY CORRISPONDE ALLA TERRA E PUO' ESSERE UTILIZZATO AL POSTO DEL MORSETTO 2 DELLA MORSETTIERA TB3. I MORSETTI 2 E 5 DELLA MORSETTIERA TB3 CORRISPONDONO ALL'USCITA COMUNE TERRA.

NOTA 4: SE SI UTILIZZA L'USCITA LOGICA PER ATTIVARE UN LED O UNA SIRENA, RICOLLEGARE IL MONTE DEL LED O DELLA SIRENA AL MORSETTO 7 DELLA MORSETTIERA TB3. PRESTAZIONI USCITA LOGICA 15mA@12V CC.

NOTA 5: UTILIZZARE LE RONDELLE IN NYLON SULLE VITI PER L'INSTALLAZIONE DEL SISTEMA DI ALIMENTAZIONE NELL'ARMADIETTO.

NOTA 6: IN CASO DI INSTALLAZIONE DEL KIT DI BASE VISTAKEY, LA CORRENTE DI ALIMENTAZIONE DEVE ESSERE + 12VCC. COLLEGARE I MORSETTI 11 E 12 AL MORSETTO 1 DELLA MORSETTIERA TB1.

ADEMCO
GROUP

165 Eileen Way, Syosset, New York 11791
Copyright © 2000 PITTMWAY CORPORATION



K4005 6/00