

PassPoint *Plus*

Versione 2.00

GUIDA ALL'INSTALLAZIONE E ALLA PROGRAMMAZIONE

Per kit di controllo di accesso

ADEMCO
GROUP
INTEGRATED SYSTEMS

K4879 3/00



INFORMAZIONE IMPORTANTE

Questo prodotto è compatibile esclusivamente con gli standard UL294. Non è stato testato per compatibilità con gli standard UL1076. Le funzionalità della parte intrusione di questo prodotto sono solo in aggiunta alle caratteristiche di controllo di accesso del prodotto. I termini utilizzati in questa guida, come zone, perimetro, ecc., non si applicano specificatamente alle funzionalità della parte intrusione approvate da UL. Questi termini si riferiscono solo alle applicazioni di controllo di accesso di questo prodotto e alle funzionalità della parte intrusione del prodotto che non sono state approvate da UL.

ALARM DEVICE MANUFACTURING COMPANY

Una divisione della Pittway Corporation
165 Eileen Way, Syosset, NY 11791

ACCORDO DI LICENZA DEL SOFTWARE

Leggete attentamente i termini e le condizioni seguenti. Se non siete d'accordo con questa Licenza, siete pregati di restituire subito il pacchetto sigillato alla persona alla quale l'avete acquistato entro quindici (15) giorni dalla data di acquisto e la persona vi restituirà l'importo pagato. Se la persona che vi ha venduto il Software dovesse rifiutarsi di restituirvi il denaro, siete pregati di mettervi in contatto immediatamente con ADEMCO all'indirizzo indicato qui sopra.

Importante: questo Software è un dispositivo di sicurezza. Si consiglia di limitarne l'accesso alle persone autorizzate.

1. **GARANZIA DI LICENZA.** In base ai termini e alle condizioni definiti nel presente accordo, Alarm Device Manufacturing company, una divisione della Pittway Corporation ("ADEMCO") garantisce all'acquirente (il "Licenziatario"), dietro pagamento integrale della quota di licenza pubblicata o di qualsiasi altra quota di licenza concordata nel documento (la "Quota di Licenza"), una licenza non trasferibile e non esclusiva per l'utilizzo del software allegato ("Programmi Autorizzati"), fornito per essere utilizzato dal Licenziatario su un solo computer per un periodo di tempo indeterminato, calcolato a partire dalla data del pagamento integrale della Quota di Licenza e fino alla cessazione dell'accordo dei termini in esso contenuti.

2. **DIRITTI DI PROPRIETÀ.** La presente licenza riconosce che i Programmi Autorizzati, inclusi gli algoritmi in esso contenuti, sono di proprietà di ADEMCO. Il Licenziatario non può vendere, trasferire, divulgare o rendere comunque disponibile un qualsiasi Programma Autorizzato, o una copia o una parte di esso a terzi. Il Licenziatario accetta di proteggere i Programmi Autorizzati per conservare i diritti di proprietà di ADEMCO, incluse le istruzioni e gli accordi con i propri dipendenti.

3. **DOCUMENTAZIONE.** La documentazione fornita con i Programmi Autorizzati è di proprietà di ADEMCO ed è protetta dai diritti di autore. Il Licenziatario non deve assolutamente divulgare o consentire di divulgare questa documentazione a terzi.

4. **COPIE.** Il Licenziatario non è autorizzato a copiare l'integrità o una parte dei Programmi Autorizzati, o della documentazione fornita; il Licenziatario è comunque autorizzato ad effettuare una (1) copia dei Programmi Autorizzati esclusivamente per un backup, a condizione che vengano copiate anche tutte le informazioni riguardanti la proprietà e i diritti di autore. Questa copia sarà considerata parte dei Programmi Autorizzati e sarà soggetta alle stesse condizioni previste nel presente accordo.

5. **CODICE DI LINGUAGGIO.** Il Licenziatario concorda e accetta che i Programmi Autorizzati sono costituiti esclusivamente da codici di linguaggio e che ADEMCO non fornirà le versioni dei codici sorgente dei Programmi Autorizzati. Il Licenziatario non deve creare o cercare di creare tramite decompilazione o altro il codice sorgente dei Programmi Autorizzati o di una parte di essi.

6. **SICUREZZA.** Il Licenziatario riconosce che i Programmi Autorizzati sono dispositivi di sicurezza e l'accesso al Software Autorizzato dovrebbe essere limitato alle persone autorizzate. Il Licenziatario si assume tutta la responsabilità per l'uso dei Programmi Autorizzati da parte di persone autorizzate o non autorizzate. Il Licenziatario riconosce che la Quota di Licenza è stata calcolata sulla base della limitazione di responsabilità contenuta nel presente accordo e che questi provvedimenti sono corretti e non irragionevoli.

ADEMCO non dichiara che i Programmi Autorizzati non possano essere compromessi o aggirati, che i Programmi Autorizzati proteggeranno da qualsiasi danno personale o perdita di beni in seguito a furto, rapina, incendio o altro, o che i Programmi Autorizzati forniscono sempre l'allarme o la protezione adeguati. Il Licenziatario riconosce che un allarme installato correttamente e soggetto a controlli regolari può solo ridurre il rischio di furto, rapina o incendio senza allarme, ma non è un'assicurazione o una garanzia che tali fatti non si producano, o che non ci saranno danni a cose o persone in seguito a tali fatti.

RINUNCIA ALLE GARANZIE. ADEMCO non garantisce che i Programmi Autorizzati soddisferanno le vostre richieste, che i Programmi Autorizzati funzionino senza interruzione o senza errori, o che gli errori dei Programmi

Autorizzati siano corretti. Il rischio della qualità e delle prestazioni dei Programmi Autorizzati è interamente a vostro carico. RINUNCIAMO AL DIRITTO DI GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ, ADATTAMENTO A UNO SCOPO SPECIFICO E NON VIOLAZIONE. NESSUNA INFORMAZIONE O CONSIGLIO ORALE O SCRITTO DA PARDU DI ADEMCO, DEI SUOI DIPENDENTI, DISTRIBUTORI, COMMERCianti O AGENTI AUMENTERÀ LO SCOPO DELLE GARANZIE DI CUI SOPRA, NÉ CREERÀ NUOVE GARANZIE. ALCUNE GIURISDIZIONI NON AUTORIZZANO L'ESCLUSIONE DI GARANZIE IMPLICITE, E L'ESCLUSIONE DI CUI SOPRA POTREBBE NON ESSERE APPLICATA AL VOSTRO CASO. IN QUESTO CASO, QUALSIASI GARANZIA IMPLICITA È LIMITATA A UNA DURATA DI NOVANTA (90) GIORNI DALLA DATA DI CONSEGNA DEI PROGRAMMI AUTORIZZATI. Questa garanzia vi conferisce diritti legali specifici. Possono eventualmente esistere altri diritti, che variano da stato a stato.

8. LIMITAZIONE DELLE RIPARAZIONI. L'unica riparazione del Licenziatario può essere la sostituzione di un dischetto o di altro strumento che non rientri nella categoria della garanzia limitata indicata precedentemente, e che venga restituito ad ADEMCO con una copia della fattura pagata dal Licenziatario, oppure, se ADEMCO non fosse in grado di fornire una sostituzione senza alcun difetto, il Licenziatario può mettere fine a questo accordo restituendo i Programmi Autorizzati, e la Quota di Autorizzazione di cui sopra verrà rimborsata. ADEMCO non è legata ad alcun obbligo riportato nel presente Accordo se i Programmi Autorizzati sono modificati o riparati in modo sbagliato da persone che non facciano parte del servizio tecnico di ADEMCO. Per lavori coperti da garanzia, vi preghiamo di restituire i Programmi Autorizzati con porto prepagato ad ADEMCO Factory Service, 165 Eileen Way, Syosset, New York 11791.

9. LIMITAZIONE DI RESPONSABILITÀ. INDIPENDENTEMENTE DAL FATTO CHE UNA DELLE RIPARAZIONI INDICATE NEL PRESENTE ACCORDO NON SIA ADATTA ALLO SCOPO ESSENZIALE, IN NESSUNO CASO ADEMCO O I RELATIVI FORNITORI POSSONO ESSERE RITENUTI RESPONSABILI DI QUALSIASI DANNO PARTICOLARE, INDIRECTO O SIMILE, COMPRESSE PERDITE DI BENEFICI O PERDITA DI DATI, CONSEGUENTE ALL'USO O ALL'INCAPACITÀ DI UTILIZZARE I PROGRAMMI AUTORIZZATI O QUALSIASI ALTRO DATO FORNITO, ANCHE SE ADEMCO O CHIUNQUE ALTRO È STATO AVVISATO IN PRECEDENZA DELLA POSSIBILITÀ DI TALI DANNI, O DI QUALSIASI DOMANDA DI INDENNIZZO PRESENTATA DA TERZI. QUESTA DISPOSIZIONE È INSERITA A FAVORE DI ADEMCO E DEI PROPRI RAPPRESENTANTI LOCALI, ED È APPLICABILE DA CIASCUNO DI ESSI.

ALCUNE GIURISDIZIONI NON PERMETTONO LA LIMITAZIONE O L'ESCLUSIONE DI RESPONSABILITÀ PER DANNI FORTUITI O INDIRECTI; IN QUESTO CASO LA LIMITAZIONE O L'ESCLUSIONE QUI SOPRA NON POTRÀ ESSERE APPLICATA.

IN NESSUN CASO LA RESPONSABILITÀ DEI FORNITORI DEI PROGRAMMI AUTORIZZATI O DI ADEMCO POTRÀ SUPERARE IL PREZZO DI ACQUISTO VERSATO PER IL PRODOTTO.

10. REGISTRAZIONE. Per ricevere avvisi di aggiornamenti dei Programmi Autorizzati da parte di ADEMCO, il Licenziatario deve compilare e inviare ad ADEMCO un Formulario di Registrazione entro venti (20) giorni dalla data di acquisto. Allo scadere di questo periodo, ADEMCO non è più tenuta a fornire aggiornamenti dei Programmi Autorizzati.

11. CONCLUSIONE. In seguito a violazione o non rispetto di uno qualsiasi dei termini previsti dal presente Accordo, ADEMCO ha il diritto di mettere fine alla licenza con avviso scritto al Licenziatario. In seguito a questa rottura di contratto, il Licenziatario è tenuto a restituire immediatamente ad ADEMCO tutte le copie dei Programmi Autorizzati e tutta la documentazione relativa fornita. Questa disposizione è da considerarsi in aggiunta e cumulativa a qualsiasi altra disposizione a favore di ADEMCO in base alla legge e equivalente alla violazione e al non rispetto dell'accordo.

12. DISPOSIZIONI VARIE. Questo accordo rappresenta una dichiarazione completa e unica degli accordi fra le parti indicate nel presente, nel rispetto delle transazioni contemplate dal presente, e sostituisce qualsiasi altra proposta o accordo precedenti. Questo Accordo potrà essere modificato solo ed esclusivamente con un documento scritto firmato dal Licenziatario e da un rappresentante autorizzato di ADEMCO, dei suoi diritti, doveri o obblighi in base al presente Accordo. Se un qualsiasi provvedimento del presente Accordo non sia ritenuto valido nei confronti di una qualsiasi altra disposizione legislativa, tale controversia dovrà essere sanata in base alle leggi dello Stato di New York e solo ed esclusivamente in un tribunale statale o federale che si trovi nello Stato e nella Città di New York. L'incapacità di ADEMCO di agire nel rispetto di tutti i diritti contemplati nel presente Accordo non deve essere considerata una rinuncia a tali diritti, né nessun altro Accordo potrà essere stipulato dopo più di due (2) anni dalla data alla quale tale azione si fosse prodotta. ADEMCO ha il diritto di esigere dal Licenziatario il rimborso di tutte le spese legali sostenute per far rispettare i propri diritti in base al presente accordo.

Sommario

Parte prima – Impostazione di PassPoint

Introduzione all'impostazione	1-1
Presentazione dei kit di PassPoint	1-2
Gerarchia del sistema	1-3
Riepilogo della prima parte	1-5
Presentazione dell'Access Starter Kit	1-6
Mappa di installazione e di impostazione	1-10
Introduzione alla fase successiva	1-11
Preparazione dell'installazione	2-1
Come preparare l'installazione	2-3
Alcune domande fondamentali	2-3
Domanda 1 – Dove saranno posizionati i miei varchi?	2-4
Domanda 2 – Quale livello di sicurezza è necessario per i varchi?	2-4
Domanda 3 – Quale tipo di hardware di controllo della porta utilizzare?	2-5
Domanda 4 – Dove sarà posizionato il computer di sistema?	2-5
Utilizzo di una mappa	2-5
Selezione dei varchi	2-8
Esempio 1 – Controllo ingresso di base	2-9
Esempio 2 – Controllo ingresso con monitoraggio stato porta	2-10
Esempio 3 – Controllo ingresso con monitoraggio stato porta e richiesta di uscita	2-11
Esempio 4 – Controllo ingresso e uscita con monitoraggio stato porta	2-12
Configurazione del Door Control Module	2-13
Tipi di lettori badges	2-15
Introduzione alla fase successiva	2-17
Installazione del sistema	3-1
Sommario delle fasi d'installazione	3-3

Fase 1 – Montaggio della centrale del sistema	3-4
Fase 2 – Collegamento dei moduli del sistema	3-5
Fase 3 – Montaggio e collegamento dei lettori di badges.....	3-7
Montaggio dei lettori	3-8
Collegamento dei lettori.....	3-8
Fase 4 – Montaggio e collegamento delle elettroserrature e delle serrature elettromagnetiche	3-10
Montaggio delle elettroserrature e delle serrature elettromagnetiche.....	3-11
Collegamento delle elettroserrature e delle serrature elettromagnetiche	3-11
Fase 5 – Collegamento del cavo del computer	3-13
Collegamento cavi.....	3-13
Collegamento terminale remoto.....	3-15
Fase 6 – Montaggio e collegamento della tastiera e accensione del sistema.....	3-18
Fase 7 – Collegare la batteria 7 amperora in opzione.....	3-20
Introduzione alla fase successiva	3-21
Impostazione del Software.....	4-1
Presentazione di PassPoint Plus	4-4
Requisiti di sistema	4-5
Fase 1 – Installazione di PassPoint Plus	4-6
Fase 2 – Avviamento di PassPoint Plus.....	4-8
Fase 3 – Creazione di un nuovo cliente	4-9
L'ambiente PassPoint Plus	4-13
Principali componenti dello schermo	4-13
Configurazione del sistema.....	5-1
Fase 1 – Avviamento del Setup Wizard	5-4
Fase 2 – Stabilire le comunicazioni.....	5-7
Fase 3 - Auto acquisizione moduli	5-9
Aut acquisizione di un solo modulo.....	5-10
Auto acquisizione di più moduli.....	5-11
Fase 4 – Aggiornamento del Database.....	5-13
Gestione dei database badges e utenti	6-1
Presentazione del database utenti.....	6-2
Utilizzo di Wizard badges.....	6-4
Aggiunta di una sola scheda.....	6-5

Aggiunta di un lotto di badges	6-9
Aggiunta manuale di badges.....	6-10
Utilizzo dell'etichetta Azioni.....	6-15
Utilizzo dell'etichetta Personale	6-16
Utilizzo dell'etichetta Impiego.....	6-18
Utilizzo dell'etichetta Personalizzazione.....	6-19
Utilizzo dell'etichetta Sommario	6-21
Utilizzo dell'etichetta Eventi	6-25
Modifica blocco badges	6-26
Modifica blocco attribuzione gruppi accesso utente	6-28
Modifica blocco privilegi executive / traccia.....	6-29
Modifica blocco disabilitazione/data di scadenza	6-30
Modifica blocco campi personalizzati utente	6-33
Monitor badge.....	6-34
Creazione del monitor badge.....	6-35
Utilizzo del monitor badge	6-36
Impostazione delle opzioni generali del sistema	7-1
Opzioni generali del sistema PassPoint	7-2
Preimpostazioni del sistema (Etichetta Predefiniti)	7-3
Attributi predefiniti del lettore	7-4
Attributi predefiniti varco	7-5
Opzioni tecnologia badge (Etichetta tecnol. badge)	7-6
Informazioni riconoscimento badges	7-6
Lunghezza badges	7-7
Schermo Configurazione MagStripe ABA	7-8
Esempio di configurazione ABA MagStripe	7-14
Codici residenti (Etichetta Residenti)	7-16
Creazione e attribuzione di codici badges residenti	7-19
Codici PIN residenti.....	7-29
Opzioni parte intrusione (Etichetta Parte intrusione)	7-29
Configurazione intrusione	7-29
Tastiera di sistema	7-32
Visualizzazioni da tastiera	7-32
Beep e video del varco (etichetta Beep/Video)	7-32
Opzioni selezionatore (Etichetta Selezionatore).....	7-34
Opzioni Modem (Etichetta Modem).....	7-34

Proprietà della sessione	7-34
Rubrica.....	7-35
Iniziatori chiamate in uscita	7-36
Opzioni rete ID (Etichetta Rete/ID).....	7-36
Rete	7-37
Identificazione	7-38
Opzioni priorità (Etichetta Priorità)	7-38
Modifica delle priorità di un evento	7-40
Modifica degli attributi di un evento.....	7-40
Impostazione cercapersone evento.....	7-42
Impostazione invio e-mail evento	7-46
Creazione istruzione eventi	7-48
Liste risorse	8-1
Impostazione liste risorse	8-2
Etichetta varchi.....	8-3
Etichetta lettori.....	8-5
Etichetta relè	8-6
Etichetta Trigger	8-8
Etichetta Zone	8-9
Utilizzo delle liste risorse.....	8-11
Aggiunta di un Door Expansion Kit	9-1
Informazioni sul Door Expansion Kit	9-2
Installazione del DEK.....	9-3
Fase 1 – Montaggio della centrale DEK.....	9-3
Fase 2 – Collegamento del DCM.....	9-5
Fase 3 – Attivazione del sistema	9-7
Fase 4 – Aggiunta e impostazione del DCM	9-8
Fase 5 - Auto acquisizione del modulo DCM	9-15
Fase 6 – Aggiornamento del database	9-20
Configurazione del DCM.....	9-21
Etichetta sistema DCM	9-22
Etichetta varco A/B.....	9-23
Etichetta Lettori	9-35
Etichetta Relè.....	9-37
Etichetta Triggers	9-39

Etichette Zona	9-41
Etichetta RCM residenti.....	9-44
Aggiunta di un Card Enrollment Kit.....	10-1
Presentazione del Card Enrollment Kit	10-2
Installazione del CEK.....	10-3
Fase 1 – Scelta di una posizione per il CEK	10-3
Fase 2 – Collegamento del CEK al sistema.....	10-3
Fase 3 – Collegamento del trasformatore e attivazione del sistema	10-4
Fase 4 – Aggiunta e impostazione del CEK.....	10-5
Fase 5 - Auto acquisizione del CPM	10-7
Fase 6 – Configurazione del lettore	10-12
Etichetta lettore	10-13
Etichetta Terminale operatore	10-15
Fase 7 – Aggiornamento del database	10-15
Aggiunta di un VISTA Gateway Module.....	11-1
Presentazione del VISTA Gateway Module	11-2
Installazione del VGM.....	11-3
Fase 1 – Montaggio del VGM	11-3
Fase 2 – Collegamento del VGM.....	11-4
Fase 3 – Aggiunta e impostazione del VGM.....	11-6
Fase 4 – Auto acquisizione del VGM.....	11-7
Fase 5 – Abilitazione del VGM in VISTA.....	11-12
Fase 6 – Configurazione del VGM.....	11-13
Impostazione del programma orario per le chiamate di prova e dell'interfaccia VGM.....	11-14
Impostazione zone VISTA	11-16
Impostazione dell'utente VISTA di default	11-21
Fase 7 – Aggiornamento del database	11-22
Aggiunta di Moduli di sistema.....	12-1
Presentazione dei moduli di sistema.....	12-2
Installazione dei moduli.....	12-3
Aggiunta e acquisizione di un modulo.....	12-3
Aggiunta di un modulo.....	12-3
Acquisizione di un modulo.....	12-5

Configurazione dei moduli	12-10
Finestra di dialogo impostazione DCM	12-11
Finestra di dialogo impostazione QRM	12-12
Etichetta sistema QRM	12-13
Etichette Relè	12-14
Etichette Trigger	12-16
Finestra di dialogo impostazione CPM	12-17
Etichetta sistema CPM	12-18
Etichetta lettore	12-18
Etichetta Terminale operatore	12-20
Finestra di dialogo impostazione VGM	12-20
Finestra di dialogo impostazione ZIM	12-21
Etichetta sistema ZIM	12-21
Etichette zone ZIM	12-22
Aggiornamento del Database	12-25
Istruzioni di cablaggio	A-1
Istruzioni di cablaggio	A-2
Topologia	A-2
Note di cablaggio	A-7
Specifiche dei cavi	A-8
Cablaggio Main Logic Board	A-9
Cablaggio Door Control Module	A-10
Specifiche di alimentazione	A-11
Aggiornamento del Firmware	B-1
Aggiornamento Firmware MLB	B-2
Aggiornamento delle informazioni cliente	B-10
Schemi di cablaggio	C-1
Cavo null-modem	C-2
Cavo estensione	C-3
Cavo modem	C-4
Door Expansion Kit	C-5
Card Enrollment Kit	C-6
VISTA Gateway Module	C-7
Main Logic Board	C-8

Door Control Module.....	C-9
Alimentazione.....	C-10
Glossario controllo di accesso	G-1
Indice controllo di accesso	I-1

Parte prima



*Impostazione di
PassPoint*

Capitolo

1

Introduzione all'impostazione

Questo capitolo fornisce una presentazione dei vari kit di controllo di accesso PassPoint e una descrizione esauriente dell'Access Starter Kit, con le fasi necessarie all'installazione e alla configurazione del sistema.

Questo capitolo comprende:

- **Il contenuto di questa prima parte**
- **Il contenuto dell'Access Starter Kit**

Presentazione dei kit di PassPoint

Questa guida riguarda i kit di PassPoint, i pacchetti di base pre configurati da utilizzare per rendere rapidamente operativo il sistema. Ogni kit è indipendente. Combinando più kit (e moduli PassPoint separati), è possibile espandere e ingrandire qualsiasi impianto PassPoint già esistente.

Esistono quattro tipi di kit PassPoint:

- **Basic Starter Kit (BSK)**

Il BSK contiene tutto tranne i lettori e i badges necessari a rendere operativo un impianto a due porte. Questo kit è stato creato essenzialmente per gli aggiornamenti degli impianti.

- **Access Starter Kit (ASK)**

L'ASK contiene tutto il necessario per rendere operativo un impianto a due lettori. Si tratta del pacchetto di base della maggior parte dei sistemi di PassPoint. La maggior parte di questa guida riguarda l'ASK.

- **Door Expansion Kit (DEK)**

Il DEK consente di aggiungere altri due lettori a un sistema PassPoint già operativo. I componenti del DEK e le istruzioni per l'installazione e la configurazione sono riportati nel capitolo "Aggiunta di un Door Expansion Kit" di questa guida.

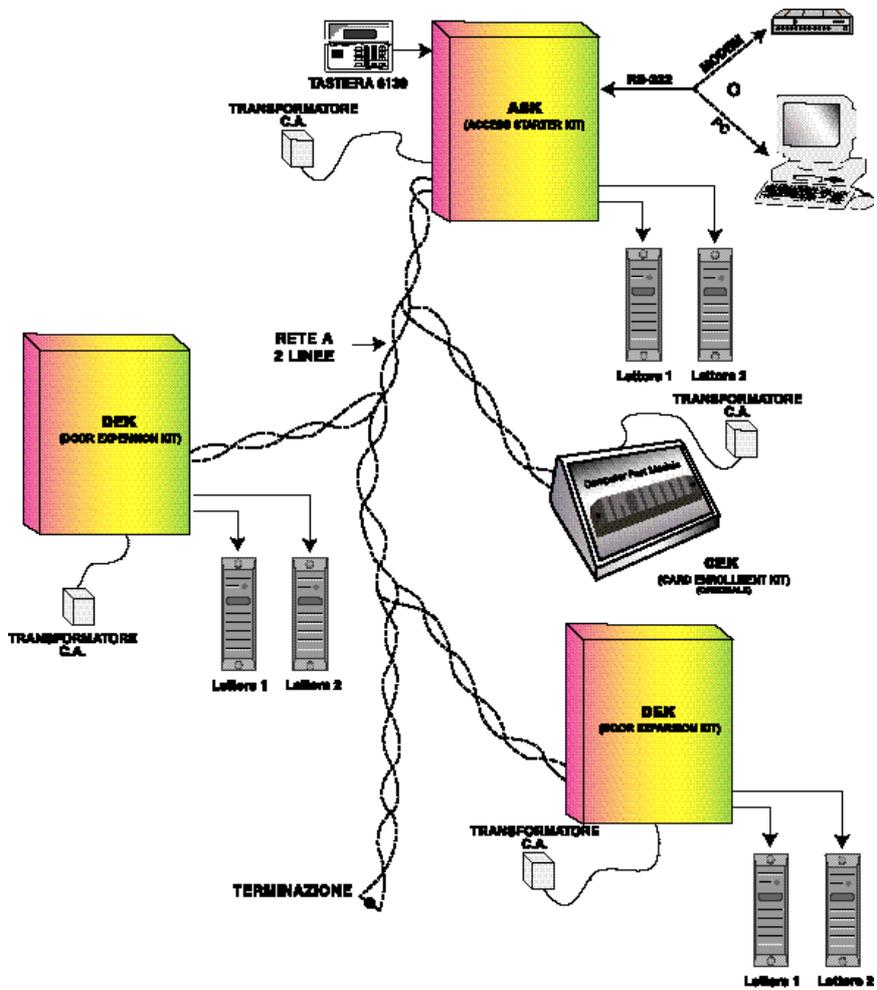
- **Card Enrollment Kit (CEK)**

Il CEK è un kit che consente di acquisire rapidamente i badges da rendere operativi nel sistema. Si compone essenzialmente di un lettore di auto acquisizione badges indipendente. Le istruzioni per l'installazione e la configurazione del CEK sono riportate nel capitolo "Aggiunta di un Card Enrollment Kit" in questa guida.

- Oltre a questi kit, è possibile aggiungere moduli personali a un sistema PassPoint. Per ulteriori informazioni sui moduli personali, vedere il capitolo “Aggiunta di moduli di sistema” in questa guida.

Gerarchia del sistema

Il sistema PassPoint è composto da kit. E' stato riprodotto qui di seguito un esempio di un impianto PassPoint di base:



Riepilogo della prima parte

La prima parte di questa guida contiene tutto il necessario per rendere operativo l'Access Starter Kit di PassPoint e guida attraverso tutte le fasi delle procedure, dall'installazione del software all'acquisizione di alcuni badges di prova. Dopo aver acquisito alcuni badges, è possibile provare il sistema per controllare che funzioni correttamente. Dopo aver installato il Basic Starter Kit, seguire le stesse istruzioni dell'Access Starter Kit. Gli argomenti non validi per il Basic Starter Kit sono indicati nei relativi punti della guida.

-
- Questa parte è stata scritta per un sistema con due sole porte. Se è stato aggiunto un Door Expansion Kit o un Card Enrollment Kit, consultare la seconda parte della guida, per avere istruzioni complete sull'installazione e la configurazione dei kit.

La prima parte della guida è stata suddivisa in quattro parti:

- **Prima parte – Preparazione all'installazione**

Prima di installare il sistema PassPoint, è necessario seguire alcune fasi di preparazione. Una preparazione adeguata faciliterà notevolmente l'installazione del sistema. Il capitolo 2 illustra come preparare l'installazione.
- **Seconda parte – Installazione del sistema**

Il capitolo 3 riguarda la fase di installazione e spiega come collegare tutti i moduli del sistema forniti con il kit, incluso il montaggio dell'armadio e il cablaggio dei lettori.
- **Terza parte – Installazione di PassPoint *Plus***

PassPoint *Plus* è il software da utilizzare per configurare e rendere operativo il sistema PassPoint. Deve essere installato sul computer dell'operatore (ad esempio il PC usato per

collegarsi alla centrale del sistema). Il capitolo 4 riguarda tutta l'installazione di PassPoint *Plus*.

- **Quarta parte – Configurazione del sistema**

Dopo aver installato l'hardware, è necessario configurare il sistema perché funzioni correttamente. La maggior parte delle opzioni di configurazione degli starter kit di PassPoint sono già state predefinite dal costruttore, ma restano alcune opzioni di configurazione da impostare in base alle necessità come l'impostazione delle porte e l'acquisizione dei badges.

Le informazioni sulla configurazione cominciano al capitolo 5.

Presentazione dell'Access Starter Kit

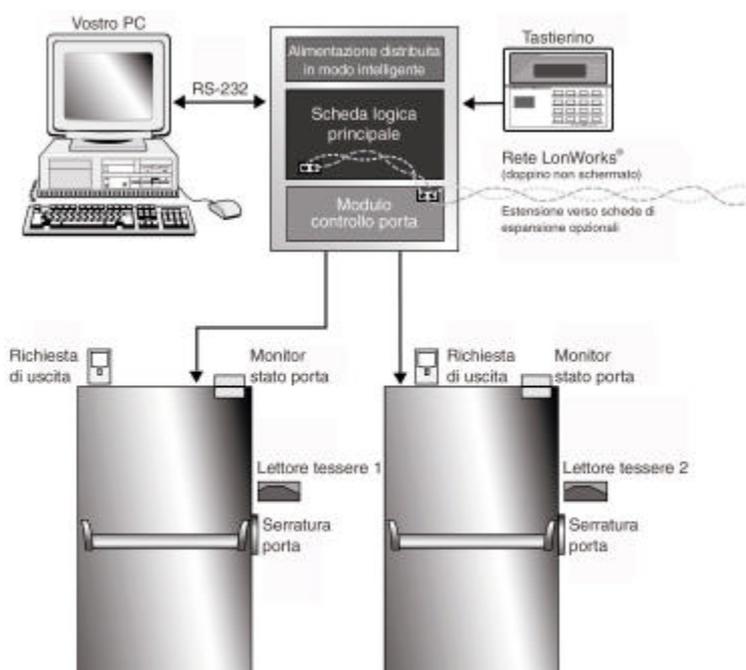
L'Access Starter Kit (ASK) è stato creato in modo tale da essere installato e configurato facilmente. Sono state fornite opzioni di configurazione predefinite quando possibile. Seguendo le procedure illustrate in questa guida, non dovrebbero esserci problemi per rendere operativo il sistema.

Cosa comprende il kit?

L'Access Starter Kit comprende i seguenti componenti hardware:

- 1 centrale di accesso pre configurata, composta da:
 - 1 custodia metallica
 - 1 Main Logic Board
 - 1 Door Control Module
 - 1 alimentatore
- 1 trasformatore
- 2 lettori di prossimità per montaggio su infisso (solo ASK)
- 1 tastiera ADEMCO 6139
- 50 Badges (solo ASK)

- Software PassPoint Plus
- 1 cavo RS-232 (cavo null-modem)
(Usato per collegare la centrale PassPoint alla porta seriale del computer)



Access Starter Kit in una configurazione di sistema tipica

Componenti principali

Esistono quattro componenti principali del sistema PassPoint:

Main Logic Board (MLB)

La MLB è l'unità di controllo del sistema. Contiene il database dei badges, la memoria eventi e le informazioni per la configurazione

del sistema. Tiene anche traccia dello stato del sistema. La MLB è alimentata dall'alimentatore di PassPoint e comunica con il Door Control Module (descritto più sotto) per decidere se autorizzare l'accesso a un determinato varco.

Door Control Module (DCM)

Il modulo DCM fornisce tutti gli ingressi e le uscite necessari a gestire due varchi (due porte). Il modulo DCM può collegare due lettori e accettare simultaneamente dati provenienti da due lettori. E' equipaggiato con due relè a scambio pulito con uscite monitorate (monitoraggio di tensione) utilizzati per attivare i blocchi elettromagnetici o le elettroserrature. Fornisce anche due uscite per l'eventuale azionamento di segnalatori acustici o LED.

L'alimentatore del sistema PassPoint

L'alimentatore del sistema PassPoint fornisce tutta l'energia necessaria per la MLB e il modulo DCM. E' collegato alla linea in c.a. tramite un trasformatore di potenza a 18VAC, 50VA (fornito in dotazione). L'alimentatore è provvisto del cavo di collegamento per la batteria di backup e nell'armadio può essere alloggiata una batteria da 7Ah (non fornita).

Le informazioni sul collegamento e le specifiche dell'alimentatore sono riportate nell'Appendice A.

Interfaccia del sistema PassPoint Plus

PassPoint *Plus* è un programma software compatibile con i sistemi operativi Windows 95, Windows 98 e Windows NT 4.0, che permette al computer di comunicare con la Main Logic Board. PassPoint *Plus* viene utilizzato per configurare il sistema. Quando il sistema è operativo, gli operatori utilizzeranno PassPoint *Plus* per la gestione in linea di PassPoint.

L'interfaccia utente di PassPoint richiede un computer, che viene utilizzato per configurare il sistema e renderlo operativo. Al termine della configurazione, non è indispensabile mantenere il computer collegato perché il sistema può funzionare senza interventi. Se si utilizza PassPoint *Plus* a distanza, saranno necessari due modem per collegare il computer al sistema.

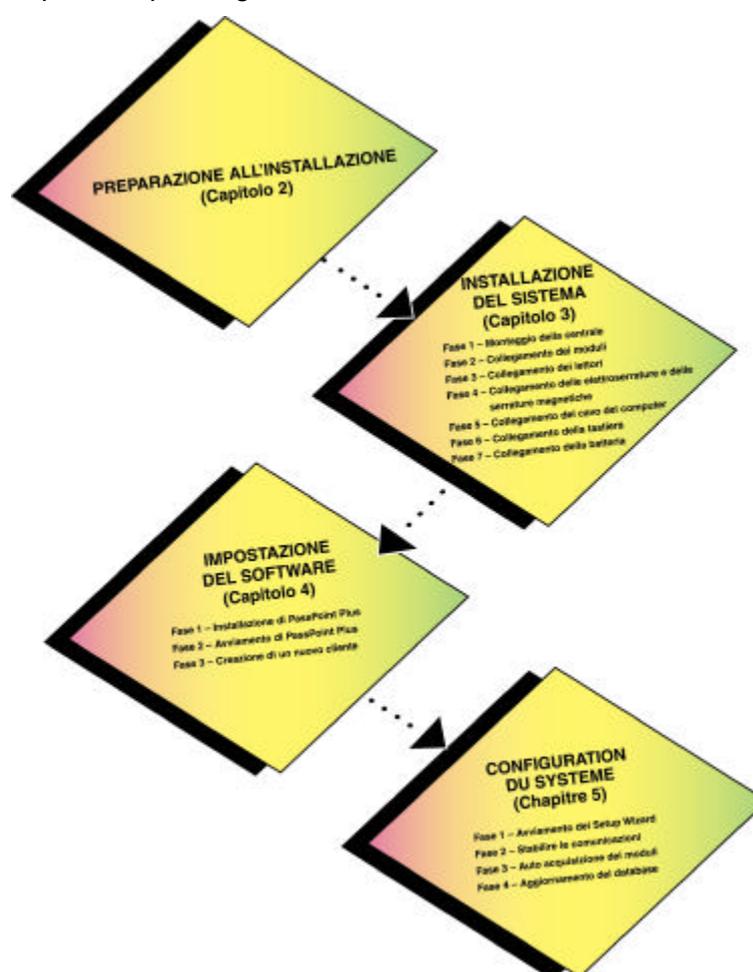
-
-

Il computer e il modem sono comunque considerati accessori e non sono forniti con lo Starter Kit.

Per ulteriori informazioni, vedere il paragrafo "Requisiti di sistema" nel capitolo 4.

Mappa di installazione e di impostazione

Qui sotto sono indicate tutte le fasi da seguire per rendere operativo il sistema PassPoint. Le fasi sono separate in varie parti, ognuna delle quali viene spiegata dettagliatamente nei vari capitoli di questa guida.



Introduzione alla fase successiva

Il capitolo successivo fornisce le istruzioni necessarie per preparare l'installazione. Verrà indicato come utilizzare una mappa per impostare la struttura del sistema, e verranno poste domande importanti da analizzare attentamente prima di procedere all'installazione del sistema.

Capitolo

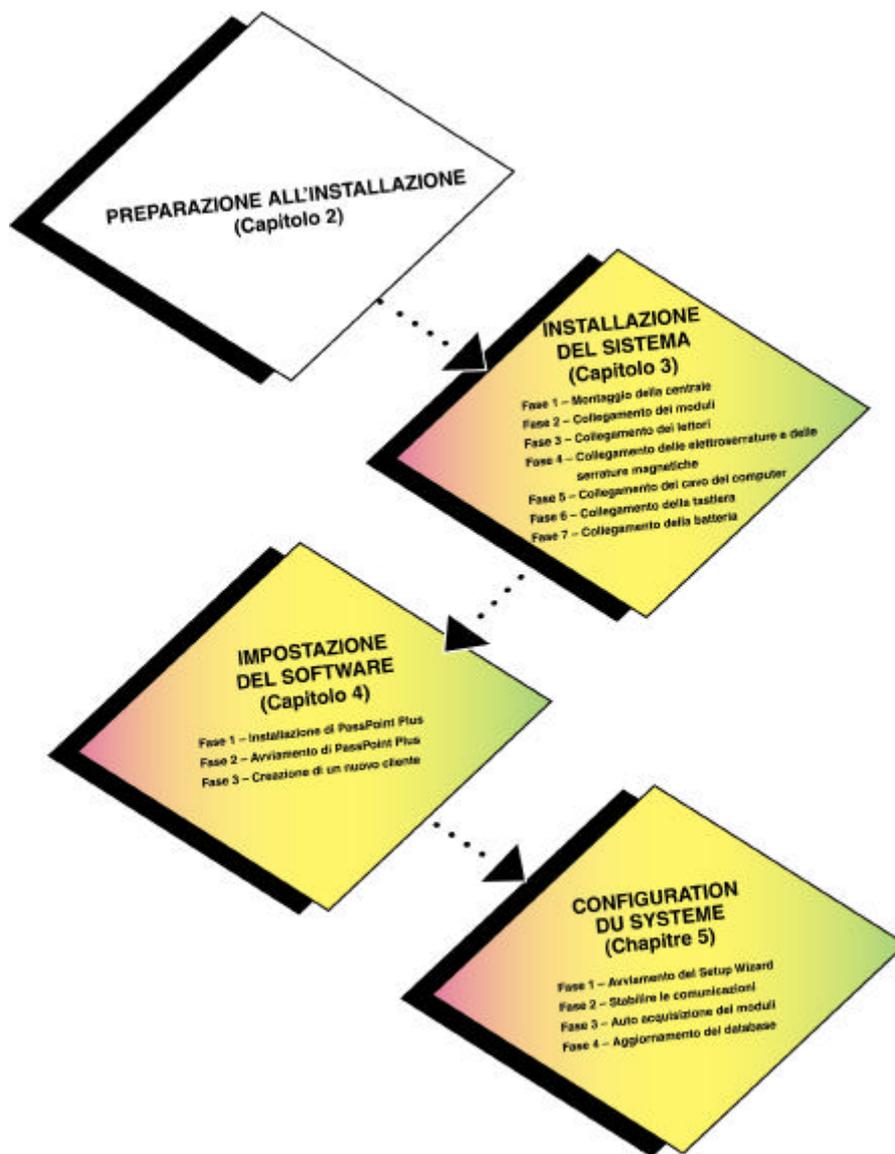
2

Preparazione dell'installazione

Prima di installare il sistema PassPoint, è necessaria una fase di preparazione, che faciliterà notevolmente tutto il processo d'installazione.

Questo capitolo comprende:

- **Come installare PassPoint per rispondere alle esigenze**
- **Come selezionare e configurare i varchi del sistema**
- **Come sistemare i componenti del sistema**
- **Quali fasi seguire per installare l'hardware**



Come preparare l'installazione

Con PassPoint, è indispensabile procedere a una fase di preparazione, perché l'installazione sia più semplice e si svolga senza problemi. E' necessario conoscere i luoghi, i varchi e il livello di sicurezza desiderato per ogni varco. L'hardware del sistema, inoltre, deve essere posizionato e utilizzato correttamente.

Il sistema è molto flessibile, ed è quindi possibile installare i componenti in modi diversi. Esistono, comunque, alcune caratteristiche comuni a tutte le installazioni, come i varchi e l'hardware. Questa configurazione comune costituisce un ottimo punto di partenza per la preparazione dell'installazione.

I varchi

La definizione di varchi di PassPoint va ben al di là di quella di semplice porta. Un varco rappresenta una serie di oggetti (risorse), che consentono di entrare o uscire da una porta. Questi oggetti comprendono tutto quanto è collegato all'hardware (lettori, serrature, ecc.) e le funzioni software che caratterizzano il varco (programmi orari, utenti, ecc.).

Alcune domande fondamentali

Il sistema migliore per cominciare la preparazione dell'installazione è quello di porsi alcune domande sul luogo nel quale verrà installato PassPoint. Rispondendo a queste domande, sarà più facile definire il tipo di hardware necessario, il luogo in cui dovrà essere installato, come dovrà essere cablato, ecc. In seguito, dopo aver installato e cablato l'hardware del sistema, sarà possibile configurarlo servendosi del software PassPoint Plus.

Di seguito sono riportate alcune domande da porsi prima di cominciare l'installazione. E' importante notare che queste domande sono di carattere generale. Considerata la grande flessibilità di PassPoint, è impossibile prevedere e descrivere tutti gli scenari possibili. Ma con una guida generale, le risposte alle domande seguenti potranno comunque guidare a una installazione ottimale di PassPoint.

Domanda 1 – Dove saranno posizionati i miei varchi?

Si tratta forse della domanda più importante nella preparazione dell'installazione. I varchi, o porte, controllano gli ingressi e le uscite di un determinato locale o edificio, e il flusso di traffico all'interno di esso. E' necessario determinare quali porte si vogliono controllare.

Vedere il paragrafo “*Selezione dei varchi*” in questo capitolo per le istruzioni sulla scelta dei varchi del sistema.

Domanda 2 – Quale livello di sicurezza è necessario per i varchi?

I livelli di sicurezza dei varchi possono essere diversi, a seconda del tipo di hardware utilizzato e della sua configurazione. E' possibile avere una porta con un solo lettore, o con una combinazione lettore/tastiera. Si può monitorare la porta o lasciarla sempre aperta. Sono disponibili molte altre opzioni di livelli di sicurezza.

Vedere il paragrafo “*Selezione dei varchi*” in questo capitolo per maggiori informazioni sui livelli di sicurezza dei varchi.

Domanda 3 – Quale tipo di hardware per il controllo della porta utilizzare?

Il tipo di hardware di controllo della porta dipende in parte dal livello di sicurezza desiderato per ogni varco. Come già indicato precedentemente, è possibile avere porte con un solo lettore o porte con una combinazione lettore/tastiera, dove l'utente dovrà digitare un codice PIN e presentare il proprio badge. Esistono diversi tipi di hardware di controllo porta disponibili, e diversi modi di configurarli.

Domanda 4 – Dove sarà posizionato il computer del sistema?

E' necessario definire la locazione in cui posizionare il computer su cui sarà installato il software, senza dimenticare che il collegamento tra il computer e la MLB non deve superare i 15 metri. Non esistono altri limiti fisici di distanza, poiché la Main Logic Board del sistema può comunicare con l'interfaccia del sistema via ethernet o via modem, sempre a condizione che il cavo RS-232 tra il sistema e il modem o l'interfaccia ethernet, o tra il modem e il computer non superi i 15 metri.

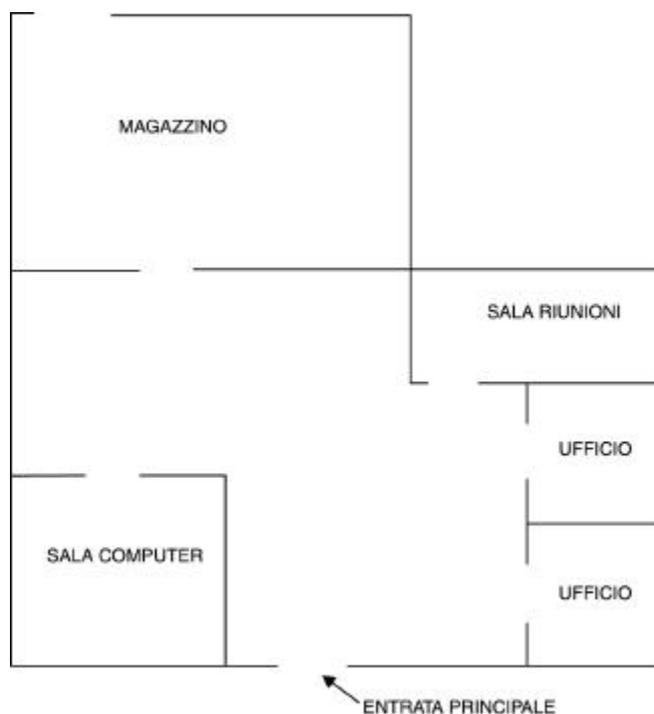
Utilizzo di una mappa

Al momento della preparazione dell'installazione di PassPoint, si consiglia di procurarsi una mappa dei luoghi d'installazione, che consente di visualizzare l'installazione e aiuta a definire i varchi e la posizione dell'hardware. Una mappa può essere una qualsiasi cianografia o una pianta che riporti la base (una visione dall'altro) dei locali.

In mancanza di una mappa dei locali, si può semplicemente disegnarne una. E' molto semplice, basta una semplice visione aerea dell'edificio, con relative porte e locali in scala con le

dimensioni approssimative. Le dimensioni sono importanti, perché bisogna tenere conto della lunghezza dei cavi al momento del cablaggio dell'hardware del sistema.

Ecco un esempio di una mappa semplice:

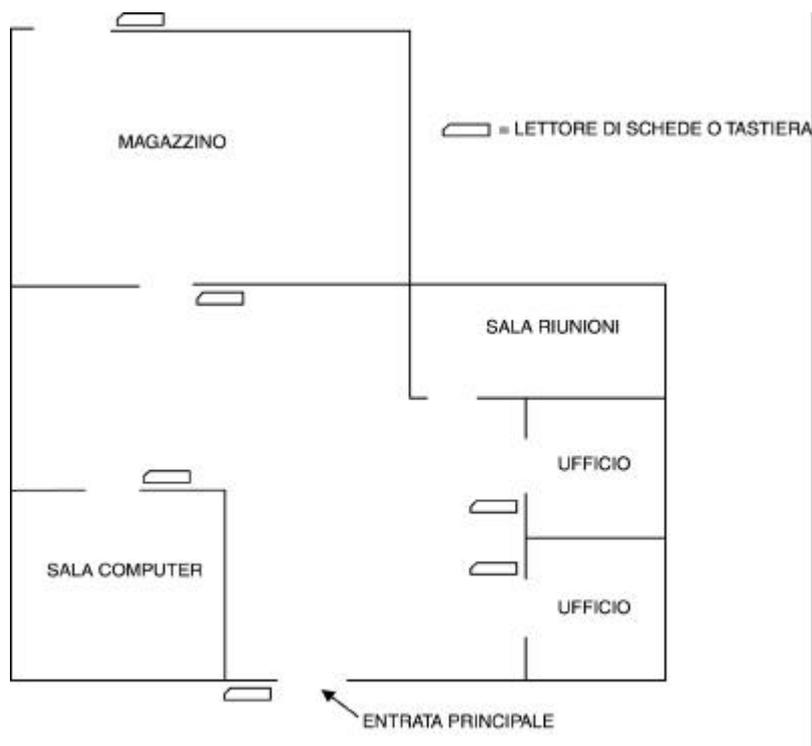


Si tratta di un ufficio senza PassPoint. Notare che tutte i locali sono accessibili a chiunque.

Naturalmente, è possibile disegnare una mappa molto più particolareggiata, ma il principio rimarrà lo stesso. Esiste un edificio con un ingresso/uscita principale, e altri locali o luoghi da proteggere.

Con la mappa si può decidere cosa si vuole proteggere e in quale modo:

Lo stesso ufficio, con l'installazione di PassPoint, che controlla il transito delle persone fra i locali.



In questa installazione di PassPoint si vede che la maggior parte delle stanze sono state protette con un lettore (o una tastiera). La sala riunioni non è stata protetta dal sistema PassPoint, perché chiunque deve potervi accedere in qualsiasi momento. Si noti anche che la mappa qui sopra indica l'uso di lettori o tastiere, ma si può trattare di un abbinamento dei due (lettore e tastiera).

Selezione dei varchi

Il primo passo nella preparazione all'installazione del sistema PassPoint è la selezione dei varchi, vale a dire le porte che le persone utilizzeranno per entrare e uscire dai luoghi controllati. Dopo aver scelto quali porte dovranno essere monitorate, è possibile decidere il livello di controllo di accesso per ognuna. Questo determinerà il tipo di hardware necessario per ogni varco.

Le configurazioni del varco possono variare

Ogni varco può essere configurato in molti modi diversi, ognuno con un grado di sicurezza diverso e con una direzione di passaggio obbligata.

Non bisogna dimenticare che il varco è davvero un insieme delle risorse di sistema (lettori, relè di controllo delle serrature e zone di protezione). Il modo in cui vengono abbinare queste risorse definisce il livello di sicurezza del varco. Lo stesso varco può essere abbinato ad una zona Monitor Stato Porta (MSP) o una zona Richiesta di uscita (RDU). MSP e RDU sono i due tipi di zone di protezione. Un varco può essere equipaggiato con uno di questi tipo di zona, con entrambi i tipi, o con nessuno.

Qui sotto sono riportati alcuni esempi di configurazione di controllo di ingresso ai varchi: essi variano dal più semplice (e quindi meno sicuro) al più complesso.

Esempio 1 – Controllo ingresso di base

La configurazione più semplice per il controllo d'ingresso è avere un lettore d'ingresso e un relè di controllo della serratura:



In questa configurazione, l'utente presenta il badge al lettore per ottenere l'accesso al varco. Il lettore legge i dati contenuti nel badge e PassPoint determina se esistono le condizioni per autorizzare l'accesso. Se l'accesso viene autorizzato, il relè di controllo della serratura viene attivato e l'elettroserratura si apre, lasciando transitare l'utente.

Esempio 2 – Controllo ingresso con monitoraggio dello stato porta

Ecco la stessa configurazione dell'Esempio 1, ma con l'aggiunta di un Monitoraggio Stato Porta:



Come indica il nome, il Monitoraggio Stato Porta consente al sistema di sorvegliare costantemente il varco e di segnalare ogni cambiamento di stato. Informa il sistema quando l'apertura di una porta è stata forzata o quando la porta è stata mantenuta aperta dopo l'accesso per un tempo superiore al consentito. Senza il MSP, come nell'esempio 1, il sistema stabilisce solo se può autorizzare l'accesso. Non controlla lo stato del varco e non rileva niente di anomalo.

Esempio 3 – Controllo ingresso con monitoraggio stato porta e richiesta di uscita

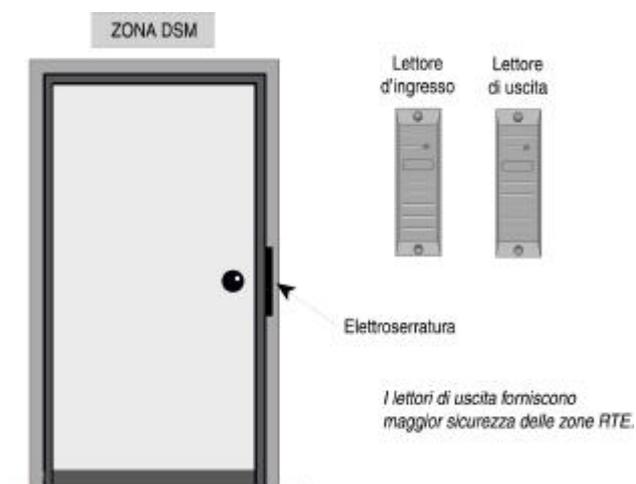
Aggiungendo un apparato di Richiesta di Uscita a un varco, è possibile autorizzare l'uscita agli occupanti dell'area:



Le zone RDU consentono al sistema di capire quando la porta del varco deve essere sbloccata per lasciare uscire un occupante. Il dispositivo utilizzato può essere un pulsante che la persona deve premere per uscire, o anche un rivelatore di movimento a infrarossi, che rivela automaticamente una persona che si trova in prossimità della porta. In entrambi i casi, il dispositivo installato sul lato protetto del varco.

Esempio 4 – Controllo ingresso e uscita con monitoraggio stato porta

Per maggior sicurezza, è possibile aggiungere un lettore di uscita al varco:

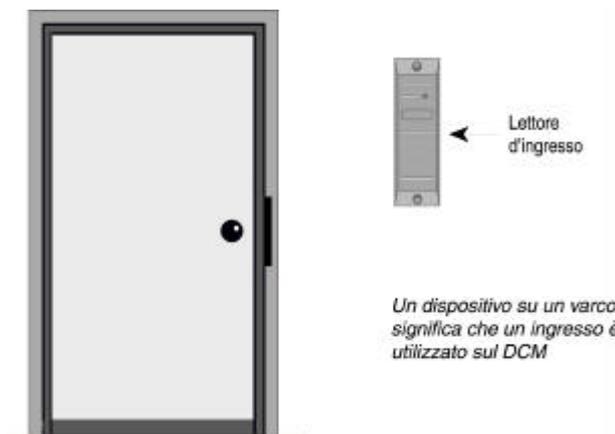


Quando al varco è stato associato anche un lettore di uscita, gli occupanti devono presentare il badge per uscire, vale a dire che devono farsi riconoscere nuovamente dal sistema. A differenza delle zone RDU descritte nell'esempio 3, questa configurazione consente al sistema di essere molto selettivo sulle autorizzazioni di uscita. Solo gli occupanti in possesso di un badge valido potranno uscire dal varco.

Configurazione del Door Control Module

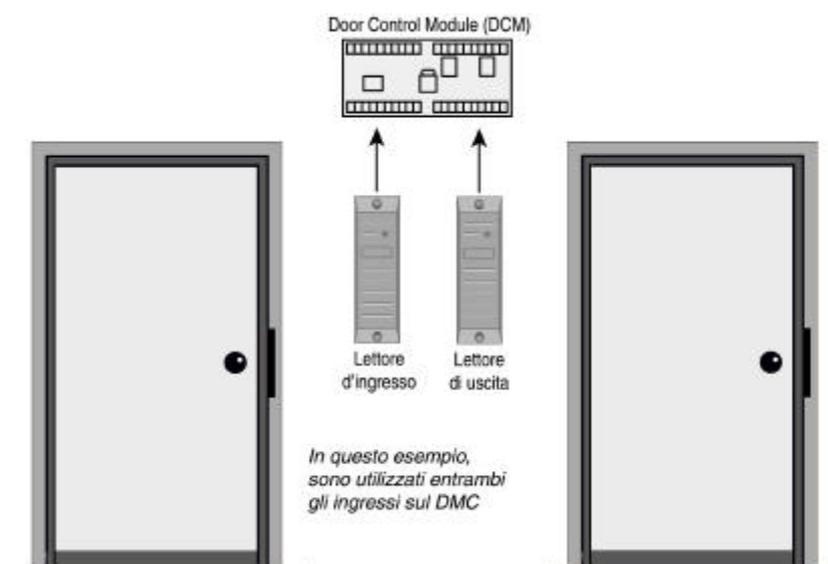
Al momento della pianificazione dell'installazione, non bisogna dimenticare che il modulo DCM può gestire solamente due dispositivi di identificazione (lettori, tastiere, o unità abbinate). Bisogna chiedersi quindi quali porte si vogliono controllare e in quale modo.

Nel paragrafo precedente, il primo esempio forniva un sistema di controllo di ingresso di base con un solo lettore:



In questo esempio, poiché è stato attribuito un solo lettore alla porta, il modulo DCM utilizzato per il varco ha ancora la disponibilità di un altro lettore.

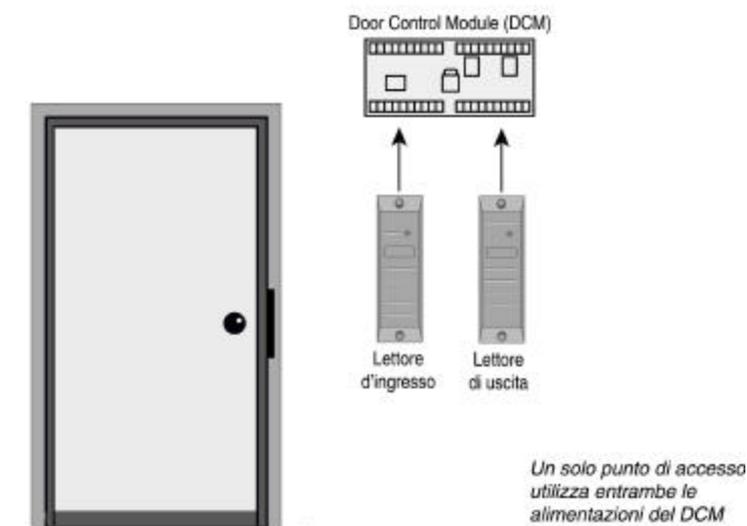
Di conseguenza, questo modulo DCM può essere utilizzato per un'altra porta (a condizione che questa richieda un solo dispositivo), come nel disegno qui sotto:



Se un varco possiede due lettori, sono necessari entrambi gli ingressi del modulo DCM. Molto spesso ci si trova in questa situazione, ed è importante saperlo per progettare correttamente l'installazione.

Nel caso di un varco che necessita sia del lettore d'ingresso sia del lettore di uscita, bisogna collegare entrambi i dispositivi all'alimentatore del DCM. E' necessario quindi utilizzare tutta la capacità di alimentazione del DCM per un solo varco.

E' il caso dell'esempio illustrato qui sotto:



Al momento dell'installazione dei moduli DCM, non dimenticare i limiti descritti qui sopra. Sapendo come i DCM devono essere configurati, è possibile determinare quanti DCM sono necessari e dove devono essere posizionati.

Tipi di lettori

Con PassPoint esistono diversi tipi di lettori da utilizzare nel sistema. Abbiamo già presentato due tipi di lettori (lettori di ingresso e lettori di uscita) negli esempi precedenti. Qui sotto sono illustrati tutti i tipi di lettori di PassPoint:

Lettori di ingresso – Questi lettori vengono utilizzati per controllare l'ingresso a un varco. L'utente presenta il proprio

badge al lettore per ottenere l'accesso. Il lettore legge i dati inviati dal badge ed il sistema determina se autorizzare l'accesso. Se l'accesso è autorizzato, la porta si sblocca per un periodo di tempo specifico (impostato dall'installatore) e l'utente può aprire la porta.

Lettori di uscita – I lettori di uscita lavorano in modo identico ai lettori d'ingresso, ad eccezione del fatto che vengono utilizzati per controllare l'uscita dal varco.

Lettori di comando – Questi lettori vengono utilizzati per funzioni specifiche, o “comandi.” Ad esempio, un lettore di comando può essere posizionato nell'atrio principale di un edificio, a portata di chiunque acceda dalla porta principale. Quando l'utente presenta il proprio badge al lettore, si accendono le luci dell'edificio. La presentazione del badge non sblocca la porta. Viene invece stabilito un rapporto evento/azione fra il badge e il lettore.

Lettori di acquisizione badges – Questi lettori vengono utilizzati per acquisire nuovi badges per il sistema. I badges possono essere aggiunti singolarmente o in lotti tramite un lettore di acquisizione badges.

Tutti i lettori, indipendentemente dalla loro funzione nel sistema, sono collegati direttamente ai moduli DCM, ad eccezione dei lettori di acquisizione badges, che possono essere collegati a un modulo DCM o possono trovarsi nel Card Enrollment Kit (CEK). Il CEK possiede un lettore integrato, utilizzato appositamente per l'acquisizione di badges.

La funzione di un lettore viene impostata al momento della configurazione dei moduli, dopo che il lettore è stato collegato a un modulo DCM. Configurando un modulo DCM, il sistema chiede informazioni sui lettori collegati al modulo. A questo punto bisogna istruire il sistema sulle funzioni desiderate per il lettore.

Lettori validi e non validi Tutti i lettori, indipendentemente dalle loro funzioni, rientrano in due categorie principali: validi e non validi.

- **Lettori validi**

I lettori validi sono lettori associati direttamente ai varchi, vale a dire che controllano l'ingresso o l'uscita da una porta. Si può trattare di semplici lettori d'ingresso, di lettori d'ingresso con monitoraggio stato porta, di lettori di semplice uscita, ecc. Il lettore valido è il tipo utilizzato più di frequente nelle installazioni, ed è quello che gli utenti conoscono meglio. L'utente presenta il proprio badge in un lettore valido per poter entrare o uscire da una porta.

- **Lettori non validi**

I lettori non validi NON sono associati ai varchi. Nonostante siano collegati ai moduli DCM esattamente come i lettori validi, non controllano gli ingressi o le uscite dalle porte. I lettori non validi possono essere i lettori di comando o i lettori di acquisizione badges. I lettori CEK/CPM sono sempre lettori non validi.

Introduzione alla fase successiva

Dopo aver progettato il sistema nel modo più consono alle esigenze del cliente, si può procedere all'installazione. Il prossimo capitolo fornirà tutte le istruzioni per l'installazione e indicherà come montare la centrale PassPoint e fare tutti i collegamenti necessari per un corretto funzionamento del sistema.

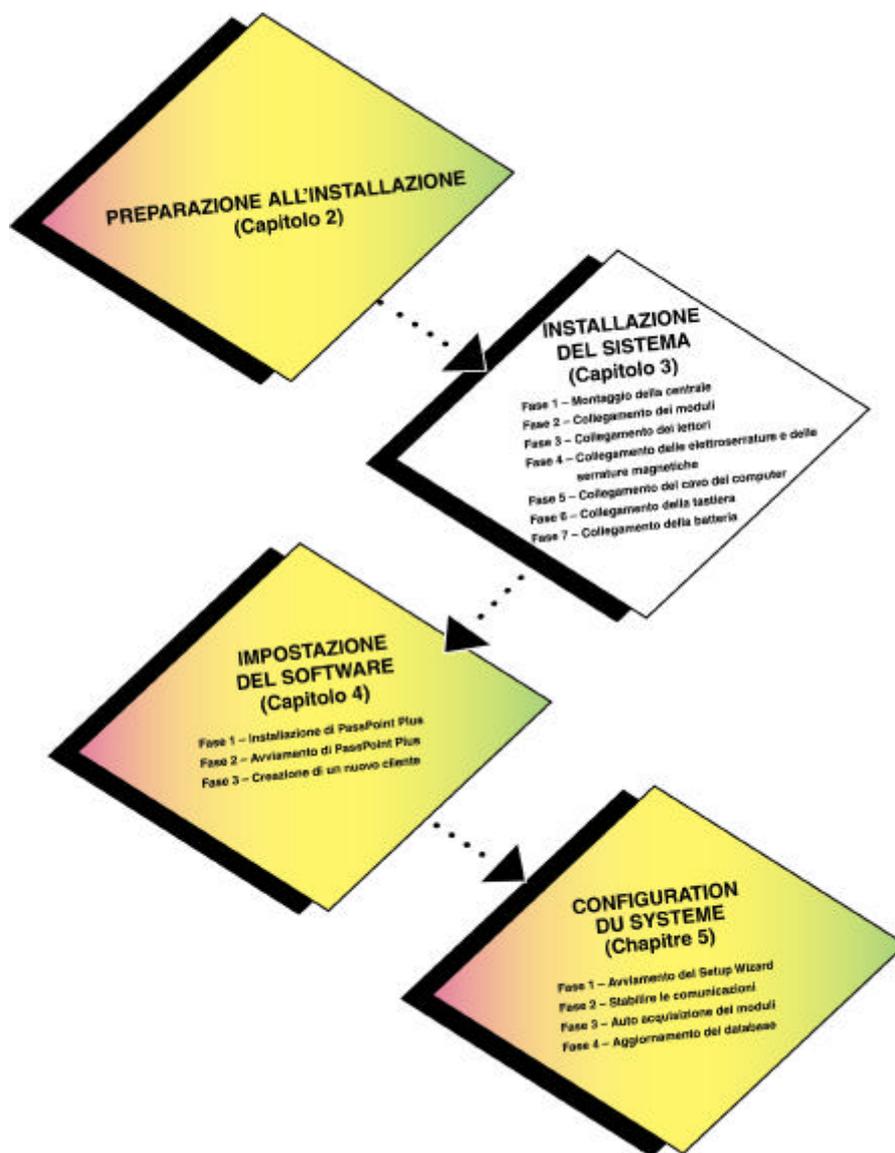
Capitolo

3

Installazione del sistema

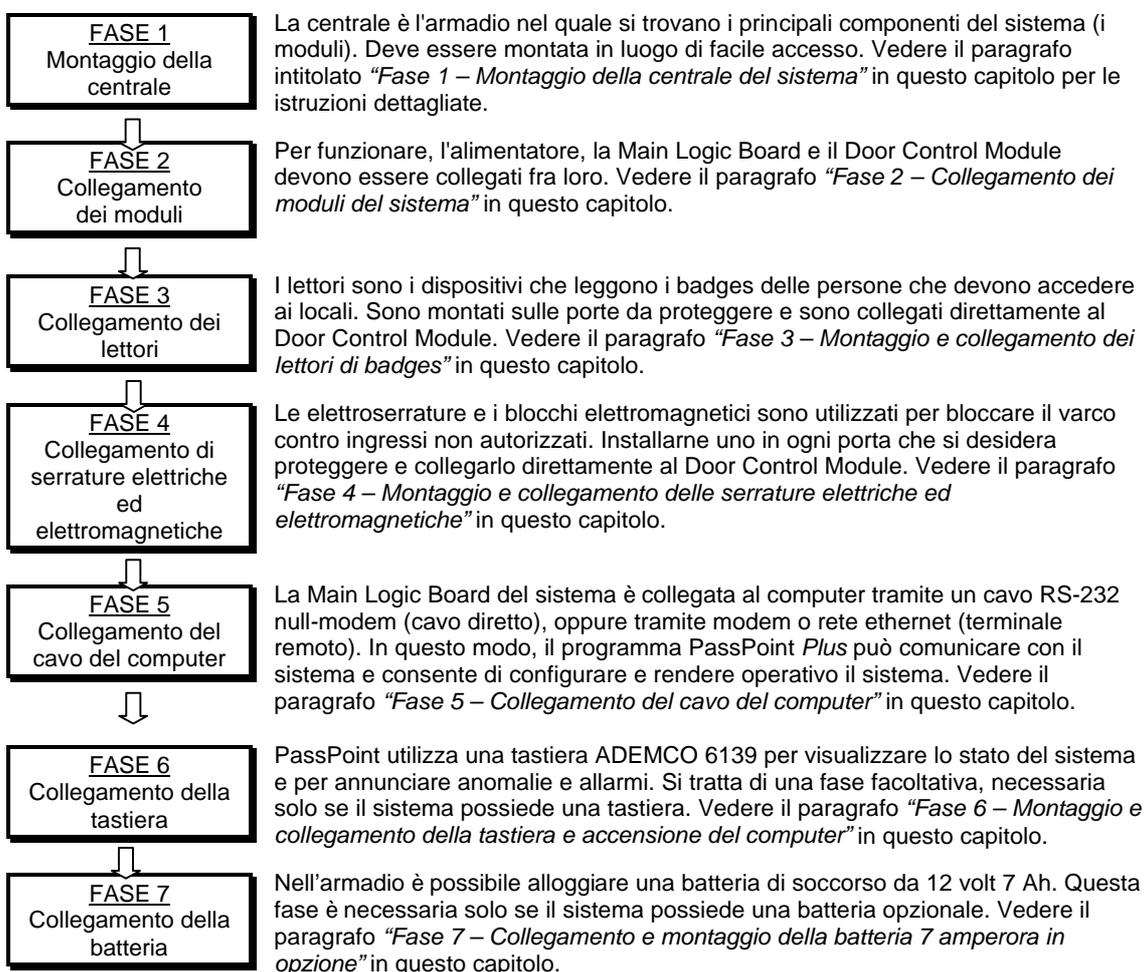
Questo capitolo aiuta nell'installazione e nel cablaggio del sistema PassPoint. Verrà spiegato come:

- **Montare la centrale del sistema**
- **Collegare i lettori**
- **Collegare le serrature**
- **Collegare il cavo del computer**
- **Montare e collegare la tastiera del sistema**
- **(Facoltativo) Montare e collegare la batteria di backup**



Sommario delle fasi d'installazione

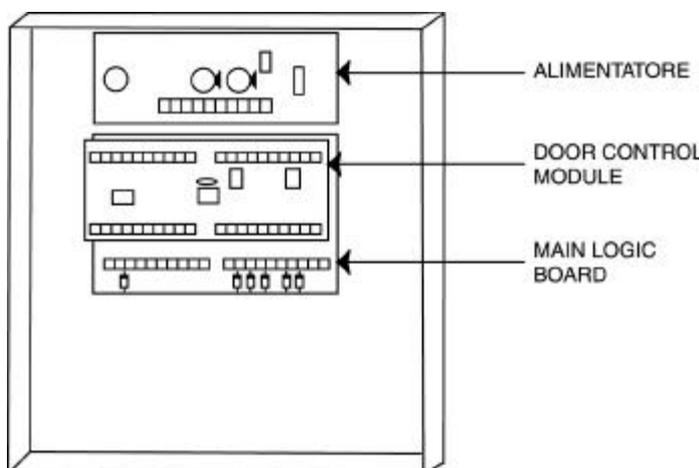
Qui di seguito sono riportate tutte le fasi da seguire per installare il sistema PassPoint. Ogni fase viene spiegata dettagliatamente in questo capitolo. Si consiglia di seguire ogni fase nell'ordine e di consultarne anche il relativo paragrafo:



Fase 1 – Montaggio della centrale del sistema

Lo Starter Kit contiene nel suo armadio tutti i moduli del sistema PassPoint, già predisposti per il cablaggio. Rimuovendo la porta dell'armadio, l'interno apparirà come nel disegno:

*Centrale con MLB,
DCM e alimentatore*



Scelta della zona di montaggio

Scegliere una posizione di montaggio della centrale in luogo pulito e asciutto, non facilmente accessibile al pubblico, ma sufficientemente accessibile ai tecnici. La centrale deve essere montata su un muro solido, con dispositivi di fissaggio o sostegni (non forniti nel kit). La centrale deve anche essere montata in prossimità di una presa di alimentazione e, possibilmente, del computer. Vedere l'Appendice A di questa guida per i parametri di distanza del cablaggio.

Seguire la procedura qui sotto per il montaggio della centrale:

1. **Posizionare l'armadio sul muro e servirsi dei fori sulla parte posteriore per segnare i quattro punti di fissaggio.**
2. **Montare l'armadio sul muro servendosi di dispositivi di fissaggio (tasselli ad espansione da 6 o 8 mm) o sostegni.**

Al momento del montaggio dell'armadio, fare molta attenzione a non danneggiare le schede contenute.

- ; Per facilitare l'installazione, sono stati inclusi nel kit sette terminali removibili, ADEMCO 4142BLK.
-

Fase 2 – Collegamento dei moduli

Il collegamento dei moduli del sistema nell'armadio si suddivide in tre fasi:

- **Collegamento della MLB all'alimentatore**
- **Collegamento del DCM alla MLB e all'alimentatore**
- **Collegamento del cavo della MLB**

-
- ; Al momento dei collegamenti, vedere l'Appendice A, Istruzioni di cablaggio, per i diagrammi e i valori.
-

Collegamento della MLB all'alimentatore

1. Collegare i conduttori del trasformatore ai morsetti 1 e 2 dell'alimentatore.
2. Collegare il cavo dell'alimentatore locale fra il connettore J1 dell'alimentatore e il connettore J1 della MLB.

E' il sistema più comodo per collegare la MLB all'alimentatore. Se non si utilizza il cavo in dotazione, è possibile collegare l'alimentatore locale alla MLB con cavi collegati ai terminali.

Non alimentare se non sono stati completati tutti i cablaggi.

- Prima di alimentare il sistema, assicurarsi che i cavi siano ben fissati nei terminali, che non siano logori e che non tocchino altre componenti nella centrale.

Collegamento del DCM alla MLB e all'alimentatore

1. Collegare il cavo dell'alimentatore *remoto* fra il connettore J5 dell'alimentatore e il connettore J1 del modulo DCM.

L'alimentatore remoto (J5) viene utilizzata per alimentare i moduli DCM quando questi sono montati nello stesso armadio della Main Logic Board.

2. Collegare due conduttori del bus fra la MLB e il modulo DCM.

Collegare un conduttore fra il morsetto 1 del modulo DCM e il morsetto 16 della MLB.

Collegare l'altro conduttore fra il morsetto 2 del modulo DCM e il morsetto 15 della MLB.

Non esistono problemi di polarità sul bus è possibile collegare indifferentemente il morsetto 1 o 2 del modulo DCM al morsetto 15 o 16 della MLB. Assicurarsi di installare la resistenza di bilanciamento al termine del bus. Si può utilizzare una sola resistenza da 52.3 ohm sui morsetti 15 e 16 della MLB, o due resistenze da 105 ohm, una sui morsetti 15 e 16 della MLB e l'altra sui morsetti 1 e 2 del DCM.

- Per questi collegamenti utilizzare doppi ritorti e i morsetti corretti. Consultare l'Appendice A per i particolari di cablaggio per sistemi più grandi.

Collegamento del cavo a nastro della MLB

Il sistema utilizza un cavo piatto a nove poli per collegare la MLB al computer. Un capo di questo cavo va collegato alla MLB. L'altro capo viene montato sull'armadio, in modo tale da potervi inserire il cavo del computer.

1. Collegare il cavo piatto RS-232 al connettore J2 ubicato sulla parte destra della MLB.

Il cavo piatto RS-232 attiva la comunicazione fra la MLB e il computer del sistema.

2. Fissare l'altro capo del cavo (il connettore "D" a 9 poli) alla parte destra dell'armadio servendosi degli accessori forniti.

Fase 3 – Montaggio e collegamento dei lettori

L'Access Starter Kit è fornito con due lettori di badges. Ogni lettore deve essere montato nelle vicinanze di un varco (una porta) ed è collegato direttamente al Door Control Module (DCM). Un solo DCM possiede connessioni di ingresso per due lettori, quindi ogni DCM può controllare due porte, ognuna con un solo lettore, oppure una porta di entrata e uscita, equipaggiata con due lettori.

Montare innanzitutto i lettori sul varco. Dopo averli montati, collegarli al modulo DCM. Le istruzioni per entrambe le procedure sono riportate in questo paragrafo.

- I particolari e le informazioni sull'alimentatore di PassPoint sono riportati nell'Appendice A, alla fine di questa guida.
-

Montaggio dei lettori

1. Utilizzando il lettore come dima, praticare due fori per il fissaggio del lettore e un foro per il passaggio del cavo su ogni parete sulla quale verrà installato un lettore.
2. Fissare i lettori alla parete utilizzando tasselli ad espansione o viti autofilettanti.

Collegamento dei lettori

Dopo aver montato i lettori, collegarli al sistema nel modo seguente:

1. **Collegare i cavi del primo lettore ai morsetti del modulo DCM.**

Servirsi dello schema illustrato qui sotto per collegare i cavi del lettore ai morsetti specifici del modulo.

Cavo del primo lettore	Colore Filo	Al morsetto DCM n.
LED verde (Lett. A)	(Vedere nota 1)	11
DATA 1 (Dati)	Bianco	12
DATA 0 (Clock)	Verde	13
Negativo	Nero	14
+5VDC	Rosso (Vedere nota 2)	15
+12VDC	Rosso (Vedere nota 2)	16

NOTE:
1. Utilizzare il cavo arancio per il segnale LED verde su alcuni lettori HID. Gli altri lettori utilizzano generalmente fili marroni. Controllare l'etichetta posta sul lettore per un collegamento corretto.
2. Collegare i lettori a +5VCC o +12VCC in base alle specifiche del produttore.

Il cavo dei lettori inclusi nel kit ha nove conduttori, ma ne vengono utilizzati e cablati solo cinque. Gli altri quattro non sono utilizzati e non hanno bisogno di essere collegati. I fili non utilizzati devono essere isolati fra loro, dagli altri cavi o da qualsiasi materiale conduttore.

■
] **2. Collegare i cavi del secondo lettore ai morsetti del modulo DCM.**

Servirsi dello schema illustrato qui sotto per collegare i cavi del lettore ai morsetti specifici del modulo.

Cavo del secondo lettore	Colore Filo	A morsetto DCM n.
+5VDC	Rosso (Vedere nota 1)	15
+12VDC	Rosso (Vedere nota 1)	16
Terra	Nero	17
LED Verde (Lett. B)	(Vedere nota 2)	18
DATB 1 (Dati)	Bianco	19
DATB 0 (Ora)	Verde	20

NOTE:
1. Collegare i lettori a +5VDC o +12VDC in base alle specifiche del produttore.
2. Utilizzare il cavo arancio per il segnale LED verde su alcuni lettori HID. Gli altri lettori utilizzano generalmente fili marroni. Controllare l'etichetta posta sul lettore per un collegamento corretto.

- Vedere l'Appendice A per la corretta lunghezza dei cavi.

;

Fase 4 – Montaggio e collegamento delle elettroserrature e dei blocchi elettromagnetici

Le elettroserrature e i blocchi elettromagnetici sono utilizzati per bloccare i varchi contro ingressi non autorizzati. Installarne uno ad ogni porta da proteggere. Le elettroserrature e i blocchi elettromagnetici sono alimentati dall'alimentatore di PassPoint tramite il relè di uscita del modulo DCM.

- Con gli Starter Kit non sono fornite le elettroserrature o i blocchi elettromagnetici. PassPoint può gestire la maggior parte di serrature compatibili con le specifiche dell'alimentatore del sistema. Queste serrature possono essere acquistate presso qualsiasi rivenditore autorizzato.
 - ⌋ Assicurarsi anche di conservare tutta la documentazione che accompagna le serrature. Sarà utile per le informazioni di montaggio e di collegamento.
-
- E' assolutamente necessario utilizzare un soppressore elettrico, tipo AN-S-4 per garantire una protezione ai transistori generati dalle elettroserrature e dai blocchi elettromagnetici. Installare un soppressore sui cavi collegati alla serratura il più vicino possibile alla serratura e
 - ⌋ installare una secondo soppressore sul collegamento del relè sul DCM.
-

Montaggio delle serrature

La procedura per il montaggio delle serrature varia in base al modello che si desidera utilizzare. Consultare la documentazione fornita a corredo delle serrature per maggiori informazioni sul montaggio.

Collegamento delle elettroserrature e dei blocchi elettromagnetici

Per collegare una serratura, seguire la procedura indicata qui sotto e fare riferimento ai diagrammi di cablaggio nell'Appendice A.

1. Collegare l'uscita per la serratura dell'alimentatore al morsetto comune del relè di uscita del modulo DCM.

Sull'alimentatore, l'uscita per la serratura è il morsetto N. 7.

I morsetti comuni di relè di uscita del modulo DCM sono il morsetto N. 29 per la porta A, e il morsetto N. 24 per la porta B.

2. Collegare il morsetto normalmente aperto (N.O.) o normalmente chiuso (N.C.) del relè DCM

all'elettroserratura o al blocco elettromagnetico. Mantenere una distanza minima di 15 cm fra il cavo della serratura e qualsiasi altro cavo.

Se si sta collegando un'elettroserratura, utilizzare un morsetto N.O. I morsetti N.O. sono il n. 28 per il varco A e il n. 23 per il varco B.

Se si sta collegando un blocco elettromagnetico, utilizzare un morsetto N.C. I morsetti N.C. sono il n. 30 per la porta A e il n.25 per la porta B.

3. Collegare il ritorno della serratura al negativo dell'alimentatore (morsetto n.8). Mantenere una distanza minima di 15 cm fra il cavo dell'elettroserratura e qualsiasi altro cavo.

- Vedere l'Appendice A per le lunghezze massime dei cavi.
- ;
-

Collegare i dispositivi MSP e RDU

Le zone comprese fra A e D del modulo DCM (morsetti da 5 a 10) possono essere utilizzate per i dispositivi Monitor Stato Porta (MSP) o Richiesta Di Uscita (RDU).

Collegare questi dispositivi in base alla tabella sommario dei collegamenti del modulo DCM. Vedere anche l'Appendice A di questa guida per informazioni sul cablaggio applicabile, e il capitolo 12 per una descrizione delle diverse configurazioni possibili delle zone.

Fase 5 – Collegamento del cavo del computer

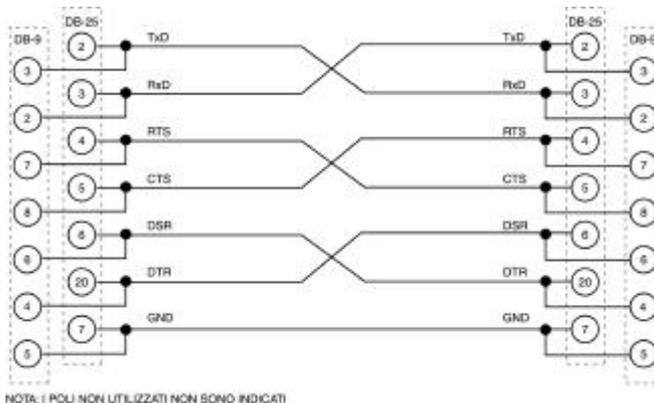
La MLB può essere collegata direttamente al computer tramite un cavo RS-232 (collegamento via cavo) oppure tramite modem o rete ethernet quando la centrale si trova in un punto distante dal computer (collegamento terminale a distanza).

Collegamento cavi

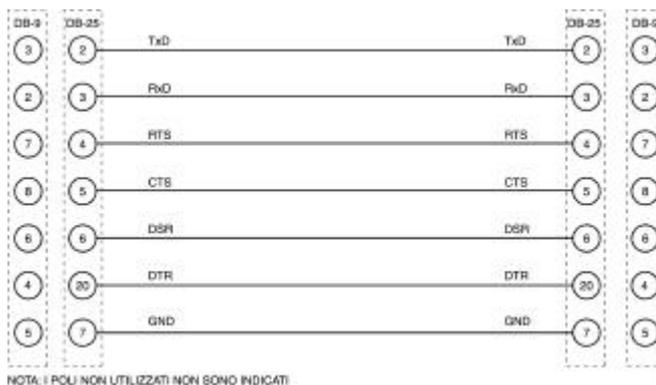
PassPoint dialoga con il software PassPoint Plus attraverso la porta seriale del computer. Il cavo va quindi dal sistema PassPoint a una porta COM disponibile sul computer.

Se si desidera utilizzare un cavo più lungo del cavo RS-232 in dotazione, acquistare o costruire un cavo "null-modem" della lunghezza desiderata, ricordando comunque di non eccedere i 15 metri. Il cavo null-modem deve essere collegato come nel disegno qui sotto.

NOTA: La lunghezza totale del cavo fra la MLB e il computer non deve superare i 15 metri.



CAVO NULL MODEM



EVENTUALE CAVO DI PROLUNGA

Per collegare il cavo RS-232:

1. Collegare il connettore "D" a 9 poli alla MLB.
2. Collegare l'altro capo del cavo a una porta COM disponibile del computer.

Prendere nota del numero della porta COM che si sta utilizzando, perché servirà al momento della configurazione del sistema.

MLB RS-232 Porta J2	Descrizione	Connettore maschio DB-9 sul lato dell'armadio
Polo 1	DCD IN	1
Polo 2	DSR IN	6
Polo 3	RXD IN	2
Polo 4	RTS OUT	7
Polo 5	TXD OUT	3
Polo 6	CTS IN	8
Polo 7	DTR OUT	4
Polo 8	RI IN	9
Polo 9	Terra	5
Polo 10	N/C	N/C

Collegamento terminale remoto

Quando utilizza un collegamento terminale remoto, PassPoint si collega al computer del sistema (il PC) tramite 2 modem, una linea telefonica e 2 cavi modem DB-9 a DB-25. Un cavo modem va dalla MLB a un modem. L'altro cavo modem va dal secondo modem a una porta COM disponibile sul computer.

I cavi e i modem compatibili sono i seguenti:

- Cavo modem DB-9 a DB-25 - ADEMCO Part Number N8337
- Hayes Accura, US Robotics Sportster, o modem compatibile 28.8kbs (o più)

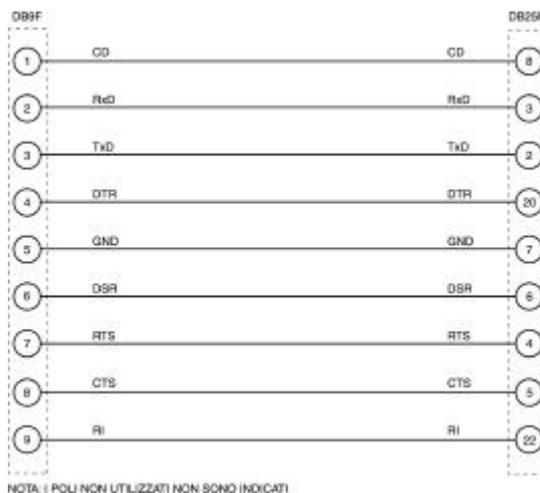
- Il modem e i cavi del modem non sono forniti come parte dello Starter Kit, devono essere acquistati separatamente.

;

Se si desidera utilizzare un cavo più lungo del cavo modem di ADEMCO, bisogna acquistarne uno altrove o fabbricarlo. Il cavo del modem deve essere collegato come indicato nel disegno qui sotto.

NOTE:

- La lunghezza totale del cavo fra la MLB e il modem o fra il modem e il computer non deve superare i 15 metri.
- I modem esterni, che possiedono connettori DB9F (9 poli femmina) possono utilizzare un cavo femmina diretto a 9 poli. Ognuno dei 9 conduttori è collegato allo stesso numero di polo su ogni lato.



CAVO MODEM

Per collegare la centrale PassPoint al computer:

Alla centrale PassPoint

1. Collegare il connettore del cavo modem a 9 poli alla centrale PassPoint.
2. Collegare l'altro capo del cavo al modem.
3. Collegare il modem alla linea telefonica.

Al computer

1. Collegare il modem alla linea telefonica.
2. Collegare il connettore del cavo modem a 25 poli al modem.
3. Collegare l'altro capo del cavo a una porta COM disponibile del computer.

Prendere nota del numero di porta COM utilizzata per il sistema PassPoint, perché servirà al momento della configurazione del sistema.

Fase 6 – Installazione e collegamento della tastiera e accensione del sistema

Il sistema PassPoint utilizza una tastiera alfanumerica standard ADEMCO 6139 (fornita con lo Starter Kit) per visualizzare lo stato del sistema e segnalare eventuali anomalie, come ad esempio un allarme per una porta che è rimasta aperta per troppo a lungo. La tastiera può essere installata sul muro accanto all'armadio della MLB o direttamente sull'armadio. In ogni caso, la tastiera deve essere montata in un punto dove la si possa vedere rapidamente e dove il segnale sonoro possa essere sentito. Con il sistema PassPoint è possibile utilizzare una sola tastiera.

-
- Le informazioni riportate in questo paragrafo servono solo a rendere operativa la tastiera. Ulteriori informazioni sulla tastiera sono riportate nelle istruzioni per l'installazione, fornite con la tastiera 6139.
-

Cablaggio e installazione della tastiera

La tastiera deve essere montata esclusivamente sull'armadio o nelle immediate vicinanze. Utilizzare un cavo 22 AWG (0,32 mmq) ed installare la tastiera ad una distanza massima di 1 metro.

- 1. Rimuovere la parte posteriore della tastiera premendo sulle due leve che si trovano sulla parte superiore dell'involucro.**
- 2. Far passare il cavo dal pannello di controllo di PassPoint attraverso l'apertura sulla parte posteriore.**
- 3. Montare la parte posteriore sul muro o sulla facciata dell'armadio.**

4. Collegare il connettore del cavo fornito alla tastiera.
5. Collegare i cavi della tastiera ai morsetti della MLB seguendo la tabella riportata qui sotto.

Cavo tastiera	Morsetto MLB
Rosso (+12VDC)	11
Nero (Terra)	12
Verde (Data In)	13
Giallo (Data Out)	14

6. Rimontare la tastiera sulla sua parte posteriore.

Impostazione dell'indirizzo della tastiera

Per un funzionamento corretto, l'indirizzo della tastiera deve essere impostato su "00". Se l'indirizzo non è impostato in modo corretto, all'accensione del sistema PassPoint appare un messaggio di errore (Open Ckt) sul display della tastiera. Per impostare l'indirizzo della tastiera:

1. **Alimentare PassPoint.**

La tastiera deve essere accesa per poter impostare l'indirizzo. Accendendo il sistema PassPoint si accende anche la tastiera.

-
- Non cercare di alimentare il sistema/tastiera senza aver prima effettuato i collegamenti descritti qui sopra.

;

2. **Entro 60 secondi dall'accensione, premere simultaneamente e mantenere premuti i tasti "1" e "3" della tastiera.**

La tastiera si posiziona in funzionalità indirizzo. Il display mostra l'indirizzo attuale della tastiera ("31," l'indirizzo predefinito).

3. Premere due volte il tasto "0" per inserire il nuovo indirizzo e premere il tasto "*".

Premendo il tasto asterisco, viene memorizzato il nuovo indirizzo.

Dopo aver impostato il nuovo indirizzo ("00"), la tastiera mostra il nome del sistema, la data e l'ora (possono essere tutti configurati dall'operatore).

Fase 7 – Collegare la batteria di soccorso

Se è stata acquistata la batteria 12 volt 7 Ah, installarla e collegarla all'alimentatore seguendo le istruzioni riportate qui sotto.

-
- Dopo aver installato la batteria, non scollegare l'alimentazione di rete per un periodo prolungato, allo scopo di non scaricare la batteria.

La batteria deve essere installata esclusivamente nell'armadio.

- 1. Inserire la batteria nell'armadio della centrale.**
- 2. Collegare il cavo nero dal morsetto BATT - dell'alimentatore al morsetto – della batteria.**
- 3. Collegare il cavo rosso dal morsetto BATT + dell'alimentatore al morsetto + della batteria.**

Introduzione alla fase successiva

Ora che l'hardware del sistema è installato e cablato, si può installare il software PassPoint *Plus*. Con esso sarà possibile configurare e rendere operativo il sistema PassPoint.

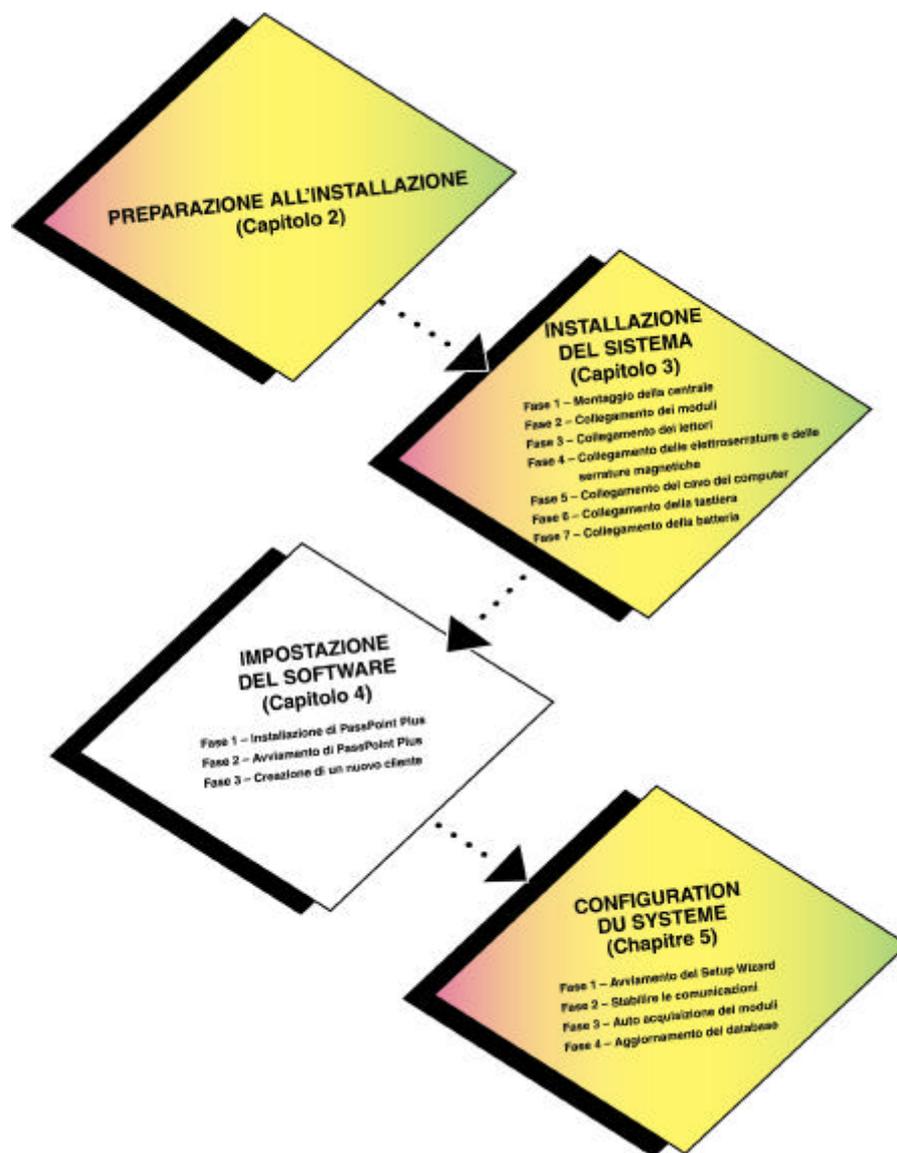
Capitolo

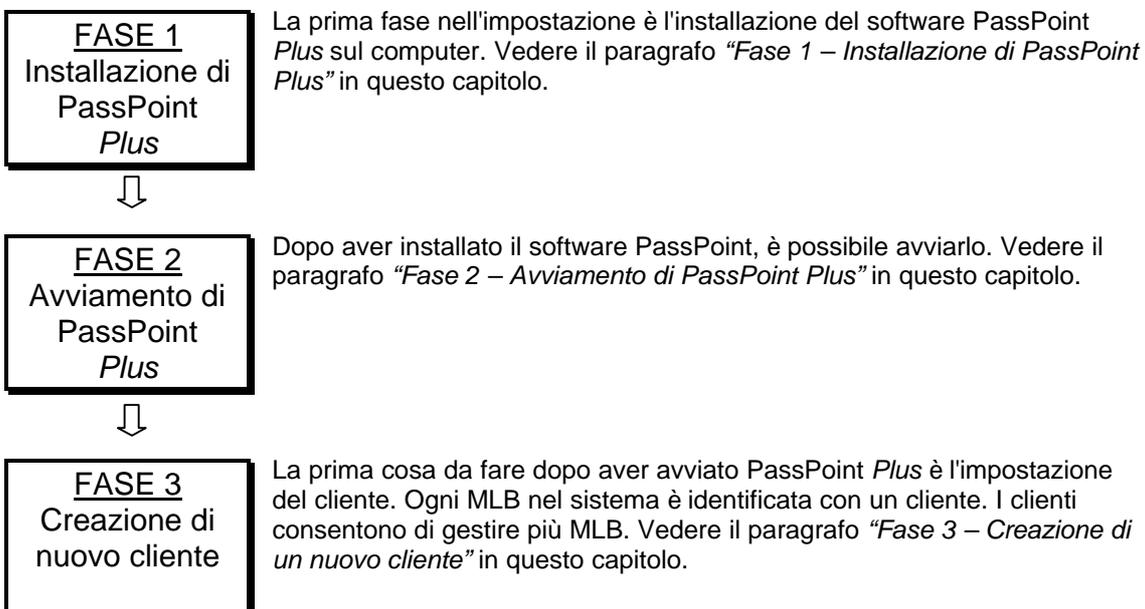
4

Impostazione del Software

Questo capitolo illustra l'utilizzo di base del programma PassPoint *Plus* su Windows e spiega:

- **Cos'è PassPoint *Plus* e quali sono i requisiti di sistema**
- **Come installare PassPoint *Plus* sul computer**
- **Come avviare PassPoint *Plus***
- **Come collegarsi a PassPoint *Plus***
- **Come impostare i parametri di comunicazione per PassPoint *Plus***





Presentazione di PassPoint Plus

PassPoint *Plus* è un programma software compatibile con Windows 95, Windows 98 e Windows NT 4.0, che consente di configurare e rendere operativo il sistema di controllo di accesso PassPoint. PassPoint *Plus* consente essenzialmente al computer di comunicare con la Main Logic Board del sistema.

Con PassPoint *Plus* è possibile configurare tutte le opzioni necessarie per rendere operativo il sistema, per la manutenzione e per le funzioni di monitoraggio del sistema. Monitorando il sistema, PassPoint *Plus* visualizza un elenco di eventi. Un operatore può collegarsi ed entrare nella visualizzazione del sistema per ottenere tutte le opzioni di configurazione.

Il sistema PassPoint non deve essere necessariamente collegato al computer di PassPoint *Plus* per funzionare. Il computer viene utilizzato innanzitutto per configurare e monitorare il sistema. Quando il sistema è operativo, si può scollegare il computer (volontariamente o involontariamente) senza interrompere il funzionamento del sistema.

■
;

Per sfruttare alcune opzioni, come un avviso via e-mail e/o cercapersone, il computer deve essere collegato costantemente perché l'informazione venga trasmessa immediatamente.

Requisiti di sistema

Per poter installare e avviare PassPoint *Plus*, il computer deve avere la configurazione minima seguente:

Minimo

- **Pentium-II® 200 MHz**
- **RAM 64 megabytes**
- **80MB di spazio libero su hard disk**
- **Windows 95, Windows 98, o Windows NT 4.0 (service Pack 3)**
- **Scheda video SVGA, risoluzione 800x600, 256 colori**
- **Mouse**
- **Stampante**

Consigliato

- **Pentium-III® 400 MHz o superiore**
- **RAM 128 megabytes o più**
- **80MB di spazio libero su hard disk o più**
- **Windows 95, Windows 98, o Windows NT 4.0 (service Pack 3)**
- **Scheda video SVGA, risoluzione 800x600, 256 colori**
- **Mouse**
- **Stampante**

Facoltativo

- **Scheda audio, Modem e collegamento Internet (per gestione personalizzata degli eventi)**

- Scheda video Integral Flashpoint Lite (o superiore) per visualizzazione supporto video
- Apparecchio compatibile per acquisizione immagine, come telecamera digitale e/o scanner, per visualizzazione immagine utente
- Stampante badge per stampa personalizzata dei badge con PassPoint Badger
- 2 modem 28.8 compatibili Hayes (o superiore) per il collegamento remoto con PassPoint

Requisiti di impostazione video

Si consiglia di utilizzare PassPoint Plus con una risoluzione video 800 X 600, con impostazione colori di almeno 16 bit e dimensione di caratteri normali o piccoli.

Altre possibilità del sistema

Le funzionalità di base del software PassPoint *Plus* funzioneranno correttamente con i requisiti minimi del sistema. Se si desiderano utilizzare molte funzionalità opzionali, come un'elaborazione degli eventi personalizzata, o se desidera una configurazione personalizzata dell'hardware e/o degli utenti, è meglio possedere i requisiti consigliati.

Fase 1 – Installazione di PassPoint Plus

Seguire la procedura riportata qui sotto per installare PassPoint *Plus* sul computer:

- 1. Chiudere tutti i programmi aperti sul computer.**

2. Inserire il CD di PassPoint nel computer. Dopo qualche secondo, apparirà la schermata di avvio.

NOTA: Se il drive del CD non possiede l'avviamento automatico, fare clic sul pulsante *Avvio* di Windows, fare clic su *Esegui* e poi sul pulsante *Sfogli* per trovare il drive del CD. Fare doppio clic sul drive del CD e doppio clic su CDLaunch.exe. Quando riappare la finestra Avvio, fare clic sul pulsante *OK*.

3. Posizionare il cursore su *Installa software PassPoint Plus* e fare clic con il pulsante sinistro del mouse.

Dopo qualche secondo apparirà la prima schermata del programma di installazione di PassPoint *Plus*.

Il programma di installazione di PassPoint *Plus* è stato creato per guidare passo dopo passo nella procedura d'installazione. Il programma chiede le informazioni necessarie. Al termine di ogni fase, fare clic su *Avanti* per passare alla fase successiva.

Al termine della procedura d'installazione, l'icona di PassPoint *Plus* appare automaticamente sul desktop e nel menu *Avvio*.



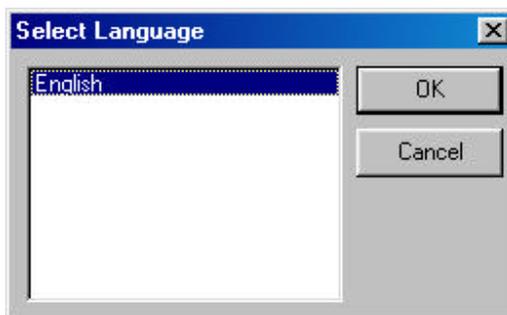
Copiare il file del dizionario multi lingue "d_express.mld" contenuto nella cartella "New Dictionary" del cd-rom nella cartella del dizionario di PassPoint Plus (per default C:\Programmi\PassPoint Plus\Lang).

Fase 2 – Avviamento di PassPoint Plus

Per avviare PassPoint *Plus* sul computer:

1. **Selezionare *PassPoint Plus* dal menu dei Programmi di Windows.**

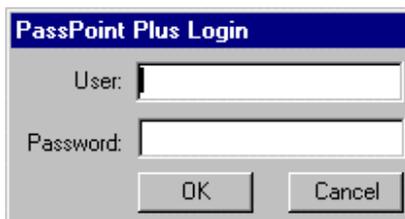
Se è la prima volta che si avvia PassPoint *Plus* dal momento dell'installazione, il sistema chiederà di impostare una lingua. La stessa domanda apparirà se agli avvii precedenti di PassPoint *Plus*, si è sempre risposto *Annulla*.



NOTA: L'unica scelta visualizzata attualmente è Inglese.

2. **Fare clic su *OK* con il mouse.**

Dopo qualche secondo, il sistema chiederà di immettere un nome operatore e una password:



3. **Immettere il nome operatore di default e la password e fare clic su *OK*.**

- Il nome operatore e la password di default sono *Installer*. Esistono dei login Installer, Master, Manager, e Operator; per poter completare l'installazione, è necessario accedere al sistema come Installer. Quando il sistema sarà operativo, si potrà modificare il nome e la password.

Dopo aver fatto clic su *OK*, il sistema presenta una finestra di creazione di un nuovo cliente. Creare un nuovo cliente per continuare (vedere fase successiva in questo capitolo).

- Chiudere sempre PassPoint *Plus* prima di spegnere il computer, per non rischiare di creare problemi di chiusura e danneggiare il database di PassPoint *Plus*.
-

Fase 3 – Creazione di un nuovo cliente

Avviando PassPoint *Plus* per la prima volta, il sistema chiede di creare un nuovo Cliente, fase necessaria per procedere alla configurazione del sistema:



Cos'è un cliente? Perché il database del sistema sia efficiente, PassPoint utilizza dei *clienti* del sistema. Un cliente è un *settore* del database che consente a *Plus* di gestire più di un sistema (più di una MLB). Ad ogni MLB viene attribuito un cliente specifico con il relativo numero di identificazione. Quando si vuole accedere a un database (per backup, visualizzazione eventi, ecc.), è necessario selezionare il numero cliente corrispondente.

I clienti aiutano a gestire il sistema PassPoint trattando ogni MLB come singola unità indipendente. Ad ogni MLB viene attribuito un numero cliente esclusivo. Utilizzando questo numero, si può fare un backup del database o ripristinarlo per una MLB specifica, visualizzare la memoria eventi, creare rapporti, ecc. Per gli installatori che utilizzano PassPoint *Plus* per gestire siti multipli che appartengono a una stessa azienda, si consiglia di impostare un cliente diverso per ogni sito, in modo tale che avviando PassPoint *Plus* si possa selezionare il cliente (il sito) con il quale si desidera lavorare.

Anche se lo Starter Kit possiede solo una MLB, bisogna comunque creare un cliente, perché non è possibile fare un backup o un ripristino del database senza un cliente. In questo caso bisognerà impostare un solo cliente.

Se il sistema è stato configurato per chiamare una centrale di allarme di una società questo numero cliente verrà utilizzato per identificare tutte le trasmissioni con la centrale di allarme.

Quali informazioni sono contenute nel database cliente? Il database cliente memorizza le informazioni di configurazione degli apparati installati nel sito. Queste comprendono configurazione hardware, programmazione oraria, gruppi di accesso, e tutte le informazioni del database dei badges. Si tratta essenzialmente di tutte le informazioni necessarie a copiare la programmazione del sito su una nuova MLB, nel caso in cui il primo sistema dovesse danneggiarsi.

La prima fase è creare un nuovo cliente per la MLB inclusa nello Starter Kit:

1. Riempire i campi della finestra di dialogo.

I campi della finestra di dialogo sono i seguenti:

Nome cliente – Si tratta del nome cliente della MLB. Si consiglia di attribuire un nome facile da ricordare, che la descriva in modo chiaro e corretto. Ad esempio, se si tratta del cliente della MLB principale del sistema, lo si può chiamare “Principale.”

Numero cliente – Si tratta del numero cliente associato al cliente. Il numero può essere composto da un massimo di 4 cifre e deve anche corrispondere alle prime quattro cifre del *Numero cliente primario* attribuito alla MLB.

Numero MLB – Si tratta del numero della Main Logic Board del cliente, ed è sempre 1.

ID Host – Si tratta del numero di identificazione dell'host computer, ovvero il computer utilizzato per la programmazione e gestione del sistema. L'ID host viene utilizzato per riempire il campo specifico nell'etichetta rete /ID nella finestra delle opzioni del sistema. L'ID host viene utilizzato per identificare l'host computer autorizzato a comunicare con la MLB. Quando il valore impostato è quello di default (FFFFFFFFFFFF), qualsiasi computer può comunicare con la MLB.

-
- E' indispensabile ricordare il numero ID host, se esso è stato modificato. Senza il nuovo numero, il computer non potrà comunicare con la MLB.
-

Porta n. – Selezionare la porta seriale del computer al quale è stato collegato il sistema PassPoint. Solitamente si tratta di un numero compreso fra 1 e 8.

- Se il sistema utilizza una connessione LAN, immettere 1 come Porta n. per poter proseguire con l'installazione di PassPoint *Plus*. La connessione LAN verrà impostata nella Configurazione del sistema, descritta più avanti in questo manuale.
-

Modem? – Se si utilizza un modem per collegarsi al sistema, selezionare *Sì*. In caso contrario, selezionare *No*.

- Se l'installazione utilizza un modem, immettere il numero di telefono per chiamare il sistema. Può essere necessario modificare anche la stringa di impostazione modem se il modem richiede funzioni operative speciali.
-

Lancio del Setup Wizard – Fare clic su questa casella se si desidera lanciare il Setup Wizard di PassPoint *Plus*; per continuare la procedura d'impostazione clienti premere OK.

2. Fare clic su **OK**.

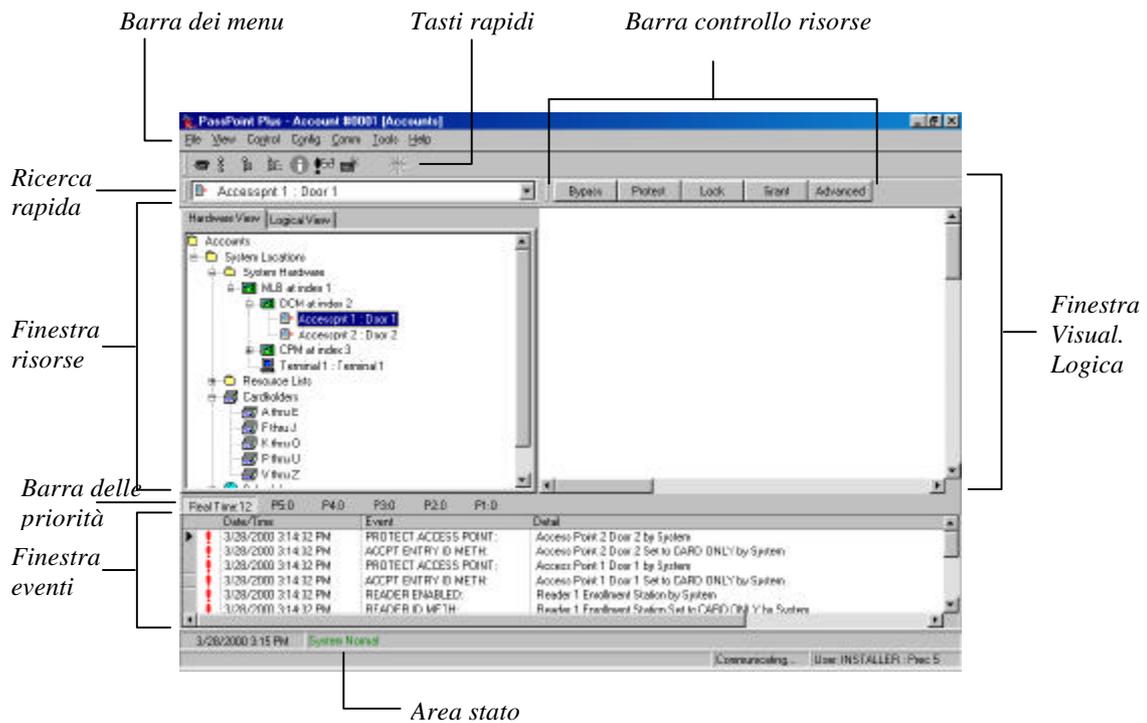
Facendo clic su *OK* si crea un nuovo cliente. Dopo aver creato il cliente, il sistema presenta il Setup Wizard se era stata selezionata la casella Lancio del Setup Wizard. Il Setup Wizard aiuta a configurare il sistema.

L'ambiente PassPoint Plus

PassPoint *Plus* è stato creato perché sia semplice da utilizzare. Se si possiede già esperienza di ambienti Windows, non dovrebbero esserci problemi nel ritrovarsi negli schermi di PassPoint *Plus*.

Principali componenti dello schermo

L'illustrazione seguente mostra la finestra principale di PassPoint *Plus* come appare quando il sistema è operativo. Include utenti, programmazioni orarie, ecc.



L'immagine qui sopra contiene l'impostazione predefinita programmata nel software PassPoint. L'installatore o l'operatore possono modificare il contenuto della finestra e la disposizione delle icone.

Barra dei menu – La barra dei menu consente di selezionare i comandi per utilizzare il programma.

Ricerca rapida – La ricerca rapida elenca tutte le componenti e le risorse del sistema. Utilizzare l'elenco per trovare rapidamente i componenti del sistema sui quali si desidera operare.

Finestra delle risorse – Tutte le risorse del sistema sono elencate nella finestra delle risorse. Si può trattare di risorse hardware (come le MLB o i DCM, relè, zone, trigger, ecc.), e di risorse software (programmi orari, database badges ecc.). E' possibile controllare alcuni oggetti che appaiono nella finestra della risorse facendo doppio clic su di essi.

Barra delle priorità – La barra delle priorità consente di selezionare gli elementi da visualizzare nella finestra eventi. E' possibile visualizzare un elenco cronologico di tutti gli eventi non appena si producono, o un elenco cronologico degli eventi per uno qualsiasi dei 5 livelli di priorità

Finestra eventi – Ogni volta che avviene un nuovo evento, questo viene visualizzato nella Finestra eventi. Alcuni esempi degli eventi di sistema sono l'esclusione di una zona, l'attivazione di un relè, la disattivazione di un lettore, ecc. L'evento più recente appare nella prima riga dell'elenco.

Area stato – L'Area stato fornisce le informazioni sulle condizioni operative attuali del sistema PassPoint. Quando si produce un evento importante o un'anomalia, appare qui in rosso un messaggio che indica l'evento.

Finestra visualizzazione logica – Nella Finestra visualizzazione logica è possibile creare mappe o visualizzazioni a 3 dimensioni, per mostrare la posizione di tutte le risorse hardware del sistema. Le risorse possono essere i moduli (come le MLB o i DCM), i relè, le zone, i trigger, ecc. E' possibile controllare alcuni oggetti nella Finestra visualizzazione logica facendo doppio clic su di essi.

Barra controllo risorse – Questa barra contiene pulsanti per selezionare alcuni elementi. Questi pulsanti consentono di

controllare facilmente gli elementi selezionati. Ad esempio, se durante le operazioni si seleziona un varco nella finestra delle risorse, vengono visualizzati 5 pulsanti (esclusione, protezione, blocco, consenso e avanzate).

Tasti rapidi – Come la barra dei menu, i tasti rapidi consentono di selezionare i comandi per le operazioni di programmazione. Ogni funzione di un tasto rapido corrisponde ad un menu di comandi corrispondente sulla barra dei menu. Se non si è sicuri della funzione di un tasto, posizionare il cursore sul tasto ne e verrà visualizzata la relativa descrizione.

Capitolo

5

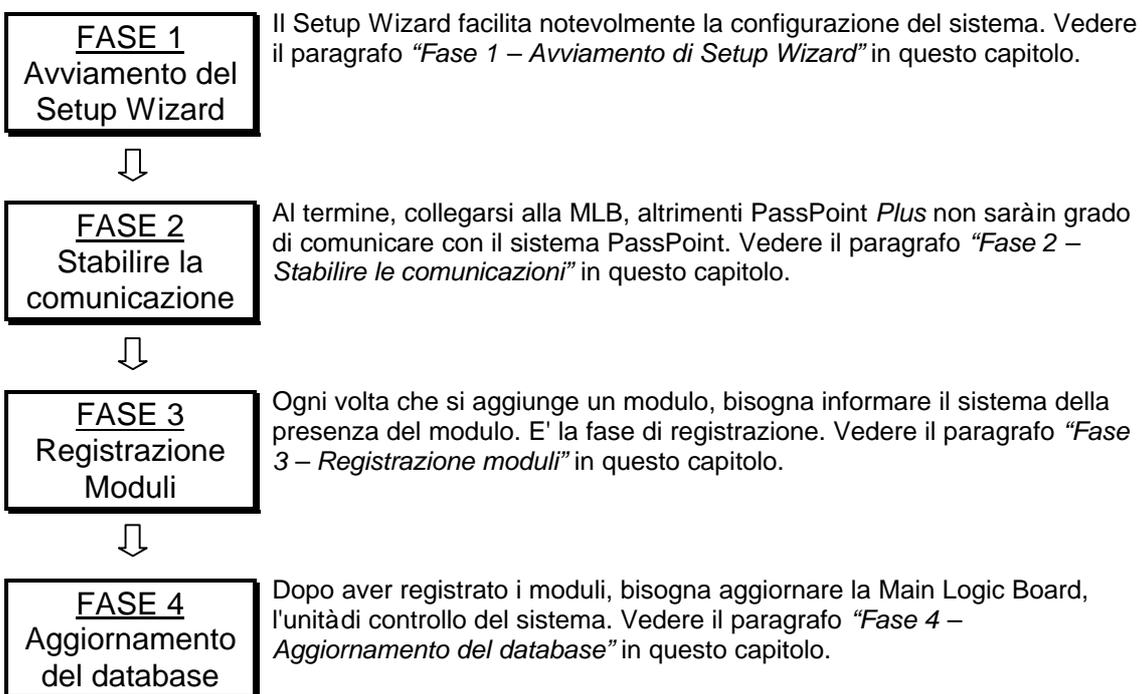
Configurazione del sistema

Questo capitolo spiega tre fasi principali per rendere operativo il sistema PassPoint a un livello tale da poter utilizzare i primi badges.

Questo capitolo spiega come:

- **Impostare i varchi**
- **Registrare il Door Control Module del sistema**
- **Aggiornare il database del sistema**
- **Registrare badges e provare il sistema**





Fase 1 – Avviamento del Setup Wizard

Il primo passo nella configurazione del sistema è l'avviamento del Setup Wizard, che aiuterà ad impostare rapidamente il sistema scegliendo fra una serie di modelli predefiniti. Utilizzando il Wizard, il sistema sarà configurato automaticamente due varchi, un gruppo di accesso di default, un modello di fascia oraria e un programma orario.

Per utilizzare Setup Wizard, basta seguire le istruzioni visualizzate sullo schermo. Il primo schermo del Wizard è il presente:



Esso spiega in breve la funzione del Wizard.

1. Fare clic su **Avanti**.

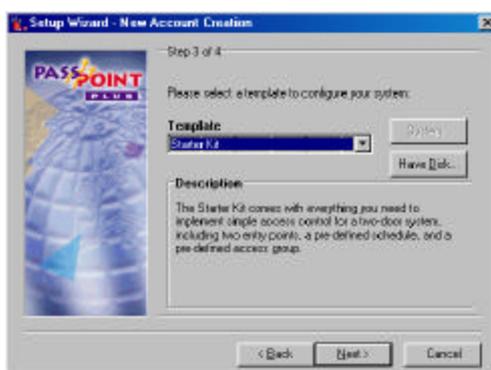
Appare il secondo schermo:



Questo schermo presenta tre opzioni di impostazione diverse. La prima opzione è la più completa. Configura il sistema, registra i moduli del sistema e aggiorna queste impostazioni nel database. Dal momento che si sta impostando un nuovo sistema, selezionare questa opzione.

2. Scegliere la prima opzione di impostazione e fare clic su *Avanti*.

Appare lo schermo successivo:

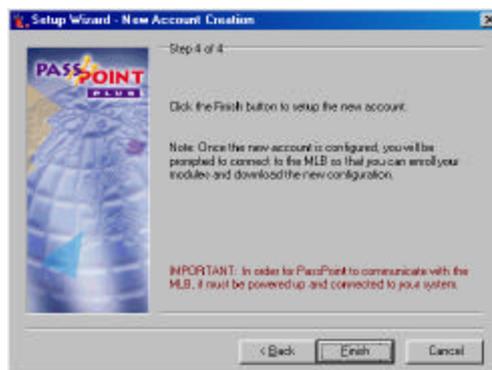


Questo schermo contiene un menu a tenda che consente di selezionare un modello di configurazione. Il sistema visualizza il Starter Kit come modello di configurazione di default. Se si sta configurando solo un Starter Kit senza Door Expansion Kit

o Card Enrollment Kit, selezionare questa opzione. In caso contrario, selezionare nel menu l'opzione adatta. Per poter continuare negli esempi, supponiamo la configurazione di uno Starter Kit.

3. Selezionare un modello e fare clic su *Avanti*.

Se si è scelto il modello Starter Kit, appare lo schermo finale del Wizard:



Fare clic su *Fine* in questo schermo per terminare la configurazione. Il sistema creerà automaticamente i due varchi (le porte) e creerà un gruppo di accesso, una fascia oraria e un programma orario di default. I capitoli seguenti della guida spiegheranno come utilizzare tutti questi elementi.

Dopo aver configurato il nuovo cliente, il sistema chiede di collegarsi alla MBL per registrare i moduli e aggiornare la nuova configurazione.

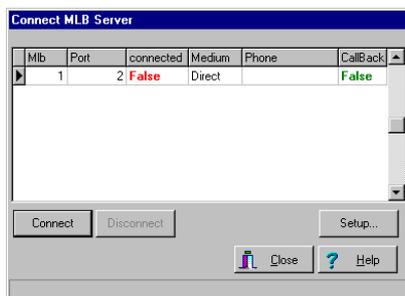
Fase 2 – Stabilire la comunicazione

Dopo aver configurato il sistema con l'aiuto del Setup Wizard, bisogna collegarsi alla MLB, altrimenti PassPoint *Plus* non potrà comunicare con il sistema PassPoint.

Prima di impostare PassPoint *Plus*, assicurarsi di aver collegato il sistema PassPoint al computer tramite il cavo diretto o il modem. Per una connessione via cavo diretto, è stato fornito un cavo null-modem per collegare il connettore RS-232 della MLB a quello della COM port del computer.

Accendere la centrale e aspettare che sul display della tastiera appaia il messaggio "LOCAL ON LINE." Se si sta utilizzando un modem, premere contemporaneamente e rilasciare i tasti * e # della tastiera AD6139 e attendere che sul display appaia il messaggio "REMOTE OFF-LINE."

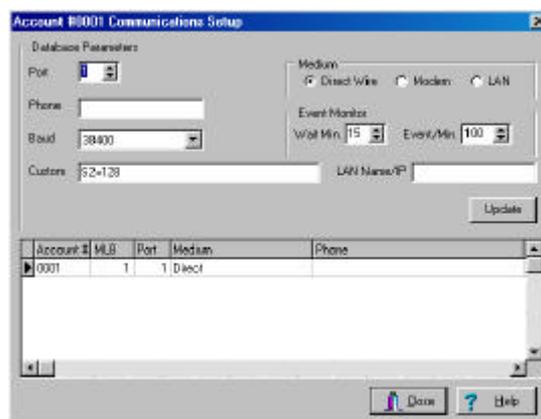
Al termine del Setup Wizard appare la finestra di collegamento con la MLB:



Questa finestra di dialogo visualizza le informazioni riguardanti i parametri di connessione della MLB.

- 1. Seguire le istruzioni per la fase "a" (connessione diretta o via modem) o "b" (connessione LAN) descritte di seguito.**

- a. Fare clic su **Connetti**.
- b. Fare clic sul pulsante **Imposta**. Si apre una finestra di dialogo Impostazione comunicazioni.



Nella finestra di dialogo, selezionare LAN, immettere l'indirizzo IP nella casella Nome/IP LAN, fare clic su **Aggiorna**, e su **Chiudi**. Riappare la finestra di dialogo della connessione MLB.

Fare clic su **Connetti**.

Dopo qualche secondo, il campo *Collegato* cambia da "No" a "Sì," per indicare che è stata stabilita la connessione fra il computer e la MLB del sistema.

Se si è scelta una connessione via modem, il modem collegato al computer comporrà il numero telefonico per collegarsi con la MLB remota.

2. Fare clic su **Chiudi** nella casella di dialogo **Connessione alla MLB se non si è ancora chiusa**. Nella maggior parte delle installazioni, la finestra di dialogo Connessione alla MLB si chiude automaticamente selezionando **Connetti**.

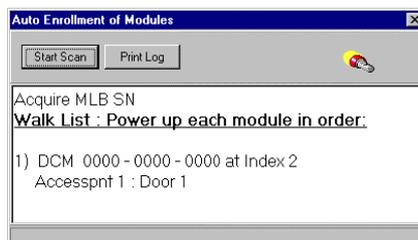
La MLB ha ora stabilito una connessione con il computer.

Fase 3 - Auto acquisizione moduli

Dopo il collegamento alla MLB, il sistema chiede automaticamente di acquisire il numero di serie dei moduli. Quando viene aggiunto un nuovo modulo al sistema, il numero di serie di quest'ultimo deve essere acquisito. L'acquisizione informa semplicemente il database del sistema che è presente un nuovo modulo.

Quando si acquisisce un modulo, il sistema ricerca tutti i moduli collegati che non siano ancora registrati. Il modello di kit definisce i moduli hardware che il sistema si aspetta di trovare. Esso sa quali moduli non sono acquisiti, perché i loro numeri di serie sono tutti a zero. Ad esempio, il modulo DCM che è appena stato aggiunto con Wizard ha un numero di serie che contiene solo zero. Ciò significa che non è stato acquisito e non fa ancora veramente parte del sistema.

La finestra di dialogo Auto acquisizione dovrebbe essere già presente sullo schermo e dovrebbe apparire come l'esempio qui sotto:



Si può vedere che la finestra di dialogo contiene alcune istruzioni. Innanzitutto, il sistema acquisisce il numero di serie della MLB. In seguito ricerca il numero di serie del modulo DCM e lo acquisisce a sua volta.

Questa operazione avviene **automaticamente** dopo aver fatto clic sul pulsante *Avvia Scansione*. L'intero procedimento durerà solo

qualche secondo. Il sistema sa già quali moduli cercare grazie al modello impostato con il Setup Wizard. Se fosse stato scelto un modello differente, ad esempio uno Starter Kit con un Card Expansion Kit, il sistema procederebbe allo stesso modo anche per un CPM. Le procedure richieste per acquisire un solo modulo sono diverse da quelle utilizzate per acquisire più moduli. Se si vuole acquisire un solo modulo, vedere il paragrafo *Auto acquisizione di un solo modulo* di seguito. Se si vogliono acquisire più moduli, vedere il paragrafo *Auto acquisizione di più moduli*.

Aut acquisizione di un solo modulo

Per acquisire un solo modulo del sistema PassPoint, seguire la seguente procedura:

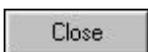
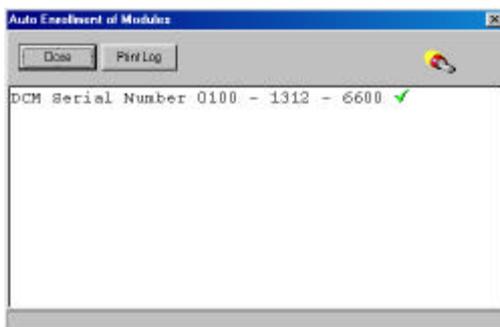
- Non spegnere mai la MLB quando il sistema sta acquisendo un modulo.
-

A rectangular button with a grey background and a black border, containing the text "Start Scan" in a sans-serif font.

1. Fare clic sul pulsante *Avvia Scansione*.

Il sistema cerca il modulo. Dopo averlo trovato, il LED giallo sul modulo lampeggia, il sistema presenta un messaggio sullo schermo, indicando che il modulo è stato acquisito, e interrompe la ricerca di moduli.

Dopo che il sistema ha acquisito il modulo, appare una schermata, che mostra il modulo registrato con il relativo numero di serie.

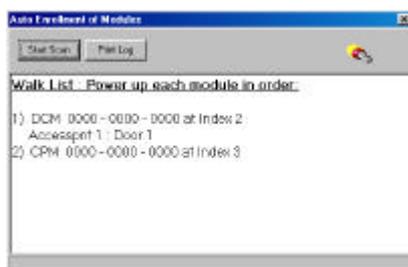


2. Fare clic sul pulsante *Chiudi*.

L'acquisizione è terminata con successo e il sistema chiuderà lo schermo di Auto acquisizione moduli.

Auto acquisizione di più moduli

La finestra di dialogo di auto acquisizione dovrebbe essere già presente sullo schermo e dovrebbe essere, per l'acquisizione di più moduli, come quella presentata qui sotto:



- Se i moduli fossero accesi prima del processo di auto acquisizione o accessi nell'ordine sbagliato, essi verranno registrati in modo errato.
- Non spegnere mai la MLB durante il processo di auto acquisizione.

Per registrare più moduli nel sistema PassPoint, questi devono essere accessi nell'ordine indicato sullo schermo. Per registrare i moduli, seguire le seguenti istruzioni:



1. **Fare clic sul pulsante *Stampa*.** Viene stampato un elenco di tutti i moduli ancora da acquisire.
2. **Controllare che solo il primo modulo nell'elenco sia accesso.**

NOTA: I moduli devono essere accesi nell'ordine in cui compaiono nell'elenco. Assicurarsi che i moduli seguenti siano spenti quando si comincia il procedimento di acquisizione. I moduli il cui numero di serie è già stato acquisito possono restare accesi.



3. **Fare clic sul pulsante *Avvia Scansione*.**

Il sistema cerca il primo modulo dell'elenco. Dopo averlo trovato, il LED giallo sul modulo lampeggia, e il sistema presenta un messaggio sullo schermo, indicando che il modulo è stato acquisito. Un altro messaggio indicherà che il sistema sta cercando il modulo successivo.

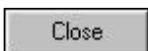
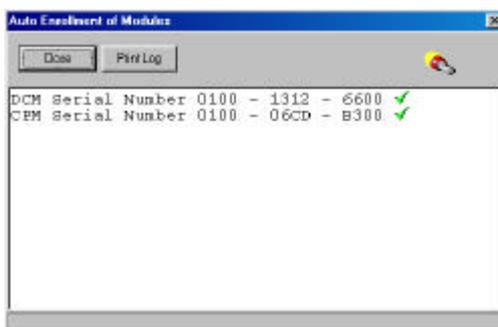
4. **Accendere il modulo successivo dell'elenco.**

Il sistema cerca il modulo seguente. Dopo averlo individuato, il LED giallo sul modulo lampeggia e il sistema presenta un messaggio sullo schermo, indicando che il modulo è stato acquisito. Se ci sono altri moduli nell'elenco, apparirà un

messaggio per avvisare che il sistema sta cercando il modulo successivo.

5. Ripetere la procedura di accensione dei moduli, uno alla volta, finché tutti i moduli saranno registrati.

Quando il sistema ha acquisito l'ultimo modulo nell'elenco, sullo schermo appare l'elenco dei moduli (con numero di serie) acquisiti.



6. Fare clic sul pulsante *Chiudi*.

L'acquisizione è terminata con successo e il sistema chiude lo schermo di Auto acquisizione.

Fase 4 – Aggiornamento del Database

L'ultima fase per rendere operativo il sistema è l'aggiornamento del database.

Il database del sistema di PassPoint risiede nella MLB. E' qui che sono memorizzati tutti i dati di configurazione del sistema. Quando vengono apportate delle modifiche al computer, queste non vengono registrate automaticamente nel database sulla MLB.

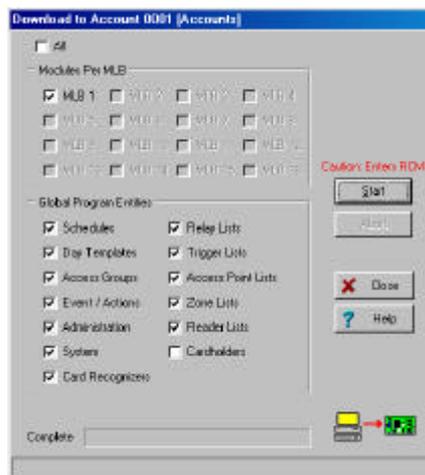
Vengono conservate nel computer finché l'operatore decide di trasferirle nel database della MLB. Perché diventino effettive, tutte le modifiche apportate sul computer devono essere aggiornate nel database.

Ad esempio, è stato aggiunto un modulo DCM al sistema. Il modulo DCM ha una o due porte che sono state configurate. Questa informazione appare nella finestra PassPoint Plus. Si trova nel database del computer, ma non ancora nel database della MLB, perché non è ancora stato aggiornato.

Per aggiornare il database, seguire le istruzioni riportate qui sotto:

1. Selezionare **Aggiorna** nel menu **Config**.

Appare la finestra di dialogo Aggiornamento:

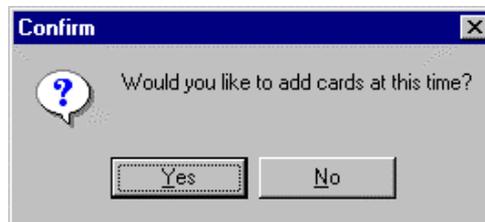


Sulla parte superiore della finestra di dialogo si trova il numero del cliente collegato. La finestra contiene le caselle per la selezione delle informazioni da aggiornare. Le caselle che fanno riferimento a parti del database modificate vengono selezionate automaticamente dal sistema.

2. Fare clic su **Avvio**.

Comincia l'aggiornamento del database. La barra di stato sulla parte inferiore della finestra di dialogo mostra l'evoluzione del procedimento.

Al termine dell'aggiornamento, appare una finestra di dialogo che chiede se si vogliono aggiungere badges.



Facendo clic su **Sì** viene lanciato automaticamente il Wizard Badges, una funzionalità PassPoint utilizzata per aggiungere rapidamente i badges al sistema. Il prossimo capitolo spiega nei particolari come aggiungere badges.

Capitolo

6

Gestione dei database badges e utenti

Questo capitolo spiega come:

- **Utilizzare il database utenti**
- **Utilizzare Wizard Badges per aggiungere un badge o un lotto di badges**
- **Aggiungere manualmente un badge al database**
- **Modificare lotto di badges**
- **Utilizzare monitor badge**

Presentazione del database utenti

Per conservare una traccia di tutti gli utenti, PassPoint utilizza un database. Il database utenti di PassPoint contiene i nomi di tutti gli utenti del sistema. Associa ogni utente al codice di identificazione proprio del badge e al codice PIN (Personal Identification Number). In questo database vengono assegnati i badges e i PIN agli utenti.

Aggiunta di utenti al sistema

Aggiungendo un badge al sistema, si aggiunge un utente al database. Oltre al nome dell'utente, al codice di identificazione del badge e al PIN, vengono inserite altre informazioni, come l'attribuzione di un gruppo di accesso dell'utente, il tipo di badge utilizzato, ecc. Alcune di queste informazioni devono essere inserite imperativamente. Altre informazioni sono facoltative e servono a gestire meglio gli utenti.

Ad esempio, si possono attribuire fino a cinque gruppi di accesso diversi ad ogni utente, mentre un utente deve essere attribuito ad almeno un gruppo di accesso. Altrimenti, non potrà accedere a nessun varco.

E' possibile attribuire ad ogni utente anche un'azione specifica, che può essere impostata per essere avviata in diverse circostanze, come un'autorizzazione di accesso, una negazione di accesso o un'autorizzazione di uscita.

E' possibile attribuire un badge a un utente anche temporaneamente, inserendo una data di scadenza o un conteggio scadenza per impostare il periodo di validità del badge.

Ad esempio, se si vuole consegnare un badge a un visitatore per un solo giorno, è possibile impostarla in modo tale che scada il giorno successivo. O si può decidere che il badge sia valido per tre ingressi nell'edificio; in questo caso si imposta il badge perché neghi qualsiasi richiesta di accesso successiva alla terza.

Da dove cominciare

Nel Capitolo 5 il sistema è stato configurato, ed è ora pronto ad aggiungere badges. L'aggiunta dei badges è essenzialmente l'ultima fase del processo di impostazione. Sullo schermo del sistema appare il Wizard badges, come nell'esempio qui sotto:



E' possibile aprire Wizard badges anche facendo clic sul pulsante **Aggiungi Badges** sulla barra dei pulsanti.

Esistono due sistemi per registrare un badge. Uno è quello di utilizzare Wizard relativo. L'altro è quello di utilizzare la funzione *Aggiungi nuovo badge*. Qui di seguito sono illustrati entrambi i metodi.

- **La funzione *Aggiungi nuovo badge***

Selezionare questa funzione dal menu *Config* per aprire una finestra di dialogo che consente di immettere i dati del badge manualmente.

Aggiungendo un badge con la funzione *Aggiungi nuovo badge*, si ha maggior flessibilità. La finestra di dialogo *Badges* contiene una serie di campi da modificare e ridimensionare per l'utente specifico.

La funzione *Aggiungi nuovo badge* consente di aggiungere solo un badge alla volta. Se si desidera aggiungere più badges, si consiglia di utilizzare il Wizard badges.

- **Il Wizard badges**

Il Wizard badges è una funzionalità di PassPoint che consente di registrare i badges in modo semplice e rapido. Con il Wizard badges è possibile registrare un badge singolo o un lotto di badges.

Aggiungendo un badge con il Wizard, si possono impostare solo informazioni di base e predefinite; esso non offre la stessa flessibilità dell'aggiunta manuale. Dopo aver aggiunto un badge utilizzando il Wizard è comunque possibile aggiungere informazioni più specifiche.

Utilizzo del Wizard badges

Il metodo più facile e più rapido per aggiungere badges è quello di utilizzare il relativo Wizard. Con il Wizard badges si può aggiungere una solo badge o un lotto di badges.

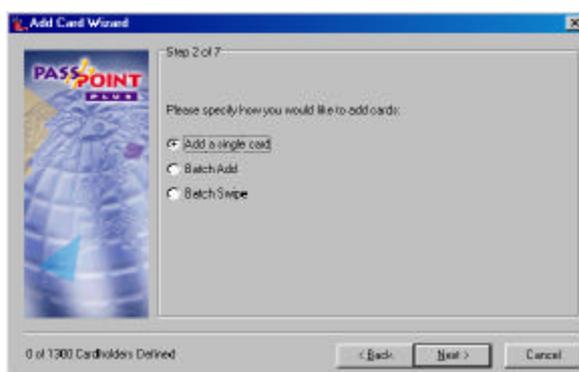
Il Wizard badges appare automaticamente come ultima fase del processo di configurazione del sistema:



Il Wizard badges funziona come il Setup Wizard (descritto precedentemente in questa guida). Per utilizzare il Wizard

badges, seguire semplicemente le istruzioni e rispondere alle domande.

La prima fase consiste nel determinare se si vuole aggiungere un solo badge o un lotto di badges. Selezionare la casella corrispondente:



Aggiunta di una solo badge

Per aggiungere un solo badge con il Wizard:

- 1. Selezionare *Aggiungi un badge* nel Wizard e fare clic su *Avanti*.**

Il Wizard chiede di immettere il cognome, il nome e l'iniziale del secondo nome dell'utente (la persona alla quale verrà attribuita il badge):

Step 3 of 7:

Enter the name of the person you wish to add:

Last:

First: MI:

0 of 1300 Cardholders Defined

< Back Next > Cancel

2. Immettere i dati e fare clic su *Avanti*.

Il sistema chiede di immettere le informazioni riguardanti il badge:

Step 4 of 7:

Please present the card to the enrollment reader now, or if you prefer, enter in the information below.

Note: You may enter either the card number (hot stamp) from the back of the card, or, if the card calculator is set to Raw Card Image, you may enter the actual card code.

When entering a card number, the card code will be computed automatically based on the current card calculator settings.

Current Card Calculator Setting: SA BRADENDD PassMOC

To change the card calculator settings, click here:

Card Number: Issue Level: Card Code:

0 of 1300 Cardholders Defined

< Back Next > Cancel

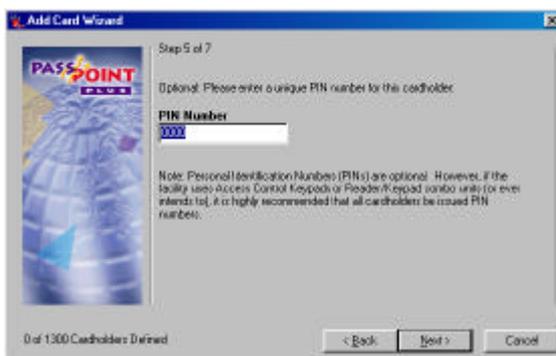
Se si possiede un Card Enrollment Kit, si può presentare il badge al lettore di acquisizione badges per immettere le informazioni riguardanti il badge. In caso contrario, immettere le informazioni manualmente nei rispettivi campi.

- L'impostazione di default è badge prossimità ADEMCO 34.

;

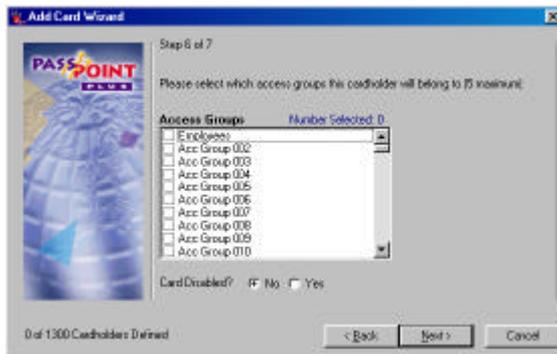
3. Immettere le informazioni riguardanti il badge e premere **Avanti**.

Il Wizard chiede di immettere un numero PIN per il badge. E' facoltativo ed è necessario solo se il sistema utilizza lettori a tastiera che richiedono un codice PIN:



4. Immettere un codice PIN (se necessario) e premere **Avanti**.

Il Wizard chiede ora di scegliere i gruppi di accesso per il badge:



Si possono attribuire fino a cinque gruppi di accesso a un utente, semplicemente selezionando la casella corrispondente al numero del gruppo.

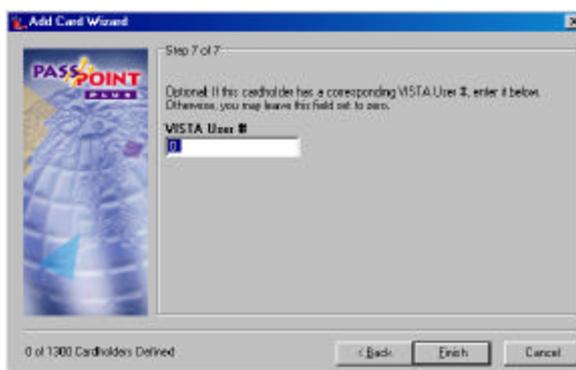


Il modello ASK include un gruppo di accesso predefinito, chiamato IMPIEGATI, che consente di scegliere un gruppo di accesso senza doverne creare uno. E' possibile modificare o eliminare il gruppo di accesso IMPIEGATI in un secondo tempo, se necessario.

Perché l'utente sia autorizzato all'accesso, deve essere associato ad almeno un gruppo di accesso (a meno che non abbia privilegi executive).

5. Selezionare i gruppi di accesso per il badge e fare clic su *Avanti*.

L'ultima fase è quella di immettere un numero utente VISTA (se utilizzato):



Qualora l'utente possedesse un numero utente VISTA corrispondente, inserirlo nell'apposito campo. Altrimenti lasciare il campo con il valore di default 0 (zero).

6. Fare clic su *Fine*.

Il badge è aggiunto al database utenti e contemporaneamente aggiornato nel database della MLB. Ora è possibile visualizzare, modificare o eliminare il badge.

Aggiunta di un lotto di badges

Esistono due metodi per aggiungere un lotto di badges: l'aggiunta manuale e l'auto apprendimento.

- **Aggiunta di un lotto**

L'aggiunta di un lotto consente di aggiungere rapidamente molti badges in una sola volta. Il Wizard chiede di immettere manualmente i numeri del PRIMO e dell'ULTIMO badge del lotto. Perché questo metodo funzioni, i badges devono essere in successione numerica. Così facendo, PassPoint acquisisce automaticamente il primo badge, l'ultimo, e tutti i badges compresi fra i due.

Questo metodo non consente di immettere i nomi utenti per i badges. Bisogna farlo in seguito per ogni singolo badge, con le ulteriori informazioni specifiche che si desidera aggiungere.

- **Striscia lotto**

La funzione striscia lotto consente di aggiungere un lotto di badges, ma è necessario presentare ogni singolo badge al lettore di acquisizione.

Prima di presentare i badges, è necessario scegliere il gruppo di accesso al quale saranno assegnati. Questo metodo offre la possibilità di immettere il nome di un utente per ogni badge acquisito.

Aggiunta manuale di badges

Se non si desidera utilizzare il Wizard badges per aggiungere un utente al database, è possibile aggiungere i badges manualmente. Aggiungendo un badge manualmente, si ha maggior flessibilità poiché è disponibile un numero maggiore di campi informazioni per personalizzare il badge.

Per aggiungere i badges manualmente, seguire la procedura descritta di seguito:



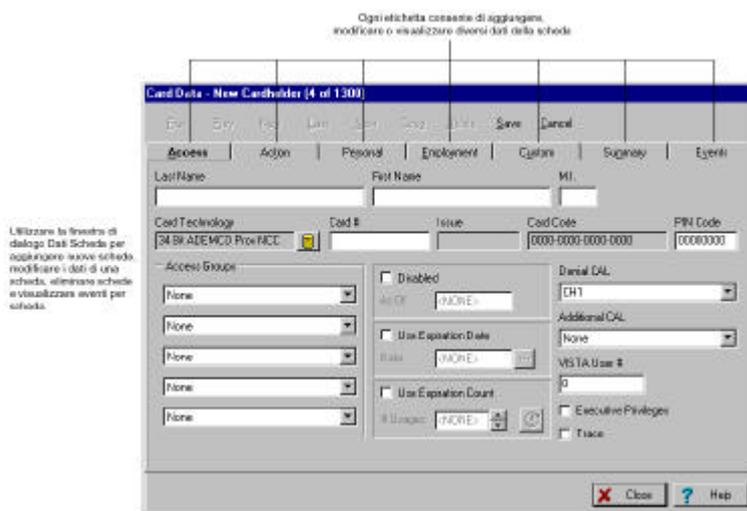
1. **Nel menu *Config*, selezionare *Badges>Aggiungi nuovo badge* o fare clic sul tasto rapido *Aggiungi nuovo badge*.**

Appare la finestra di dialogo Conferma:



2. **Per aggiungere i badges manualmente fare clic su *NO*.**

Appare la finestra di dialogo Dati Badge:



La finestra di dialogo Dati Badge consente di immettere diversi tipi di informazione riguardanti ogni badge. Ogni etichetta della finestra visualizza una serie di dati diversi. Creando un nuovo badge, riempire questi campi con le informazioni necessarie. Alcuni di questi campi, come il *Codice badge* e/o il *Codice PIN* sono obbligatori, mentre altri, come il *Nome* e i *Gruppi di accesso* sono facoltativi. Altri ancora non hanno bisogno di essere riempiti, o contengono già dati predefiniti che possono essere utilizzati. I campi che si sceglie di riempire per ogni badge dipendono dall'utente, dalle necessità dell'installazione e da altri fattori specifici del sistema.

3. Riempire i campi della prima etichetta, **Accesso**.

La prima etichetta della finestra di dialogo Dati Badge è l'unica a contenere campi da riempire obbligatoriamente perché il badge funzioni. I campi dell'etichetta sono illustrati qui sotto:

Nome (Cognome, Nome, Iniziale del secondo nome) – Immettere in questi campi il nome dell'utente. Il nome non

deve essere necessariamente esclusivo, e non importa l'uso delle lettere maiuscole o minuscole.

N. badge – Immettere in questo campo il numero di identificazione impresso sul badge. Il numero di badge immesso elaborerà automaticamente il *Codice badge* corretto, a condizione che sia stata scelta la *Tecnologia badge* adatta.

Tecnologia badge – Selezionare in questo campo il tipo di tecnologia badge utilizzato dal sistema.

- Questo campo deve essere riempito in modo corretto perché il badge funzioni. Nelle impostazioni predefinite, appare “34 Bit ADEMCO Prox NCC,” che è il tipo di badge in dotazione all'Access Starter Kit.
-

Codice badge – Il codice badge è il codice attuale incluso nel badge. È il codice che il sistema legge quando il badge viene presentato a un lettore. Questo campo non può essere modificato, a meno che la tecnologia utilizzata non sia una raw card image data, solitamente non utilizzata. Si aggiorna automaticamente in base al *N. badge* inserito e alla *Tecnologia badge* selezionati nei due campi precedenti.

Codice PIN – Nel caso in cui venissero utilizzati tastiere o lettori combinati a tastiera, immettere in questo campo un numero di identificazione personale (PIN) che si desidera attribuire all'utente.

I codici PIN possono avere una lunghezza compresa tra le 3 e le 8 cifre. Un'opzione del sistema stabilisce la lunghezza del codice PIN utilizzato nel sistema. Tutti i codici PIN del sistema devono essere diversi l'uno dall'altro in tutte le cifre meno 1 rispetto alla lunghezza del codice PIN del sistema. In altre parole, se la lunghezza del codice PIN del sistema è di 4 cifre, le prime 3 cifre di TUTTI i codici PIN DEVONO essere diverse le une dalle altre. L'ultimo carattere non ha nessuna importanza – è possibile attribuire una qualsiasi cifra in questa posizione. In ogni caso, non attribuire mai un codice PIN che

finisca con "0", perché un qualsiasi codice PIN che termini con "0" può essere interpretato dal sistema come richiesta di accesso sotto costrizione. Si consiglia di attribuire codici PIN che terminino tutti con la stessa cifra — ad esempio "9", poiché altri "ultimi" caratteri speciali potrebbero essere utilizzati per future versioni del sistema. Notare che se non viene immesso un numero di badge per un utente (come potrebbe essere il caso per sistemi solo PIN), è **OBBLIGATORIO** immettere un dato in questo campo.

Gruppi di accesso – Nell'elenco fornito, selezionare fino a cinque gruppi di accesso per il badge.

Perché l'utente abbia un qualsiasi privilegio di accesso, deve essergli attribuito almeno un gruppo di accesso (a meno che l'utente non abbia privilegi executive).

Disabilitato – Se si desidera disabilitare l'utente, selezionare questa casella. Quando gli utenti sono disabilitati, tutti i privilegi di accesso sono revocati. E' possibile ripristinare i privilegi dell'utente in qualsiasi momento togliendo la selezione alla casella. Anche quando disattivato, il badge resta nel database del sistema. Disabilitando un badge, impostare una data alla quale il sistema deve disabilitare il badge.

Utilizzare data di scadenza – Se si desidera che un badge non sia più valido dopo una certa data, selezionare questa casella e selezionare la data nell'apposito campo. Qualsiasi richiesta di accesso successiva a questa data verrà negata.

Utilizzare il conteggio scadenza – Se si desidera che il badge non sia più valido dopo un certo numero di utilizzi, selezionare questa casella e immettere un numero di utilizzi nell'apposito campo. Immettere, ad esempio, "10" se si desidera che il badge autorizzi solo dieci accessi.

Rifiuto CAL e CAL addizionale – Questi campi sono per un utilizzo successivo e non sono attivi in questa versione di PassPoint Plus.

Utente VISTA n. – Se c'è un numero utente per la centrale di allarme VISTA 120 abbinato all'utente, inserirlo in questo campo.

Privilegi Executive – Selezionare questa casella se si desidera che l'utente abbia privilegi executive: accesso completo a tutti i varchi del sistema. I gruppi di accesso attribuiti all'utente non sono selezionati, in modo tale che non sia strettamente necessario attribuire dei gruppi di accesso (anche se è fortemente consigliato, poiché i privilegi executive sono revocati quando il sistema si trova in Livello di pericolo 5).

Si fa notare che abilitando questo campo si avranno ramificazioni nella gestione del sistema di sicurezza che dovranno essere gestite dall'amministratore del sistema. Inoltre, se il sistema utilizza livelli di pericolo, tutti i badges con privilegi executive dovrebbero avere almeno un gruppo di accesso attribuito. Il gruppo di accesso attribuito DEVE essere valido in caso di Livello di pericolo 5, in modo tale che la persona abbia la possibilità di uscire dai locali senza mettere in pericolo la sua vita e la sua sicurezza. I badges con privilegi executive conservano anche tutti i privilegi di accesso di tutti i livelli di autorità degli utenti.

Traccia – Selezionare questa casella se si vuole memorizzare la traccia di un evento ogni volta che viene utilizzato un badge o un codice PIN. La traccia di un badge appare nella memorizzazione eventi del sistema e conserva una traccia dei movimenti e delle azioni dell'utente. Solitamente questo campo non viene utilizzato, a meno che non sia necessario "sorvegliare" un badge per un motivo qualsiasi.

4. Riempire i campi delle altre etichette o fare clic su *Salva*.

Dopo aver riempito i campi della prima etichetta, è possibile memorizzare i dati del badge e aggiungere il badge al database in qualsiasi momento.

Le altre etichette della finestra di dialogo consentono di immettere ulteriori informazioni sull'utente. Ad esempio,

l'etichetta *Personale* consente di immettere dati personali sull'utente, come l'indirizzo. L'etichetta *Sommario* consente di visualizzare l'intero sommario delle informazioni riguardanti l'utente.

Utilizzo dell'etichetta Azioni

E' possibile configurare il sistema perché si verifichino una serie di azioni in seguito ad un evento specifico legato a un badge (come un'autorizzazione di accesso). A questo scopo, utilizzare i campi nell'etichetta Azioni:

Utilizzare l'etichetta Azioni per associare un'azione all'utilizzo del badge.

Card Data - New Cardholder (4 of 1300)

First Prev Next Last New Copy Delete Save Cancel

Access **Action** Personal Employment Custom Summary Events

Action Desired: None Specifier Not Used: 0 Max Threat Level: Threat Level 0

Precedence Change: None Invoke Action: Never Invoke

Perform Action at Uncommitted Readers?

Close Help

Azione desiderata – E' la funzione che si desidera attivare all'utilizzo di un badge. Selezionare dall'elenco di azioni predefinite.

Oggetto – E' l'oggetto del sistema sul quale si agisce. Ad esempio, se è stato scelto "Relè Attivo" come azione, l'oggetto è il nome attribuito a quel relè al momento della configurazione.

NOTA: Impostare e configurare le risorse prima di utilizzarle nel campo Oggetto.

Livello di pericolo massimo – Si tratta del livello di pericolo al quale l'azione può prodursi. Se il livello di pericolo del sistema supera l'impostazione dell'azione, questa non potrà prodursi. Il valore di default per questo campo è 0, vale a dire normale.

Cambio precedenza – Questo campo indica come sarà influenzato il livello di precedenza dell'Oggetto (sopra), quando avviene l'azione. Le scelte possibili sono Nessuno, Cancella (imposta il livello di precedenza a 0), o Aggiorna perché la risorsa passi al livello di precedenza dell'utente.

Richiama azione – Selezionare in questo campo l'evento di sistema specifico sul quale si vuole che avvenga l'azione. L'azione avverrà solo quando il badge incontrerà la situazione specificata in questo campo. Si può selezionare, ad esempio, che un'azione si produca quando viene autorizzato un accesso o quando viene negata un'autorizzazione di accesso.

Esegui azione su lettori non validi – Selezionare questa casella se si vuole che l'azione specificata avvenga quando il badge viene presentato a un lettore non valido (non configurato come parte di un varco).

Utilizzo dell'etichetta Personale

E' possibile immettere informazioni personali sull'utente. Utilizzare a questo scopo i campi dell'etichetta Personale:

Card Data - New Cardholder (4 of 1300)

First Prev Next Last New Copy Delete Save Cancel

Access Action **Personal** Employment Custom Summary Events

Last Name First Name M.I. Picture Signature Fingerprint

Address Line 1

Address Line 2

City State Zip Code

Home Phone

Acquire Image

Close Help

Cognome, Nome, S.I. – Questi campi sono delle copie dei campi dell'etichetta Accesso e sono stati inseriti in questo punto per comodità di utilizzo.

Indirizzo riga 1, Indirizzo riga 2, Città, Stato, CAP e Telefono abitazione - L'indirizzo e il numero di telefono di casa dell'utente possono essere memorizzati in questi campi.

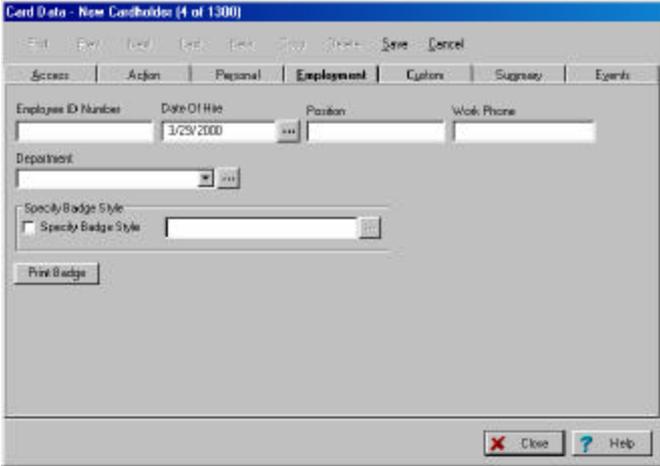
Acquisizione immagine (Immagine, firma, impronte digitali) – Le etichette di Acquisizione immagine vengono utilizzate per memorizzare varie immagini bitmap dell'utente. Queste immagini possono essere acquisite con il pulsante Acquisizione immagine, che consente di importare un'immagine da una qualsiasi fonte compatibile o da un disk file. Un'immagine disk file può essere in un formato immagine qualsiasi, come Bitmap, JPEG e GIF. L'etichetta Firma può essere utilizzata in abbinamento alla maggior parte dei sistemi di scrittura compatibili con Windows per catturare la firma dell'utente.

Notare che quando la fotografia dell'utente viene inserita nel database, la funzione Monitor badge (descritta più avanti in

questo capitolo) può essere utilizzata per visualizzare la fotografia dell'utente sugli eventi iniziati dall'utente.

Utilizzo dell'etichetta Impiego

Il database utenti può contenere anche dati di identificazione riguardanti la posizione del dipendente. Per immettere un dato di identificazione di un dipendente, utilizzare i campi dell'etichetta Personale:



The screenshot shows a software window titled "Card Data - New Cardholder (4 of 1300)". The window has a menu bar with "File", "Edit", "View", "Tools", "Data", "Query", "Print", "Save", and "Cancel". Below the menu bar is a tabbed interface with tabs for "Access", "Action", "Personal", "Employment" (which is selected), "Custom", "Summary", and "Event". The "Employment" tab contains the following fields and controls:

- Employee ID Number:** A text input field.
- Date of Hire:** A date input field containing "3/29/2000". To its right is a small calendar icon.
- Position:** A text input field.
- Work Phone:** A text input field.
- Department:** A dropdown menu with a small "..." icon to its right.
- Specify Badge Style:** A checkbox labeled "Specify Badge Style" which is currently unchecked. To its right is a text input field with a small "..." icon.
- Print Badge:** A button located below the "Specify Badge Style" section.

At the bottom right of the window are two buttons: "Close" (with a red X icon) and "Help" (with a question mark icon).

N. ID dipendente – Questo campo viene utilizzato per registrare il numero di matricola aziendale del dipendente.

Data di assunzione - Questo campo viene utilizzato per registrare la data di assunzione dell'utente. Le date valide sono comprese fra il 1° gennaio 1950 e il 31 dicembre 3999. Facendo clic sul pulsante che si trova a destra del campo Data di assunzione, apparirà un calendario.

Posizione – Questo campo viene utilizzato per registrare la posizione o la qualifica dell'utente.

Telefono ufficio – Questo campo viene utilizzato per registrare il numero di telefono dell'ufficio dell'utente.

Reparto – Questo campo viene utilizzato per registrare il reparto nel quale lavora l'utente. Si può scegliere da un elenco di reparti già impostati facendo clic sulla freccia che si trova a destra di questo campo. Si può anche creare un nuovo reparto facendo clic sul pulsante a destra del campo. Facendo clic sul pulsante, appare lo schermo Reparto / Stile badge, per aggiungere o eliminare i reparti e selezionare gli stili badge.

Specifica stile del badge e stampa badge – Questo campo e il pulsante sono utilizzati per specificare uno stile badge e stampare un badge se si sta utilizzando PassPoint Badger e se è già stato creato almeno un master badge file.

Utilizzo dell'etichetta Personalizzazione

L'etichetta *Personalizzazione* contiene campi che possono essere configurati dall'operatore e che includano qualsiasi informazione si ritenga indispensabile. Quando la si apre per la prima volta, l'etichetta *Personalizzazione* è vuota, perché i campi non sono ancora stati configurati, ad eccezione del campo 6 che, nelle impostazioni predefinite, contiene il numero del badge.

Per configurare i campi dell'etichetta *Personalizzazione*:

- 1. Nel menu *Config*, selezionare *Utenti>Campi personalizzati*.**

Appare la finestra di dialogo Campi personalizzati utente:

Enable Field	Vis. Ver. Form	Field Name	Field Description	Special Purpose
<input type="checkbox"/> Custom 1	<input type="checkbox"/>			
<input type="checkbox"/> Custom 2	<input type="checkbox"/>			
<input type="checkbox"/> Custom 3	<input type="checkbox"/>			
<input type="checkbox"/> Custom 4	<input type="checkbox"/>			
<input type="checkbox"/> Custom 5	<input type="checkbox"/>			<input type="checkbox"/> Issue Level
<input type="checkbox"/> Custom 6	<input type="checkbox"/>			<input checked="" type="checkbox"/> Card Number
<input type="checkbox"/> Custom 7				
<input type="checkbox"/> Custom 8				

Questa finestra di dialogo contiene vari campi per personalizzare l'etichetta *Personalizzazione*.

- 2. Selezionare le caselle dei campi da attivare.**

- Il campo 6 è riservato all'uso del Programma PassPoint *Plus* e non può essere modificato.

;

Abilita campo – L'operatore può immettere dati in questi campi dell'etichetta *Personalizzazione* nella finestra di dialogo Dati badge.

Verifica visiva – Selezionare questa casella se si desidera che il campo venga visualizzato sulla finestra di dialogo Verifica visiva.

Nome campo – Immettere in questo campo il testo da utilizzare come titolo del campo nell'etichetta *Personalizzazione*.

Descrizione campo – Immettere in questo campo il testo da utilizzare come testo guida del campo nell'etichetta *Personalizzazione*.

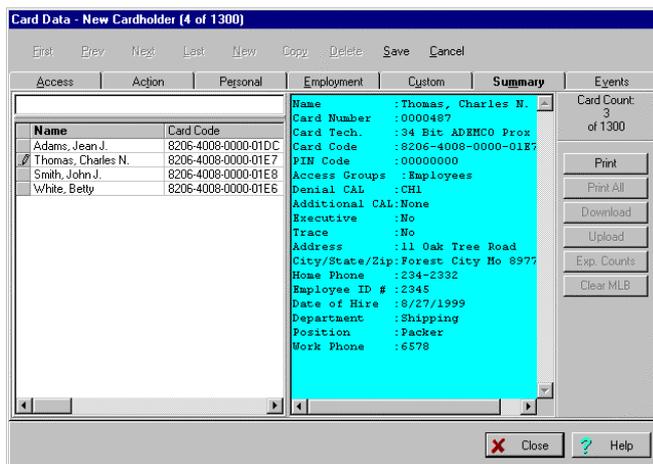
3. Fare clic su **OK**.

Il sistema aggiornerà automaticamente le informazioni nell'etichetta *Personalizzazione*. La prossima volta che si aprirà la finestra di dialogo Dati badge, l'etichetta *Personalizzazione* comprenderà anche i dati inseriti..

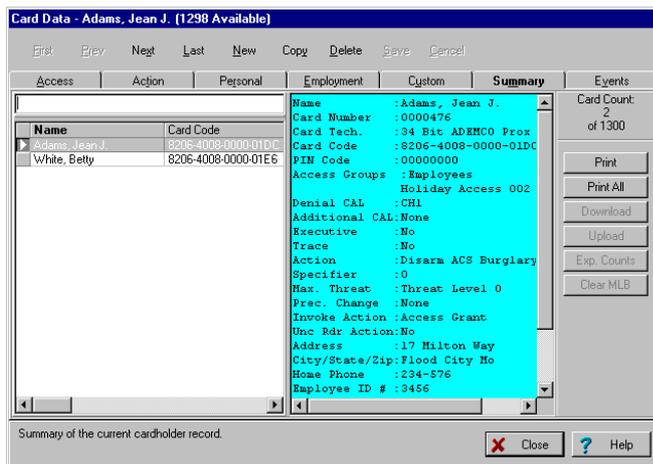
Utilizzo dell'etichetta Sommario

L'etichetta Sommario visualizza un sommario di tutte le informazioni registrate che riguardano l'utente. Quando si memorizzano i dati, il simbolo della matita a sinistra del nome indica l'utente al quale si riferiscono le informazioni visualizzate. Quando si imposta un nuovo utente, facendo clic con il pulsante destro sul simbolo della matita, appare un sottomenu, che chiede

se si desidera salvare o annullare le informazioni utente modificate.



Quando si accede al sommario utente durante una selezione del database Badges / Esplora, lo schermo Utente appare in modo leggermente diverso e funziona in modo diverso, come nell'esempio qui sotto:



Le funzioni seguenti sono disponibili utilizzando la selezione database badges/esplora:

1. Facendo clic sull'intestazione di una colonna si ottiene l'elenco dei badges nell'ordine dell'intestazione. Ad esempio, facendo clic sull'intestazione della colonna Nome, i badges appaiono in ordine di nome. (Nota: modificando l'ordinamento di questa lista, viene modificato anche l'ordine del database dei badges, poiché si riferisce ai pulsanti di navigazione sulla parte superiore del badge).
2. Facendo clic con il pulsante destro nell'area che contiene l'elenco degli utenti, appare una lista di opzioni per disporre l'elenco in ordine di nome, codice badge, codice PIN, numero ID o numero di badge.
3. Dopo aver riordinato gli utenti in base al campo desiderato, si può iniziare la ricerca inserendo le informazioni necessarie nella casella Trova modifica sopra all'elenco degli utenti. Mentre si inserisce il dato, l'informazione viene completata automaticamente, poiché il sistema trova automaticamente i dati che corrispondono. Se si seleziona un ordinamento in base al Codice badge e si è in linea con la MLB, si può presentare il badge ad un lettore di acquisizione badges qualsiasi quando il cursore si trova nella casella Trova modifica. Il sistema cerca il badge nel database dei badges. Quando la trova, il badge verrà evidenziato nell'elenco. In caso contrario, appare un messaggio sullo schermo che informa che il badge non è stato trovato.
4. La freccia a sinistra del nome indica a quale utente si riferisce il sommario visualizzato.
5. Tutti i pulsanti di comando sulla parte destra dello schermo diventano attivi quando il computer è collegato a una MLB. Se non è collegato alla MLB, solo i pulsanti Stampa e Stampa tutto sono attivi. I pulsanti consentono di accedere alle funzioni seguenti:

Stampa – Con questo pulsante si stampano le informazioni del sommario riguardante l'utente selezionato.

Stampa tutto – Con questo pulsante si stampano tutte le informazioni del sommario riguardanti tutti gli utenti.

Aggiorna – Con questo pulsante si aggiornano tutte le modifiche nel database badges e le si trasmettono alla MLB. Questo pulsante deve essere utilizzato solo se il database badges è stato modificato in modalità non in linea.

Carica – Questo pulsante azzera il database badges utenti dal computer e carica il database utenti dalla MLB nel computer.

- -
- ATTENZIONE: Il pulsante Carica deve essere utilizzato solo in condizioni estreme e con la massima cautela, poiché cancella tutte le informazioni utenti non legate all'accesso (indirizzo, campi personalizzati, ecc.).
-

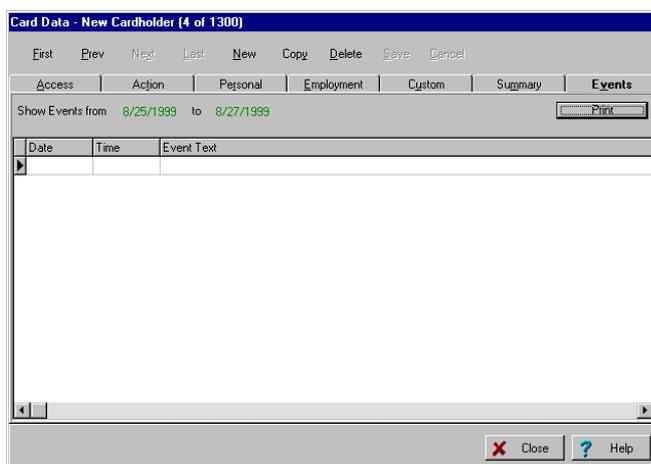
Conteggio scad. – Questo pulsante sposta tutto il database badges nella MLB e carica il conteggio scadenza per tutte i badges che lo utilizzano.

Cancella MLB – Questo pulsante chiede che la MLB cancelli la propria copia del database badges e chiede di ricreare tutti i dati dei badges sulla MLB scaricando il database utenti dal computer.

- -
- ATTENZIONE: Il pulsante Cancella MLB deve essere utilizzato solo in condizioni estreme, perché si cerca di ripristinare la funzionalità di una MLB cancellata.
-

Utilizzo dell'etichetta Eventi

Il sistema PassPoint può visualizzare gli eventi relativi all'utente su un periodo di tempo selezionato. Per ottenere questa funzione, selezionare l'etichetta Eventi. Appare lo schermo seguente:



Per selezionare un periodo di tempo riguardante gli eventi da visualizzare, posizionare il cursore sul campo data "da" e fare clic con il mouse. Appare una finestra di dialogo, che chiede di selezionare una data iniziale. Selezionare la data iniziale. Poi posizionare il cursore sul campo "a" e fare clic con il mouse. Appare una finestra di dialogo, che chiede di selezionare una data finale. Selezionare la data finale.

Vengono visualizzati gli eventi che si sono prodotti durante il periodo selezionato e per l'utente selezionato.

Notare che su un nuovo utente la memorizzazione eventi sarà vuota, a meno che non venga attribuito nuovamente un badge che era stato cancellato precedentemente. Se si sta riattribuendo un badge, verranno visualizzate tutte le attività che si sono prodotte nel periodo selezionato.

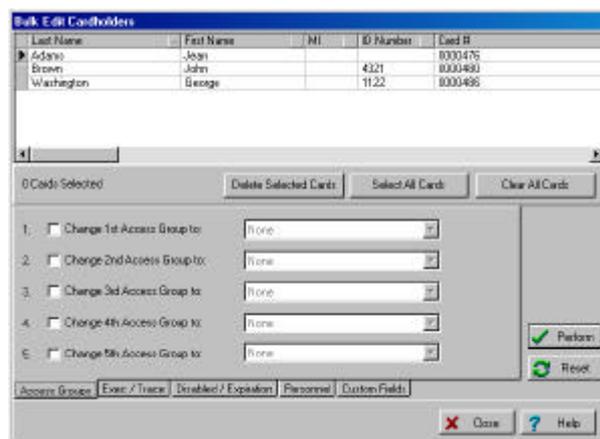
Modifica blocco badges

PassPoint Plus consente di modificare lotti di badges. Questa funzione viene solitamente utilizzata per modificare il contenuto di un campo nel database utente contemporaneamente per diversi utenti. Utilizzando questa funzione, non è necessario richiamare continuamente i dati utente per effettuare modifiche ripetitive.

Per modificare blocchi di badges, seguire la procedura qui sotto:

1. Nel menu Config, selezionare Utenti>Modifica Utenti.

Appare la finestra di dialogo Modifica blocco utenti:



La finestra di dialogo contiene diversi elementi comuni a tutte le etichette nella finestra di dialogo Modifica blocco utenti.

Questi elementi sono:

Area selezione utente – Quest'area dello schermo contiene i nomi dell'utente, i numeri ID, i numeri di badge, i dati personali, i gruppi di accesso e i privilegi. E' possibile selezionare più utenti con le funzioni standard di Windows™ SHIFT-click e CONTROL-click, o si può fare clic con il pulsante sinistro e trascinare ovunque nell'area dati per selezionare più dati utenti successivi. Si può utilizzare i

pulsanti **Seleziona tutte i badges** o **Cancella tutti i badges** per impostare la selezione di tutti gli utenti (vedere più sotto).

La presentazione di questi dati in quest'area può essere modificata come segue:

- L'ordine in cui sono elencati gli utenti può essere modificato facendo clic sulla freccia che si trova sull'intestazione di ogni colonna. Le possibilità di ordinamento sono ascendente (primo clic), discendente (secondo clic) o nessuno (default o terzo clic). Notare che il sistema ordina le colonne in base alla precedenza al momento dell'ordinamento: l'ordinamento è impedito sulle colonne a destra della prima colonna selezionata dall'utente dalla parte sinistra dello schermo.
- L'ordine nel quale vengono presentate le colonne può essere modificato facendo doppio clic sull'intestazione della colonna per selezionarla, e tenendo premuto il pulsante del mouse mentre si trascina la colonna nella posizione desiderata.

Cancella i badges selezionati – Facendo clic su questo pulsante, il sistema chiede conferma per cancellare i badges selezionati. Rispondendo “Sì,” il badge viene cancellato o selezionato per essere cancellato, in base allo stato del record utenti, e viene rimosso dall'elenco visibile di utenti.

Seleziona tutti i badges – Fare clic su questo pulsante per selezionare tutti gli utenti nella griglia di selezione.

Cancella tutti i badges – Fare clic su questo pulsante per deselegionare tutti gli utenti nella griglia di selezione.

Esegui – Fare clic su questo pulsante per immettere nei dati utenti tutte le modifiche apportate sullo schermo attuale. Al termine del processo di modifica, verrà comunicato esattamente quanti record sono stati modificati. Questo numero potrebbe non corrispondere a quello degli utenti selezionati, perché se i dati di un utente selezionato corrispondono già alle impostazioni che si desiderano

immettere, di conseguenza il record dell'utente non verrà modificato. Se sono state effettuate modifiche sullo schermo attuale e se è stata selezionata un'etichetta Modifica blocco badges senza aver fatto clic sul pulsante Esegui, il sistema presenta un messaggio, nel quale si chiede se si vogliono eseguire le modifiche prima di uscire. Rispondendo *Sì*, le modifiche verranno applicate; rispondendo *No*, le modifiche verranno annullate; rispondendo *Annulla*, si rimane nell'etichetta attuale.

Reset – Fare clic su questo pulsante per azzerare tutte le modifiche apportate nello schermo attuale.

Chiudi – Fare clic su questo pulsante quando sono state apportate tutte le modifiche. Lo schermo viene azzerato e le modifiche scaricate nella MLB.

Help – Fare clic su questo pulsante per visualizzare la guida di Modifica blocco utenti.

Modifica blocco attribuzione gruppi accesso utente

Quando è stato selezionato Badges >Modifica utenti nel menu Config, appare la finestra di dialogo Modifica blocco utenti:

Last Name	First Name	MI	ID Number	Card #
Adams	John			0000475
Brown	John		4321	0000488
Washington	George		1122	0000488

0 Cards Selected Delete Selected Cards Select All Cards Clear All Cards

1. Change 1st Access Group to: None

2. Change 2nd Access Group to: None

3. Change 3rd Access Group to: None

4. Change 4th Access Group to: None

5. Change 5th Access Group to: None

Perform Reset

Access Group: Exec / Tact Disabled / Expired Personnel Custom Fields

Close Help

Per modificare le attribuzioni dei gruppi di accesso degli utenti, seguire la procedura seguente:

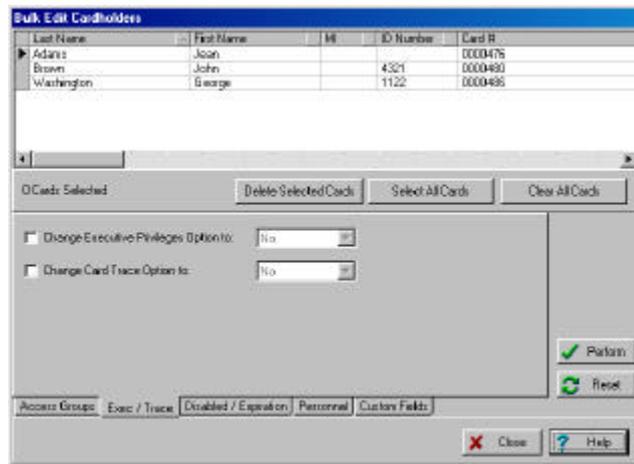
1. **Selezionare gli utenti desiderati per la modifica dell'attribuzione del gruppo di accesso utilizzando uno dei tre metodi seguenti: premere il pulsante Seleziona tutti i badges; Shift-Click sugli utenti; o Ctrl-Click sugli utenti.**

Notare che se la selezione viene facilitata, l'ordine nel quale appaiono gli utenti può variare a seconda delle funzionalità di ordinamento descritte precedentemente.

2. **Selezionare il Gruppo di accesso da modificare (da 1 a 5) facendo spuntando la casella corrispondente.**
3. **Fare clic sulla freccia a destra del gruppo di accesso da modificare e selezionare nell'elenco un nuovo gruppo.**
4. **Fare clic sul pulsante Esegui. Le modifiche vengono inserite nei dati utente.**
5. **Ripetere i punti 2 e 4 per ogni gruppo di accesso da modificare.**

Modifica blocco privilegi executive / traccia

Per modificare l'attribuzione dei privilegi executive e della traccia, fare clic sull'etichetta Exec / Traccia. Appare la finestra di dialogo Modifica blocco privilegi executive / traccia utenti:



Per modificare le attribuzioni privilegi executive / traccia degli utenti, seguire la procedura seguente:

- 1. Selezionare gli utenti per i quali si vogliono modificare le attribuzioni dei gruppi di accesso con uno dei tre metodi seguenti: premere il pulsante Seleziona tutti i badges; Shift-Click sugli utenti; oppure Ctrl-Click sugli utenti.**

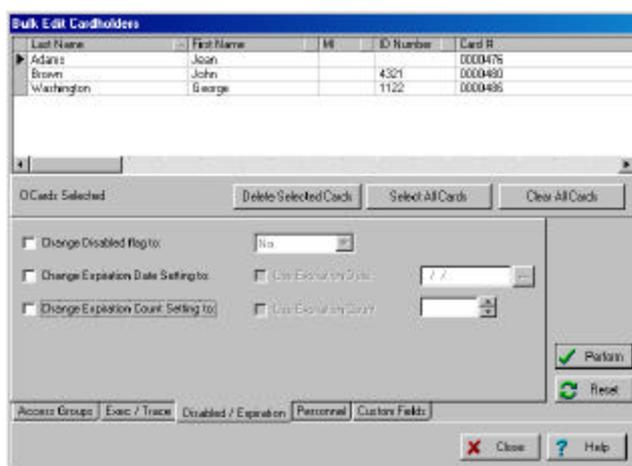
Notare che se la selezione è più semplice, l'ordine nel quale appaiono gli utenti può variare a seconda delle funzionalità di ordinamento descritte precedentemente.

- 2. Selezionare la voce da modificare spuntando la casella corrispondente.**
- 3. Fare clic sul pulsante Esegui. Le modifiche vengono inserite nei dati utente.**

Modifica blocco disabilitazione/data di scadenza

Per modificare in blocco alcuni utenti disabilitati e date di scadenza, fare clic sull'etichetta Disabilitazione/Scadenza. Appare

la finestra di dialogo Modifica blocco disabilitazione/scadenza utenti:



Per modificare la data di disabilitazione/scadenza degli utenti, seguire la procedura seguente:

1. **Per modificare la disabilitazione di alcuni utenti, procedere nel modo seguente:**
 - a. **Selezionare gli utenti desiderati con uno dei tre metodi seguenti: premere il pulsante Seleziona tutti i badges; Shift-Click sugli utenti; oppure Ctrl-Click sugli utenti.**

Notare che se la selezione è più semplice, l'ordine in cui gli utenti appaiono può essere modificato in base alle funzionalità di ordinamento descritte precedentemente.
 - b. **Selezionare “Modifica la disabilitazione in:” facendo clic sulla casella corrispondente.**
 - c. **Fare clic sulla freccia che si trova a destra dell'opzione selezionata e selezionare Sì o No nell'elenco presentato.**

- d. Fare clic sul pulsante **Esegui**. Le modifiche vengono inserite nei dati utente.
2. Per modificare le impostazioni della data di scadenza, procedere nel modo seguente:
 - a. **Selezionare gli utenti desiderati con uno dei tre metodi seguenti: premendo il pulsante Seleziona tutti i badges; Shift-Click sugli utenti; oppure Ctrl-Click sugli utenti.**

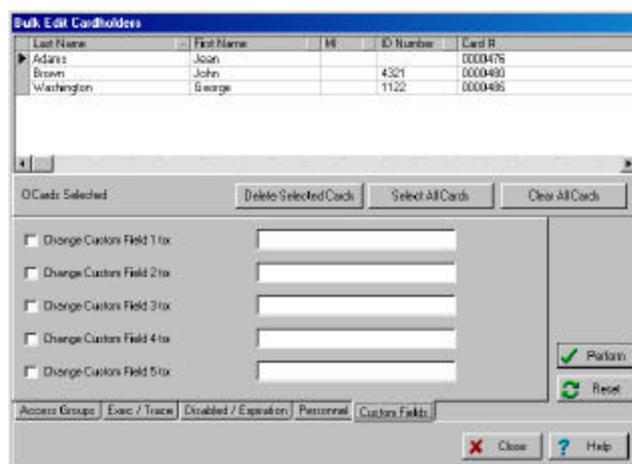
Notare che se la selezione è più semplice, l'ordine in cui appaiono gli utenti può essere modificato utilizzando le caratteristiche di ordinamento descritte precedentemente.
 - b. **Selezionare “Modifica la data di scadenza in:” facendo clic sulla casella corrispondente. Il campo Utilizza data di scadenza diventa attivo.**
 - c. **Fare clic sulla casella Data Scadenza. Il campo del calendario a destra della casella diventa attivo.**
 - d. **Immettere una data nel campo del calendario direttamente con la tastiera o facendo clic sul pulsante a destra del campo del calendario, e selezionando una data nel calendario visualizzato.**
 - e. **Fare clic sul pulsante Esegui. Le modifiche vengono inserite nei dati utente.**
 3. Per modificare il Conteggio scadenza per alcuni utenti, procedere nel modo seguente:
 - a. **Selezionare gli utenti desiderati con uno dei tre metodi seguenti: premere il pulsante Seleziona tutti i badges; Shift-Click sugli utenti; oppure Ctrl-Click sugli utenti.**

Notare che se la selezione è più semplice, l'ordine in cui appaiono gli utenti può essere modificato utilizzando le funzionalità di ordinamento descritte precedentemente.

- b. Selezionare “Modificare conteggio scadenza in:” facendo clic sulla casella corrispondente. Il campo Conteggio scadenza diventa attivo.
- c. Fare clic sulla casella Conteggio scadenza. Il campo conteggio a destra della casella diventa attivo.
- d. Immettere un numero nel campo conteggio direttamente con la tastiera o facendo clic sul pulsante che si trova a destra del campo conteggio, finché viene visualizzato il numero desiderato. Sono validi i numeri compresi fra 1 e 65.534.
- e. Fare clic sul pulsante Esegui. Le modifiche sono inserite nei dati utenti.

Modifica blocco campi personalizzati utente

Per modificare un blocco di dati nei campi personalizzati utente, fare clic sull'etichetta Campi personalizzati. Appare la finestra di dialogo Campi personalizzati utenti:



Per modificare i dati nei campi personalizzati utente, seguire la procedura seguente:

NOTA: Se uno o più campi personalizzati non sono stati impostati nel sistema, non saranno attivi sullo schermo.

1. **Selezionare gli utenti desiderati sui quali operare le modifiche con uno dei tre metodi seguenti: premere il pulsante Seleziona tutti i badges; Shift-Click sugli utenti; oppure Ctrl-Click sugli utenti.**

Notare che se la selezione è più facile, l'ordine nel quale appaiono gli utenti può essere modificato utilizzando le caratteristiche di ordinamento descritte precedentemente.

2. **Selezionare il Campo personalizzato da modificare (da 1 a 5) facendo clic sulla casella corrispondente.**
3. **Immettere la nuova informazione nella casella del campo personalizzato a destra del "Modifica campo personalizzato in:" selezionato.**
4. **Fare clic sul pulsante Esegui. Le modifiche sono inserite nei dati utente.**
5. **Ripetere i punti da 2 a 4 per ogni campo personalizzato da modificare.**

Monitor badge

Il programma PassPoint *Plus* consente di visualizzare la fotografia di un utente sullo schermo del computer, quando l'utente provoca un evento che deve apparire nella memorizzazione eventi (ad esempio l'accesso consentito). Per utilizzare questa funzione, la fotografia dell'utente deve far parte dei record "*Personal*" nel database utenti e il computer deve essere collegato alla MLB. Di seguito sono illustrate le procedure per creare uno Strumento per richiamare il Monitor badge e per utilizzare il monitor badge.

Creazione del monitor badge

E' possibile avviare il monitor badge aggiungendolo come strumento in PassPoint *Plus*. Per aggiungere il Monitor badge al menu degli strumenti, seguire la procedura seguente:

1. **Fare clic sull'etichetta *Strumenti* sulla parte superiore dello schermo PassPoint *Plus*.**
2. **Fare clic su *Configura strumenti* nel menu a tenda.** Appare uno schermo Configura strumenti.
3. **Fare clic sul pulsante *Aggiungi*.** Appare uno schermo Proprietà strumenti.
4. **Nell'area *Titolo* dello schermo Proprietà strumenti, digitare "Monitor badge."**
5. **Posizionare il cursore nell'area Programma dello schermo Proprietà strumenti e fare clic sul pulsante *Esplora*.** Viene visualizzata la directory dei file PassPoint *Plus*.
6. **Far scorrere la directory dei file PassPoint *Plus* fino a raggiungere "CardActMon.exe" e fare doppio clic su di esso.** Il file viene aggiunto all'area Programma dello schermo e l'area Directory dello schermo viene riempita automaticamente.
7. **Fare clic sul pulsante *OK* nello schermo Proprietà strumenti. Lo schermo si chiude e il Monitor badge viene aggiunto allo schermo Configura strumenti.**
8. **Fare clic sul pulsante *Chiudi* sullo schermo Configura strumenti.** Il Monitor badge è ora disponibile in PassPoint *Plus*.

Utilizzo del monitor badge

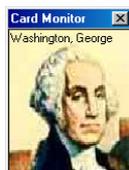
Il Monitor badge viene avviato selezionandolo dal menu Strumenti in PassPoint *Plus*. Per utilizzare il Monitor badge procedere nel modo seguente:

NOTA: Affinché l'applicazione funzioni correttamente, il computer deve essere collegato con la MLB e le fotografie degli utenti devono essere memorizzate nei record Personali nel database utenti.

1. **Fare clic sull'etichetta *Strumenti* sulla parte superiore dello schermo PassPoint *Plus*.**
2. **Nel menu a tenda fare clic su *Monitor badge*.** Il monitor badge è operativo e viene aggiunta una finestra monitor badge sullo schermo. La finestra è riportata nel modello qui sotto:



Quando si produce un evento (accesso consentito), la fotografia dell'utente appare nella finestra Monitor badge come nell'esempio qui sotto:



E' possibile ottenere informazioni utilizzando il Monitor badges, che può essere spostato, ridotto e abbandonato come spiegato qui sotto:

Ottenere informazioni evento utente – Posizionare il puntatore sulla fotografia nella finestra Monitor badge e fare clic con il pulsante sinistro del mouse. Vengono presentate le informazioni sull'evento che ha fatto visualizzare la fotografia dell'utente. L'informazione apparirà come nell'esempio qui sotto:



Spostare la finestra Monitor badge – La finestra Monitor badge può essere spostata in due modi:

- a. Posizionare il cursore sulla barra che si trova sulla parte superiore della finestra Monitor badge, tenere premuto il pulsante sinistro del mouse e trascinare la finestra nella posizione desiderata.
- b. Posizionare il cursore sulla barra che si trova sulla parte superiore della finestra Monitor badge e fare clic con il pulsante destro. Appare un menu, nel quale selezionare *Sposta*. Per spostare la finestra Monitor badge, utilizzare le frecce della tastiera del computer o tenere premuto il pulsante sinistro del mouse e trascinare la finestra.

Ridurre la finestra Monitor badge – Le dimensioni della finestra Monitor badge possono essere ridotte in tre modi:

- a. Posizionare il cursore sulla X che si trova nell'angolo superiore destro della finestra Monitor badge e fare clic con il pulsante sinistro del mouse.
- b. Posizionare il cursore sulla fotografia della finestra Monitor badge e fare clic con il pulsante destro. Appare un menu, nel quale selezionare *Riduci* per ridurre la finestra Monitor badge.

- c. Posizionare il cursore sulla barra che si trova sulla parte superiore della finestra Monitor badge e fare clic con il pulsante destro. Appare un menu nel quale selezionare *Chiudi* per ridurre la finestra Monitor badge.

Uscire da Monitor badge – Si può uscire da Monitor badge facendo clic con il pulsante destro sulla fotografia della finestra monitor badge. Appare un menu nel quale selezionare *Uscita* per eliminare dallo schermo la finestra Monitor badge.

Capitolo

7

Impostazione delle opzioni generali del sistema

Questo capitolo spiega come impostare molti parametri generali di PassPoint:

- **Impostare le preimpostazioni del sistema**
- **Impostare le tecnologie del badge**
- **Impostare e utilizzare codici residenti**
- **Impostare le opzioni della parte intrusione**
- **Impostare le opzioni selezionatore**
- **Impostare i parametri modem**
- **Impostare i parametri rete / ID**
- **Impostare le priorità del sistema**

Opzioni generali del sistema PassPoint

Le opzioni generali del sistema sono parametri che controllano alcuni aspetti delle operazioni del sistema. Impostando queste opzioni in base secondo le necessità dell'installazione, è possibile adattare il sistema alle condizioni particolari dei locali.

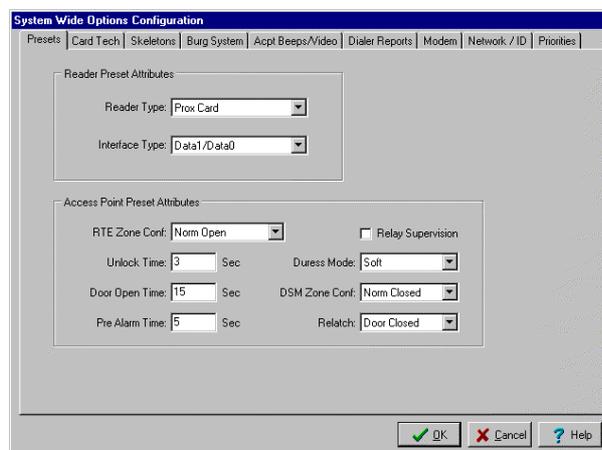
Le opzioni generali del sistema comprendono:

- **Preimpostazioni**
- **Tecnologia del badge**
- **Codici residenti**
- **Parte intrusione**
- **Beeps/video**
- **Opzioni selezionatore**
- **Parametri modem**
- **Parametri rete / ID**
- **Priorità del sistema**

I particolari di tutte queste opzioni sono illustrati in questo capitolo.

Tutte le opzioni generali del sistema sono impostate in una finestra di dialogo dedicata, chiamata Sistema. Per accedere a questa finestra di dialogo, selezionare *Opzioni generali del sistema* nella finestra Configurazione Installatore o dal menu Config:

Utilizzare questo schermo per impostare le opzioni generali del sistema



Impostazione delle opzioni generali del sistema

Utilizzare questa finestra di dialogo esattamente come qualsiasi altra finestra PassPoint. Immettere i dati necessari nei relativi campi. In alcuni campi, bisogna scegliere fra alcune impostazioni preconfigurate del sistema. Altri campi consentono di immettere i dati direttamente dalla tastiera. Il paragrafo seguente offre istruzioni dettagliate su ogni campo.

Al termine dell'impostazione, fare clic su *OK*.

Preimpostazioni del sistema (Etichetta Preimpostati)

Questo schermo consente all'installatore di scegliere alcuni parametri di configurazione dell'hardware che verranno richiamati quando si aggiungeranno elementi hardware al sistema.

Impostando questi campi con i valori che verranno utilizzati più di frequente, si guadagnerà tempo al momento della configurazione di nuovi hardware, poiché queste impostazioni verranno richiamate automaticamente.

The screenshot shows a software configuration window titled "System Wide Options Configuration". It has a tabbed interface with tabs for "Presets", "Card Tech", "Skeletons", "Burg System", "Acpt Beeps/Video", "Dialer Reports", "Modem", "Network / ID", and "Priorities". The "Card Tech" tab is active. Under "Reader Preset Attributes", "Reader Type" is a dropdown menu set to "Prox Card" and "Interface Type" is a dropdown menu set to "Data1/Data0". Under "Access Point Preset Attributes", "RTE Zone Conf" is a dropdown menu set to "Norm Open", "Relay Supervision" is an unchecked checkbox, "Unlock Time" is a text input set to "3" with "Sec" next to it, "Duress Mode" is a dropdown menu set to "Soft", "Door Open Time" is a text input set to "15" with "Sec" next to it, "DSM Zone Conf" is a dropdown menu set to "Norm Closed", "Pre Alarm Time" is a text input set to "5" with "Sec" next to it, and "Relatch" is a dropdown menu set to "Door Closed". At the bottom right, there are three buttons: "OK" (with a green checkmark), "Cancel" (with a red X), and "Help" (with a question mark).

- Cambiando le opzioni a questo livello, non si modificano le impostazioni nelle opzioni configurate preesistenti. Queste preimpostazioni verranno utilizzate quando verranno aggiunti nuovi apparati al sistema. E' possibile riconfigurare gli apparati se si desidera personalizzare ulteriormente un componente.

Attributi predefiniti del lettore

Gli attributi predefiniti del lettore inseriti nei campi seguenti verranno riempiti automaticamente quando vengono attribuiti dei lettori al sistema; è comunque possibile modificarli selezionando impostazioni diverse al momento della configurazione dei singoli moduli hardware.

Tipo di lettore – Selezionare in questo campo il tipo di lettore, tastiera o abbinamento che verrà utilizzato nell'impianto.

Tipi di interfaccia – Selezionare in questo campo l'interfaccia elettrica che i lettori devono utilizzare, ovvero il protocollo tramite il quale dialogano con il modulo DCM.

Attributi predefiniti varco

Gli attributi predefiniti del varco inseriti nei seguenti campi verranno riempiti automaticamente quando si configurano i varchi del sistema; è comunque possibile modificarli selezionando attributi diversi al momento di configurare i singoli varchi.

Zona RDU – Selezionare la configurazione della zona che verrà utilizzata per le zone RDU (Richiesta Di Uscita).

Tempo sblocco – Immettere il tempo di sblocco di default (in secondi) per i varchi.

Tempo porta aperta – Immettere il tempo porta aperta di default (in secondi) per i varchi.

Tempo di preallarme – Immettere il tempo di preallarme di default (in secondi) per i varchi.

Supervisione relè – Selezionare questa casella se si desidera la funzionalità di supervisione relè per i varchi attivati al momento della configurazione di un nuovo varco.

Costrizione – Scegliere in questo campo l'impostazione del modo costrizione per i varchi.

Zona MSP – Selezionare la configurazione della zona che verrà utilizzata dalle zone MSP (Monitor Stato Porta).

Sblocca – Scegliere in questo campo l'opzione sblocca per i relè ariporta dei varchi.

Si consiglia di utilizzare lo sblocco sulla chiusura con i blocchi elettromagnetici, e lo sblocco sull'apertura con le elettroserrature.

Opzioni tecnologia badge (Etichetta tecnol. badge)

Perché PassPoint possa comunicare adeguatamente con l'hardware di controllo della porta (i lettori), deve essere a conoscenza di alcuni parametri.

Ad esempio, il sistema deve sapere quanti bit d'informazione contiene il badge che si sta utilizzando. Inoltre, il sistema deve ricevere informazioni "di riconoscimento", in modo tale che possa decifrare i dati trasmessi dai badges e cercare di riconoscerli.

The screenshot shows the 'System Wide Options Configuration' dialog box. The 'Card Tech' tab is selected. Under 'Card Recognizers', there is a table with the following data:

Num	Name	Field A	Field B	Field C
1	NCC Wiegand 26	0	0	256
2	NCC Ademco Wiegand 34	0	0	256
3	NCC Dorado EMPIII 34	0	0	0
4	Bit Image of Specified Length	0	0	0

Below the table, the 'Card Lengths' section contains the following fields:

- Weigand Card Bits: 26
- Proximity Card Bits: 34
- Magnetic Strip Card Bits: 26 (with a 'Config Mag' button)
- Keypad PIN Digits: 4 (with a dropdown arrow)

At the bottom right, there are buttons for 'OK', 'Cancel', and 'Help'.

Informazioni riconoscimento badges

Questi campi visualizzano le informazioni riguardanti i formati dei badges di accesso supportate dal sistema. In genere, questi campi non hanno bisogno di essere modificati.

Lunghezza badges

Bit badge Wiegand – E' il numero di bit utilizzati dai lettori di badges Wiegand utilizzati nel sistema PassPoint. Impostando questo campo a 255 si permette automaticamente al sistema di utilizzare qualsiasi badge con lunghezza superiore a 26 bit. Notare che se non è necessaria una lunghezza di badge variabile (impostazione 255), è meglio lasciare questo campo con l'esatta lunghezza di badge richiesta dall'installazione.

Bit badge prossimità – E' il numero di bit utilizzati dai lettori di badges di prossimità utilizzati nel sistema PassPoint. Impostando questo campo a 255 si permette automaticamente al sistema di utilizzare qualsiasi badge con lunghezza superiore a 26 bit. Notare che se non è necessaria una lunghezza di badge variabile (impostazione 255), è meglio lasciare questo campo con l'esatta lunghezza di badge richiesta dall'installazione.

Bit badge a banda magnetica - E' il numero di bit utilizzati dai lettori di badges a banda magnetica nel sistema PassPoint. Impostando questo campo a 255 si permette automaticamente al sistema di utilizzare qualsiasi badge con lunghezza superiore a 26 bit. Notare che se non è necessaria una lunghezza di badge variabile (impostazione 255), è meglio lasciare questo campo con l'esatta lunghezza di badge richiesta dall'installazione. Impostando la lunghezza a 254, si tolgono i bit di parità di ogni carattere American Banking Association (ABA) e si semplifica l'identificazione dei dati dei badges raw. Impostando la lunghezza a 254 si attiva anche il pulsante *Config Mag*. Selezionando il pulsante *Config Mag* si apre una schermata nella quale sarà possibile modificare il formato del badge magnetico. Vedere il paragrafo sulla Configurazione dei badges magnetici ABA per i particolari dello schermo Configurazione badges magnetici ABA.

Lunghezza PIN – La lunghezza di questo campo può variare da tre a otto caratteri per il Codice di identificazione personale (PIN). L'ultima cifra attribuita al codice PIN NON DEVE essere ZERO. I codici PIN che finiscono con zero sono considerati dal sistema

Formato C, Formato Kronos – Questo formato può essere utilizzato per riconoscere badges Kronos di un sistema rilevamento presenze esistente. Se vengono utilizzati lettori di codice a barre tipo “Time Keeping System’s ACM” (configurati per formato ABA), questo formato dovrebbe funzionare correttamente.

Formato D – Un esempio di un formato ABA.

Formato E – Un altro esempio di un formato ABA.

Formato F – Un esempio di formato di carta di credito. In alcuni casi si può utilizzare una carta di credito per il controllo di accesso. **Attenzione:** per ragioni di riservatezza, molti utenti non desiderano che il proprio numero di carta di credito sia registrato in un sistema di controllo di accesso.

NOME

Il campo Nome aiuta semplicemente a identificare un formato particolare. Questi nomi dovrebbero essere il più descrittivi possibile. Se descrive il formato codificato della società lo si può chiamare “Formato standard della societàABC.”

LUNGHEZZA

Lunghezza badge – Rappresenta il numero totale di caratteri che saranno riconosciuti dal sistema. Include:

- **Start Sentinel** – Questo carattere deve essere B esadecimale e indica l'inizio dei dati del badge. E' sempre considerato a zero offset quando descrive le caratteristiche di posizionamento dei dati del badge.
- **Separatore di campo** – Questo carattere deve essere D esadecimale e indica la fine di un campo e/o l'inizio di un nuovo campo. I separatori di campo sono ignorati nelle

impostazioni di formato di PassPoint e sono rappresentati da un carattere non utilizzato o da X nell'area della struttura dati. I separatori di campo sono necessari per separare i campi.

- **End Sentinel** – Questo carattere deve essere F esadecimale e indica la fine dei dati del badge. Questi caratteri sono ignorati nelle impostazioni di formato PassPoint e vengono trattati esattamente come i Separatori di campo.
- **Checksum** – Questo carattere può essere un qualsiasi valore esadecimale singolo (da 0 a F) e si trova subito dopo la End Sentinel. Questo carattere non viene utilizzato dal sistema di controllo di accesso PassPoint, ma deve essere riconosciuto come spazio riservato nel valore di Lunghezza del badge.

Lunghezza badge cifre esatte – Quando questa casella è selezionata, il numero di caratteri letti sul badge deve corrispondere esattamente al valore di lunghezza badge. In caso contrario, la lettura del badge verrà ignorata. Notare che molti badges a banda magnetica hanno degli zeri programmati prima della Start Sentinel e dopo il checksum e la End Sentinel. Questi zeri verranno ignorati dal sistema e non verranno considerati nel computo del numero esatto di caratteri letti sul badge. Questo perché il numero dei primi e degli ultimi zero può variare da un passaggio badge a un altro. Sono usati anche per aiutare a sincronizzare la lettura del badge con l'interfaccia.

CODICE DI SISTEMA

Questo campo viene indicato anche come codice sito. E' consigliabile per aziende con due o più sedi. Ogni sede può essere identificata con un proprio Codice di sistema, in modo da consentire anche al sistema di distinguere numeri di badge identici fra loro.

Inizio – Questo valore rappresenta l'offset (dalla cifra zero) da cui inizia il Codice di sistema. Questo valore è impostato a zero offset. Se questo valore è impostato a zero, significa che il Codice

di sistema non esiste (o non è utilizzato) in questa impostazione di formato particolare.

Lunghezza – Questo valore rappresenta il numero di caratteri utilizzati nel Codice di sistema. PassPoint accetta valori compresi fra 1 e 9.

NUMERO BADGE

Il campo Numero badge è solitamente utilizzato per distinguere un utente da un altro. Dovrebbe essere esclusivo per ogni utente, ma può essere copiato per altri utenti se vengono utilizzati Codici di sistema diversi e/o Duplicati.

Inizio – Questo valore rappresenta l'offset (dalla cifra zero) da cui inizia il campo Numero del badge. Ricordare che la Start Sentinel è sempre a offset zero. Se questo valore è impostato a zero, significa che il Numero badge non esiste (o non è utilizzato) in questa impostazione di formato particolare. Il campo Numero badge dovrebbe *sempre* essere usato in qualsiasi impostazione di formato.

Lunghezza – Questo valore rappresenta il numero di caratteri utilizzati nel Numero badge. PassPoint accetta valori compresi fra 1 e 16. Notare che il numero massimo di caratteri che PassPoint può accettare è 16. Questo valore comprende anche il campo Duplicato (descritto qui sotto). Aumentando il numero di caratteri della lunghezza del dato Numero Badge, non è possibile sovrascrivere il campo Duplicato, poiché la somma dei due dati non deve eccedere i 16 caratteri.

DUPLICATO

Il Duplicato viene utilizzato quando il numero del badge deve essere conservato, anche in caso di smarrimento del badge originale. Ad esempio, il Numero del badge potrebbe

corrispondere al Numero di Matricola del dipendente. Se il dipendente perdesse il proprio badge, non sarà comunque possibile modificare il numero di matricola del dipendente per adattarsi alle necessità del sistema di controllo di accesso. In caso di smarrimento del badge, si può aumentare il Duplicato e il numero del badge e i codici sistema possono restare gli stessi..

Inizio – Questo valore rappresenta l'offset (dalla cifra zero) da cui inizia il Duplicato. Ricordare che la Start Sentinel è sempre a offset zero. Se questo valore è impostato su zero, significa che il Duplicato non esiste (o non è utilizzato) in questa impostazione di formato particolare.

Lunghezza – Questo valore rappresenta il numero di caratteri utilizzati nel Duplicato. PassPoint accetta valori compresi fra 1 e 16. Ricordare che il numero massimo di caratteri che PassPoint può rappresentare è 16. Questo valore comprende anche il campo Numero badge (descritto precedentemente). Aumentando il numero di caratteri della lunghezza del dato Duplicato, non è possibile sovrascrivere il campo Numero Badge, poiché la somma dei due dati non deve eccedere i 16 caratteri.

STRUTTURA DATI

L'area Struttura dati fornisce una rappresentazione grafica dei dati contenuti nel badge. Oltre a indicare la collocazione di ogni campo nei dati, avvisa anche l'operatore in caso di conflitto o di sovrapposizione nell'impostazione dei dati.

La legenda con i colori sulla parte superiore dell'area Struttura dati descrive il significato di ogni campo. Se qualche campo si sovrappone a causa della lunghezza o per conflitti offset, l'area di sovrapposizione diventa rossa e contiene un punto esclamativo per ogni carattere sovrapposto. PassPoint *Plus* non consente di salvare un'impostazione con campi sovrapposti.

CODICI DI SISTEMA

PassPoint offre la possibilità di impostare fino a 16 Codici di sistema diversi per ogni formato badge. I valori immessi in questi campi appaiono nel Calcolatore badges, dove possono essere attribuiti al badge appropriato quando viene magnetizzato.

Nel caso in cui fossero necessari più di 17 Codici di sistema, il formato del badge può essere copiato fino a tre volte (per un totale di quattro impostazioni identiche). In questo modo, se uno stesso formato viene utilizzato da un solo cliente, quel cliente può identificare fino a 64 Codici di sistema esclusivi.

CARICA DA FILE

Selezionando questo pulsante, si carica un'impostazione formato precedentemente salvata in un file nell'attuale impostazione del formato. E' possibile creare più formati identici, come descritto nei Codici di sistema più sopra. Inoltre, altri clienti possono caricarli, in modo tale che un formato impostato precedentemente possa essere utilizzato per più clienti. Tutte le informazioni visualizzate su ogni etichetta Impostazione formato verrà sostituita. Ciò include anche l'elenco dei Codici di sistema.

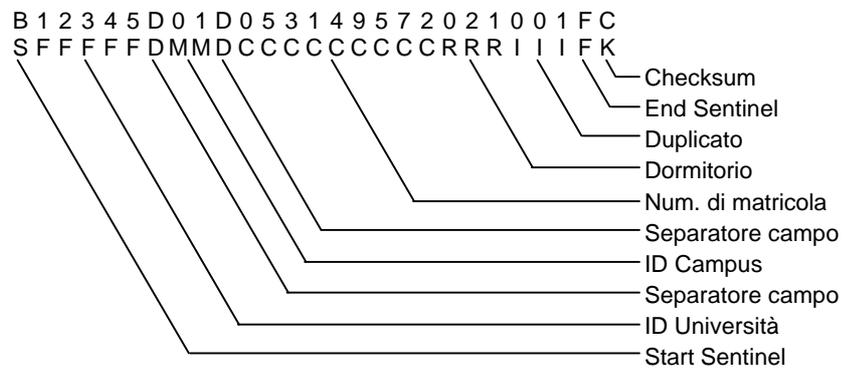
SALVA NEL FILE

Selezionando questo pulsante si salva l'impostazione attuale del formato badge sul disco. Tutte le informazioni visualizzate su ogni etichetta Impostazione formato verranno salvate. Ciò comprende l'elenco dei Codici di sistema.

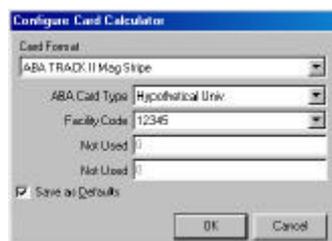
Esempio di configurazione ABA MagStripe

Qui sotto è stata presentata una configurazione ipotetica del formato di un badge magnetico per un'università

L'università possiede cinque campus diversi, ognuno con una serie di dormitori. Ogni studente è registrato in base al proprio numero di matricola. Per non avere eventuali problemi di smarrimento badges, è stato inserito anche un campo Duplicato. Il formato e i dati tipici dell'utente sono indicati qui sotto.

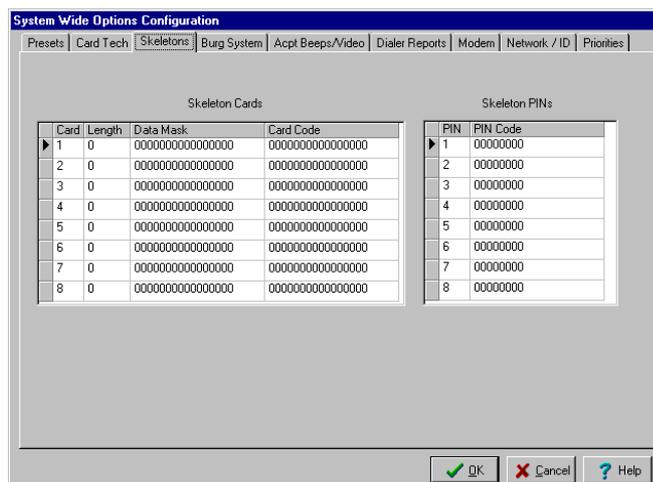


L'ID Università(12345) verrà utilizzato come Codice di sistema. Il Numero di matricola dello studente (053-14-9572) verrà utilizzato come numero badge. Il Duplicato (001) verrà utilizzato come duplicato. Tutti gli altri campi verranno ignorati. Lo schermo con il formato risultante sarà il seguente:



Codici residenti (Etichetta Residenti)

Questo schermo consente all'installatore di modificare i badges residenti del sistema e i codici PIN residenti:



I codici residenti sono un metodo con il quale il sistema può autorizzare l'accesso a codici PIN o badges specifici e/o gruppi specifici di badges nel raro caso in cui si verificasse una interruzione di comunicazione fra un modulo DCM e la MLB. I badges residenti sono soggetti a un'analisi dei bit, in base alle impostazioni dell'installatore. Quest'analisi confronta i campi all'interno della zona dati codificata (i dati letti sul badge) con una

maschera dati del badge, e poi con un modello bit specifico (codice badge).

Dopo aver letto il badge, i dati vengono confrontati con ognuno degli otto dati della tabella badges residenti descritta qui sotto. Il confronto avviene in modo tale che appaiano i dati della tabella. Esistono quattro campi programmabili utilizzati durante il confronto. Sono Lunghezza, Maschera dati, Codice badge e Codice PIN. I primi tre campi sono utilizzati per valutare i dati del badge. L'ultimo campo viene utilizzato per valutare una serie di caratteri digitati tramite tastiera.

Innanzitutto, si imposta nel sistema la lunghezza generale del badge. Si possono impostare fino a otto lunghezze di badges diverse. I dati del badge che non corrispondono alle lunghezze sono ignorati. Se non corrispondono, il procedimento continua fino al dato successivo della tabella, finché si trova una corrispondenza o finché si constata l'errore anche nell'ultimo dato della tabella.

Una Maschera dati di un badge deve filtrare i campi specifici di interesse. Quando appare un uno (1) in una posizione bit del filtro, un bit nella stessa posizione nei dati del badge (di lunghezza corrispondente) viene confrontato con un bit nella posizione corrispondente del Codice badge. Quando appare uno zero (0) nella posizione bit, questo bit viene ignorato durante il confronto.

I codici badge (la cui posizione bit nella maschera dati dei badges residenti è impostata su uno) devono corrispondere esattamente ai dati filtrati del badge, bit per bit. In questo caso, se la Maschera dati si compone di soli uno nell'area del codice di sistema (considerato anche come codice sito), verrà accettata qualsiasi badge con un codice di sistema corrispondente.

Dopo aver individuato la corrispondenza, la riga della tabella Badges residenti che contiene i campi Maschera dati e Codice badge corrispondenti viene utilizzata per indicare la stessa riga della colonna RCM residente, Funzionamento lettore A in RCM

residente (o Lettore B in RCM residente), Badges. Dopo aver identificato la riga, viene eseguita l'operazione in essa impostata. In altre parole, se un badge presentato al lettore B corrisponde ai dati del badge residenti della seconda riga della tabella, e la seconda riga della colonna Lettore B in RCM residente, Scheda contiene il comando Sblocca, il punto di accesso che utilizza il Lettore B si sblocca (passa in modalità Escluso).

Parte della terminologia utilizzata nella modalità RCM residenti è leggermente diversa dai termini utilizzati nelle normali operazioni. "Apri" autorizza comunque un accesso. "Escludi" passa la porta in modalità Esclusione (o libero accesso). "Blocca" mette la porta in modalità Protetta dopo che il varco esegue la sequenza Consenso. La sequenza "Protezione blocco dopo Consenso" consente all'utente di uscire da una porta esclusa prima di impostare il varco in modalità "protetto".

Se un lettore utilizza un abbinamento badge/codice PIN, il badge deve corrispondere in base ai criteri impostati in precedenza, e bisogna digitare un codice PIN. I codici PIN non sono comunque controllati accuratamente, si controlla solo che la quantità di caratteri sia corretta.

I campi PIN sono utilizzati solo se un lettore combinato si trova in modalità solo PIN, e il lettore collegato a quel varco è (o ha) una tastiera. Il codice PIN inserito nel campo Codice PIN del menu di sistema, funziona esattamente come i campi PIN normali. Vale a dire che un codice PIN a quattro caratteri è allineato a sinistra. Un codice PIN 1234 apparirà come 12340000 nella colonna Codice PIN (supponendo che il sistema utilizzi quattro caratteri per il codice PIN).

Un ingresso solo PIN corrispondente provoca l'operazione che appare nella stessa posizione della tabella Funzionamento lettore A in RCM residente (o Funzionamento lettore B in RCM Residente). Ad esempio, se un codice PIN inserito nel lettore A corrisponde al codice PIN nella terza riga della colonna Sistema, PIN residenti, Codice PIN, l'azione programmata nello schermo di

impostazione del modulo DCM, etichetta RCM residenti, Funzionamento lettore A in RCM residenti, colonna PIN, terza riga verrà eseguito sul punto di accesso corrispondente.

Le opzioni sono le stesse per i badges e per i codici PIN. Possono essere Non usato, Apri, Escludi o Blocca.

E' possibile avere fino a otto strutture di badges residenti e otto strutture di PIN residenti.

Creazione e attribuzione di codici badges residenti

I codici badges residenti lavorano in modo leggermente diverso dai codici PIN residenti. E' possibile impostare otto codici badges residenti, ma poiché le maschere dei badges residenti possono essere impostate come filtri, ogni descrizione di badge residente può essere utilizzata per l'identificazione di molti badges.

Impostazione di un badge residente per filtrare i badges accettabili

Quando si desidera che un badge residente filtri i badges accettabili, bisogna immaginare che la Maschera dati sia una specie di setaccio (il filtro) e che il Codice badge sia il modello con cui confrontare il dato che viene passato nel filtro. Per capire le operazioni che avvengono sul numero del badge, bisogna conoscere l'aritmetica esadecimale e binaria e le operazioni booleane.

-
- Un 1 in una posizione della maschera dati significa che la posizione del bit nel codice badge e nel badge letto devono essere identiche.

Quando un badge viene presentato ad un varco in RCM, il dato in esso contenuto viene passato attraverso il filtro Maschera dati. Il valore risultante (Dati badge filtrati) viene confrontato con il

Codice badge. Una corrispondenza ESATTA fra i Dati badge filtrati e il Codice badge verrà accettata dal varco.

Ad esempio, supponiamo che si voglia che tutti i badges con Codice di sistema 41 (decimale) passino da un varco chiamato Porta principale. Inoltre, negli esempi seguenti, supponiamo che il numero del badge sia 1827 (decimale).

In questo esempio, i badges utilizzati nel sistema sono badges codificati a 26 bit. Per questo formato, il Codice di sistema è codificato in otto bit, a cominciare dal 25° bit.

	P	F								C										P						
POSIZIONE BIT	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

NOTA: I NOMI DEI CAMPI SONO I SEGUENTI
 P = BIT PARITA' F = CODICE SISTEMA C = NUMERO SCHEDA

Poiché si vuole cercare il Codice di sistema di tutti i badges presentati al lettore del varco, si vuole controllare che tutti i bit del badge nella zona del Codice di sistema passino attraverso il filtro. Si vuole inoltre verificare una corrispondenza ESATTA del Codice di sistema, in modo tale da accettare solamente alcuni badges. La maschera dati badge del badge residenti dovrà allora essere impostata nel modo seguente:

NOTA: Solo i 26 bit inferiori sono utilizzati nella Maschera dati badge e nel Codice badge.

	P	F							C											P						
POSIZIONE BIT	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
POSIZIONE FILTRO PER PASSAGGIO CODICE SISTEMA		1	1	1	1	1	1	1	1																	
POSIZIONE NON UTILIZZATO DA BLOCCARE CON FILTRO	0									0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MASCHERA DATI SCHEDA EFFETTIVA	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EQUIVALENTE ESADECIMALE MASCHERA DATI SCHEDA	1	F							E											0						

NOTA: I NOMI DEI CAMPI SONO I SEGUENTI
P = BIT PARITA' F = CODICE SISTEMA C = NUMERO SCHEDA

Il Codice badge deve essere impostato nel modo seguente per un codice di sistema di 41 (decimale) o di 29 (esadecimale):

	P	F							C											P						
POSIZIONE BIT	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
CODICE SCHEDA	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EQUIVALENTE ESADECIMALE CODICE SCHEDA	0	5							2											0						

NOTA: I NOMI DEI CAMPI SONO I SEGUENTI
P = BIT PARITA' F = CODICE SISTEMA C = NUMERO SCHEDA

Il Codice badge (52000 esadecimale) fornisce una corrispondenza sui dati badge filtrati come illustrato qui sotto:

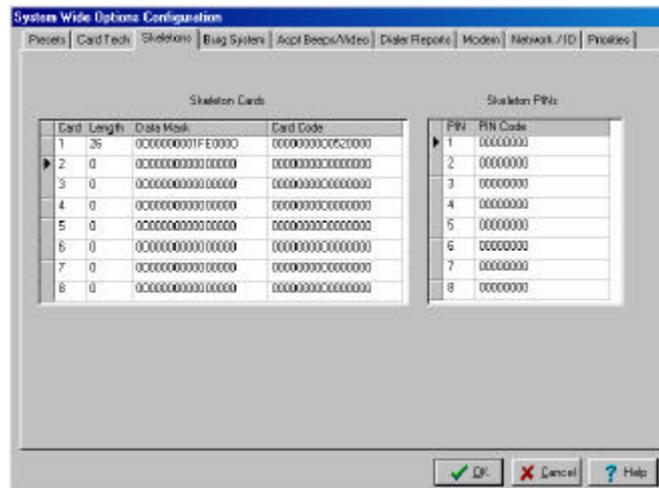
	P		F						C										P							
POSIZIONE BIT	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
DATI SCHEDA	1	0	0	1	0	1	0	0	1	0	0	0	0	0	1	1	0	0	0	1	0	0	0	1	1	0
MASCHERA DATI SCHEDA	0	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DATI SCHEDA FILTRATI	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CODICE SCHEDA	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DATI SCHEDA FILTRATI ED EQUIVALENTE ESADECIMALE CODICE SCHEDA	0		5						2						0				0							

NOTA: I NOMI DEI CAMPI SONO I SEGUENTI

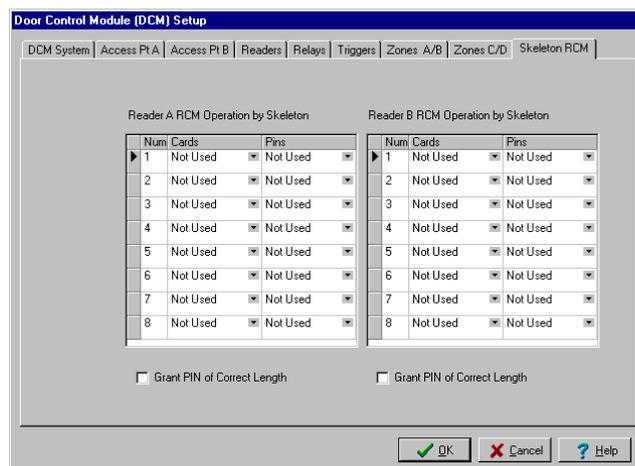
P = BIT PARITA' F = CODICE SISTEMA C = NUMERO SCHEDA

Lunghezza Maschera dati badge Codice badge risult.
026 000000001FE000 00000000052000

Ora che la Maschera dati (1FE000 Esadecimale) e il Codice badge (520000 Esadecimale) sono stati determinati, i dati devono essere inseriti nel sistema nello schermo Residenti. Nella linea Badge 1 dello schermo, dovremo immettere una Lunghezza di 26, una Maschera dati di 1FE000 e un Codice badge di 520000. Lo schermo appare come nell'esempio qui sotto:



La fase successiva è quella di rendere il badge residente riconoscibile dal varco (chiamato Porta principale in questo esempio) in modo tale che, se il sistema dovesse passare in modo RCM, gli utenti con un determinato codice di sistema possano entrare dalla Porta principale (controllata dal lettore A). Il varco viene configurato utilizzando lo schermo Impostazione Hardware, Door Control Module (DCM), etichetta RCM Residente, rappresentato qui sotto. Per sapere come raggiungere gli schermi Impostazione Door Control Module (DCM) e per una descrizione completa, vedere il capitolo "Aggiunta di un Door Expansion Kit" in questo manuale.



In questa schermata, nella riga 1, facciamo clic sulla freccia sotto Badges e dal menu a tendina selezioniamo Apri, confermando la scelta cliccando su OK. Ora, quando il badge verrà letto, il suo contenuto verrà filtrato per isolare il codice di sistema, e i dati filtrati risultanti verranno confrontati con il Codice badge. Una corrispondenza ESATTA fra i Dati badge filtrati e il Codice badge consentirà l'accesso al varco (se il sistema è in modo RCM). Notare che è stato attribuito alla riga 1 perché questo è il Numero badge residenti creato. Se si stessero usando più badges residenti, il numero selezionato sullo schermo dovrebbe

corrispondere al numero di badge residente desiderato che si vuole che esegua questa funzione.

In altre parole, impostando un modello particolare nella quarta riga delle Opzioni generali del sistema, etichetta RCM Residenti, l'azione impostata in Impostazioni DCM, RCM residenti, Lettore A in RCM, campo Badges nella riga quattro verrà eseguita quando un badge i cui dati corrispondono a quanto specificato verrà presentato al Lettore A di quel modulo DCM. Esiste una mappatura di valore univoco fra le righe di queste due tabelle.

Negli esempi seguenti (A e B), supponiamo di utilizzare badges codificati con il formato standard ADEMCO di 34 bit. Il formato standard ADEMCO consiste in tre campi, come descritto qui sotto:

Codice di sistema: Un valore binario a otto bit, che è solitamente lo stesso per tutti i badges appartenenti ad un sistema. Utilizzando questo campo, sarà possibile avere un badge numero 00001 nell'azienda A e un badge numero 00001 nell'azienda B, ma nessuno dei due badges potrà funzionare nell'altro sistema.

Codice RCM: Un campo di 4 bit che può essere utilizzato per raggruppare badges con modelli identici in questo campo. Questi gruppi diversi possono essere poi autorizzati a eseguire funzioni specifiche. Questo campo non è ancora stato implementato all'interno del sistema.

Numero badge: Una valore di venti bit utilizzato per indicare il numero identificativo del badge presentato.

Sono presenti anche 2 bit di parità (uno all'inizio e uno alla fine dei dati del badge), che vengono utilizzati per autenticare la validità dei dati stessi, quando vengono trasmessi dal lettore all'unità di controllo. Per le operazioni residenti RCM, i bit di parità possono essere ignorati, in base alle impostazioni del badge utilizzate.

L'esempio A rappresenta alcuni dati di un badge ADEMCO avente Codice di sistema 8, Codice RCM 4, e Numero badge 1827 (723 Esadecimale). La lunghezza totale dei Dati badge è di 34 bit. Se vogliamo utilizzare solo il Codice di sistema per consentire l'accesso durante il funzionamento RCM, dobbiamo creare una maschera che abbia i bit che rappresentano il Codice di sistema impostato a 1, e tutti gli altri impostati a 0. La Maschera dati apparirà come nell'Esempio B.

Esempio A

NOME CAMPO	P	F						R		C														P											
POSIZIONE BIT	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	
DATI SCHEDA	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	1	0	0	0	1	1	0

NOTA: I NOMI DEI CAMPI SONO I SEGUENTI

P = BIT PARITA'

F = CODICE SISTEMA

R = CODICE RCM

C = NUMERO SCHEDA

Esempio B

NOME CAMPO	P	F						R		C														P												
POSIZIONE BIT	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1		
DATI SCHEDA	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	1	0	0	0	1	1	0	
MASCHERA DATI	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

NOTA: I NOMI DEI CAMPI SONO I SEGUENTI

P = BIT PARITA'

F = CODICE SISTEMA

R = CODICE RCM

C = NUMERO SCHEDA

Impostazione di un badge residente per la ricerca di una corrispondenza esatta

Quando si desidera che un badge residente abbia una corrispondenza esatta, bisogna impostare tutti i bit a uno (ad eccezione dei bit di parità) nella maschera dati del badge; e bisogna immettere un valore esadecimale dei dati del badge come viene letto sul badge nel campo codice badge. L'esempio seguente rappresenta un badge 34 bit, il cui numero, espresso in valore esadecimale, è 010800E46.

Dati badge originali:

NOME CAMPO	P	F						R		C														P											
POSIZIONE BIT	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	
DATI SCHEDA	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	1	0	0	0	1	1	0

NOTA: I NOMI DEI CAMPI SONO I SEGUENTI

P = BIT PARITA'

F = CODICE SISTEMA

R = CODICE RCM

C = NUMERO SCHEDA

Maschera dati badge:

NOME CAMPO	P	F						R		C														P											
POSIZIONE BIT	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	
DATI SCHEDA	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	1	0	0	0	1	1	0
MASCHERA DATI	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0

NOTA: I NOMI DEI CAMPI SONO I SEGUENTI

P = BIT PARITA'

F = CODICE SISTEMA

R = CODICE RCM

C = NUMERO SCHEDA

La Maschera dati deve essere ora convertita in un numero esadecimale:

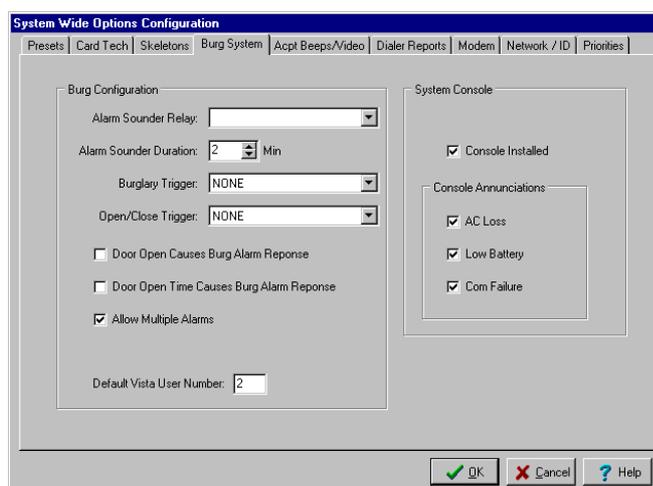
Codici PIN residenti

Immettere un massimo di otto codici PIN allineati a sinistra, che saranno utilizzati come codici residenti. Le funzioni eseguite da questi codici PIN in RCM possono essere impostate per ogni singolo varco nello schermo di configurazione DCM.

L'utilizzo dei codici PIN per ottenere un accesso consentito, un blocco o uno sblocco di un varco è spiegato in questo manuale al capitolo "Aggiunta di un Door Expansion Kit", nella parte riguardante l'etichetta RCM residente.

Opzioni parte intrusione (etichetta Sistema Intrusione)

Questa schermata consente di impostare alcune opzioni generali di configurazione del sistema intrusione:



Configurazione intrusione

Relè sirena – Fare clic sulla freccia a destra del campo Relè sirena e selezionare dall'elenco presentato il relè non valido che si

intende utilizzare come uscita allarme intrusione. Il relè indicato può essere attivato solo dalla parte intrusione del sistema PassPoint. Il relè deve essere assegnato durante la configurazione hardware del sistema tra quelli disponibili sui moduli DCM prima di essere selezionato in quest'area.

Tempo sirena – E' il periodo di tempo (in minuti) per il quale si attiva il Relè Sirena in seguito ad un allarme intrusione. La sirena può essere tacitata con un comando *Off*. La sirena si tacita comunque automaticamente al termine del tempo impostato.

Trigger intrusione – Fare clic sulla freccia a destra del campo Trigger intrusione e selezionare nell'elenco il trigger non valido che si vuole utilizzare come indicatore di Trigger intrusione. Il trigger indicato può essere attivato solo dalla parte intrusione del sistema PassPoint. Questo trigger può essere utilizzato per attivare il sistema radio lunga portata a fronte di un allarme intrusione. Questo trigger deve essere assegnato durante la configurazione hardware del sistema tra quelli disponibili sui moduli DCM prima di essere selezionato in quest'area.

Il Trigger intrusione è attivo quando non ci sono allarmi in corso. Elettricamente, il trigger attira corrente; vale a dire che indica uno zero logico se misurato con un voltmetro quando viene utilizzata una resistenza di pull-up.

Il Trigger intrusione è disattivato quando ci sono allarmi in sospeso. Elettricamente, il trigger non attira corrente; vale a dire che indica un uno logico se misurato con un voltmetro quando viene utilizzata una resistenza di pull-up.

Trigger Ins./Dis. – Fare clic sulla freccia a destra del campo Trigger Ins./Dis. e selezionare nell'elenco presentato il trigger non valido che si vuole utilizzare come indicatore dello stato di Inserimento e Disinserimento della parte intrusione del sistema PassPoint. Questo trigger non può essere controllato manualmente, perché è creato per notificare elettronicamente ad

un sistema estraneo la condizione di inserimento Inserito o Disinserito della parte intrusione di PassPoint. Questo trigger può essere utilizzato per pilotare il canale di inserimento di un sistema radio a lunga portata. Il trigger deve essere assegnato durante la configurazione hardware del sistema tra quelli disponibili sui moduli DCM prima di essere selezionato in quest'area.

Il Trigger Ins./Dis. è attivo quando il sistema è inserito in modo totale o parziale. Elettricamente, il trigger attira corrente; vale a dire che indica uno zero tensione logico se misurato con un voltmetro quando viene utilizzata una resistenza di pull-up.

Il Trigger Ins./Dis. non è attivo quando il sistema è disinserito. Elettricamente, il trigger non attira corrente; vale a dire che indica un uno tensione logico se misurato con un voltmetro quando viene utilizzata una resistenza di pull-up.

Porta aperta causa allarme intrusione – Selezionare questa casella se si desidera che l'allarme porta aperta del controllo accessi attivi un allarme intrusione. Selezionando questa casella, il relè sirena selezionato si attiverà per la durata prevista per il tempo sirena.

Temporizzazione porta aperta causa allarme intrusione – Selezionare questa casella se si desidera che l'allarme temporizzazione porta aperta attivi un allarme intrusione. Selezionando questa casella, il relè sirena selezionato si attiverà per la durata prevista nel tempo sirena.

Consenti allarmi multipli – Selezionare questa casella se si desidera che situazioni di allarme successive su uno stesso varco o zona attivino un allarme intrusione entro un solo periodo di inserimento. Se non si seleziona questa casella, ogni varco o zona potrà generare un solo allarme durante un solo periodo di inserimento.

Utente VISTA di default – Poiché tutte le azioni eseguite su una centrale di allarme VISTA collegata a PassPoint tramite il modulo

VGM sono registrate nella memoria eventi della centrale VISTA, qualsiasi azione che il sistema PassPoint attiva sulla centrale VISTA verrà associata ad un utente VISTA. Il numero utente VISTA indicato in questo campo dovrà quindi essere associato ad un codice valido della centrale VISTA.

Tastiera di sistema

Tastiera installata – Selezionare questa casella se alla MLB è stata collegata una tastiera ADEMCO 6139 da utilizzare come tastiera del sistema. Verificare che questa casella non sia selezionata se non ci sono tastiere installate.

Visualizzazioni da tastiera

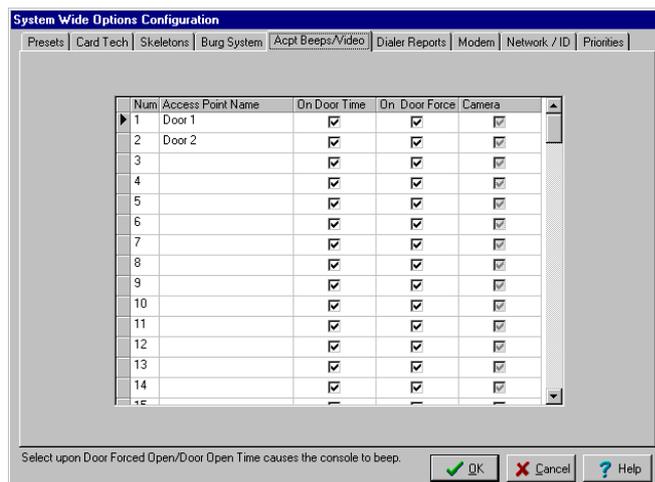
Mancanza rete – Selezionare questa casella se si desidera che la tastiera del sistema emetta dei segnali acustici nel caso in cui si verifichi una mancanza di rete su un QUALSIASI modulo del sistema PassPoint.

Batteria scarica – Selezionare questa casella se si desidera che la tastiera emetta dei segnali acustici nel caso in cui un QUALSIASI modulo del sistema PassPoint abbia la batteria scarica.

Com fall. - Selezionare questa casella se si desidera che la tastiera emetta dei segnali acustici nel caso in cui si verificasse un errore di comunicazione fra la MLB del sistema e un QUALSIASI modulo del sistema PassPoint.

Beep e video del varco (Etichetta Beep/Video)

Questa etichetta consente di selezionare opzioni di avviso per la tastiera del sistema e di indicare quali varchi sono dotati di telecamera.



Sono elencati tutti i varchi. Selezionare le caselle nelle rispettive colonne per indicare i varchi per i quali si desidera un avviso acustico per Allarme porta aperta e Temporizzazione porta aperta. Se il computer possiede una scheda di acquisizione video, verrà attivata la colonna riguardante la telecamera: sarà possibile in tal modo richiamare un'immagine video dal vivo durante un controllo vivo e se si possiede una telecamera puntata sul varco, selezionare la casella corrispondente.

Il beep è rapido per gli allarmi di apertura varco e lento per gli allarmi di temporizzazione varchi.

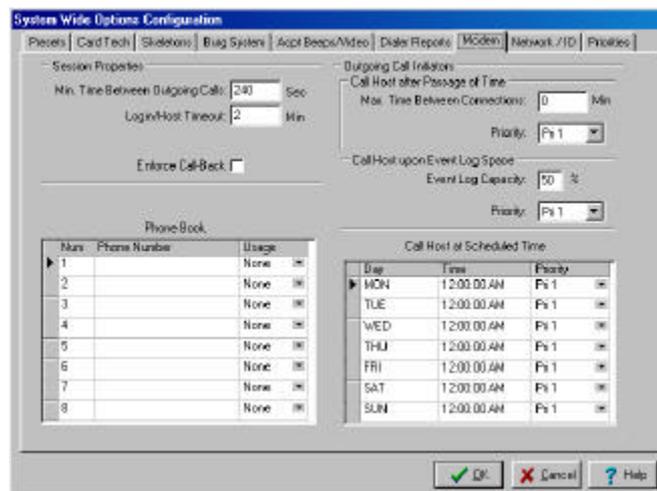
- E' possibile effettuare delle selezioni nella colonna *Telecamera* solo se è stata installata l'attrezzatura adeguata per l'acquisizione video.

Opzioni selezionatore (Etichetta Selezionatore)

Questa finestra consente di attivare i messaggi in protocollo Contact ID che si desidera inviare a un ricevitore digitale di allarmi ADEMCO 685 o FBII CP220 sfruttando il selezionatore digitale della centrale VISTA. Questa finestra si riferisce quindi solo ai sistemi che utilizzano un VGM.

Opzioni Modem (Etichetta Modem)

Questa finestra imposta la configurazione delle connessioni di comunicazione e delle proprietà della sessione:



Proprietà della sessione

Intervallo minimo fra chiamate – E' il numero minimo di secondi che possono intercorrere fra due chiamate effettuate dal sistema PassPoint. Questa impostazione determina una fascia oraria

durante la quale è possibile collegarsi remotamente al sistema PassPoint, anche quando il sistema è occupato da chiamate in uscita. Questa fascia oraria riguarda solo l'intervallo fra chiamate in uscita realizzate con successo e non riguarda l'intervallo fra tentativi di chiamata in uscita infruttuosi.

Tempor. Login/Host – E' il periodo di tempo (in minuti) che può trascorrere dopo una connessione in entrata o in uscita. E' anche il periodo di tempo che, quando trascorso, forza un nuovo tentativo di riconnessione con un Computer Host (in una versione futura del prodotto). Quando si utilizza una connessione remota, se questo tempo trascorre senza che qualcuno si colleghi, il sistema mette fine alle connessioni riagganciando. Impostando questo campo a 0, si disattiva la temporizzazione.

- E' importante impostare questo campo a un valore diverso da 0 se si sta utilizzando una connessione modem. Non impostare questo campo a un valore diverso da 0 se si sta utilizzando un collegamento via cavo.

Richiamata forzata – Spuntando la casella relativa a questa opzione, si obbliga il sistema PassPoint a riagganciare su una chiamata in entrata e richiamare automaticamente un numero di telefono predefinito. Ciò aumenta il livello di sicurezza del sistema, poiché qualsiasi chiamata alla quale risponde PassPoint viene terminata e il sistema inizia una chiamata verso un numero di telefono conosciuto.

Rubrica

La Rubrica viene utilizzata per memorizzare otto possibili numeri di telefono attraverso i quali il sistema PassPoint può contattare un computer remoto. Non è necessario immettere questi numeri se l'unico computer utilizzato per gestire il sistema è collegato direttamente al sistema.

Le impostazioni di utilizzo specificano il numero utilizzato in alcune circostanze. E' necessario impostare un numero da utilizzare come richiamata se è stata selezionata l'opzione *Richiamata forzata*. E' il numero che il sistema PassPoint chiama dopo aver ricevuto a sua volta una chiamata.

Tutti gli altri numeri sono utilizzati per chiamare un computer particolare quando si produce un evento associato ad una soglia di priorità particolare. Ciò consente al sistema di chiamare diversi host per gestire diversi tipi di eventi.

Iniziatori chiamate in uscita

Chiama host dopo un intervallo definito

Il sistema inizia una chiamata al numero associato alla priorità attribuita a quell'evento qualora il numero di minuti impostato dovesse trascorrere senza che il sistema generi connessioni remote.

Capacità e priorità memoria eventi

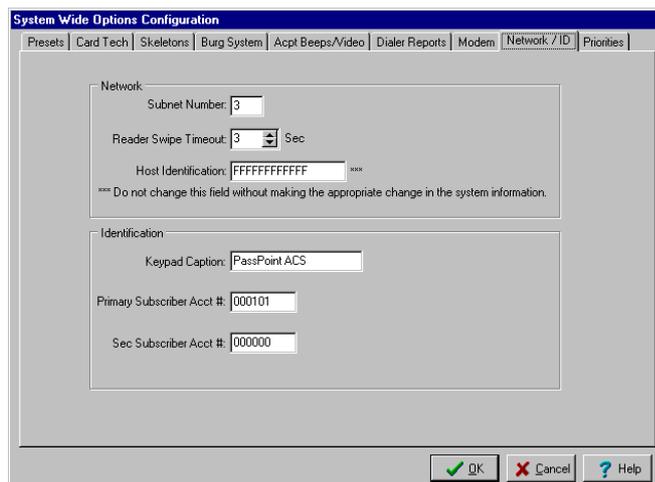
Il sistema inizia una chiamata al numero associato alla priorità attribuita a quell'evento quando la capacità memoria eventi raggiunge la percentuale indicata.

Chiama host a orari fissi

Il sistema inizia una chiamata al numero associato alla priorità attribuita a quell'evento all'ora indicata nel giorno selezionato.

Opzioni rete ID (Etichetta Rete/ID)

La finestra fornisce le impostazioni per parametri di rete e le informazioni di identificazione del sistema:



Rete

Numero di Subnet – Questo numero, che va da 1 a 255, seleziona un raggruppamento comune di moduli di rete. Nella maggior parte dei casi questo numero **NON DOVREBBE ESSERE MODIFICATO** e dovrebbe essere modificato solo se necessario quando si utilizza lo stesso cavo per il bus del sistema PassPoint e altri dispositivi compatibili Echelon LonWorks. Contattare ADEMCO per maggiori informazioni.

Temporizzazione passaggio lettore – E' il numero di secondi durante i quali il modulo DCM o CPM attende istruzioni dalla MLB dopo la presentazione di un badge o la digitazione di un PIN. In condizioni normali, la MLB risponde al modulo generando un segnale di consenso o di negazione. Se comunque la MLB non rispondesse entro il periodo di tempo previsto, l'interfaccia del lettore si azzerà. L'impostazione di default è 3 secondi. Si consiglia di impostare un valore superiore nel caso in cui si effettui il controllo visivo.

ID Host – Questo numero a 12 caratteri esadecimale è utilizzato per confermare una connessione con il software PassPoint Plus. Il

numero impostato qui DEVE corrispondere al numero impostato nel software del computer per poter eseguire caricamenti, aggiornamenti e acquisire gli eventi.

Nonostante l'ID Host abbia un valore iniziale di "FFFFFFFFFFFF," l'installatore dovrebbe modificarlo per ragioni di sicurezza.

Identificazione

Logo tastiera – E' la stringa di caratteri visualizzata sulla prima linea della tastiera 6139 del sistema.

Numero cliente primario – Le prime quattro cifre di questo numero sono inviate al numero primario del ricevitore digitale di allarmi nel caso in cui venga eseguita una chiamata. Gli ultimi due numeri rappresentano il numero della MLB. Questo campo non può essere modificato perché viene creato automaticamente al momento della creazione del database cliente.

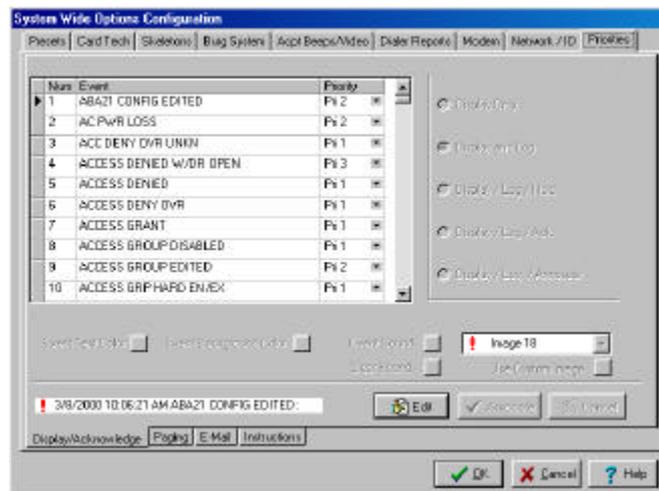
Numero cliente secondario – Immettere il numero cliente secondario per questo cliente. Le prime quattro cifre di questo numero sono inviate al numero secondario del ricevitore digitale di allarmi nel caso in cui la chiamata al numero principale non vada a buon fine. Gli ultimi due numeri rappresentano il numero della MLB.

Opzioni priorità (Etichetta Priorità)

Questa finestra visualizza le impostazioni della priorità di tutti gli eventi che possono essere generati dal sistema PassPoint. Le impostazioni di priorità variano da Nessuno a Livello di priorità 5. Gli eventi che sono stati impostati con livello di priorità Nessuno non sono memorizzati nella memoria eventi del sistema. Gli eventi con Livello priorità 1 sono quelli con livello priorità più basso e gli eventi con livelli di priorità 5 sono quelli con il massimo livello di priorità che possono essere memorizzati. Tutti gli eventi che sono

stati impostati con livello di priorità Nessuno non potranno essere usati come trigger per un rapporto Evento-Azione, poiché l'evento non viene memorizzato. Notare che quando gli eventi vengono scaricati verso l'host computer, la MLB trasmette prima gli eventi più vecchi con la priorità più alta trasferendo gradatamente gli eventi più recenti e con priorità inferiore.

Bisogna ricordare che queste opzioni di priorità possono agire sulle connessioni remote. Una modifica alle priorità eventi può causare chiamate all'host ed impedire che gli eventi vengano memorizzati. Inoltre, molti eventi con una caratteristica guasto/ripristino appaiono solo una volta nell'elenco. Modificando le priorità di uno, si modificano le priorità di entrambi (ad esempio Porta aperta varco e Ripristino allarme).



La finestra delle priorità può essere usata per modificare la priorità e gli attributi di un evento, impostare un cercapersone per un particolare evento e creare istruzioni per un evento. Le procedure per eseguire queste azioni sono fornite nei paragrafi seguenti.

Modifica delle priorità di un evento

Per modificare le priorità di un evento:

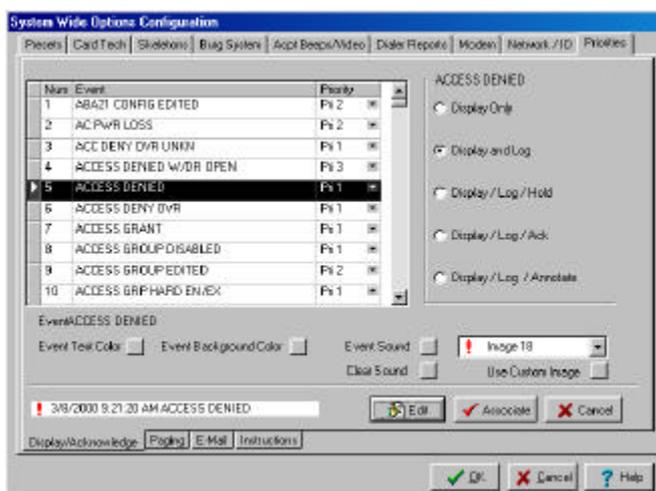
- 1. Scorrere l'elenco degli eventi fornito nella griglia fino a trovare quello al quale si desidera modificare la priorità**
 - 2. Fare clic sulla freccia in basso a destra dell'elenco degli eventi.** Appare un elenco di priorità
 - 3. Fare clic sul livello di priorità desiderato.** Il livello di priorità di quell'evento è ora modificato.
-

- E' importante notare che impostando la priorità di un evento a 0, verranno annullati tutti gli altri attributi dell'evento stesso, poiché un evento con priorità 0 non dovrebbe mai prodursi e non verrà neanche visualizzato.
-

- 4. Ripetere i punti da 1 a 3 per ogni evento da modificare.**

Modifica degli attributi di un evento

- 1. Scorrere l'elenco degli eventi fino a trovare l'evento di cui si desidera modificare un attributo.**
- 2. Selezionare l'evento facendo clic sulla colonna più a sinistra nella griglia eventi.** Verrà evidenziata tutta la riga dell'evento, come nell'esempio qui sotto.
- 3. Fare clic sul pulsante *Modifica*, per attivare gli altri pulsanti.**



4. Modificare gli attributi dell'evento utilizzando i pulsanti sullo schermo. I pulsanti hanno le funzioni seguenti:

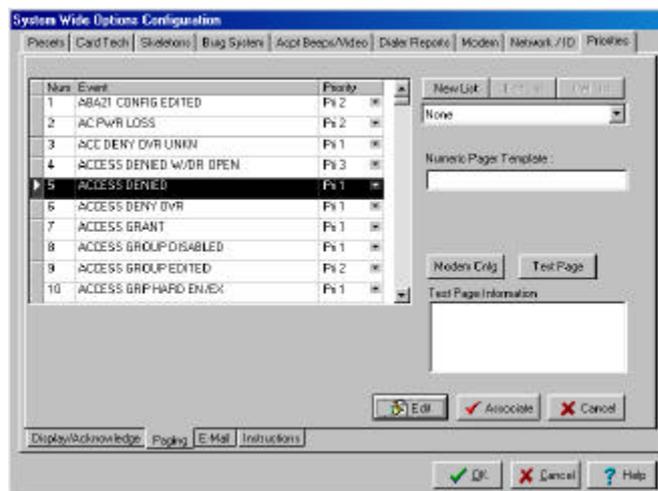
- Colore testo* Fare clic su questo pulsante per modificare il colore del testo dell'evento.
- Colore sfondo* Fare clic su questo pulsante per modificare il colore dello sfondo dell'evento.
- Suono evento* Fare clic su questo pulsante per associare un file wav che sarà attivato in occasione dell'evento. Si consiglia di utilizzare files brevi.
- Annulla suono* Fare clic su questo pulsante per eliminare un file wav dall'evento.
- Immagini* Esistono 46 immagini nell'elenco, che possono essere associate all'evento.
- Personalizza immagine* E' possibile creare la propria immagine bitmap e associarla a un evento. L'immagine creata deve essere di 15 x 15 pixel.

<i>Visualizza solo</i>	L'evento deve essere solo visualizzato e non salvato nel database per un rapporto successivo.
<i>Visualizza e registra</i>	L'evento deve essere visualizzato e salvato nel database.
<i>Visualizza/Memorizza /Mantieni</i>	L'evento deve essere visualizzato e salvato nel database. Deve essere conservato anche nel gruppo di priorità corrispondente al suo livello.
<i>Visualizza/Memorizza /Acquisisci</i>	L'evento deve essere visualizzato e salvato nel database. Verrà conservato nel gruppo di priorità corrispondente al suo livello. L'evento richiede anche l'acquisizione da parte dell'operatore.
<i>Visualizza/Memorizza /Annota</i>	L'evento deve essere visualizzato e salvato nel database. Verrà conservato nel gruppo del proprio livello di priorità. L'evento richiede anche un'annotazione da parte dell'operatore.

- 5. Dopo aver modificato gli attributi degli eventi, fare clic sul pulsante *Associa* per associare le modifiche apportate all'evento.**
- 6. Ripetere le fasi da 1 a 5 per ogni evento del quale si desiderano modificare gli attributi.**

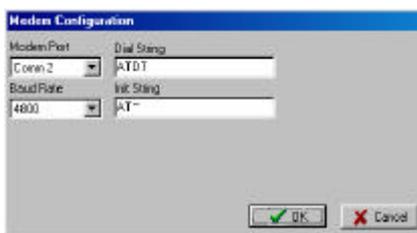
Impostazione cercapersone evento

Per poter utilizzare la funzionalità del cercapersone di PassPoint, il PC host deve essere sempre collegato alla MLB. Per impostare PassPoint in modo tale che invii un messaggio sul cercapersone in caso di evento, bisogna configurare il modem e creare un elenco di cercapersone. Facendo clic sull'etichetta cercapersone, appare lo schermo seguente.



Configurazione del Modem

1. Collegare un modem a un porta di comunicazione disponibile sul computer.
2. Fare clic sul pulsante **Conf. Modem**. Appare la finestra seguente:



3. Impostare la porta di comunicazione alla quale è collegato il modem selezionandola dall'elenco **Porta Modem**.
4. Impostare la **Stringa numerazione** a ATDT per composizione a toni e ATDP per composizione a impulsi.

5. **Lasciare il campo *Iniz. stringa vuoto* per il momento.** Con il campo vuoto, il Modem invierà un AT+ e ritorno. Se questa impostazione di default non funzionasse, sarà necessario consultare il manuale del modem. La maggior parte dei terminali cercapersone utilizzano vecchi modem che non possono accettare protocolli di correzione errori dei modem V.xx più recenti. Sarà quindi necessaria una stringa di inizializzazione modem che imposterà il modem in modo Normal Bell 212.
6. **Impostare il campo *Baud Rate* con il baud rate del terminale cercapersone.** (2400 è corretto per PageNet.)

Creazione di un evento Cercapersone

1. **Scorrere l'elenco degli eventi nella finestra fino a raggiungere l'evento da abbinare al cercapersone.**
2. **Selezionare l'evento facendo clic sulla colonna più a sinistra nella griglia.**
3. **Fare clic sul pulsante *Modifica*.** In questo modo si attiva il pulsante *Nuova lista*.
4. **Fare clic sul pulsante *Nuova lista*.** In questo modo si apre la finestra di dialogo *Lista membri cercapersone*, come nell'esempio qui sotto:



5. **Immettere nella casella *Nome lista* il nome dell'elenco cercapersone.**
6. **Immettere il *Pin Cercapersone*.**

- 7. Immettere il N. accesso cercapersona.** (il numero di telefono del terminale cercapersona.)
- 8. Fare clic sul pulsante +.** In questo modo il dato si sposta sull'elenco *Membri*.
- 9. Fare clic con il pulsante destro nell'area *Membri*.** Viene presentata una finestra di dialogo per selezionare il tipo di cercapersona (alfanumerico o numerico). Selezionare il tipo che corrisponde al cercapersona.
- 10. Ripetere le fasi da 1 a 9 per ogni evento e/o cercapersona desiderato.**
- 11. Fare clic sul pulsante OK per salvare l'elenco.**

Questo elenco può essere ora associato a molteplici eventi.

NOTA: L'elenco esistente può essere modificato utilizzando il pulsante *Modifica Lista*.

Utilizzo del formato cercapersona numerico

Il testo che va al cercapersona è il testo evento più il numero cliente su un cercapersona alfanumerico. Se si possiede un cercapersona numerico, si deve utilizzare il *Formato cercapersona numerico*. Il *Formato cercapersona numerico* utilizza spazi riservati:

%A per sostituire il numero cliente

%T per sostituire il tipo di risorsa (1=Varco, 2= Lettore, 3 = Relè, 4=Lettore, 5=Trigger)

%R per sostituire il numero della risorsa

Ad esempio, se il numero cliente è 1234 e l'evento è un Allarme porta aperta, il formato può essere come nell'esempio seguente:

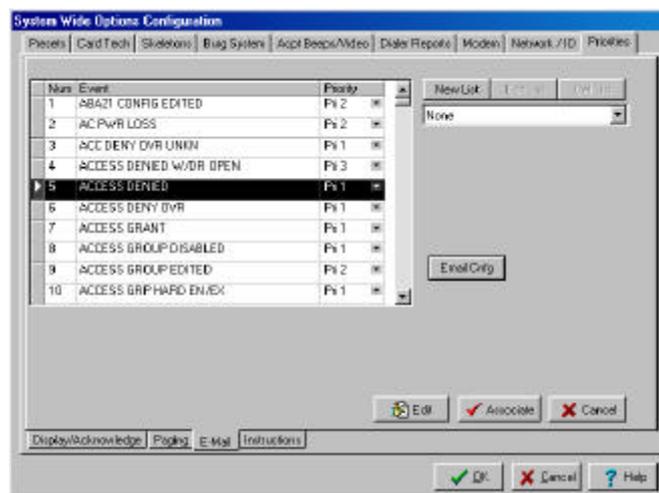
911 %T %R 000 A%

Questo verrà trasmesso come:

911 1 1 000 1234

Impostazione invio e-mail per un evento

Per utilizzare la funzionalità e-mail di PassPoint, il PC host deve essere sempre collegato alla MLB. Inoltre, bisogna avere accesso a un server SMTP (Simple Mail Transport Protocol). Per impostare PassPoint in modo tale che invii un e-mail in seguito a un evento, è necessario configurare il vostro e-mail e creare un elenco di indirizzi e-mail. Facendo clic sull'etichetta e-mail, appare lo schermo seguente:



Configurazione dell'e-mail

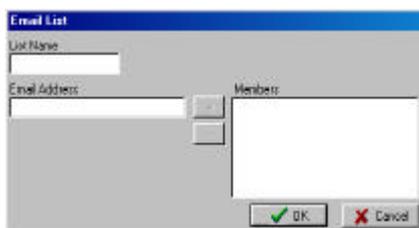
1. Fare clic sul pulsante **Conf. e-mail**. Appare il seguente schermo *Configurazione E-mail*:



2. Immettere l'indirizzo dell'host SMTP nel campo **SMTP Host Address**.
3. Immettere nel campo **ID Operatore** il nome operatore che potrebbe essere necessario per accedere al server SMTP.
4. Immettere l'indirizzo che si vuole utilizzare come indirizzo mittente nel campo **Dall'indirizzo**.
5. Immettere nel campo **Oggetto** il testo che si vuol far apparire sulla riga Oggetto dell'e-mail.
6. Fare clic sul pulsante **OK**.

Creazione di un elenco E-mail

1. Scorrere l'elenco degli eventi fino a visualizzare l'evento per il quale si desidera inviare l'e-mail.
2. Selezionare l'evento facendo clic sulla colonna più a sinistra nella griglia.
3. Fare clic sul pulsante **Modifica**. In questo modo si attiva il pulsante **Nuova lista**.
4. Fare clic sul pulsante **Nuova lista**. In questo modo si apre la finestra di dialogo **Elenco Email**:



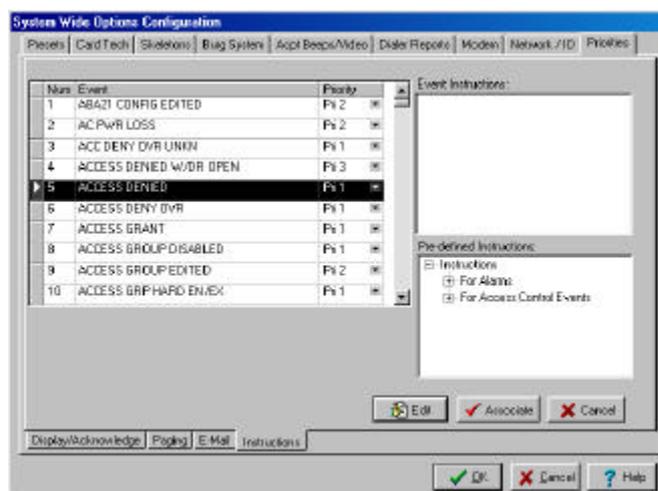
5. Immettere il nome dell'elenco degli indirizzi e-mail nella casella *Nome Lista*.
6. Immettere *l'Indirizzo Email*.
7. Fare clic sul pulsante **+**. In questo modo l'indirizzo si sposta nell'elenco *Membri*.
8. Ripetere le fasi 6 e 7 per ogni indirizzo e-mail che si desidera aggiungere alla lista.
9. Fare clic sul pulsante *Associa*.

La lista così creata può essere associata a più eventi.

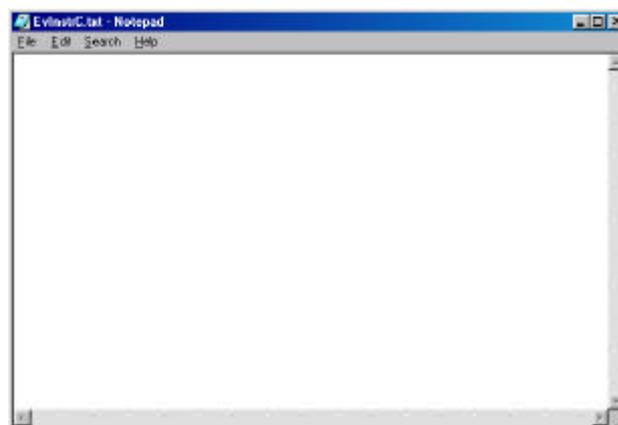
NOTA: L'elenco esistente può essere modificato utilizzando il pulsante *Modifica Lista*.

Creazione istruzioni per gli eventi

E' possibile creare istruzioni relative agli eventi utilizzando l'etichetta *Istruzioni*. Facendo clic sull'etichetta *istruzioni*, appare la finestra seguente:



Si possono immettere istruzioni nella casella *Istruzioni eventi*, inserendo istruzioni estratte dalla casella *Istruzioni predefinite* facendo doppio clic su di esse, o aggiungendo istruzioni personalizzate facendo clic con il pulsante destro sulla casella *Istruzioni predefinite* e selezionando *Modifica istruzioni personalizzate*. Selezionando *Modifica istruzioni personalizzate*, appare la finestra seguente:



Dopo aver inserito le nuove istruzioni personalizzate, uscire dallo schermo *Modifica istruzioni personalizzate*, fare ancora clic con il pulsante destro nella casella *Istruzioni predefinite* e scegliere *Ricarica istruzioni*. In questo modo le nuove istruzioni vengono aggiunte all'elenco delle Istruzioni predefinite, e possono quindi essere inserite nella casella *Istruzioni eventi*.

Per associare le istruzioni evento all'evento selezionato, fare clic sul pulsante *Associa*.

Capitolo

8

Liste risorse

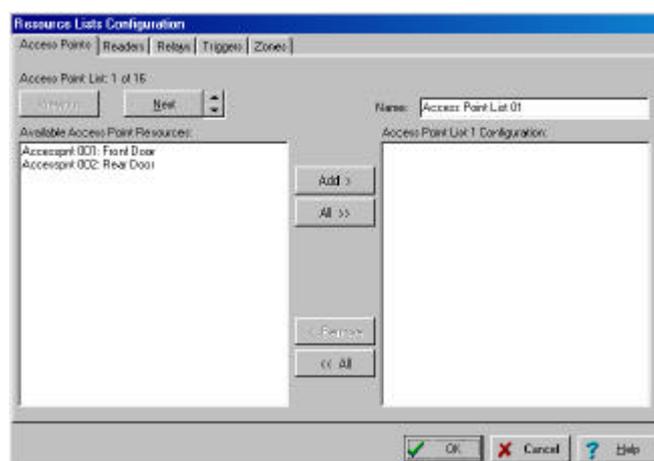
Questo capitolo spiega come impostare le Liste risorse, e in particolare come:

- **Impostare le liste risorse**
- **Utilizzare le liste risorse**

Impostazione liste risorse

E' possibile creare liste delle risorse seguenti: varchi, lettori, relè, trigger e zone. Dopo averle configurate, queste risorse possono essere controllate in modo indipendente o come lista. Ogni tipo di risorsa può essere associata fino a 16 liste.

Tutte le liste di risorse sono configurate in una casella di dialogo dedicata, chiamata Configurazione Liste Risorse. Per arrivare a questa finestra di dialogo, selezionare *Lista risorse* dalla finestra di dialogo Configurazione Hardware:



Tutte le etichette (Varchi, Lettori, Relè, Triggers e Zone) contengono i campi e i pulsanti seguenti:

Precedente/Successivo– Questi pulsanti visualizzano la lista di risorse successiva o precedente.

Disponibile (Risorsa) – Questo campo visualizza tutte le risorse disponibili ad essere associate a una lista di risorse.

Nome – Si può immettere in questo campo un nome per la lista attuale.

(Risorsa) Configurazione lista – In questo campo sono visualizzate tutte le risorse che appartengono alla lista selezionata.

Aggiungi > – Facendo clic su questo pulsante si attribuisce la risorsa selezionata alla lista.

Tutto>> – Facendo clic su questo pulsante si attribuiscono tutte le risorse disponibili alla lista.

< Rimuovi – Facendo clic su questo pulsante si rimuove la risorsa selezionata dalla lista.

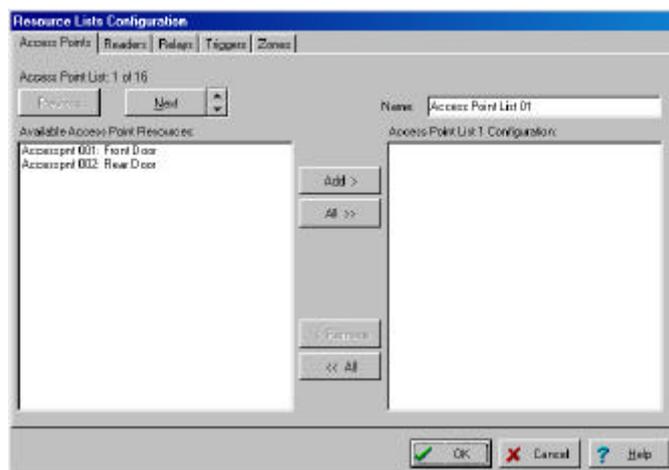
<< Tutto – Facendo clic su questo pulsante si rimuovono tutte le risorse dalla lista.

OK – Fare clic su questo pulsante quando si è finito di configurare le liste delle risorse.

Annulla – Fare clic su questo pulsante quando si vuole uscire dalla Configurazione senza salvare le modifiche.

Etichetta varchi

Utilizzare questo schermo per impostare l'elenco dei varchi:



E' possibile configurare fino a 16 liste varchi. Ogni varco può essere associato a più di una lista. Per configurare una lista varchi, seguire la procedura seguente:

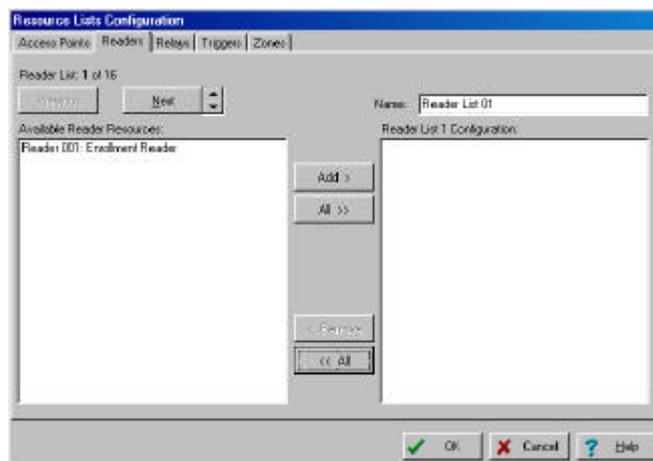
1. **Selezionare il varco nella lista della finestra Risorse disponibili utilizzando i metodi a. o b. descritti di seguito:**
 - a. **Per selezionare i varchi singolarmente, basta fare clic su di essi. Si possono selezionare più varchi utilizzando le combinazioni standard di Windows™ SHIFT-clic e CONTROL-clic. Dopo aver selezionato i varchi, fare clic sul pulsante *AGGIUNGI* >. I varchi selezionati vengono spostati nella finestra Configurazione lista varchi.**
 - b. **Per aggiungere tutti i varchi, fare clic sul pulsante *Tutto* >>. I varchi appaiono nella finestra Configurazione lista varchi.**
2. **Immettere il nome della lista nell'area "Nome".**

3. Fare clic su **Successivo** e ripetere le fasi 1 e 2 per ogni lista di varchi che si desidera creare.
4. Quando sono state configurate tutte le liste varchi, si può fare clic su una delle etichette per creare liste per un'altra risorsa; oppure, se sono state configurate tutte le liste, fare clic su **OK**. Riappare lo schermo Configurazione Installatore (Hardware).

Quando si esce dallo schermo Configurazione Installatore, il sistema informa che il database deve essere aggiornato. Se la configurazione dell'hardware è terminata, seguire le istruzioni per aggiornare la MLB.

Etichetta lettori

Utilizzare questo schermo per impostare la lista lettori:



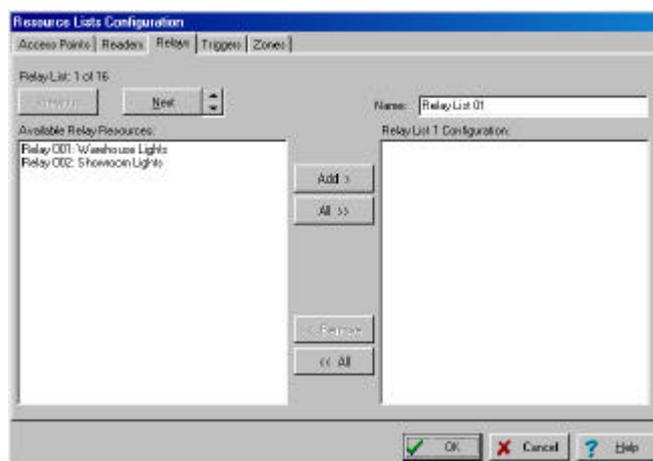
E' possibile configurare fino a 16 liste di lettori. Ogni lettore può essere associato a più di una lista. Per configurare una lista di lettori, procedere nel modo seguente:

1. **Selezionare i lettori elencati nella finestra Risorse lettore utilizzando i metodi a. o b. descritti di seguito:**
 - a. **Per selezionare i lettori singolarmente, fare clic su di essi. Si possono selezionare più lettori utilizzando le combinazioni standard di Windows™ SHIFT-clic e CONTROL-clic. Dopo aver selezionato i lettori, fare clic sul pulsante *AGGIUNGI* >. I lettori selezionati appaiono nella finestra Configurazione lista lettori.**
 - b. **Per aggiungere tutti i lettori, fare clic sul pulsante *Tutto* >>. I lettori appaiono nella finestra Configurazione lista lettori.**
2. **Immettere il nome della lista nell'area "Nome".**
3. **Fare clic su *Successivo* e ripetere le fasi 1 e 2 per ogni lista lettori che si desidera creare.**
4. **Quando sono state configurate tutte le liste lettori, si può fare clic su una delle etichette per creare liste per un'altra risorsa; oppure, se sono state configurate tutte le liste, fare clic su *OK*. Riappare lo schermo Configurazione Installatore (Hardware).**

Quando si esce dallo schermo Configurazione Installatore, il sistema ricorda che il database deve essere aggiornato. Se la configurazione dell'hardware è terminata, seguire le istruzioni per aggiornare la MLB.

Etichetta relè

Utilizzare questo schermo per impostare le liste relè:



E' possibile configurare fino a 16 liste di relè. Ogni relè può essere associato a più di una lista. Per configurare una lista di relè, procedere nel modo seguente:

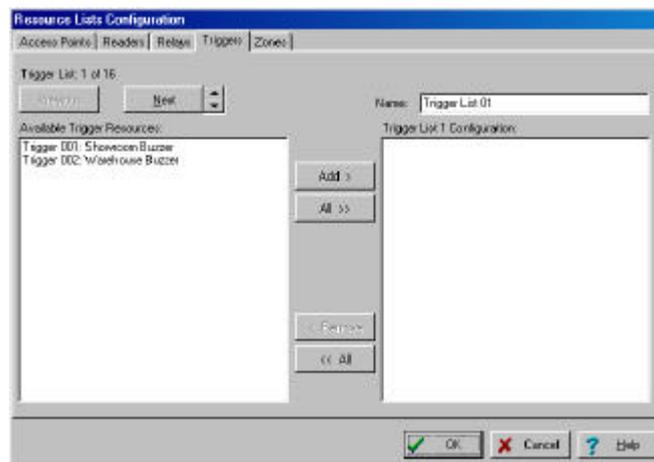
1. **Selezionare i relè elencati nella finestra Risorse relè utilizzando i metodi a. o b. descritti di seguito:**
 - a. Per selezionare i relè singolarmente, fare clic su di essi. Si possono selezionare più relè utilizzando le combinazioni standard di Windows TM SHIFT-clic e CONTROL-clic. Dopo aver selezionato i relè, fare clic sul pulsante **AGGIUNGI >**. I relè selezionati appaiono nella finestra Configurazione lista relè.
 - b. Per aggiungere tutti i relè, fare clic sul pulsante **Tutto>>**. I relè appaiono nella finestra Configurazione lista relè.
2. Immettere il nome della lista nell'area "Nome".
3. Fare clic su **Successivo** e ripetere le fasi 1 e 2 per ogni lista relè desiderata.

4. Quando sono state configurate tutte le liste relè, si può fare clic su una delle etichette per creare liste per un'altra risorsa; oppure, se sono state configurate tutte le liste, fare clic su **OK**. Riappare lo schermo Configurazione Installatore (Hardware).

Quando si esce dallo schermo Configurazione Installatore, il sistema ricorda che il database deve essere aggiornato. Se la configurazione dell'hardware è terminata, seguire le istruzioni per aggiornare la MLB.

Etichetta Trigger

Utilizzare questo schermo per impostare le liste trigger:



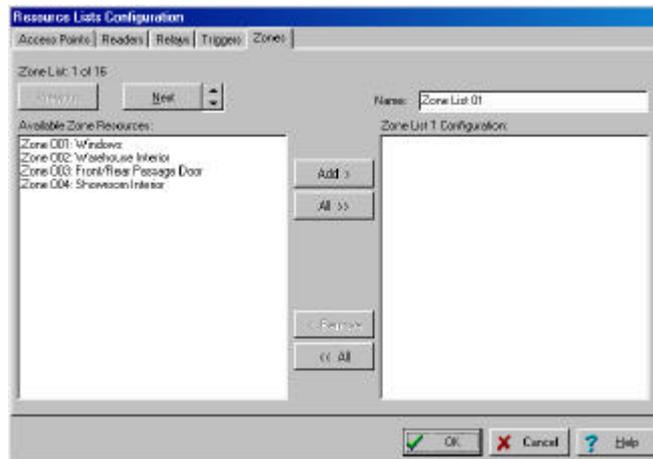
E' possibile configurare fino a 16 liste di triggers. Ogni trigger può essere associato a più di una lista. Per configurare una lista di triggers, procedere nel modo seguente:

1. **Selezionare i triggers elencati nella finestra Risorse triggers utilizzando i metodi a. o b. descritti di seguito:**
 - a. **Per selezionare i trigger singolarmente, fare clic su di essi. Si possono selezionare più triggers utilizzando le combinazioni standard di Windows™ SHIFT-clic e CONTROL-clic. Dopo aver selezionato i triggers, fare clic sul pulsante *AGGIUNGI* >. I triggers selezionati appaiono nella finestra Configurazione lista triggers.**
 - b. **Per aggiungere tutti i trigger, fare clic sul pulsante *Tutto* >>. I trigger appaiono nella finestra Configurazione lista trigger.**
2. **Immettere il nome della lista nell'area “Nome”.**
3. **Fare clic su *Successivo* e ripetere le fasi 1 e 2 per ogni lista trigger desiderata.**
4. **Quando sono state configurate tutte le liste triggers, si può fare clic su una delle etichette per creare liste per un'altra risorsa; oppure, se sono state configurate tutte le liste, fare clic su *OK*. Riappare lo schermo Configurazione Installatore (Hardware).**

Quando si esce dallo schermo Configurazione Installatore, il sistema ricorda che il database deve essere aggiornato. Se la configurazione dell'hardware è terminata, seguire le istruzioni per aggiornare la MLB.

Etichetta Zone

Utilizzare questo schermo per impostare le liste zona:



Si possono configurare fino a 16 liste zona. Tutte le zone possono essere attribuite a più di una lista. Per configurare una lista zona, procedere nel modo seguente:

1. **Selezionare le zone elencate nella finestra Risorse zone utilizzando i metodi a. o b. descritti di seguito:**
 - a. **Per selezionare le zone singolarmente, fare clic su di esse. Si possono selezionare più zone utilizzando le combinazioni standard di Windows™ SHIFT-clic e CONTROL-clic. Dopo aver selezionato i triggers, fare clic sul pulsante *AGGIUNGI >*. Le zone selezionate appaiono nella finestra Configurazione lista zone.**
 - b. **Per aggiungere tutte le zone, fare clic sul pulsante *Tutto>>*. Le zone appaiono nella finestra Configurazione lista zone.**
2. **Immettere il nome della lista nell'area “Nome”.**
3. **Fare clic su *Successivo* e ripetere le fasi 1 e 2 per ogni lista zona desiderata.**

- 4. Quando sono state configurate tutte le liste zone, si può fare clic su una delle etichette per creare liste per un'altra risorsa; oppure, se sono state configurate tutte le liste, fare clic su *OK*. Riappare lo schermo Configurazione Installatore (Hardware).**

Quando si esce dallo schermo Configurazione Installatore, il sistema ricorda che il database deve essere aggiornato. Se la configurazione dell'hardware è terminata, seguire le istruzioni per aggiornare la MLB.

Utilizzo delle liste risorse

Dopo aver configurato una lista di risorse, essa appare sotto al titolo Liste risorse nell'albero del sistema sulla schermata principale di PassPoint. Facendo clic su una lista, si hanno a disposizione le stesse opzioni che si avrebbero se si selezionasse una risorsa particolare. La differenza è che l'operazione viene eseguita su tutte le risorse comprese nella lista. Ad esempio, facendo clic sulla lista varchi e selezionando *Esclusione*, verranno esclusi tutti i varchi compresi nella lista.

Parte seconda



*Espansione di
PassPoint*

Capitolo

9

Aggiunta di un Door Expansion Kit

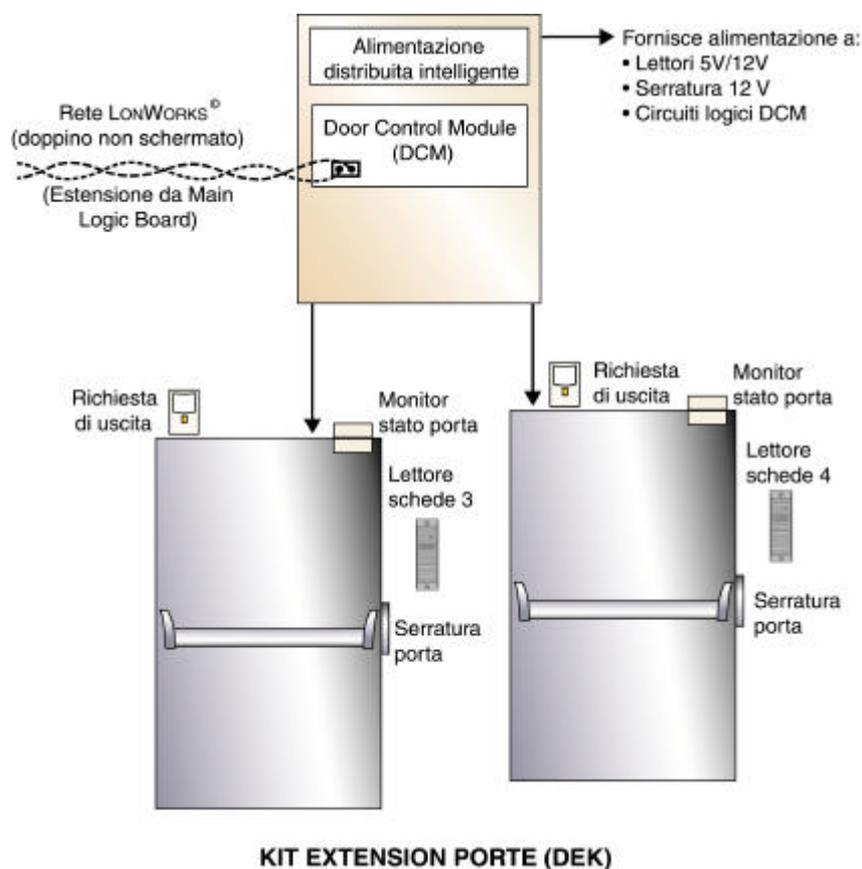
Aggiungendo un Door Expansion Kit (DEK) è possibile aggiungere rapidamente due lettori ad un sistema PassPoint esistente.

Questo capitolo spiega come:

- **Montare il Door Expansion Kit**
- **Cablare tutti i componenti del DEK**
- **Attivare e impostare il DEK**
- **Registrare il DEK in un sistema PassPoint esistente**

Informazioni sul Door Expansion Kit

Il Door Expansion Kit di PassPoint consente di aggiungere rapidamente due lettori ad un sistema PassPoint esistente. Il DEK consiste essenzialmente in un Door Control Module e in un alimentatore, montati in un armadio standard Ademco. Dopo aver collegato il DEK al sistema esistente, si deve solamente acquisire il nuovo Door Control Module e impostare i nuovi varchi.



**Cosa comprende
il Door Expansion
Kit?**

Il DEK di PassPoint è composto dai seguenti componenti hardware:

- **1 centrale pre configurata, che comprende:**
 - 1 armadio metallico
 - 1 Door Control Module
 - 1 alimentatore
- 1 trasformatore

Installazione del DEK

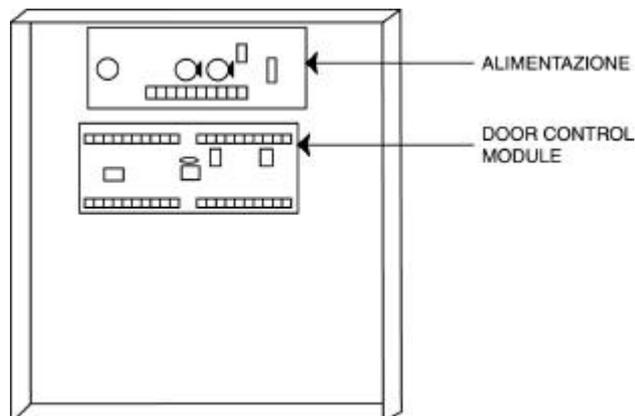
Per l'installazione del Door Expansion Kit e per acquisirlo in un sistema PassPoint esistente si devono seguire sei fasi semplici descritte di seguito.

Fase 1 – Montaggio del DEK

Il DEK contiene il Door Control Module ed il relativo alimentatore.

Rimuovendo lo sportello dell'armadio, l'interno appare come nel disegno qui sotto:

*DEK con DCM
e alimentatore.*



Scegliere la posizione

Per l'installazione del kit, scegliere un punto pulito e asciutto, non facilmente accessibile a tutti, ma sufficientemente pratico per un eventuale intervento tecnico. Il kit deve essere montato su un muro solido, utilizzando ancoraggi adeguati (non forniti).

- 1. Posizionare l'armadio sul muro e utilizzare i fori che si trovano sulla parte posteriore per segnare i punti di ancoraggio.**
- 2. Forare il muro in corrispondenza dei punti tracciati e fissare l'armadio utilizzando ancoraggi idonei.**

- Fare molta attenzione a non danneggiare le schede del sistema al momento del montaggio.

Fase 2 – Collegamento del DCM

Per collegare il DCM seguire le fasi seguenti:

- **Collegare il DCM all'alimentatore e alla MLB del sistema**
 - **Collegare il trasformatore**
 - **Collegare i lettori**
 - **Collegare i dispositivi MSP e RDU**
 - **Collegare la batteria da 7 Ah**
-

- Al momento dei collegamenti, fare riferimento all'Appendice A, Istruzioni di cablaggio, per ulteriori diagrammi e informazioni sul sistema.
-

Collegare il DCM alla MLB e all'alimentatore

- 1. Collegare il connettore J5 dell'alimentatore e al connettore J1 del modulo DCM, utilizzando il cavo in dotazione.**
- 2. Collegare due fili del bus di comunicazione fra la MLB e il modulo DCM.**

Collegare un filo fra il morsetto 1 del modulo DCM e il morsetto 16 della MLB.

Collegare l'altro filo fra il morsetto 2 del modulo DCM e il morsetto 15 della MLB.

- Per questi collegamenti utilizzare un doppino ritorto. Consultare l'Appendice A per le informazioni particolareggiate.
-

Collegamento del trasformatore

Il DEK è fornito con un trasformatore, che deve essere cablato al nel modo seguente:

- 1. Collegare i due fili di uscita del trasformatore ai morsetti 1 e 2 dell'alimentatore del DEK.**
- 2. Collegare l'alimentazione di rete ai morsetti del trasformatore.**

Collegamento dei lettori

I lettori non sono forniti con il DEK e devono quindi essere acquistati separatamente.

Consultare la documentazione che accompagna i lettori per le istruzioni di montaggio. Se si tratta di lettori di prossimità PassPoint, consultare la parte relativa in questa guida.

Collegamento dei dispositivi MSP e RDU

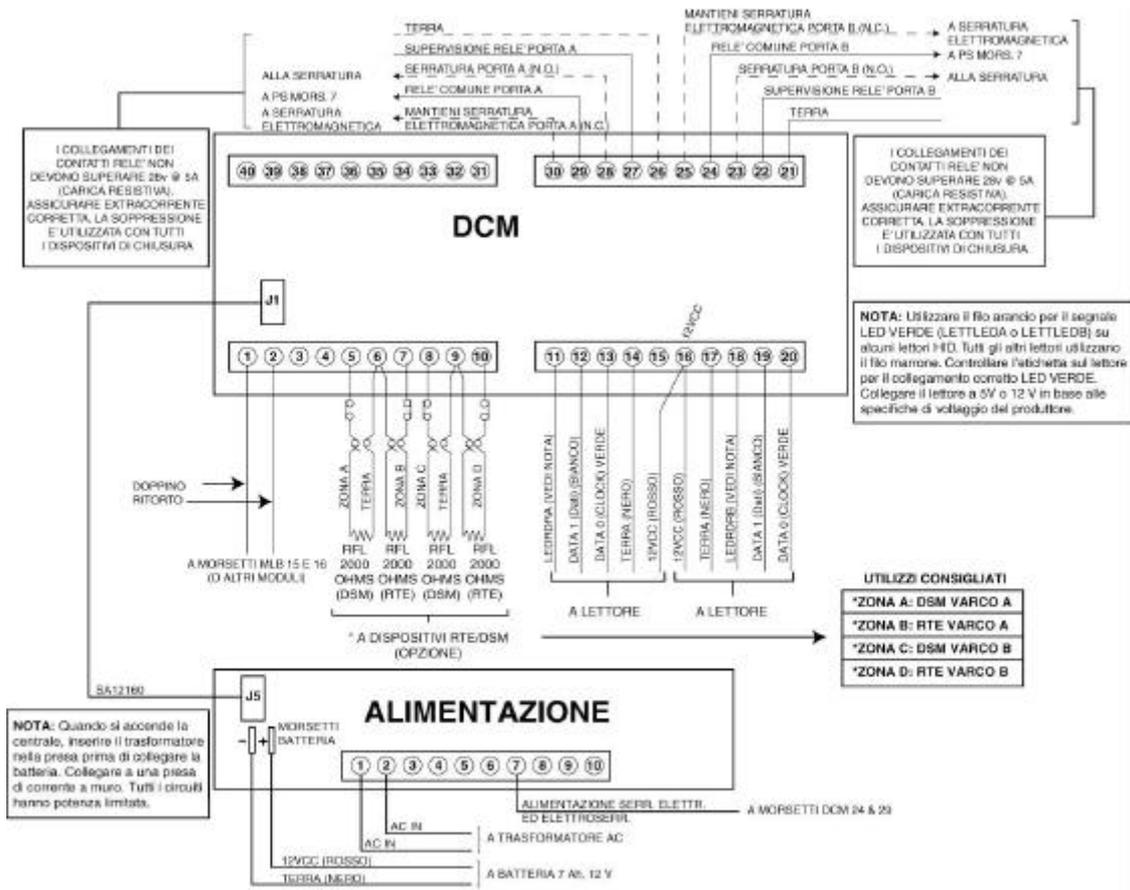
Le zone da A a D del DCM (morsetti da 5 a 10) possono essere utilizzate per i dispositivi Monitor Stato Porta (MSP) o Richiesta Di Uscita (RDU).

Collegamento della batteria 7 amperora

Se è stata acquistata anche la batteria da 7 amperora, 12 volt in opzione, installarla e collegarla all'alimentatore del DEK.

-
- Allo scopo di non scaricare la batteria, non scollegare il trasformatore del sistema per periodi di tempo troppo lunghi.

Collegare questi dispositivi in base al diagramma di collegamento illustrato qui sotto. Fare riferimento anche all'Appendice A di questa guida per le informazioni sul cablaggio, e al Capitolo 12 per una descrizione delle diverse configurazioni di zona possibili.



Fase 3 – Attivazione del sistema

Dopo aver collegato il DCM, aver montato e cablato al sistema i dispositivi di controllo porte, si può ora alimentare e attivare il sistema.

Fase 4 – Aggiunta e impostazione del DCM

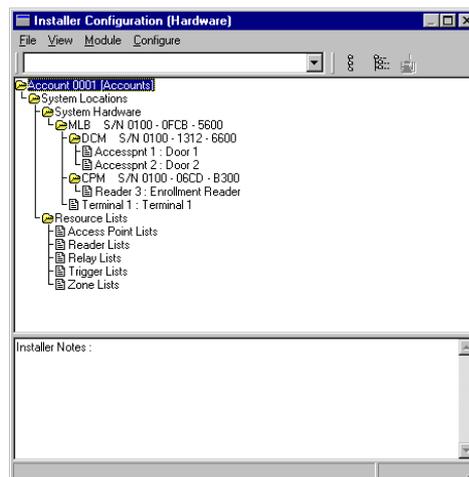
Ora che il DEK è collegato all'alimentatore, aggiungere il nuovo DCM all'installazione esistente e impostare le porte, utilizzando il Wizard DCM.

Per aggiungere e impostare il nuovo DCM, seguire la procedura qui sotto:

1. Nel menu **Config**, selezionare **Hardware**.

Appare la finestra di dialogo Configurazione Installatore:

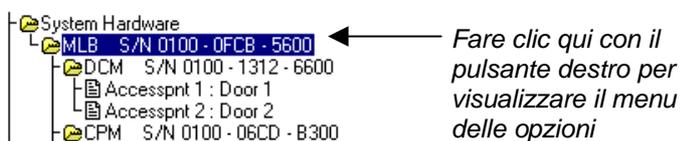
Utilizzare la finestra di dialogo Configurazione Installatore per visualizzare/modificare le componenti del sistema e per impostare varie opzioni di sistema.



La finestra di dialogo Configurazione Installatore elenca tutti i componenti del sistema. E' qui che si aggiungono i moduli di espansione, come i DCM. La finestra di dialogo è utilizzata anche per impostare varie opzioni del sistema, come i codici residenti e le impostazioni del modem.

- Dopo aver apportato le modifiche in questo schermo, bisogna aggiornarle nel database del sistema perché diventino effettive.

2. Fare clic con il pulsante *destro* sulla MLB, oppure selezionare *Aggiungi* nel menu *Modulo*.



Apparirà così il menu delle opzioni.

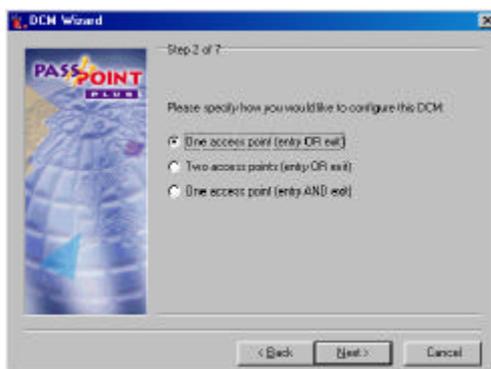
3. Selezionare *Aggiungi DCM* nel menu.

Appare il Wizard DCM:



4. Fare clic sul pulsante “*Successivo*” per continuare.

Facendo clic su *Successivo* si passa sempre allo schermo successivo del Wizard:



5. Specificare quali varchi si vogliono configurare.

Il Wizard offre tre opzioni:

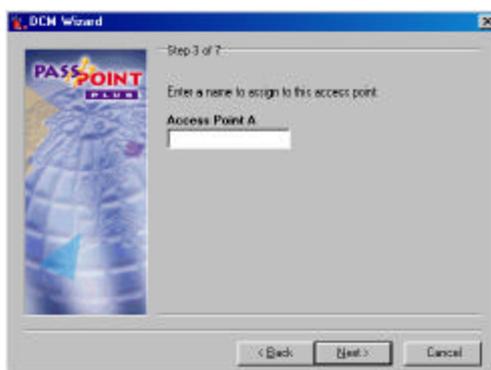
- **Un varco d'ingresso o di uscita**
- **Due varchi d'ingresso o di uscita**
- **Un varco d'ingresso/uscita**

L'opzione da selezionare dipende dalle necessità dell'installazione. In questo esempio, supponiamo che si stia configurando solo un varco d'ingresso. La procedura per configurare due varchi d'ingresso è praticamente la stessa.

Dopo aver fatto la selezione, fare clic sul pulsante *Successivo* per continuare.

6. Immettere il nome del varco.

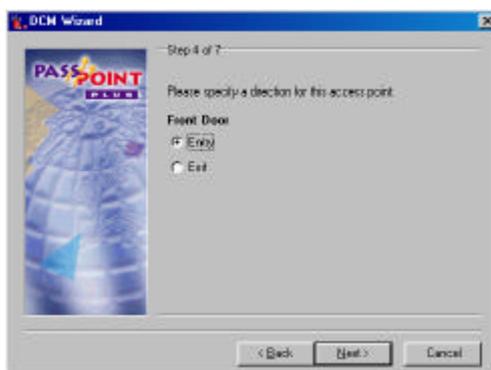
Il nome del varco deve descrivere la porta, come "Porta principale" o "Porta magazzino."



Dopo aver immesso il nome del varco, fare clic sul pulsante *Successivo* per continuare.

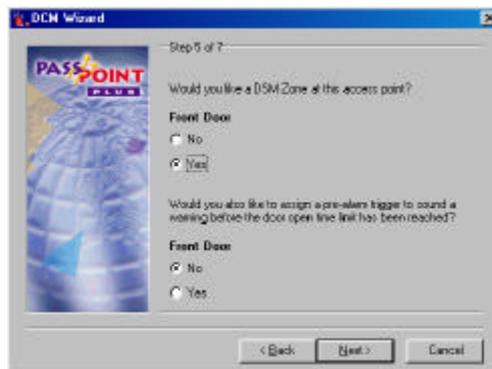
7. Scegliere la direzione del varco.

Si può scegliere se il varco deve essere d'ingresso o di uscita:



Dopo aver scelto la direzione, fare clic sul pulsante *Successivo*.

8. Scegliere se si desidera utilizzare un apparato Monitor Stato Porta (MSP) per il varco.

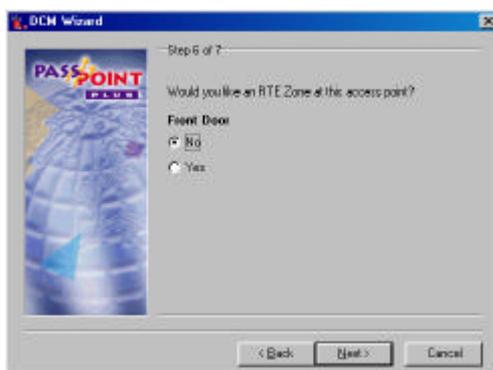


Il MSP è una funzionalità che consente al sistema di monitorare la posizione della porta, quindi il sistema è in grado di decidere se essa viene violata e, in seguito ad un accesso consentito, attiva l'allarme se viene superato questo un tempo limite senza che essa venga richiusa.

Selezionando l'uso del MSP (come mostrato nell'esempio), il sistema chiede se si vuole impostare un trigger preallarme per la porta. Il trigger preallarme è un segnale di allarme che si attiva prima che si attivi l'allarme della porta. Viene utilizzato per ricordare all'utente che l'allarme si attiva se non si richiude immediatamente la porta.

Dopo aver selezionato il MSP, fare clic su *Successivo* per continuare.

9. Scegliere se si desidera utilizzare un apparato Richiesta Di Uscita (RDU) per il varco.



Una zona RDU è un dispositivo collegato ad un varco che necessita di un controllo prima di consentire l'uscita a un utente. Un dispositivo RDU può essere un pulsante che l'utente deve premere, o un rivelatore volumetrico che segnala quando una persona si avvicina alla porta per uscire. Premendo il dispositivo (nel caso del pulsante) o quando la persona si avvicina (nel caso del rivelatore), il sistema sblocca la porta e consente alla persona di uscire.

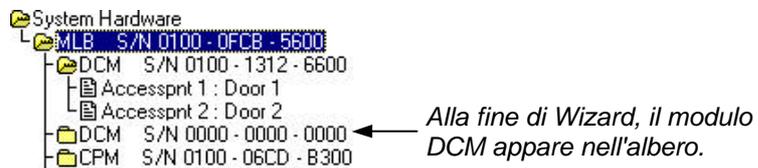
Dopo aver selezionato una zona RDU, fare clic sul pulsante *Successivo* per continuare. Il Wizard presenta uno schermo con il sommario delle scelte di configurazione per i varchi:



10. Fare clic sul pulsante *Fine* per uscire dal Wizard e salvare le modifiche.

L'albero nella finestra di dialogo Configurazione Installatore mostra ora il nuovo modulo DCM:

NOTA: Se è il primo DCM nell'albero, vengono mostrati anche i varchi impostati utilizzando il Wizard DCM.



Dopo aver configurato il modulo DCM e i varchi, bisogna ora acquisirne il numero di serie, in modo tale che il sistema lo riconosca, insieme a tutte le impostazioni di configurazione. La fase seguente riguarda l'acquisizione del modulo DCM.

Fase 5 - Autoacquisizione del modulo DCM

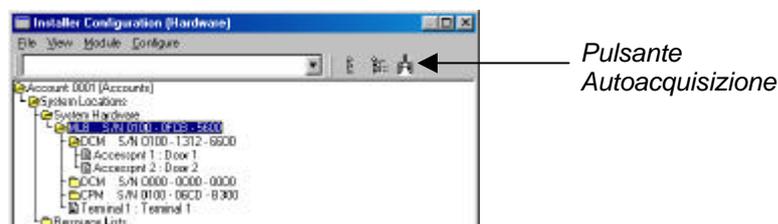
Quando si aggiunge un nuovo modulo al sistema, lo si deve acquisire. L'acquisizione informa semplicemente il database che esiste un nuovo modulo.

Quando si acquisisce un modulo, il sistema ricerca tutti i moduli collegati che non siano ancora stati registrati. Li riconosce perché hanno numeri di serie che contengono solo zeri. Ad esempio, il modulo DCM che è appena stato aggiunto con il Wizard ha un numero di serie che contiene solo zeri. Ciò significa che non è stato registrato e non fa ancora veramente parte del sistema.

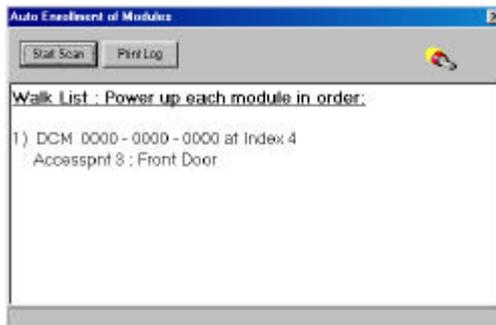
Per registrare il modulo DCM appena configurato, seguire la procedura seguente:

1. **Fare clic sul pulsante Autoacquisizione sulla finestra di dialogo Configurazione Installatore.**

Nella figura seguente è illustrata la posizione del pulsante Autoacquisizione:



Facendo clic su questo pulsante, si apre la finestra di dialogo Auto acquisizione:



La procedura di registrazione avviene **automaticamente** dopo aver premuto sul pulsante *Avvia Scansione*. L'intera procedura impiega solo qualche istante.

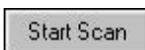
Le procedure per registrare un solo modulo sono diverse da quelle necessarie per registrare più moduli. Se si registra un solo modulo, seguire le istruzioni indicate nel punto 2a qui sotto. Se si registra più di un modulo, seguire le istruzioni indicate al punto 2b.

2a. Registrazione di un solo modulo.

Per acquisire un solo modulo nel sistema PassPoint, procedere come segue:

-
- ;

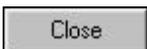
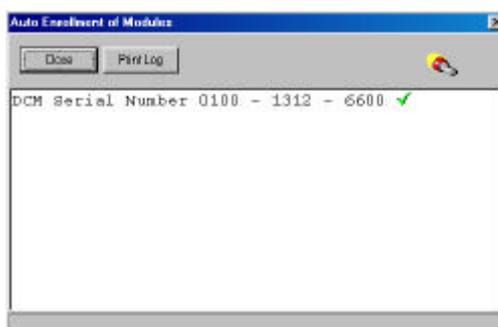
Non spegnere mai la MLB mentre il sistema sta acquisendo un modulo.



(1) Fare clic sul pulsante *Avvia Scansione*.

Il sistema cerca il nuovo modulo. Quando l'ha trovato, il LED giallo sul modulo lampeggia e appare un messaggio sullo schermo che indica che il modulo è stato registrato e la scansione si interrompe.

Dopo la registrazione, appare uno schermo che mostra il modulo (con il numero di serie) acquisito.

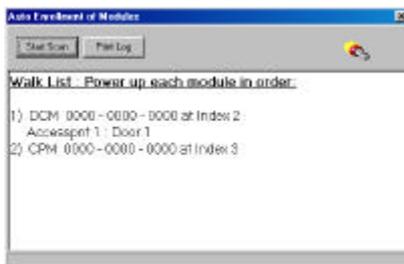


(2) Fare clic sul pulsante *Chiudi*.

La registrazione si è conclusa con successo e il sistema chiuderà lo schermo Auto acquisizione dei moduli.

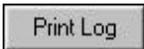
2b. Registrazione di più moduli.

La finestra di dialogo Auto acquisizione dovrebbe essere già sullo schermo e dovrebbe apparire come nell'esempio qui sotto per la registrazione di più moduli:



- Se i moduli vengono accesi prima del procedimento di acquisizione o accesi nell'ordine sbagliato, verranno registrati in modo sbagliato.
 - Nonno spegnere mai la MLB durante l'acquisizione dei nuovi moduli.
-

Per eseguire correttamente l'acquisizione di più moduli nel sistema PassPoint, essi devono essere accesi nell'ordine elencato sullo schermo. Per registrare i moduli, procedere come segue:



(1) Fare clic sul pulsante *Stampa*. Sulla stampante del sistema viene stampato un elenco di tutti i moduli da registrare.

(2) Verificare che solo il primo modulo nell'elenco sia acceso.

NOTA: I moduli devono essere accesi nell'ordine in cui appaiono nell'elenco. Assicurarsi che i moduli successivi siano spenti prima di cominciare il procedimento di acquisizione. Dopo aver avviato la scansione e aver registrato correttamente ogni modulo, essi possono rimanere accesi.



(3) Premere il pulsante *Avvia Scansione*.

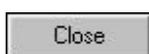
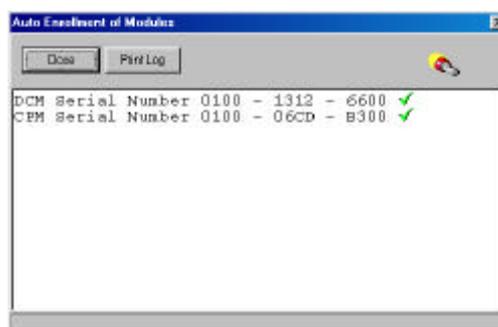
Il sistema cerca il primo modulo nell'elenco. Quando lo trova, il LED giallo sul modulo lampeggia e il sistema presenta un messaggio che indica che il modulo è stato registrato. In seguito, un altro messaggio indica che il sistema sta cercando il modulo successivo che appare sull'elenco.

(4) Accendere il modulo successivo.

Il sistema cerca il modulo successivo nell'elenco. Quando lo trova, il LED giallo sul modulo lampeggia e il sistema presenta un messaggio che indica che il modulo è stato acquisito. Se ci sono altri moduli nell'elenco, apparirà un altro messaggio che informa che il sistema sta cercando il modulo successivo.

(5) Alimentare i moduli, uno alla volta, finché tutti i moduli non sono acquisiti.

Quando il sistema ha acquisito l'ultimo modulo, lo schermo mostra un elenco con i moduli acquisiti (ed i relativi numeri di serie).



(6) Fare clic sul pulsante *Chiudi*.

La registrazione si è conclusa con successo e il sistema chiude lo schermo Autoacquisizione.

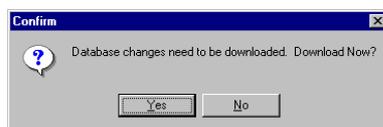
Fase 6 – Aggiornamento del database

L'ultima fase per rendere operativo il DEK è l'aggiornamento del database.

Si ricorda che il database del sistema PassPoint si trova nella MLB, dove vengono memorizzati tutti i dati di configurazione del sistema. Quando vengono apportate delle modifiche sul computer, queste non vengono trasferite automaticamente al database sulla MLB. Vengono conservate in un'area di memorizzazione temporanea sul computer, fino a quando l'operatore decide di scaricarle nel database della MLB. Tutte le modifiche apportate sul computer devono essere aggiornate sul database perché diventino effettive.

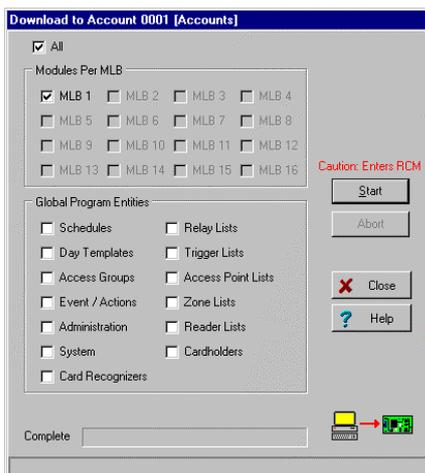
1. Chiudere la finestra di dialogo Configurazione Installatore.

Il sistema chiede se si vuole aggiornare il database:



2. Fare clic su Sì.

Appare la finestra di dialogo Aggiorna:



Sulla parte superiore della finestra di dialogo si trova il numero cliente da aggiornare. Il sistema seleziona automaticamente le voci relative alle parti del sistema che sono state modificate, consentendo comunque all'operatore di selezionare o deselezionare altre voci da aggiornare.

3. Fare clic su **Avvio**.

Comincia l'aggiornamento del database. La barra di stato sul fondo della finestra di dialogo mostra l'avanzamento del procedimento.

Configurazione del DCM

PassPoint fornisce un elenco di funzioni da utilizzare per modificare le impostazioni di default del modulo DCM fornito dal modello (o Wizard), per vogliono espandere queste impostazioni o per desidera modificare alcuni dati inseriti precedentemente. Con queste funzioni, è possibile modificare i moduli DCM del sistema in vari modi.

I moduli DCM vengono configurati utilizzando la finestra di dialogo Impostazione DCM, che si può raggiungere nel modo seguente:

1. Nel menu Config, selezionare Hardware.

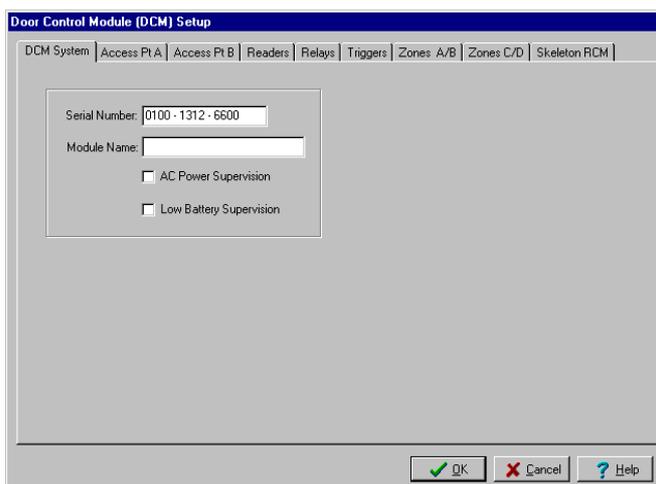
Appare la finestra di dialogo Configurazione installazione.

2. Fare clic una con il pulsante destro sul DCM interessato.

Apparirà un menù di opzioni.

3. Selezionare *Proprietà*

Appare la finestra di dialogo Impostazione DCM:



**Utilizzo della
finestra
Impostazione
DCM**

Come si può vedere, la finestra di dialogo Impostazione DCM contiene nove etichette. Ogni etichetta contiene campi che descrivono/controllano varie funzioni e impostazioni del modulo DCM. Le etichette e i relativi campi sono descritti qui di seguito.

Etichetta sistema DCM

Numero di serie - Si può immettere manualmente il numero di serie del modulo, se lo si conosce, o lasciare questo campo a

0000-0000-0000 per acquisire automaticamente in seguito il numero di serie. Il numero di serie è unico. Notare che se si sostituisce un modulo DCM esistente, si può riempire questo campo con zero, sostituire il modulo DCM e registrare automaticamente il nuovo modulo DCM, che avrà le stesse impostazioni di quello vecchio dopo averlo aggiornato sulla MLB.

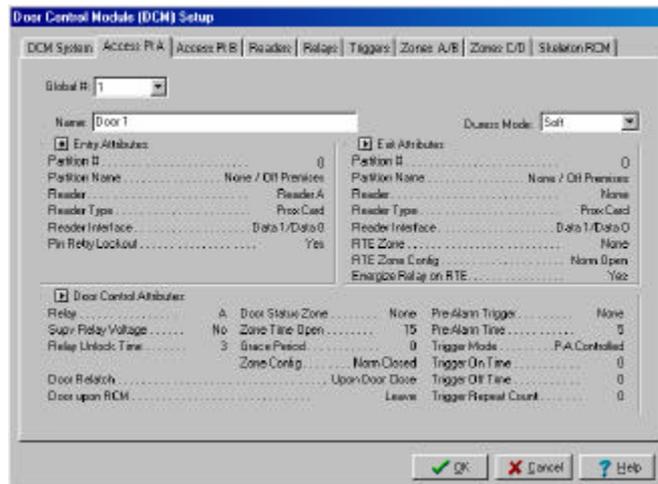
Nome modulo – Si può immettere un nome per il modulo, se si desidera. Questo apparirà sullo schermo come parte delle informazioni di identificazione del modulo DCM.

Monitor mancanza rete – Quando questo campo è attivato, il modulo informa il sistema in caso di mancanza della alimentazione di rete. Quando la rete viene a mancare o viene ripristinata, si registra un evento. Questa funzionalità dovrebbe essere attivata su tutti i moduli alimentati localmente.

Monitor batteria scarica – Quando questo campo è attivato, il modulo informa il sistema in caso di batteria scarica. Viene registrato un evento in caso di batteria scarica o di ripristino batteria. Questa funzionalità dovrebbe essere attivata su tutti i moduli alimentati localmente.

Etichetta varco A/B

La configurazione del varco indica i dispositivi di controllo di entrata e di uscita installati su quel varco:



La configurazione del varco comprende anche informazioni riguardanti il comando della serratura della porta e descrive i parametri di temporizzazione tipici che regolano il passaggio attraverso il varco (come ad esempio il tempo in cui serratura deve restare attivata, quanto tempo la porta può restare aperta, ecc.). La configurazione del varco comprende anche il nome del varco stesso e altre caratteristiche che potrebbe essere necessario specificare perché il varco funzioni correttamente.

In questa etichetta dello schermo Impostazione DCM, sono visualizzati tre gruppi di caratteristiche (Entrata, Uscita e Controllo porta). **NON E' POSSIBILE** modificare queste caratteristiche su questo schermo, poiché agisce solo da sommario. Fare doppio clic all'interno di uno dei gruppi o fare clic sulla freccia che si trova a sinistra del nome dei gruppi per aprire uno schermo che consentirà di modificare le caratteristiche visualizzate.

Notare che se il Numero globale del varco è impostato su 0, i campi successivi non saranno visualizzati, poiché non riguardano un varco non utilizzato.

Numero globale varco – Questo campo seleziona il numero di questa risorsa dal numero totale di risorse disponibili. Utilizzare questo menu a tenda per selezionare fra i valori disponibili. Il sistema visualizza automaticamente solo i numeri disponibili.

Nome – Utilizzare questo campo per immettere un nome per il varco che si sta impostando.

Modo costrizione – Nel caso vengano utilizzati lettori abbinati a tastiere, quando una persona viene obbligata a passare da un varco, può segnalarlo al sistema sostituendo l'ultima cifra del suo codice PIN con uno "0".

Ad esempio, se il codice PIN della persona è "1234," il codice di costrizione sarà "1230." "0" verrà ricordato facilmente, poiché è il numero di telefono del centralino. In caso di costrizione, un messaggio speciale appare nella memorizzazione eventi del sistema PassPoint. Il sistema può allora chiamare il servizio di sicurezza.

Il sistema offre tre modi di operazione costrizione: Normale, Soft e Hard. Se il modo costrizione è impostato su Soft, l'entrata o l'uscita è consentita indipendentemente dai privilegi di accesso della persona. Se la persona è solitamente autorizzata a entrare, la costrizione verrà sospesa e la persona potrà passare. Nel modo costrizione Normale, la persona è autorizzata a passare solo se i suoi privilegi di accesso lo autorizzano solitamente ad entrare. Nel modo costrizione Hard, l'accesso sarà sempre negato. Notare che l'utilizzo di costrizione Hard può mettere in pericolo la sicurezza delle persone e deve essere utilizzato nelle applicazioni più importanti. Utilizzare questo menu a tenda per selezionare il modo di operazione desiderato.

Attributi di ingresso

Questo gruppo visualizza un sommario di tutte le proprietà che descrivono il modo di controllo di ingresso per il varco. Per

modificare una di queste impostazioni, posizionare il cursore sulla freccia piccola che si trova a sinistra degli Attributi di ingresso e fare clic con il mouse; oppure, fare doppio clic con il mouse sull'area Attributi di ingresso. Appare il menu seguente, sul quale si può modificare l'informazione:



Ingresso al settore – I dati di configurazione del varco che descrivono l'area di accesso o il settore al quale accede una persona quando è autorizzata ad entrare dal varco. Utilizzare questo elenco per selezionare l'Ingresso al settore adeguato.

Lettoie ingresso – Descrive il dispositivo d'ingresso installato sul lato ingresso del varco. Tramite questo dispositivo, le persone devono identificarsi presso il sistema, in modo tale che il sistema possa esaminare i privilegi di accesso e determinare se la persona è autorizzata a penetrare nell'area protetta. Il termine utilizzato è "lettore ingresso" perché nella maggior parte dei casi il dispositivo è un lettore al quale l'utente deve presentare il proprio badge di identificazione. Il dispositivo può comunque essere una tastiera, sulla quale l'utente deve digitare il proprio Codice di Identificazione Personale (codice PIN). In alcuni casi, quando è necessaria maggior sicurezza, il lettore d'ingresso può essere un dispositivo con abbinamento di tastiera e lettore di badges.

Nel sistema PassPoint, i varchi sono configurati sui Door Control Modules (DCM). Dal momento che è possibile collegare due lettori su ogni modulo DCM, bisogna specificare il lettore utilizzato come lettore di controllo di ingresso. Notare che se l'installatore utilizza una configurazione varco predefinita, il lettore di ingresso (A o B) viene attribuito automaticamente e non è necessario modificarlo.

Tipo di lettore – Il tipo di tecnologia lettore o tastiera utilizzato sul varco. Le selezioni in questo campo comprendono tastiere, diversi tipi di lettori di badges (Wiegand, prossimità a banda magnetica) e combinazioni lettori/tastiera. Utilizzare questo elenco per selezionare il tipo di lettore.

Interfaccia lettore – E' il tipo di interfaccia elettrico del lettore. I lettori supportati dal sistema sono di due tipi: Data1/Data0 (stile Wiegand) e Clock & Dati. L'installatore deve selezionare quello adatto. Per la maggior parte dei lettori che non siano lettori di badges a banda magnetica, la soluzione adatta è solitamente Data1/Data0. Questa informazione è generalmente specificata sull'etichetta del lettore o della tastiera. Selezionare il tipo di interfaccia appropriato.

Blocco tentativi PIN – Una funzionalità che disattiva la tastiera di un lettore d'ingresso per un periodo di tempo definito dopo diversi tentativi d'inserimento di codice PIN errato. Il blocco tentativi PIN protegge i locali da intrusi che manomettono il varco controllato da una tastiera, perché rallenta il tentativo d'inserimento di qualsiasi combinazione di codice possibile. Per attivare questa funzionalità selezionare *Si*.

Il numero di tentativi PIN è impostato nella finestra di dialogo Amministrazione. Per aprire questa finestra, selezionare *Ammin* nel menu *Config*.

Attributi di uscita

Questo gruppo racchiude tutte le proprietà delle modalità di controllo di uscita per un Varco. Per modificare queste impostazioni, posizionare il cursore sulla freccia che si trova a sinistra degli Attributi di uscita e fare clic con il mouse, oppure fare doppio clic sull'area Attributi di uscita. Appare il seguente menu, nel quale si possono modificare le informazioni:



Uscita al settore – I dati di configurazione del varco che descrivono l'area di accesso o il settore nel quale entra una persona quando viene autorizzata l'uscita dal varco. Se il varco esce da tutte le aree controllate, il campo dovrebbe essere Nessuno / Fuori edificio. Utilizzare l'elenco per selezionare l'Uscita al settore adatta.

Letture di uscita – Un dispositivo installato sulla parte di uscita della porta. La persona deve identificarsi a questo dispositivo, in modo tale che il sistema possa esaminarne i privilegi di accesso e determinare se può uscire dall'area protetta.

Nel sistema PassPoint, i varchi possono essere configurati sui Door Control Modules (DCM). Dal momento che è possibile collegare due lettori su ogni modulo DCM, bisogna specificare il

lettore utilizzato come lettore di controllo di uscita. Notare che se l'installatore utilizza una configurazione varco predefinita, il lettore di uscita (A o B) viene attribuito automaticamente e non è necessario modificarlo.

Tipo lettore di uscita – Il tipo di lettore o tastiera utilizzato per uscire da un varco. Utilizzare l'elenco per selezionare il Tipo di lettore.

Interfaccia lettore uscita – E' il tipo di interfaccia elettrico del lettore. I lettori supportati dal sistema sono di due tipi: Data1/Data0 (stile Wiegand) e Clock & Dati. L'installatore deve selezionare quello adatto. Per la maggior parte dei lettori che non siano lettori di badges a banda magnetica, la soluzione adatta è solitamente Data1/Data0. Questa informazione è generalmente specificata sull'etichetta del lettore o della tastiera. Selezionare il tipo di interfaccia appropriato.

Zona Richiesta di Uscita (RDU) – E' la zona che verrà utilizzata per la Richiesta Di Uscita. Nelle installazioni nelle quali non viene utilizzato un lettore di uscita, essa è necessaria al sistema per monitorare le uscite da un varco e/o aprire il varco stesso. Quando viene utilizzato un MSP, se il sistema PassPoint non è dotato di un lettore dal quale consentire l'uscita, è necessario installare un dispositivo Richiesta Di Uscita.

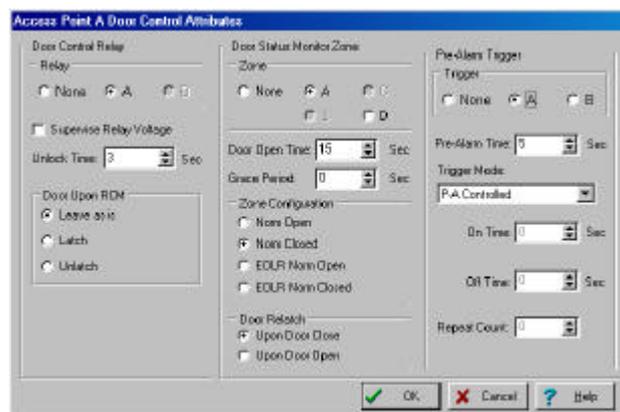
Il dispositivo RDU può essere un pulsante a muro sulla parte protetta della porta, oppure un rivelatore a infrarossi con visione limitata, puntato sull'area prossima alla porta dal lato protetto. In entrambi i casi, il dispositivo RDU è collegato a una zona d'ingresso sul Door Control Module. Quando una persona chiede di uscire dal varco, la zona RDU viene aperta premendo il pulsante o attivando il rivelatore. Il sistema PassPoint sblocca la serratura e consente alla persona di uscire dalla porta. Dal momento in cui il sistema PassPoint consente l'uscita, automaticamente la zona MSP viene esclusa.

Il campo zona RDU è utilizzato per indicare quale delle quattro zone d'ingresso del modulo DCM (dalla ZONA A alla ZONA D) sarà utilizzata a questo scopo. Notare che scegliendo una configurazione varco predefinita, questo campo viene impostato automaticamente nel sistema PassPoint.

Configurazione delle zone RDU – Configurazione hardware della zona (normalmente aperta, normalmente chiusa, con resistenza di fine linea) per il dispositivo RDU. Questa impostazione deve corrispondere alla configurazione del contatto del dispositivo RDU. Inoltre, si può fare in modo che il relè ariporta sia attivato dal dispositivo RDU.

Attributi controllo porta

Questo gruppo è il riepilogo di tutte le proprietà che descrivono il modo di controllo del varco. Per modificare una di queste impostazioni, posizionare il cursore sulla freccia a sinistra degli Attributi controllo porta e fare clic con il mouse; oppure, fare doppio clic nell'area Attributi Controllo porta. Appare il menu seguente, nel quale è possibile modificare le informazioni:



Relè apriporta – Un relè del modulo DCM utilizzato per controllare il flusso di elettricità al meccanismo di chiusura della porta. Il relè di controllo della porta è un contatto di scambio pulito, e può essere collegato come circuito normalmente aperto o normalmente chiuso.

I blocchi elettromagnetici sono collegati solitamente al contatto parte normalmente chiuso del relè, mentre le elettroserrature sono solitamente collegate al contatto normalmente aperto del relè. Da notare che le elettroserrature sono disponibili in versione Fail Safe (quando viene tolta l'alimentazione, la porta si può aprire) o Fail Secure (quando viene tolta l'alimentazione, la porta è bloccata).

Dal momento che il funzionamento dei dispositivi di sicurezza può avere conseguenze importanti per la sicurezza delle vite umane, è necessario sottolineare che quando si utilizza una elettroserratura, il sistema di rivelazione incendio deve essere in condizione di gestirne l'attivazione.

Poiché il modulo DCM contiene due uscite relè (A e B), questo campo consente di selezionare quale dei due relè verrà utilizzato per controllare la porta di questo varco. Se l'installatore ha scelto una configurazione varco predefinita, la selezione del relè apriporta viene eseguita automaticamente.

Supervisione tensione al relè – In situazioni in cui viene utilizzato un alimentatore estraneo al sistema per alimentare il meccanismo di apertura della porta, l'installatore può scegliere che il sistema PassPoint controlli l'alimentatore e avvisi l'operatore in caso di problema sull'alimentatore che protegge la porta. Selezionare questa casella per attivare questa funzionalità

Se l'installatore utilizza l'alimentatore contenuto nel kit, non è necessario attivare questa funzionalità poiché l'alimentatore è già controllato dal modulo DCM.

Tempo di sblocco - E' il numero di secondi per i quali il relè di controllo della porta deve essere attivato per aprire la porta. Perché la porta si apra durante questo periodo di tempo, il dispositivo di apertura della porta deve essere collegato correttamente al contatto normalmente aperto o normalmente chiuso del relè della porta.

Porta su RCM – Nel raro caso in cui un Door Control Module perda il collegamento con il resto del sistema, una porta che ha ricevuto l'ordine di aprirsi (manualmente o con temporizzazione) può essere richiusa automaticamente. Questa impostazione consente parametri di “blocco,” per maggior sicurezza sulla porta esterna; “sblocco,” per porte interne, che creerebbero problemi se non funzionassero correttamente, o “lascia com'è”, che lascia le porte nello stato attuale (chiusa o aperta). Nella maggior parte dei casi, l'impostazione “lascia com'è” è quella consigliata, per maggior sicurezza, mentre consente alle persone con badges (o codici) di passare da un varco se sono state configurate le impostazioni Reduced Capability Mode adatte.

Zona Monitor Stato Porta – Una zona di ingresso sul modulo DCM, che può essere collegata a un contatto magnetico installato sulla porta, in modo tale che il sistema PassPoint possa determinare se un intruso ha forzato l'apertura della porta, quando questa avrebbe dovuto restare chiusa. Questa zona può essere usata anche per consentire al sistema di determinare se una porta è stata aperta nel modo corretto, ma non è stata chiusa entro il periodo di tempo prestabilito.

La Zona Monitor Stato Porta viene utilizzata per indicare quale delle quattro zone d'ingresso del DCM (Zone da A a D) verrà utilizzata per questo scopo. Se l'installatore sceglie una configurazione varco predefinita, questo campo verrà riempito automaticamente dal sistema PassPoint. Se la porta può essere aperta manualmente dall'interno quando le persone escono, è necessario installare un dispositivo Richiesta Di Uscita, in modo tale che, uscendo, gli utenti non attivino allarmi Porta forzata.

Temporizzazione porta – Il numero di secondi durante i quali la porta è autorizzata a restare aperta quando l'accesso o l'uscita dal varco sono autorizzati. Se la porta resta aperta per un periodo di tempo superiore a quello specificato, si attiva un allarme Temporizzazione porta aperta.

Antirimbazzo – Il numero di secondi, in seguito a un ripristino della zona MSP, durante i quali una riapertura della porta non attiverà una situazione di allarme Porta forzata. Genererà invece, un ciclo RDU. In questo caso si genera un evento Porta varco riaperta.

Questa funzionalità è fornita solo per casi in cui il MSP possa ripristinarsi prima che la serratura blocchi la porta. Questo aiuta a eliminare eventuali casi di falso allarme. L'impostazione predefinita è zero (0), che disattiva il periodo di antirimbazzo ed è l'impostazione più sicura. Per motivi di sicurezza, questo valore dovrebbe essere impostato al valore più basso che possa comunque ovviare al problema.

Configurazione zona – Questa impostazione consente di impostare una zona MSP normalmente aperta, normalmente chiusa o controllata dalla resistenza di fine linea. Questa impostazione deve corrispondere alla configurazione del contatto del dispositivo MSP.

Porta richiusa – Quando viene installata una zona MSP a una porta, il sistema PassPoint può determinare se la porta viene chiusa prima del periodo di tempo durante il quale la serratura dovrebbe essere sbloccata. In questo caso, se la serratura non è scattata quando la porta si è richiusa, il sistema PassPoint blocca automaticamente la porta, per evitare che una seconda persona apra una porta sbloccata. Questa caratteristica è chiamata anche "Anti-Passaggio continuo". La maggior parte delle volte, questa opzione viene impostata per bloccare la porta non appena si richiude. Selezionare l'impostazione "Per porta chiusa" quando si

utilizza un blocco elettromagnetico. L'impostazione "Per porta aperta" può essere utilizzata ai varchi dotati di elettroserrature.

Trigger preallarme – Se una porta che utilizza un MSP viene tenuta aperta più del periodo di temporizzazione porta aperta, lo storico eventi memorizza un allarme Temporizzazione porta. Per evitare inutili allarmi Temporizzazione porta aperta, si può installare in prossimità del varco un segnale acustico per avvisare la persona che sta tenendo la porta aperta che si sta per verificare una situazione di allarme. Questo dispositivo sonoro è chiamato Avviso di preallarme.

Quando il varco è stato configurato con un avviso di preallarme, se la porta è ancora aperta oltre un periodo di tempo predefinito prima che si attivi l'Allarme porta aperta, il preallarme si attiva ed emette un segnale acustico (o anche luminoso) per avvisare la persona che sta tenendo la porta aperta. Per la segnalazione di preallarmi si utilizzano solitamente cicalini piezoelettrici gestiti da uno dei due trigger disponibili del modulo DCM. Ogni trigger del modulo DCM è un driver configurato con collettore aperto, con una resistenza in serie di 680 Ohm. Quando vengono attivati, essi forniscono una corrente di 15mA. Se viene utilizzato un dispositivo piezoelettrico a 12-Volt, il suo collegamento positivo deve essere collegato a una fonte da 12 Volt (con una terra comune alla terra del sistema PassPoint) e il suo collegamento negativo deve essere collegato al trigger del modulo DCM. Quando il preallarme è operativo, il dispositivo sonoro si attiva. Poiché su ogni DCM sono disponibili due trigger, è importante selezionare quello giusto (TRIGGER A o TRIGGER B). Dal momento che i preallarmi sono facoltativi, non sono mai predefiniti nel sistema PassPoint e devono essere selezionati dall'installatore.

Periodo di preallarme – Il periodo di tempo, in secondi, prima dell'insorgere di un allarme Porta aperta di un varco, al quale dovrà essere attivato il preallarme. Ad esempio, se la porta è impostata per restare aperta per 30 secondi, un periodo di preallarme corretto potrebbe essere 10 secondi, vale a dire che si

danno 10 secondi di avviso a una persona che sta tenendo la porta aperta. Il Trigger di preallarme inizia ad operare 20 secondi dopo che il relè apriporta è stato attivato, se la porta è ancora aperta. Se la porta è ancora aperta al termine dei 30 secondi, si attiva un Evento allarme temporizzazione porta. Il dispositivo di preallarme resta attivato (a seconda della modalità) finché la porta viene chiusa, ripristinando l'Allarme temporizzazione porta.

Modo trigger – L'attivazione del trigger di preallarme può essere impostata come "Controllato", "Singolo" o "Ripetuto". Un trigger di preallarme Controllato si attiva e resta attivo finché la porta si chiude. Un trigger di preallarme a Singolo si attiva una volta e si disattiva dopo il tempo impostato. Un trigger di preallarme ripetitivo segue cicli di impulsi e pause per il numero di ripetizioni specificato. Se il numero di ripetizioni è impostato su 0, i cicli continuano finché non si chiude la porta. Notare che, indipendentemente dal modo di attivazione, il trigger si spegne non appena la porta si chiude.

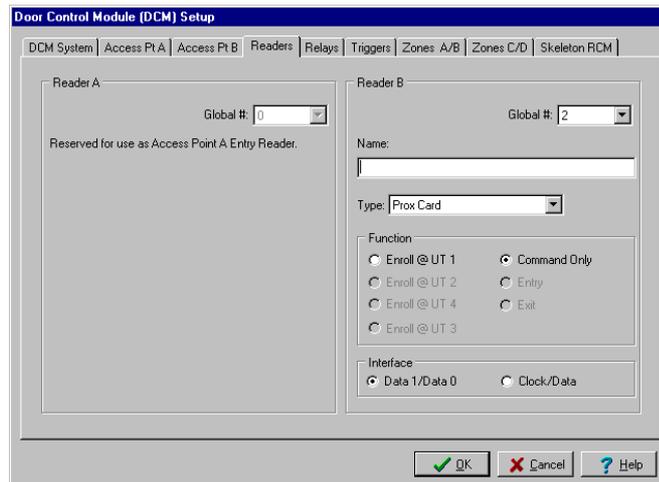
Impulso – E' il periodo di tempo, in secondi, durante il quale il trigger di preallarme resta attivato se il modo di attivazione è impostato su Singolo o Ripetuto.

Pausa – E' il periodo di tempo, in secondi, durante il quale il trigger di preallarme resta disattivato se il modo è impostato come Ripetuto. E' il tempo che costituisce il tempo "Fine" del ciclo ripetitivo.

Numero di ripetizioni – E' il numero di cicli Impulso/Pausa per il trigger di preallarme. Se questo numero è impostato su 0, il trigger ripete continuamente, fino alla chiusura della porta.

Etichetta Lettori

L'etichetta lettori è illustrata qui sotto:



-
- ,

Notare che se il Numero globale è impostato su 0, i campi seguenti non saranno visualizzati, poiché non riguardano un lettore non valido o non utilizzato.

N. globale – Questo campo seleziona il numero della risorsa dal numero totale di risorse disponibili. Utilizzare questo elenco per selezionare fra i valori disponibili. Il sistema mostra automaticamente solo i numeri disponibili. Ogni lettore deve possedere un numero globale unico.

Nome – Utilizzare questo campo per immettere un nome per il lettore che si sta impostando.

Tipo – Questo campo seleziona il tipo di tecnologia del lettore. Utilizzare il menu per selezionare il tipo desiderato. Per il CEK scegliere prossimità in questo campo.

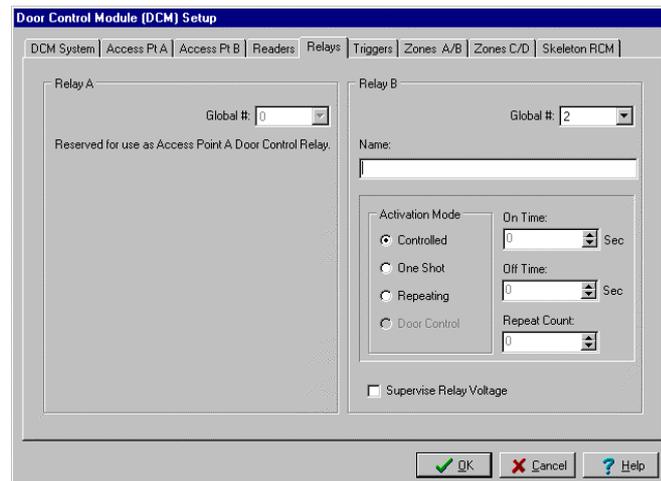
Funzione – Questo campo seleziona la funzione del lettore non valido. Impostando questo campo su Lettore di acquisizione

badges per il terminale operatore x, si seleziona questo lettore in modo tale che invii numeri di badge al terminale operatore indicato quando l'operatore si trova in un campo dove bisogna immettere un numero di badge. In questo modo il lettore viene utilizzato come stazione di acquisizione badges. Impostando questo campo come Lettore di comando, è possibile attivare azioni all'interno del sistema passando un badge nel lettore. Le azioni possono essere programmate attraverso l'impostazione eventi/azioni del sistema o tramite le azioni assegnate ai singoli utenti.

Interfaccia – Le specifiche elettriche del lettore collegato a questa interfaccia devono essere indicate in questo campo. La maggior parte delle unità corrispondono ai protocolli Data1/Data0, o Wiegand. Molti lettori di badges a banda magnetica corrispondono al protocollo Clock/Dati. Specificare il tipo di interfaccia elettrico corrispondente utilizzato dal lettore installato, selezionando il tipo di protocollo relativo.

Etichetta Relè

L'etichetta Relè è la seguente:



- Notare che se il Numero globale è impostato su 0, i campi seguenti non saranno visualizzati, poiché non riguardano un relè non valido o non utilizzato.
 -
-

Numero globale – Questo campo seleziona il numero della risorsa dal numero totale di risorse disponibili. Utilizzare la lista per selezionare fra i valori disponibili. Il sistema visualizza solo i numeri disponibili. Ogni relè utilizzato nel sistema deve avere un numero globale di relè unico se non viene utilizzato per un varco.

Nome – Utilizzare questo campo per immettere un nome per il relè che si sta impostando.

Attivazione – Si può selezionare uno dei tre modi seguenti:

- **Fisso:** Il sistema o un operatore possono comandare l'attivazione e la disattivazione del relè.
- **Un impulso:** Quando comandato dal sistema o da un operatore, il relè si attiva per un numero di secondi specificato e poi si disattiva. [1 - 65535 secondi]
- **Ripetuta:** Quando comandato dal sistema o da un operatore, il relè si attiva e si disattiva per un numero di secondi specificato. Questo ciclo viene ripetuto per un numero di volte specificate, o viene ripetuto continuamente finché viene inviato un comando di arresto. [Impulso = 1-65535 secondi] [Pausa = 1-65535 secondi] [Conteggio ripetizioni = 0 (Infinito) o 1-65535 volte]

Impulso – Questo campo è attivo solo se è stato scelto *Un impulso* o *Ripetuta* come modalità di attivazione. Immettere il tempo in secondi (1 - 65535) di attivazione del relè.

Pausa – Questo campo è attivo solo se è stata scelta la modalità di attivazione *Ripetuta*. Immettere il tempo in secondi (1 - 65535)

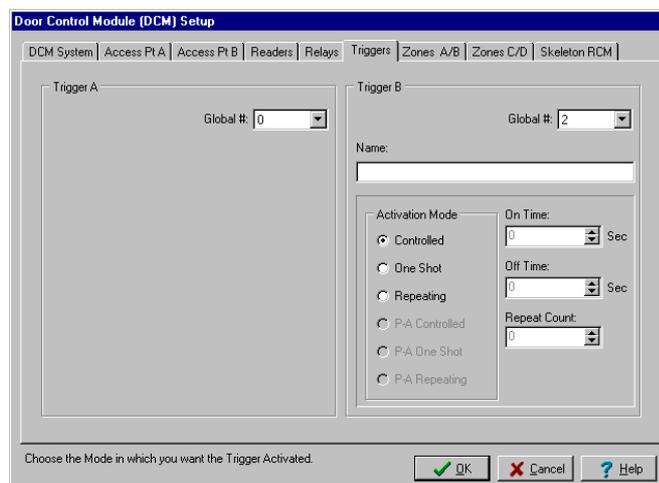
per definire per quanto tempo il relè deve restare disattivo prima di attivarsi nuovamente.

Numero di ripetizioni – Questo campo è attivo solo se è stata scelta la modalità di attivazione *Ripetuta*. Immettere il numero di volte per le quali il relè deve ripetere il ciclo di attivazione/disattivazione. E' possibile scegliere un numero compreso fra 0 e 65535. Notare che il valore 0 fa in modo che il relè continui il ciclo finché riceva un comando di arresto.

Supervisione tensione relè – Selezionare questo campo se si vuole controllare la tensione collegata ai morsetti del relè. Selezionando questo campo, il sistema controlla continuamente la tensione del relè e ne visualizza lo stato su uno schermo di stato separato.

Etichetta Triggers

L'etichetta Trigger appare qui sotto:



- Notare che se il Numero globale è impostato su 0, i campi seguenti non sono visualizzati, perché non riguardano un trigger non valido o non usato.

Numero globale – Questo campo seleziona il numero della risorsa dal numero totale di risorse disponibili. Utilizzare la lista per selezionare fra i valori disponibili. Il sistema visualizza solo i numeri disponibili. Ogni trigger utilizzato nel sistema deve avere un numero globale di trigger unico se non viene utilizzato per fornire un preallarme di un varco.

Nome – Utilizzare questo campo per immettere un nome per il trigger che si sta impostando.

Attivazione – Si può selezionare uno dei tre modi seguenti:

- **Fisso:** Il sistema o un operatore possono comandare l'attivazione e la disattivazione del trigger.
- **Un impulso:** Quando comandato dal sistema o da un operatore, il trigger si attiva per un numero di secondi specificato e poi si disattiva. [1 - 65535 secondi]
- **Ripetuta:** Quando comandato dal sistema o da un operatore, il trigger si attiva e si disattiva per un numero di secondi specificato. Questo ciclo viene ripetuto per un numero di volte specificate, o viene ripetuto continuamente finché viene inviato un comando di arresto. [Impulso = 1-65535 secondi] [Pausa = 1-65535 secondi] [Conteggio ripetizioni = 0 (Infinito) o 1-65535 volte]

Impulso – Questo campo è attivo solo se è stato scelto *Un impulso* o *Ripetuta* come modalità di attivazione. Immettere il tempo in secondi (1 - 65535) di attivazione del trigger.

Pausa – Questo campo è attivo solo se è stata scelta la modalità di attivazione *Ripetuta*. Immettere il tempo in secondi (1 - 65535) per definire per quanto tempo il trigger deve restare disattivo prima di attivarsi nuovamente.

Numero di ripetizioni – Questo campo è attivo solo se è stata scelta la modalità di attivazione *Ripetuta*. Immettere il numero di volte per le quali il trigger deve ripetere il ciclo di attivazione/disattivazione. E' possibile scegliere un numero compreso fra 0 e 65535. Notare che il valore 0 fa in modo che il trigger continui il ciclo finché riceva un comando di arresto.

Etichette Zona

La finestra di dialogo ha due etichette Zona. Ogni etichetta contiene informazioni su due zone diverse.

Le zone non utilizzate dal sistema di controllo accessi possono essere utilizzate per funzioni supplementari come la segnalazione di alcune condizioni. La loro compatibilità UL non è stata testata e non possono quindi essere utilizzati per funzioni anti intrusione nelle installazioni UL.

Le due etichette Zona contengono informazioni simili. L'etichetta Zona A/B appare come nell'esempio qui sotto:

The screenshot shows the 'Door Control Module (DCM) Setup' dialog box. It features a tabbed interface with the following tabs: DCM System, Access Pt A, Access Pt B, Readers, Relays, Triggers, Zones A/B (selected), Zones C/D, and Skeleton RCM. The 'Zones A/B' tab is divided into two sections: Zone A and Zone B. Zone A includes a 'Global #' dropdown menu set to '1', a 'Name' text input field, a 'Response Type' section with radio buttons for 'No Alarm - monitored' (selected), '24 Hour', 'Perimeter', 'DSM', 'Interior', and 'RTE', and a 'Configuration' section with radio buttons for 'Norm Open' (selected), 'EOLR Norm Closed', 'Norm Closed', 'EILR Norm Open', 'EOLR Norm Open', and 'EILR Norm Closed'. Zone B includes a 'Global #' dropdown menu set to '0'. At the bottom of the dialog are three buttons: 'OK' (with a green checkmark), 'Cancel' (with a red X), and 'Help' (with a question mark).

- ,
- Notare che se il Numero globale è impostato su 0, i seguenti campi non verranno visualizzati, perché non riguardano una zona non utilizzata.

Numero globale – Questo campo seleziona il numero della risorsa dal numero totale di risorse disponibili. Utilizzare la lista per selezionare fra i valori disponibili. Il sistema visualizza solo i numeri disponibili. Ogni zona utilizzata nel sistema deve avere un numero globale unico se non viene utilizzata per il controllo di un varco.

Nome – Utilizzare questo campo per immettere un nome per la zona che si sta impostando.

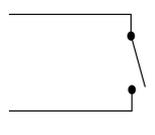
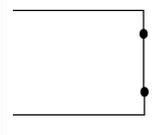
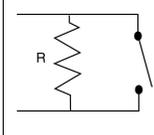
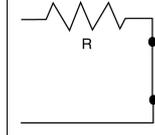
Tipo risposta – Selezionare un tipo di risposta per la zona. Sono disponibili quattro opzioni diverse:

- **No allarmi - monitorato:** Ciò consente al sistema di vedere la zona e di individuarne le aperture e i ripristini. Queste zone sono utilizzate principalmente nei rapporti eventi/azioni e dagli script del sistema.
- **Perimetro:** Aperture/ripristini sono sempre riconosciuti su questa zona, ma possono provocare un allarme solo se il sistema anti intrusione è inserito **TOTALMENTE** o **PARZIALMENTE**. Una zona perimetro si ripristina quando la zona ritorna in stato normale.
- **Interno:** Aperture/Ripristini sono sempre riconosciuti in questa zona, ma possono attivare un allarme solo quando il sistema anti intrusione è inserito **TOTALMENTE**. Una zona Interna si ripristina quando la zona ritorna in stato normale.
- **24 Ore:** Aperture/Ripristini saranno sempre riconosciuti in questa zona. Un allarme si attiverà ad ogni apertura della zona. Una zona 24 ore si ripristina quando la zona ritorna in stato normale.

Configurazione – Selezionare una configurazione hardware per la zona. Si può scegliere fra le seguenti possibilità

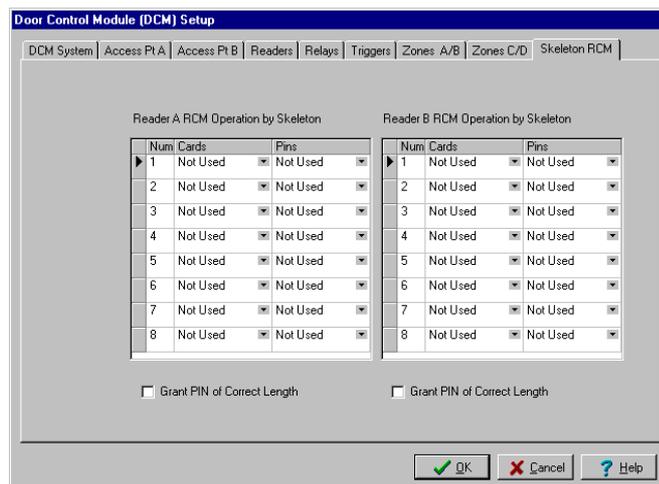
- Normalmente aperta
- Normalmente chiusa
- Normalmente aperta con resistenza di fine linea (bilanciata)
- Normalmente chiusa con resistenza di fine linea (bilanciata)

NOTA: le zone bilanciate necessitano di resistenze di terminazione da 2KOhm.

Stato sensore normale	STATI ZONA			
	ZONA A DUE STATI (non bilanciata)		ZONA A TRE STATI (bilanciata)	
	Normalmente Aperta (N.O.)	Normalmente Chiusa (N.C.)	Normalmente Aperta (N.O.)	Normalmente Chiusa (N.C.)
0 (corto circuito)	APERTA	CHIUSA	APERTA	GUASTA
R	-	-	CHIUSA	CHIUSA
2R	-	-	-	-
infinito (circuito aperto)	NORMALE	APERTA	GUASTA	APERTA
Connessioni Sensore				

Etichetta RCM residenti

Nel caso in cui un modulo DCM perdesse il collegamento con il resto del sistema PassPoint, è possibile programmare il modulo DCM per operare autonomamente. Quando ciò accade, il modulo DCM viene posto in Reduced Capability Mode (RCM). Notare che la sicurezza del sistema non è compromessa se il modo RCM è configurato correttamente. Innanzitutto, ogni varco può essere impostato per bloccare la porta, sbloccarla o mantenere lo stato invariato. In questo modo è possibile proteggere le porte perimetrali, mentre le porte interne o le zone protette possono essere lasciate aperte. E' possibile quindi continuare a utilizzare i badges e i codici PIN sui lettori e sulle tastiere del modulo DCM in modo RCM. Nella maggior parte dei casi, è possibile configurare e utilizzare i badges residenti e i codici PIN residenti per sbloccare una porta, per un singolo ciclo o per periodo di tempo più lungo. I badges o i codici PIN residenti possono anche essere usati anche per bloccare la porta. I badges residenti vengono configurati descrivendo i pattern presenti nella firma elettronica del badge. I codici PIN residenti vengono configurati attribuendo codici PIN speciali che richiamino queste caratteristiche.



Selezionare le funzioni per ogni badge/codice PIN residente. Ogni badge/codice può avere una delle tre funzioni seguenti:

- **Apri (Accesso consentito)**
- **Escludi (Sblocco per un tempo indeterminato)**
- **Blocca (Blocco per un tempo indeterminato)**

L'Accesso consentito opera in modo simile a un ciclo di accesso normale.

Lo Sblocco per un tempo indeterminato sblocca la porta finché interviene un comando diverso.

Il Blocco per un tempo indeterminato blocca la porta finché interviene un comando diverso.

Le funzioni di blocco e sblocco possono essere utilizzate dall'amministratore del sistema che, in caso di guasto del sistema, vuole consentire il passaggio durante il giorno, fino alla fine dell'orario di lavoro, quando viene utilizzato il badge o il codice PIN, o finché il sistema non riprenda nuovamente la completa operatività

Il tipo di codice residente che si può immettere per un varco dipende dal tipo di lettore che è stato configurato. Se il varco

possiede un lettore, ad esempio, sarà possibile configurare solo badges, senza codici PIN. Se si possiede un'unità combinata lettore/tastiera, sarà possibile configurare entrambi i tipi di codici residenti.

- **Importante:** in quest'area si sta configurando solo la funzione dei codici PIN residenti. I numeri del badge/codice PIN per i codici residenti sono attribuiti in un'altra area del programma, "Opzioni generali del sistema", presentato precedentemente.
-

PIN di consenso della lunghezza esatta – Attivando questa funzione, si disattiva l'uso di codici PIN residenti. Il codice PIN può essere usato solo su varchi che utilizzano una tastiera per ingresso o uscita. Attivando questa funzione, il sistema perde gran parte delle sue specifiche di sicurezza. Tutto quello che si deve fare per poter accedere è digitare la quantità corretta di caratteri del codice PIN. Le vere cifre del codice non sono importanti, qualsiasi combinazione di cifre sarà sufficiente, a condizione che sia della lunghezza corretta.

Capitolo

10

Aggiunta di un Card Enrollment Kit

Aggiungendo un Card Enrollment Kit (CEK) si possono aggiungere rapidamente badges al sistema. I badges vengono registrati nel sistema presentandoli alla stazione di acquisizione badges del desktop.

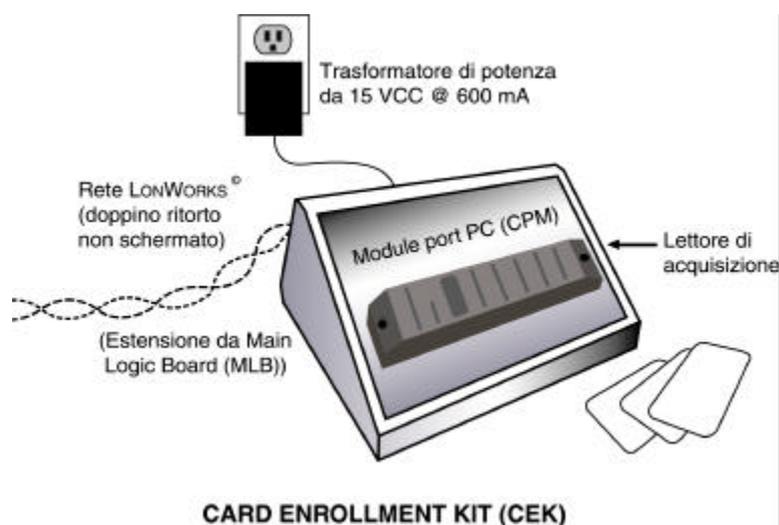
In questo capitolo viene spiegato come:

- **Collegare i componenti del CEK**
- **Attivare e impostare il CEK**
- **Registrare il CEK in un sistema PassPoint esistente**

Presentazione del Card Enrollment Kit

Il Card Enrollment Kit (CEK) è un modulo di sistema completo che può essere aggiunto a un'installazione PassPoint esistente per una gestione di badges (inclusa l'acquisizione badges) semplicissima. Il CEK consiste essenzialmente in un lettore di acquisizione (nel disegno qui sotto). Gli amministratori del sistema possono presentare i badges a questo lettore per registrarli rapidamente nel sistema.

Il CEK si collega al sistema PassPoint come qualsiasi altro modulo di sistema, utilizzando una connessione in rete con doppino ritorto. Deve essere alimentato localmente ad una tensione compresa tra i 12Vcc e i 15Vcc.



- Cosa comprende il Card Enrollment Kit?** Il CEK di PassPoint è un kit che comprende:
- **1 involucro desktop, che contiene:**
 - Computer Port Module (ADPTCPM)
 - Lettore di prossimità per l'acquisizione di badges (ANPTPROX)
 - **1 cavo per la connessione sul bus Echelon**

Installazione del CEK

L'installazione e l'acquisizione del CEK in un sistema PassPoint esistente si svolge in sette fasi. Seguire le fasi indicate e fare riferimento agli schemi di cablaggio forniti.

Fase 1 – Scelta della posizione del CEK

Il CEK è un'unità stand-alone, vale a dire che può essere posto su una scrivania o su qualsiasi area di lavoro. Deve comunque essere posizionato vicino al computer del sistema, perché è qui che vengono registrati i badges. L'amministratore avrà bisogno di accedere facilmente al computer e al CEK nel momento dell'acquisizione dei badges.

Fase 2 – Collegamento del CEK al sistema

Collegare il CEK al sistema significa semplicemente collegare il CEK alla rete. Seguire le fasi indicate qui sotto e fare riferimento ai diagrammi di connessione forniti:

1. Collegare il cavo del bus nella presa del lettore di acquisizione con l'etichetta *RETE*.

Il cavo del bus fornito con il CEK ha due estremità. Un'estremità contiene un connettore tipo "jack" a due poli: è l'estremità da collegare al lettore di acquisizione.

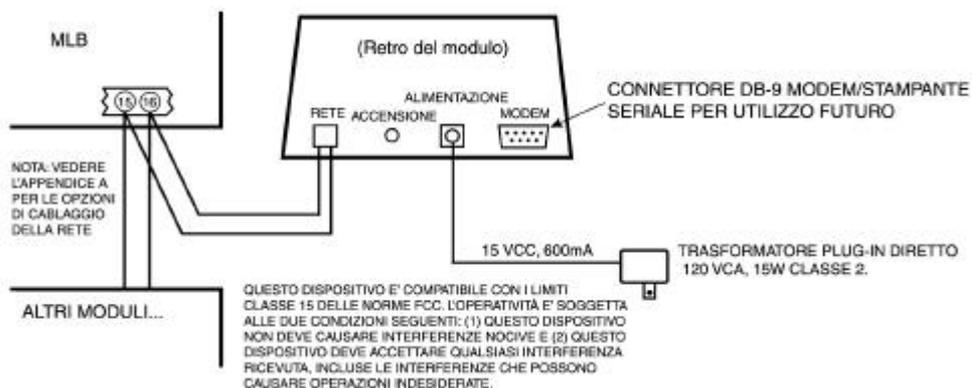
2. Collegare l'altra estremità del cavo del bus ai morsetti 15 e 16 della MLB.

I due cavi possono essere collegati indistintamente a uno o all'altro dei morsetti della MLB.

- Vedere l'Appendice A per le opzioni di cablaggio.
 - ;
-

Fase 3 – Alimentazione e attivazione

Il CEK può essere alimentato prelevando l'alimentazione a 12Vcc da qualsiasi kit del sistema.



COLLEGAMENTI DEL CARD ENROLLMENT KIT

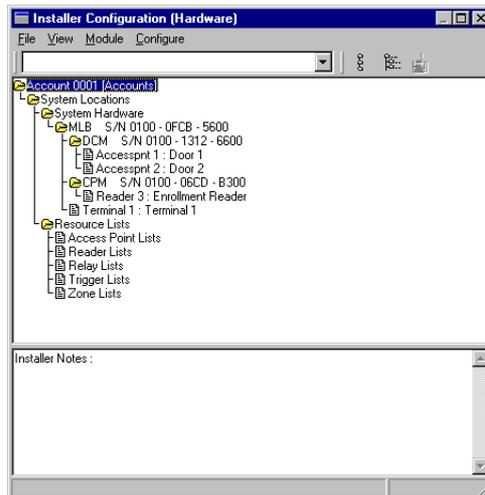
Fase 4 – Aggiunta e impostazione del CEK

Ora che il CEK è attivato, aggiungere il nuovo modulo (CPM) all'installazione esistente. Per aggiungere e impostare il nuovo modulo CPM, seguire la procedura seguente:

1. Nel menu **Config**, selezionare **Hardware**.

Appare la finestra di dialogo Configurazione Installatore:

Utilizzare la finestra di dialogo Configurazione Installatore per visualizzare o modificare i componenti del sistema e per impostare le varie opzioni del sistema.



La finestra di dialogo Configurazione Installatore elenca tutti i componenti del sistema. E' qui che vengono aggiunti i nuovi moduli.

-
-

Dopo aver apportato le modifiche sullo schermo, devono essere scaricate sul database del sistema perché diventino effettive.

2. Fare clic con il pulsante *destro* sulla MLB.

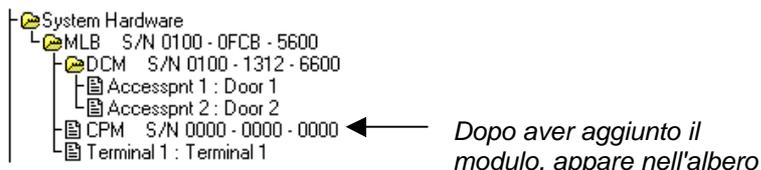


Fare clic qui con il pulsante destro per vedere un menu di opzioni.

In questo modo apparirà un menu di opzioni.

3. Nel menu selezionare **Agg. CPM.**

L'albero nella finestra di dialogo Configurazione Installatore mostra ora il nuovo CPM:



Bisogna ora registrare il CPM nel sistema PassPoint in modo tale che il sistema riconosca il dispositivo e tutte le sue impostazioni di configurazione. Il prossimo paragrafo spiega la registrazione del CPM.

Fase 5 - Auto acquisizione del CPM

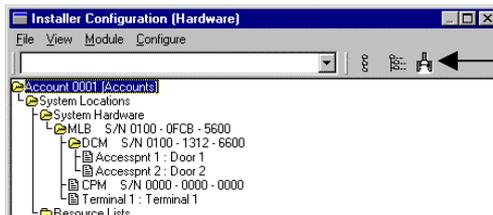
Ogni volta che un nuovo modulo viene aggiunto al sistema, esso deve essere registrato. La registrazione informa semplicemente il database del sistema che è presente un nuovo modulo.

Quando si registra un modulo, il sistema cerca i nuovi moduli collegati che non siano ancora stati registrati e li riconosce perché hanno numeri di serie che contengono solo zeri. Ad esempio, il modulo CPM appena aggiunto ha un numero di serie che contiene solo zeri e nessun altro carattere. Ciò significa che non è stato registrato e non fa ancora veramente parte del sistema.

Per registrare il modulo CPM appena aggiunto, seguire la procedura seguente:

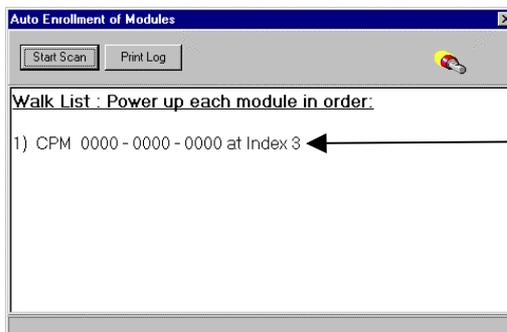
- 1. Fare clic sul pulsante Auto acquisizione sulla finestra di dialogo Configurazione Installatore.**

Vedere nel diagramma qui sotto dove si trova il pulsante Auto acquisizione:



*Pulsante
Auto
acquisizione*

Facendo clic su questo pulsante si apre la finestra di dialogo Auto acquisizione:



*Il sistema
riconosce che un
CPM deve essere
registrato.*

La procedura di acquisizione viene fatta **automaticamente** dopo aver premuto il pulsante *Avvia Scansione*. L'intero procedimento impiega solo qualche secondo.

Le procedure per acquisire un solo modulo sono diverse da quelle per acquisire più moduli. Per acquisire un solo modulo, seguire le istruzioni riportate al punto 2a. Per acquisire più di un modulo, seguire le istruzioni riportate nel punto 2b.

2a. Registrazione di un solo modulo.

Per registrare un solo modulo nel sistema PassPoint procedere nel modo seguente:

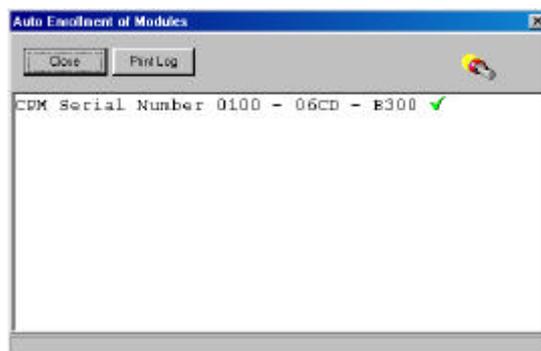
- Non spegnere mai la MLB mentre il sistema sta registrando un modulo.

Start Scan

(1) Fare clic sul pulsante *Scansione*.

Il sistema cerca il modulo; quando lo trova, il LED sul modulo lampeggia e un messaggio sullo schermo segnala che il modulo è stato registrato e la scansione si interrompe.

Quando il sistema ha registrato il modulo, appare uno schermo con il modulo acquisito (e il numero di serie).



Close

(2) Fare clic sul pulsante *Chiudi*.

La registrazione è terminata con successo e il sistema chiude lo schermo Auto acquisizione dei moduli.

2b. Registrazione di più moduli.

La finestra di dialogo Auto acquisizione dovrebbe già essere presente sullo schermo e dovrebbe apparire come nell'esempio qui sotto per la registrazione di più moduli:



Se i moduli vengono accesi prima della procedura di registrazione o nell'ordine sbagliato, non saranno registrati correttamente.

- Non spegnere mai la MLB durante il procedimento di registrazione.



Per registrare più moduli nel sistema PassPoint, questi devono essere accessi nell'ordine in cui sono elencati sullo schermo. Per registrare i moduli, procedere nel modo seguente:

(1) Fare clic sul pulsante *Stampa*. Viene stampato un elenco dei moduli da registrare.

(2) Controllare che il primo modulo sull'elenco sia acceso.

NOTA: Accendere i moduli nell'ordine in cui appaiono nell'elenco. Assicurarsi che i moduli successivi siano spenti. Dopo aver avviato la scansione e aver terminato l'acquisizione, i moduli possono rimanere accesi.

Start Scan

(3) Fare clic sul pulsante *Scansione*.

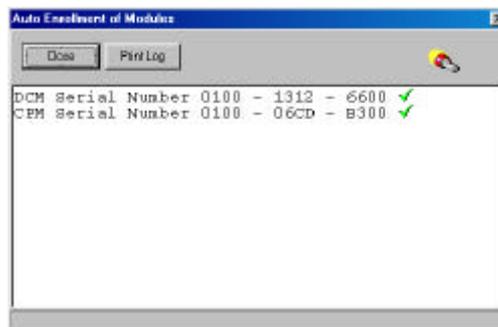
Il sistema cerca il primo modulo nell'elenco. Quando ha trovato il modulo, il LED giallo sul modulo lampeggia e un messaggio sullo schermo informa che il modulo è stato registrato. Un secondo messaggio informerà che il sistema sta cercando il modulo successivo nell'elenco.

(4) Accendere il modulo successivo nell'elenco.

Il sistema cerca il modulo successivo nell'elenco. Quando l'ha trovato, il LED giallo sul modulo lampeggia e un messaggio sullo schermo informa che il modulo è stato registrato. Se ci sono altri moduli nell'elenco, un altro messaggio indicherà che il sistema sta cercando il modulo successivo.

(5) Ripetere l'accensione dei moduli, uno allo volta, finché tutti i moduli sono stati registrati.

Quando il sistema ha registrato l'ultimo modulo nell'elenco, appare sullo schermo un elenco dei moduli registrati (con i relativi numeri di serie).



Close

(6) Fare clic sul pulsante *Chiudi*.

La registrazione si è conclusa con successo e il sistema chiude lo schermo Auto acquisizione dei moduli.

Fase 6 – Configurazione del lettore

Perché il lettore CEK funzioni, deve essere configurato. Bisogna dirgli come funzionare, in modo tale che il sistema sappia come utilizzarlo. La stessa procedura può essere usata per modificare la funzionalità di un CEK configurato precedentemente.

Per configurare il lettore CEK:

1. Nella finestra di dialogo Configurazione Installatore, fare clic con il pulsante destro sul CPM.

Appare un sottomenu con alcune scelte.

2. Selezionare *Proprietà* nel sottomenu.

Selezionando *Proprietà* si apre una finestra di dialogo per il modulo, che contiene etichette e campi di informazione che descrivono il funzionamento del modulo. Ogni campo può essere modificato perché si adatti al funzionamento del modulo.

3. Fare clic sull'etichetta *Lettore*.

4. Riempire i campi dell'etichetta *Lettore* con le informazioni necessarie.

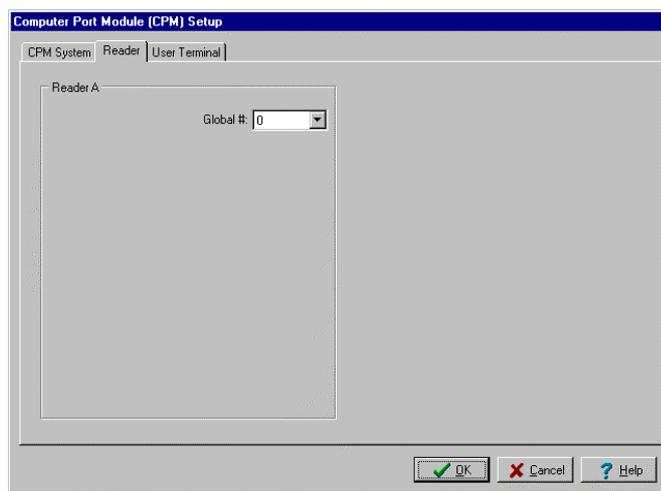
Vedere la parte seguente per le descrizioni dei campi.

5. Al termine, fare clic su *OK*.

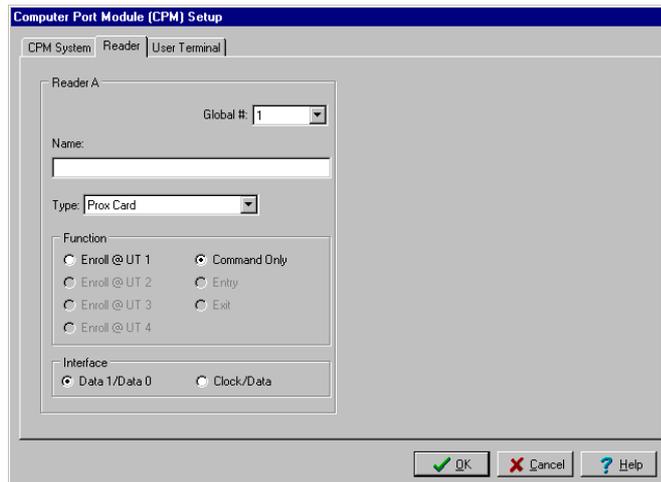
Dopo aver fatto clic su *OK*, si può aggiornare il database per salvare le modifiche. Vedere il paragrafo intitolato "Aggiornamento del Database" in questo capitolo per le relative informazioni.

Etichetta lettore

L'etichetta lettore appare come nell'esempio qui sotto:



Numero globale – Questo campo seleziona il numero della risorsa dal numero totale di risorse disponibili. Quando il numero corrisponde a 0, non viene visualizzato nessun altro campo. Utilizzare l'elenco per selezionare fra i valori disponibili, che sono gli unici visualizzati. Ogni lettore deve possedere un numero globale unico. Dopo aver selezionato un numero globale, l'etichetta lettore appare come nell'esempio seguente:



Nome – Utilizzare questo campo testuale per immettere il nome che si desidera dare al lettore da impostare.

Tipo – Questo campo seleziona il tipo di tecnologia del lettore. Utilizzare il menu per selezionare il tipo di tecnologia desiderata. Per il CEK, scegliere "Prox Card".

Funzione – Questo campo seleziona la funzione del lettore non valido. Impostando questo campo su Lettore di acquisizione al terminale operatore x si seleziona questo lettore per inviare numeri di badge al Terminale operatore indicato ogni volta che l'operatore si trova in un campo nel quale bisogna immettere un badge. In questo modo il lettore può essere usato come Stazione di acquisizione. Impostando questo campo su Lettore di comando, il lettore legge dei badges che attivano un'azione all'interno del sistema. Le azioni possono essere programmate attraverso le impostazioni eventi/azioni del sistema o attraverso le azioni attribuite ai singoli utenti.

Interfaccia – Le specifiche elettriche del lettore collegato a quest'interfaccia devono essere indicate in questo campo. La maggior parte delle unità corrispondono allo standard

Data1/Data0 (protocollo Wiegand). Molti lettori di badges a banda magnetica corrispondono al metodo d'interfaccia Clock/Dati. Specificare il tipo di interfaccia elettrico utilizzato dal lettore che si sta installando selezionando il tipo di interfaccia adeguato.

Etichetta Terminale operatore

Le selezioni comprese in questa etichetta non sono solitamente utilizzate e sono riservate a una versione futura del prodotto.

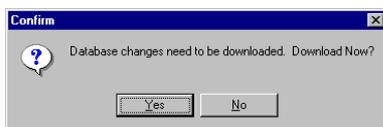
Fase 7 – Aggiornamento del database

L'ultima fase perché il CEK sia operativo, è l'aggiornamento del database.

- Non bisogna dimenticare che il database del sistema PassPoint si trova sulla MLB. E' qui che sono conservati tutti i dati della configurazione del sistema. Quando si apportano delle modifiche al computer, queste non vengono trasmesse contemporaneamente al database sulla MLB, ma vengono conservate in un'area temporanea, finché si aggiorna il database della MLB. Le modifiche apportate sul computer devono essere scaricate nel database della MLB perché diventino effettive.

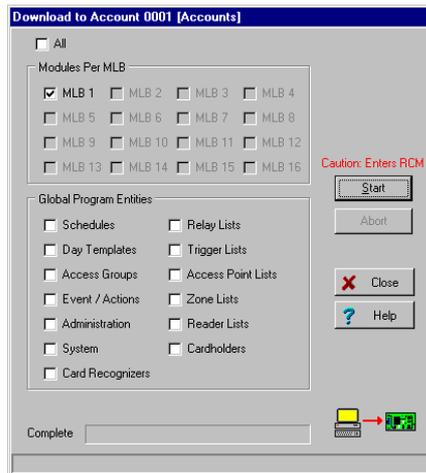
1. Chiudere la finestra di dialogo Configurazione Installatore.

Quando si chiude la finestra, il sistema chiede automaticamente se si vuole aggiornare il database:



2. Fare clic su Sì.

Appare la finestra di dialogo Aggiorna:



Sulla parte superiore della finestra di dialogo, si trova il numero cliente da aggiornare. Assicurarsi di aggiornare il cliente esatto. Esistono anche alcune caselle, per determinare le informazioni da aggiornare. Queste caselle sono selezionate automaticamente dal sistema in base alle opzioni modificate. Se ci sono opzioni specifiche da aggiornare e che non sono state selezionate automaticamente, fare clic sulla casella corrispondente.

3. Fare clic su **Avvio**.

Comincia l'aggiornamento del database. La barra di stato sulla parte inferiore della finestra di dialogo mostra l'avanzamento della procedura. Questa operazione potrebbe richiedere diversi minuti, in base alle dimensioni del database.

Capitolo

11

Aggiunta di un VISTA Gateway Module

Aggiungendo un VISTA Gateway Module (VGM), si fornisce un'interfaccia fra PassPoint e un sistema di allarme anti intrusione ADEMCO VISTA 120. Per determinare se il sistema di allarme VISTA è compatibile con il VGM, consultare i Manuali del sistema di allarme.

Questo capitolo spiega come:

- **Cablare il VGM**
- **Attivare e impostare il VGM**
- **Registrare il VGM in un sistema PassPoint esistente**

Presentazione del VISTA Gateway Module

Quando si utilizza un VGM per collegare PassPoint a una centrale VISTA 120, PassPoint utilizza il selezionatore digitale della centrale di allarme. Gli eventi da trasmettere tramite il selezionatore vengono inviati tramite il VGM alla centrale VISTA 120, che procede all'inoltro delle segnalazioni. La centrale VISTA 120 supporta tutti i codici eventi Contact ID relativi al sistema di controllo accessi. Inoltre, collegando questi due sistemi, si può modificare il comportamento di ogni sottosistema in base ai cambiamenti di stato o agli eventi che si producono. Qui sotto appare un elenco di alcune caratteristiche disponibili utilizzando un VGM come interfaccia fra PassPoint e VISTA 120:

- **I dispositivi radio della VISTA, come i pulsanti a distanza, i trasmettitori, le tastiere senza filo e i rivelatori volumetrici possono controllare le funzioni di accesso.**
- **La quantità di zone presenti nella centrale VISTA espande le capacità di PassPoint.**
- **Gli utenti possono essere programmati per disinserire o inserire entrambi i sistemi.**
- **Le modalità di operazione dei varchi (PROTEGGI, ESCLUDI, o CHIUDI) possono essere controllate dalla tastiera della centrale VISTA.**
- **E' possibile programmare il sistema PassPoint perché, in caso di allarme incendio rivelato nel VISTA, i varchi vengano esclusi, consentendo agli occupanti l'uscita incondizionata dall'edificio e ai vigili del fuoco di entrare nell'edificio.**
- **E' possibile programmare un accesso consentito per disinserire sia la centrale VISTA che la parte intrusione**

del sistema PassPoint, e contemporaneamente attivare altri servizi, quali il riscaldamento o l'illuminazione.

- **E' possibile programmare un ingresso consentito per inserire sia la centrale VISTA che la parte intrusione del sistema PassPoint, e contemporaneamente disattivare altri servizi.**
- **I sistemi già installati con un VISTA 120 o PassPoint possono essere aggiornati facilmente installando il VGM.**

Installazione del VGM

L'installazione e l'acquisizione del VGM in un sistema PassPoint avvengono in sette fasi. Seguire le istruzioni riportate qui sotto e consultare il diagramma di cablaggio fornito.

Fase 1 – Installazione del VGM

Il VGM deve essere situato a prossimità della centrale VISTA. Il VGM dovrebbe essere montato su una parete solida, utilizzando gli appositi ancoraggi (non forniti).

Montare il VGM al muro utilizzando gli ancoraggi.

- **Attenzione a non danneggiare il circuito stampato del modulo al momento del montaggio.**
-

Fase 2 – Collegamento del VGM

Collegare il VGM significa in realtà

- **Collegare il VGM alla centrale VISTA (e all'alimentatore esterno, se utilizzato)**
- **Collegare il modulo VGM alla MLB di PassPoint**

Non accendere il sistema finché non si è finito di collegare tutti i cavi, compresa l'alimentazione. Assicurarsi che il componente che fornisce l'alimentazione al VGM, che si tratti di un alimentatore o di un altro modulo, non sia acceso mentre lo si collega al VGM. Dopo aver completato tutti i collegamenti, sarà possibile accendere il sistema.

Collegare il VGM alla MLB

- 1. Rimuovere completamente l'alimentazione (principale e batteria) a PassPoint e a VISTA.**
- 2. Collegare i due cavi del bus fra la MLB e il VGM.**

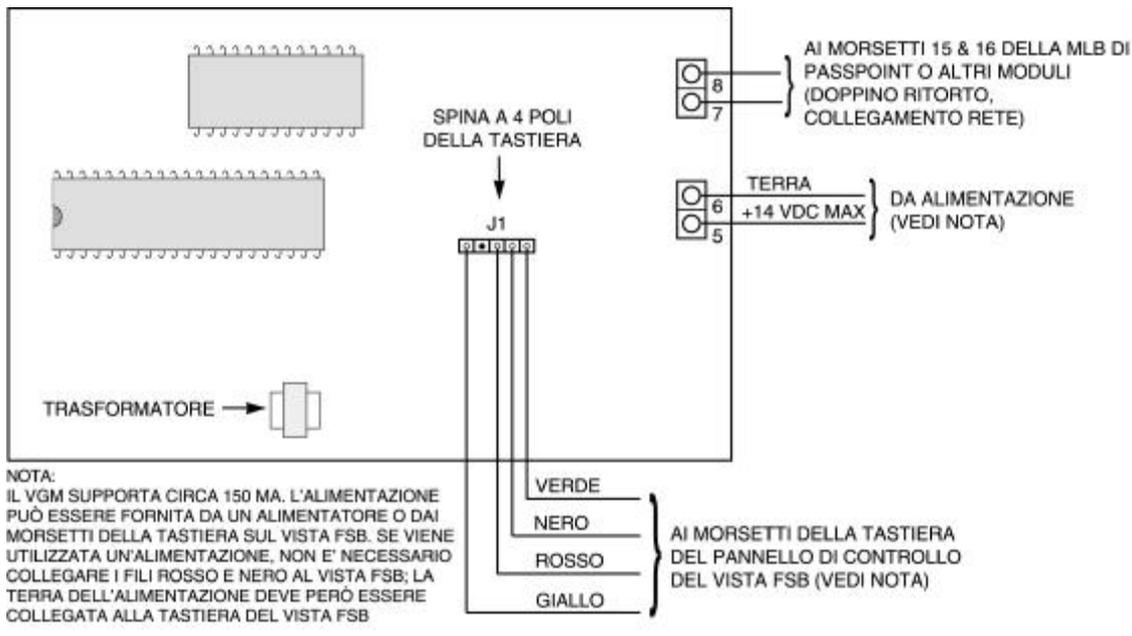
Collegare un cavo fra il morsetto 7 del VGM e il morsetto 16 della MLB.

Collegare l'altro cavo fra il morsetto 8 della VGM e il morsetto 15 della MLB.

Per questi collegamenti, utilizzare dei doppi ritorti. Utilizzare anche i morsetti adeguati per i moduli. Consultare l'appendice A per i particolari.

**Collegamento
del VGM alla
centrale VISTA**

1. Collegare il cavo a 4 morsetti della tastiera (fornito) al connettore J1 del VGM.
2. Collegare i fili verde e giallo nel cavo al bus della tastiera della centrale VISTA.
3. Se si sta utilizzando la centrale VISTA per alimentare il VGM (scelta consigliata), collegare i fili rosso e nero nel cavo al bus della tastiera della centrale VISTA. Se non si sta utilizzando la centrale VISTA per alimentare il VGM, collegare il polo positivo dell'alimentatore al morsetto 5 del VGM e il polo negativo dell'alimentatore al morsetto 6 del VGM e al polo negativo della tastiera della centrale VISTA (nero).
4. Accendere PassPoint e la centrale VISTA.



- Vedere l'appendice per le opzioni di cablaggio.
-

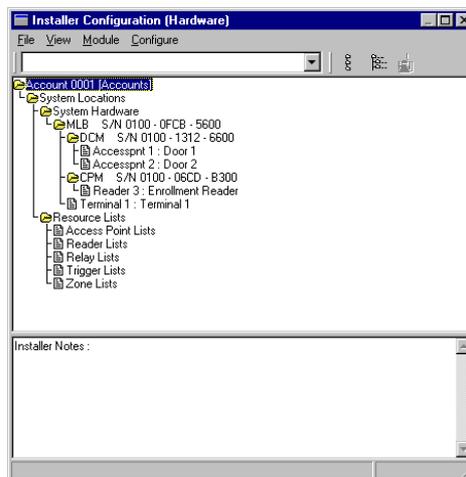
Fase 3 – Aggiunta e impostazione del VGM

Dopo aver alimentato il VGM, è necessario aggiungere il nuovo modulo all'installazione esistente. Seguire le istruzioni riportate di seguito per aggiungere e impostare il VGM:

1. Nel menu *Config*, selezionare *Hardware*.

Appare la finestra di dialogo Configurazione Installatore:

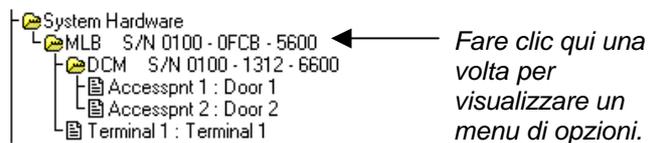
Utilizzare la finestra di dialogo Configurazione Installatore per visualizzare o modificare i componenti del sistema e per impostarne le varie opzioni.



La finestra di dialogo Configurazione Installatore elenca tutte le componenti del sistema ed è qui che si aggiungono i nuovi moduli di sistema.

- Dopo aver inserito le modifiche in questo schermo, aggiornare il database del sistema perché esse diventino effettive.

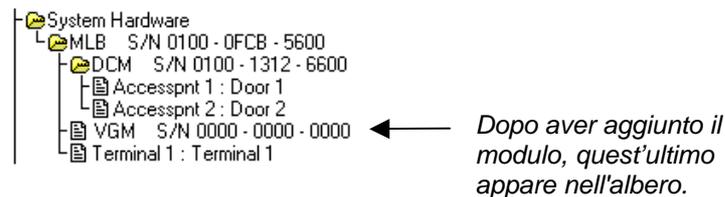
2. Fare clic una volta con il pulsante destro sulla MLB.



Apparirà un menu di opzioni.

3. Nel menu selezionare *Aggiungi VGM*.

L'albero nella finestra di dialogo Configurazione Installatore mostra il nuovo VGM:



Ora bisogna registrare il VGM nel sistema PassPoint, in modo tale che il sistema riconosca il dispositivo e tutte le sue impostazioni di configurazione. Il paragrafo seguente spiega come acquisire il VGM.

Fase 4 – Auto acquisizione del VGM

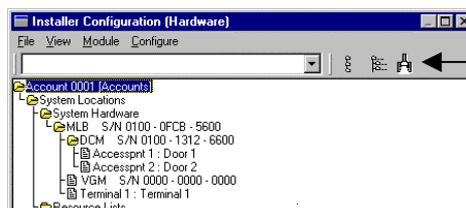
Ogni volta che si aggiunge un nuovo modulo nel sistema, lo si deve anche registrare. La registrazione informa semplicemente il database del sistema della presenza di un nuovo modulo.

Quando si aggiunge un modulo, il sistema cerca tutti i moduli collegati che non siano ancora stati registrati e che riconosce perché hanno numeri di serie che contengono solo zeri. Ad esempio, il VGM che è appena stato aggiunto ha un numero di serie composto da soli zeri, e da nessun altro carattere. Ciò significa che non è stato registrato, e non fa ancora veramente parte del sistema.

Per registrare il VGM appena aggiunto, seguire le istruzioni riportate qui sotto:

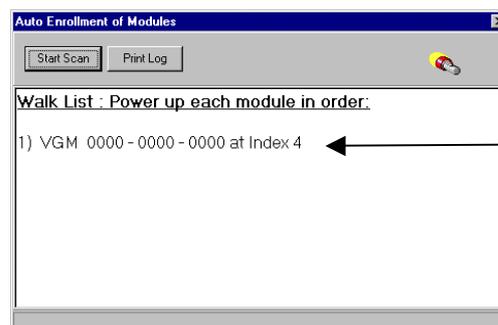
1. Fare clic sul pulsante Auto acquisizione nella finestra di dialogo Configurazione Installatore.

Il diagramma qui sotto mostra dove trovare il pulsante Auto acquisizione:



Pulsante Auto acquisizione

Facendo clic su questo pulsante, si apre la finestra di dialogo Auto acquisizione, come nell'esempio qui sotto:



Il sistema riconosce che esiste un VGM da registrare .

L'acquisizione avviene **automaticamente** premendo il pulsante *Avvia Scansione*, e impiegherà solo qualche istante.

La procedura è diversa quando si registra un solo modulo o quando si registrano più moduli. Per registrare un solo modulo, seguire le istruzioni riportate al punto 2a. Per registrare più moduli, seguire le istruzioni riportate al punto 2b.

2a. Acquisizione di un solo modulo.

Per registrare un solo modulo nel sistema PassPoint, seguire le istruzioni seguenti:

-
- ;

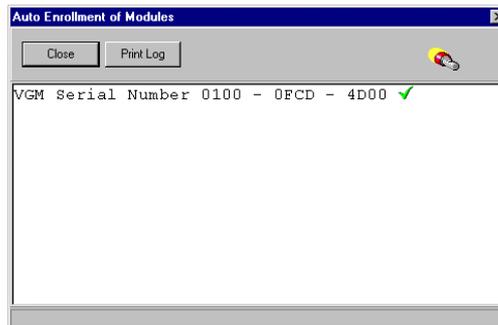
Non spegnere mai la MLB mentre il sistema sta registrando un modulo.

A rectangular button with a thin border and the text "Start Scan" inside.

(1) Premere il pulsante *Avvia Scansione*.

Il sistema ricerca il modulo. Quando lo trova, il LED giallo sul modulo lampeggia, un messaggio indica che il modulo è stato registrato e il sistema smette di cercare altri moduli.

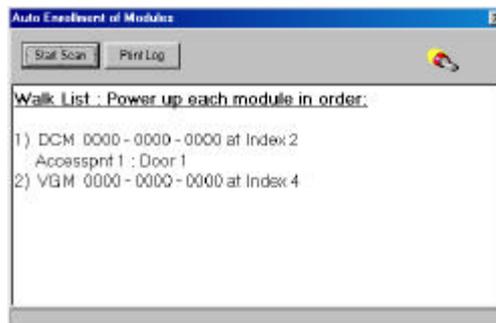
Quando il sistema ha acquisito il modulo, questo appare su uno schermo completo del relativo il numero di serie.

**(2) Premere il pulsante *Chiudi*.**

L'acquisizione si è conclusa con successo e il sistema chiude lo schermo Auto acquisizione dei moduli.

2b. Registrazione di più moduli.

La finestra di dialogo Auto acquisizione dovrebbe essere già presente sullo schermo e dovrebbe apparire come nell'esempio qui sotto per la registrazione di più moduli:



-
-

Se i moduli vengono accesi prima del procedimento di acquisizione o se vengono accesi nell'ordine sbagliato, verranno registrati in modo errato.
Non spegnere mai la MLB durante il procedimento di acquisizione.

Per registrare più moduli nel sistema PassPoint, questi devono essere accessi nell'ordine in cui appaiono nell'elenco. Seguire la procedura seguente per registrare i moduli:

Print Log

(1) Fare clic sul pulsante *Stampa*. Viene stampato un elenco di tutti i moduli da registrare.

(2) Controllare che solo il primo modulo nell'elenco sia acceso.

NOTA: I moduli devono essere accesi nell'ordine in cui appaiono nell'elenco. Assicurarsi che i moduli seguenti siano spenti quando si comincia la registrazione. Dopo aver avviato la scansione e aver acquisito ogni modulo correttamente, lo si può lasciare acceso.

Start Scan

(3) Fare clic sul pulsante *Avvia Scansione*.

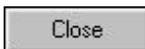
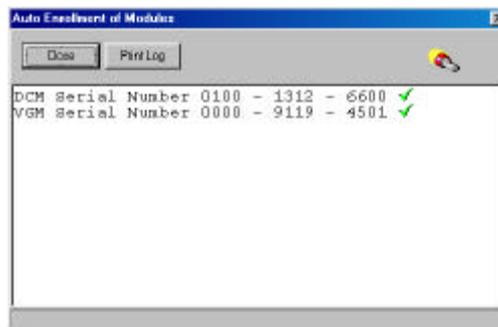
Il sistema cerca il primo modulo nell'elenco. Quando lo ha trovato, il LED giallo lampeggia e un messaggio informa che il modulo è stato acquisito. In seguito, un altro messaggio informa che il sistema sta cercando il modulo successivo nell'elenco.

(4) Accendere il modulo successivo nell'elenco.

Il sistema cerca il modulo successivo nell'elenco. Dopo averlo trovato, il LED giallo sul modulo lampeggia e un messaggio informa che il modulo è stato acquisito. Se ci sono altri moduli nell'elenco, un ulteriore messaggio indicherà che il sistema sta cercando il modulo successivo.

(5) Ripetere l'accensione dei moduli, uno alla volta, finché tutti i moduli sono stati acquisiti.

Quando anche l'ultimo modulo nell'elenco è stato acquisito, appare un elenco dei moduli registrati (con i relativi numeri di serie).



(6) Fare clic sul pulsante *Chiudi*.

L'acquisizione è terminata con successo e il sistema chiude lo schermo Auto acquisizione dei moduli.

3. Fare clic sul pulsante *Chiudi*.

Il numero di serie del VGM viene aggiunto all'elenco nello schermo Configurazione Installatore (Hardware).

Fase 5 – Abilitazione del VGM nella centrale VISTA 120

Per un corretto funzionamento, il VGM deve essere abilitato anche nella centrale VISTA. Consultare la *Guida all'installazione e all'impostazione* della centrale VISTA per conoscere le procedure di attivazione del VGM. Quando si attiva il VGM nella centrale VISTA, prendere nota dell'indirizzo del dispositivo attribuito al VGM, poiché servirà per configurare il VGM in PassPoint.

Fase 6 – Configurazione del VGM

Per far funzionare il VGM, lo si deve configurare correttamente. La configurazione del VGM consiste nell'impostare la programmazione della chiamata di test periodico, programmare il VGM perché agisca come interfaccia, e impostare i controlli delle Zone PassPoint. La stessa procedura può essere usata per modificare le informazioni su un VGM già configurato.

Per configurare il VGM:

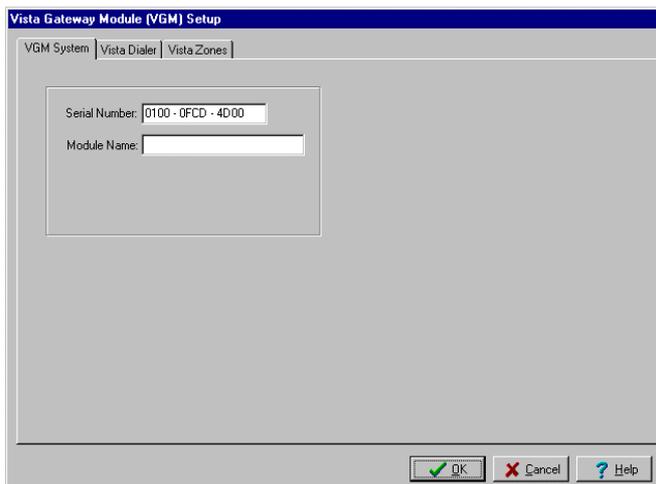
- 1. Nella finestra di dialogo Configurazione Installatore, fare clic con il pulsante destro sul VGM.**

Appare un sottomenu delle scelte.



- 2. Selezionare *Proprietà***

Selezionando *Proprietà*, si apre una finestra di dialogo, che contiene etichette e campi di informazione, che descrivono il funzionamento del modulo. Ogni campo può essere modificato per adattare il funzionamento del modulo alle necessità dell'installazione.

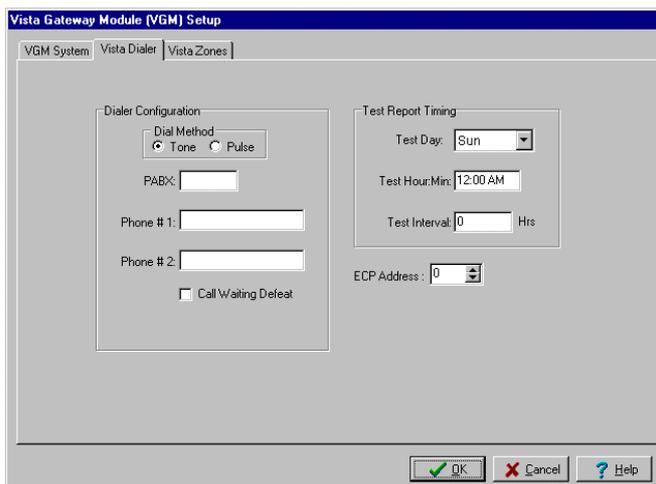


Impostazione del programma orario per le chiamate di test periodico e dell'interfaccia VGM

Per configurare la programmazione delle chiamate di test periodico e il VGM come interfaccia fra PassPoint e VISTA 120, seguire la procedura seguente:

1. Selezionare l'etichetta *Selezionatore Vista* sullo schermo.

Appare lo schermo Configurazione selezionatore qui sotto:



2. Configurare il Programma orario delle chiamate di test periodico del VGM e impostare il VGM perché agisca come interfaccia fra PassPoint e VISTA 120, completando i dati sullo schermo.

I campi sullo schermo consentono di impostare la configurazione nel modo seguente:

Configurazione selezionatore – Tutti i campi in quest'area (Numerazione, PABX, Tel n. 1, Tel n. 2 e Attesa chiamata fallita) possono essere lasciati in bianco. Le funzioni di composizione saranno eseguite dalla centrale VISTA. Notare che quest'area non sarà visibile dopo aver impostato l'indirizzo ECP.

Test periodico – Quest'area campo è utilizzata per impostare le chiamate di test periodico di PassPoint inviate al ricevitore di allarmi. I sottocampi seguenti impostano l'ora della chiamata di prova:

Giorno – Selezionare il giorno della settimana in cui verrà inviata la prima chiamata di prova.

Ora:Minuti – Scegliere l'ora del giorno in cui verrà inviata la prima chiamata di prova.

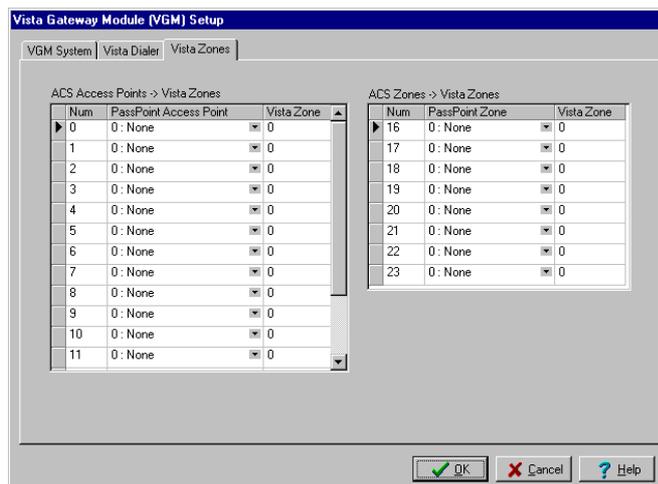
Intervallo test – Immettere il numero di ore che intercorrono fra due chiamate di prova. Non verranno effettuate chiamate se questo campo è impostato su zero.

Indirizzo – Impostare questo campo in modo tale che corrisponda all'indirizzo del dispositivo attribuito al VGM nel bus tastiere della centrale VISTA.

- L'indirizzo deve essere impostato a un valore diverso da zero e deve corrispondere all'indirizzo programmato nella centrale VISTA.
-

Impostazione zone VISTA

Selezionare l'etichetta **Zone Vista** sullo schermo. Apparirà il seguente schermo, utilizzato per la mappatura dei varchi e delle zone PassPoint sulla centrale Vista:



Impostazione Mappatura varchi PassPoint come zone VISTA

16 varchi di PassPoint possono essere riportati alla centrale VISTA, dove possono essere anche trattate come zone multiplexer. In questo modo, è possibile installare un contatto magnetico sulla porta, e contemporaneamente configurare con quella porta un varco PassPoint e una zona allarme VISTA. Il varco verrà riflesso nella centrale VISTA senza dover installare cavi inutili. Quando programmati, gli allarmi porta aperta e temporizzazione porta, con i relativi ripristini e anomalie sono trasmessi da PassPoint alla centrale VISTA. Notare che l'elaborazione degli eventi sui due sistemi può avvenire in modo indipendente. Si possono utilizzare rapporti eventi/azioni su PassPoint per gli allarmi e ripristino varchi, in aggiunta all'inizializzazione allarmi nella centrale VISTA, in base alle modalità di attivazione. Un altro vantaggio dell'impostazione dei varchi come zone VISTA, è che come centrale di allarme, VISTA impedisce l'inserimento con zone aperte, una porta in allarme temporizzazione porta (cioè mantenuta aperta oltre il tempo consentito) impedisce alla centrale VISTA di inserirsi.

I rapporti sui cambiamenti di stato dei varchi vengono inviati alla centrale VISTA come indicato qui sotto:

Stato	MODALITA' VARCO	
	Bloccato, Protetto, e Solo uscita	Escluso
Apertura	Immediatamente se Forzata Immediatamente con temporizzazione porta aperta	Immediatamente su Apertura porta
Ripristino apertura	Immediatamente quando la porta forzata viene richiusa Immediatamente quando la porta in allarme temporizzazione viene richiusa	Immediatamente su Chiusura porta
Anomalia	Immediatamente quando avviene	Immediatamente quando avviene
Ripristino anomalia	Immediatamente quando avviene	Immediatamente quando avviene

Quando si presenta un badge a un varco Bloccato, Protetto o Solo uscita, o se l'apertura della porta avviene entro i parametri di tempo programmati, la centrale VISTA non "vede" mai un'apertura e un ripristino. Se l'operazione sulla porta corrisponde a un allarme porta forzata o a un allarme temporizzazione porta, la centrale VISTA viene informata dell'errore. Il rapporto di stato della zona di un varco escluso impedisce che la centrale VISTA attivi l'allarme in seguito a una condizione di apertura, per un varco escluso che venga tenuto aperto.

- I varchi esclusi o le zone ACS NON causeranno uno stato Apertura, Ripristino apertura, Anomalia o Ripristino anomalia da inviare alla centrale VISTA, causando una mancanza di protezione.

Per configurare il VGM in modo tale che il sistema assimili i varchi di PassPoint alle zone VISTA 120, seguire le seguenti istruzioni:

Il varco da impostare deve essere già stato configurato nel sistema PassPoint prima di cominciare la procedura seguente.

1. **Nell'area dello schermo Mappature varchi -> Zone Vista, posizionare il puntatore sul pulsante con la freccia in basso nella colonna Varco PassPoint per impostare il numero (0-15). Fare clic con il pulsante sinistro del mouse, e dal menu a tenda selezionare il varco desiderato.**
2. **Spostare il puntatore nell'area Zona vista e digitare il numero della zona della centrale VISTA che si vuole attribuire a quel varco di PassPoint.**
3. **Ripetere i punti 1 e 2 per ogni varco (fino a 16) da trasferire alla centrale VISTA.**
4. **Prendere nota della corrispondenza tra varchi e zone VISTA così impostata. Questa informazione servirà poi per programmare la centrale VISTA.**
5. **Consultare la Guida all'Installazione e alla Programmazione della centrale VISTA per programmare le zone che corrispondono ai varchi.**

Impostazione delle Zone di allarme PassPoint come Zone VISTA 120

Per godere di tutti i vantaggi della rete LonWorks di PassPoint, si possono mappare fino a otto zone di allarme PassPoint nelle zone della centrale di allarme VISTA. In questo modo si può trattare una zona che possa essere in prossimità di un modulo PassPoint come se si trattasse di una zona VISTA, senza dover far posare cavi inutili. Per far ciò, PassPoint deve essere configurato per riportare le modifiche negli stati di zona al VGM sulle zone che devono essere trasferite alla centrale VISTA. Aperture zona, ripristini, e anomalie vengono inviati non appena avvengono.

Per configurare il VGM in modo tale che rapporti le zone di PassPoint come zone VISTA, seguire le seguenti istruzioni:

Le zone da configurare devono essere già state configurate nel sistema PassPoint già presenti nella MLB, nei moduli DCM, o negli ZIM prima di cominciare la procedura seguente.

- Le zone PassPoint escluse NON causano stati di Apertura, Ripristino apertura, Anomalie o Ripristino Anomalie da inviare alla centrale VISTA, creando così una mancanza di protezione.

1. **Nell'area Mappatura zone -> Zone Vista dello schermo, posizionare il puntatore sul pulsante con la freccia in basso nella colonna Zona di PassPoint per impostare il numero (16-23). Fare clic con il pulsante sinistro del mouse, e dal menu a tenda selezionare la zona desiderata.**
2. **Spostare il puntatore nell'area Zona Vista e immettere il numero della zona nella centrale VISTA che verrà attribuito a questa zona di PassPoint.**

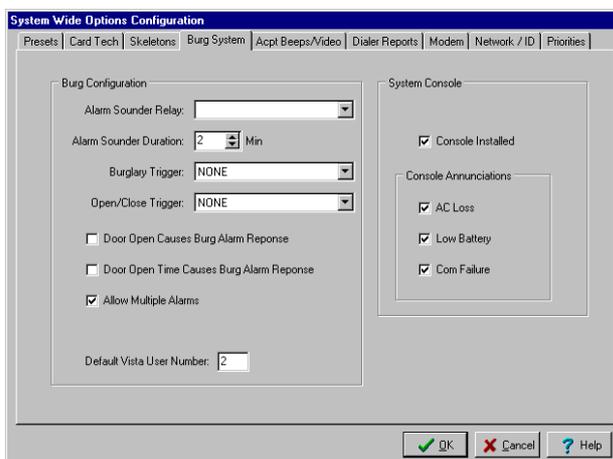
- Il numero di zona VISTA deve essere un valore diverso da zero per una zona mappata in modo corretto.

3. **Ripetere i punti 1 e 2 per ogni zona (fino a 8) da riportare nella centrale VISTA.**
4. **Prendere nota della corrispondenza tra le zone PassPoint e le zone VISTA così impostata. Questa informazione servirà poi per programmare la centrale VISTA.**
5. **Consultare la Guida all'Installazione e alla Programmazione della centrale VISTA per programmare le zone che corrispondono ai varchi.**

Impostazione dell'utente VISTA di default

Tutte le azioni generate da un sistema PassPoint collegato a una centrale di allarme VISTA vengono conservate nella memoria eventi della centrale di allarme. Poiché tutti i comandi sono memorizzati completi del numero dell'utente che le ha generate, ogni comando che il sistema PassPoint invia alla centrale VISTA deve essere associato a un utente VISTA. L'utente VISTA di default impostato in questo campo sarà quindi memorizzato dalla centrale. Per impostare l'utente VISTA di default, seguire le istruzioni qui sotto:

1. **Selezionare *Configura* nella barra dei menu Configurazione Installatore.**
2. **Selezionare *Opzioni generali* nell'elenco del menu Configurazione. Appare lo schermo Configurazione opzioni generali.**
3. **Selezionare l'etichetta *Sistema Intrusione* e appare lo schermo illustrato qui sotto.**



- 4. Il campo Utente Vista di default visualizza un numero 2 (valore predefinito) se il campo non è mai stato modificato. Si può scegliere di conservare il numero 2, se è accettabile, o di immettere un nuovo numero. Al termine premere il pulsante OK.**

Quando si programma la centrale VISTA, è importante ricordare gli elementi seguenti:

- L'Utente impostato in questo schermo deve essere abilitato nella centrale VISTA ad accedere al Settore/Zona al quale si riferisce PassPoint.
- Se si utilizza un ACS PassPoint per inserire o disinserire un settore VISTA, l'Utente deve avere facoltà di inserimento/disinserimento nella centrale VISTA.
- Se si utilizza un badge di PassPoint per generare un evento che risulta in un'azione associata VISTA, l'utente VISTA deve avere gli stessi diritti di realizzare l'azione nella centrale VISTA. Quando l'azione viene riferita a una centrale, l'utente VISTA verrà riportato come l'iniziatore dell'azione.

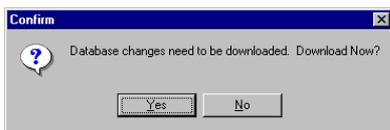
Fase 7 – Aggiornamento del database

L'ultima fase per rendere operativo il VGM è l'aggiornamento del database.

- Non dimenticare che il database del sistema PassPoint si trova nella MLB. E' qui che sono conservati tutti i dati di configurazione del sistema. Quando si effettuano delle modifiche sul programma PassPoint Plus, queste non vengono trasferite automaticamente alla MLB. Vengono conservate in un file temporaneo del computer, finché vengono scaricati nel database della MLB. Tutte le modifiche apportate sul computer devono quindi essere scaricate nel database perché diventino effettive.

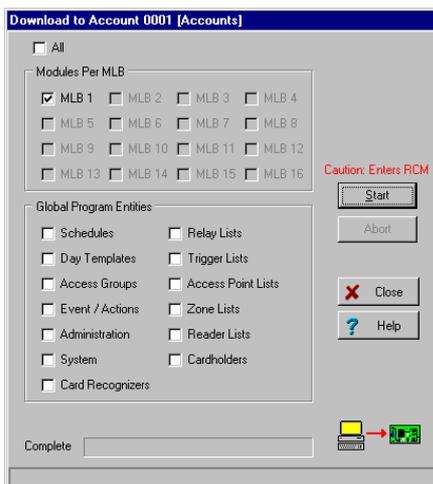
1. Chiudere la finestra di dialogo Configurazione Installatore.

Al momento della chiusura, il sistema chiede automaticamente se si vuole aggiornare il database:



2. Fare clic su Sì.

Appare la finestra di dialogo Aggiorna:



Sulla parte superiore della finestra di dialogo, appare il cliente da aggiornare. Assicurarsi che il cliente sia quello giusto. Sono visualizzate inoltre le caselle per selezionare le informazioni da aggiornare. Queste caselle sono selezionate automaticamente in base alle modifiche apportate. Qualora ci fossero opzioni che si desidera aggiornare e che non sono state selezionate, fare clic nella casella corrispondente.

3. Fare clic su *Avvia*.

Comincia l'aggiornamento del database. La barra di stato sulla parte inferiore della finestra di dialogo informa sull'avanzamento dell'aggiornamento, che potrebbe impiegare diversi minuti, a seconda delle dimensioni del database.

Capitolo

12

Aggiunta di Moduli di sistema

I moduli di sistema sono moduli che non fanno parte dei kit PassPoint e che non sono necessariamente connessi al controllo dei varchi.

Questo capitolo illustra:

- **Quali tipi di moduli possono essere aggiunti al sistema**
- **Come aggiungere e registrare singoli moduli di sistema**
- **Come configurare ogni tipo di modulo di sistema**

Presentazione dei moduli di sistema

Finora è stato spiegato come aggiungere kit al sistema PassPoint per aumentarne le funzionalità. I kit contengono anche moduli, come le MLB e i DCM. Ma il sistema PassPoint può essere espanso anche senza kit, aggiungendo moduli singoli. Ad esempio, se si desidera aggiungere un modulo DCM al sistema, lo si può fare senza aggiungere tutto un Door Expansion Kit. Aggiungendo i moduli separatamente si ottiene maggior flessibilità di espansione del sistema.

Sono disponibili cinque tipi di moduli da aggiungere al sistema, e sono:

- **Door Control Module (DCM)**
- **Quad Relay Module (QRM)**
- **Computer Port Module (CPM)**
- **VISTA Gateway Module (VGM)**
- **Zone Input Module (ZIM)**

-
- Se, aggiungendo i moduli, fosse necessario un alimentatore supplementare, è disponibile anche un alimentatore (ADPTCANPOWER), uguale a quello installato nei kit, ad eccezione del fatto che è montato in un armadio metallico nel quale possono essere alloggiati altri due moduli.
-

Come si aggiunge un modulo a un sistema?

Si devono seguire essenzialmente quattro fasi per aggiungere singoli moduli a un sistema PassPoint esistente. Queste quattro fasi sono uguali per tutti i moduli e sono:

Fase 1 – Installazione del modulo

Fase 2 – Acquisizione del modulo

Fase 3 – Configurazione del modulo

Fase 4 – Aggiornamento del database

Installazione dei moduli

Ogni modulo acquistato è fornito con le proprie istruzioni per l'installazione, che spiegano nei particolari tutte le fasi necessarie per installare un modulo in un sistema PassPoint esistente. Queste istruzioni comprendono anche informazioni per il cablaggio, per il montaggio, ecc. Consultare la documentazione fornita con il modulo per queste operazioni.

Aggiunta e acquisizione di un modulo

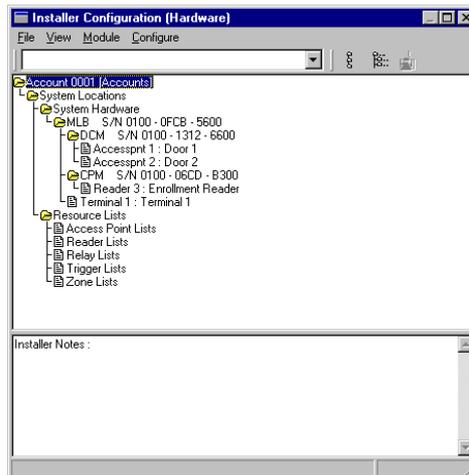
Dopo aver installato fisicamente il modulo, lo si deve aggiungere al sistema e registrare, in modo tale che il sistema sappia che esiste e lo possa riconoscere. Per aggiungere il nuovo modulo al sistema, seguire le istruzioni riportate qui sotto:

Aggiunta di un modulo

1. Nel menu ***Config***, selezionare ***Hardware***.

Appare la finestra di dialogo Configurazione Installatore:

Utilizzare la finestra di dialogo Configurazione Installatore per visualizzare o modificare i componenti del sistema e per impostare le varie opzioni del sistema.

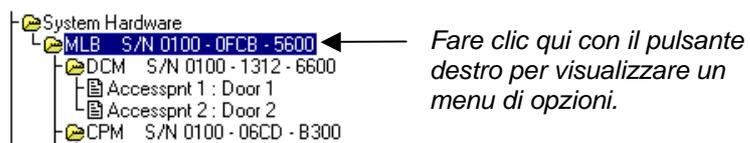


La finestra di dialogo Configurazione Installatore elenca tutti i componenti del sistema ed è qui che si aggiungono nuovi moduli di sistema.

- Dopo aver inserito le modifiche in questo schermo, scaricarle nel database del sistema perché siano effettive.
- ⌋

2. Fare clic una volta con il pulsante destro sulla MLB.

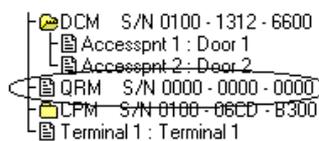
Si apre un menu di opzioni.



3. Nel menu selezionare *Aggiungi QRM* (o *DCM*, *CPM*, *VGM*, o *ZIM*).

NOTA: Appare anche un menu di scelta per un PPM (Printer Port Module – Interfaccia Stampante). Questa scelta non viene utilizzata ed è riservata a versioni future del prodotto.

L'albero nella finestra di dialogo Configurazione Installatore mostra ora il nuovo modulo:



Dopo che è stato aggiunto, il modulo appare nell'albero. In questo esempio, è stato aggiunto un QRM.

Adesso è necessario registrare il modulo in PassPoint, in modo tale che il sistema riconosca il dispositivo e le sue impostazioni di configurazione. Il paragrafo seguente riguarda l'acquisizione del modulo.

Acquisizione di un modulo

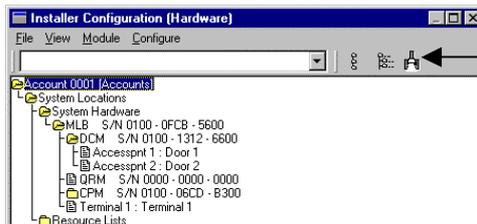
Ogni volta che si aggiunge un modulo al sistema, lo si deve acquisire (o registrare). L'acquisizione informa semplicemente il database del sistema che esiste un nuovo modulo.

Quando si registra un modulo, il sistema cerca tutti i moduli collegati che non siano ancora stati registrati, che riconosce perché i loro numeri di serie contengono solo zeri.

Per acquisire un modulo appena aggiunto, seguire le istruzioni riportate qui sotto:

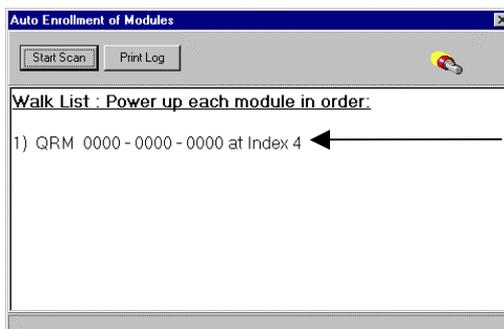
- 1. Fare clic sul pulsante Autoacquisizione sulla finestra di dialogo Configurazione Installatore.**

(Vedere nel disegno qui sotto)



Pulsante Auto
acquisizione

Facendo clic sul pulsante si apre la finestra di dialogo
Autoacquisizione:



Il sistema
riconosce i nuovi
moduli non
ancora registrati

Il procedimento di acquisizione viene fatto **automaticamente** dopo aver premuto il pulsante *Avvia Scansione* e dura solo pochi istanti.

Il procedimento per acquisire un solo modulo è diverso da quello per acquisire più moduli. Per registrare un solo modulo, seguire le istruzioni riportate al punto 2a. Per registrare più moduli, seguire le istruzioni riportate al punto 2b.

2a. Acquisizione di un solo modulo.

Per registrare un solo modulo nel sistema PassPoint, seguire le istruzioni seguenti:

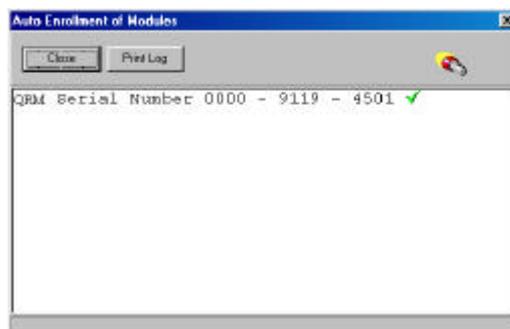
- Non spegnere mai la MLB mentre il sistema sta acquisendo un modulo.

Start Scan

(1) Fare clic sul pulsante *Avvia Scansione*.

Il sistema cerca il modulo. Quando lo trova, il LED sul modulo lampeggia, un messaggio informa che il modulo è stato registrato e il sistema smette di cercare altri moduli.

Dopo aver registrato il modulo, il modulo registrato (con il numero di serie) appare su un nuovo schermo.



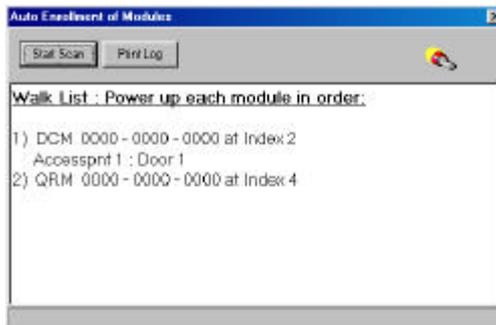
Close

(2) Fare clic sul pulsante *Chiudi*.

L'acquisizione si è svolta con successo e il sistema chiude lo schermo Auto acquisizione di Moduli.

2b. Acquisizione di più moduli.

La finestra di dialogo Auto acquisizione dovrebbe già essere aperta e dovrebbe apparire come nell'esempio qui sotto quando si registrano più moduli:



-
-

Se i moduli vengono accesi prima del procedimento di acquisizione o nell'ordine sbagliato, essi verranno registrati in modo errato.
Non spegnere mai la MLB durante il procedimento di acquisizione.

Per registrare più moduli nel sistema PassPoint, questi devono essere alimentati nell'ordine in cui appaiono nell'elenco. Seguire la procedura seguente per registrare i moduli:



(1) Fare clic sul pulsante *Stampa*. Viene stampato un elenco di tutti i moduli da registrare.

(2) Controllare che solo il primo modulo dell'elenco sia acceso.

NOTA: I moduli devono essere alimentati nell'ordine in cui appaiono nell'elenco. Assicurarsi che i moduli seguenti siano spenti quando si comincia la registrazione. Dopo aver avviato la scansione e aver registrato ogni modulo correttamente, lo si può lasciare alimentato.

Start Scan

(3) Fare clic sul pulsante Avvia Scansione.

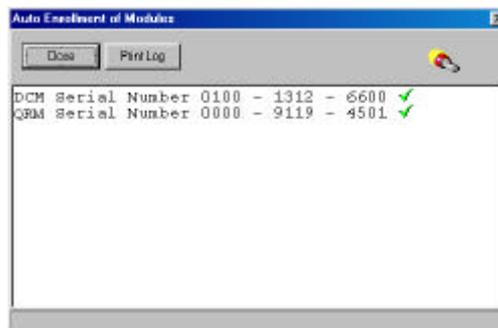
Il sistema cerca il numero di serie del primo modulo nell'elenco. Quando lo ha trovato, il LED giallo lampeggia e un messaggio informa che il modulo è stato registrato. In seguito, un altro messaggio informa che il sistema sta cercando il numero di serie del modulo successivo nell'elenco.

(4) Accendere il modulo successivo nell'elenco.

Il sistema cerca il numero di serie del modulo successivo nell'elenco. Dopo averlo trovato, il LED giallo sul modulo lampeggia e un messaggio informa che il modulo è stato registrato. Se ci sono altri moduli nell'elenco, un altro messaggio indicherà che il sistema sta cercando il modulo successivo.

(5) Ripetere l'alimentazione dei moduli, uno alla volta, finché tutti i moduli sono stati registrati.

Quando anche l'ultimo modulo nell'elenco è stato registrato, appare un elenco dei moduli che sono stati registrati (con relativi numeri di serie).



Close**(6) Fare clic sul pulsante *Chiudi*.**

L'acquisizione si è svolta con successo e il sistema chiude la finestra di Autoacquisizione dei moduli.

2. Fare clic sul pulsante *Avvia Scansione*.

Il sistema cerca il numero di serie del nuovo modulo. Quando lo trova, un messaggio indica che il modulo è stato registrato.

Il sistema smette di cercare i moduli. Se si stava registrando più di un modulo, bisognerà aspettare che il sistema dica che tutti i moduli sono stati acquisiti.

Configurazione dei moduli

Quando si configura un modulo, si forniscono al sistema le istruzioni su come si desidera che il modulo operi e quali funzioni deve eseguire. Ogni tipo di modulo deve svolgere compiti specifici e contenere componenti diversi. Ognuno può determinare come queste componenti devono operare nel sistema.

Oltre ai relè, utilizzati sui DCM e sui QRM, ci sono altre componenti da configurare, come i trigger (per i DCM e i QRM) e le zone (per gli ZIM).

Notare che la procedura descritta per la configurazione dei moduli può essere utilizzata anche per modificare le informazioni su un modulo già configurato.

Per configurare un modulo:

- 1. Nella finestra di dialogo Configurazione Installatore, fare clic con il pulsante destro sul modulo da configurare.**

Appare un sottomenu.

- 2. Selezionare *Proprietà***

Selezionando *Proprietà* si apre una finestra di dialogo relativa al modulo, che contiene etichette e campi d'informazione, che descrivono il funzionamento del modulo. E' possibile modificare ogni campo per adattare il funzionamento del modulo.

- 3. Riempire i campi della finestra di dialogo con le informazioni necessarie.**

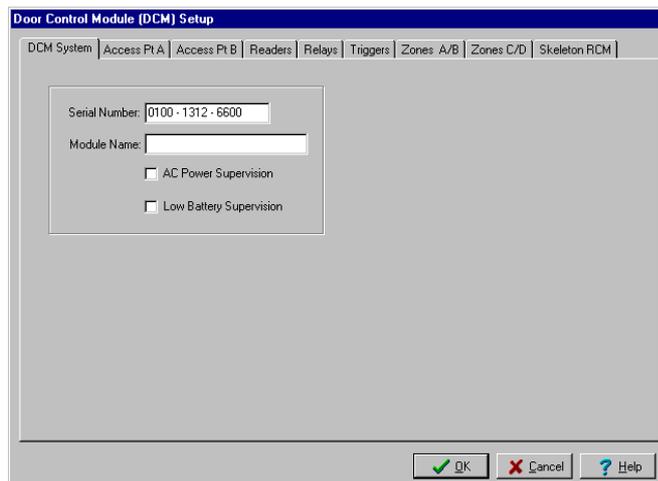
Le etichette e i campi di ogni tipo di modulo sono diversi. Consultare i paragrafi seguenti per trovare la descrizione di ogni campo per il tipo di modulo da configurare.

- 4. Al termine fare clic su *OK*.**

Dopo aver fatto clic su *OK*, si può aggiornare il database per salvare le modifiche. Consultare il paragrafo "Aggiornamento del database" in questo capitolo per ulteriori informazioni a riguardo.

Finestra di dialogo impostazione DCM

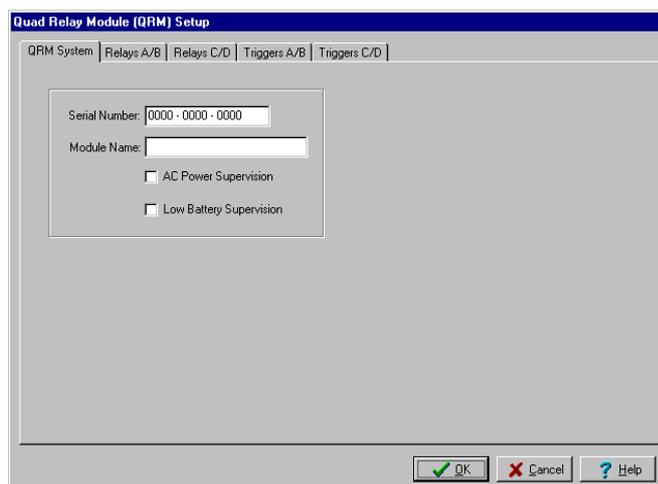
La finestra di dialogo impostazione DCM appare come nell'esempio qui sotto:



La finestra di dialogo contiene nove etichette, ognuna con campi che descrivono le varie funzioni e impostazioni per il controllo del modulo DCM. Consultare il capitolo 9 di questa guida per la descrizione di questi campi.

Finestra di dialogo impostazione QRM

La finestra di dialogo impostazione QRM appare come nell'esempio qui sotto:



La finestra di dialogo contiene cinque etichette, ognuna con campi che descrivono le varie funzioni e impostazioni per il controllo del QRM. Le etichette e i relativi campi sono descritti qui sotto.

Etichetta Sistema QRM

Numero di serie – Si può immettere direttamente il numero di serie del modulo, se lo si conosce. Se il modulo è già stato registrato, il numero di serie è visualizzato in questo campo.

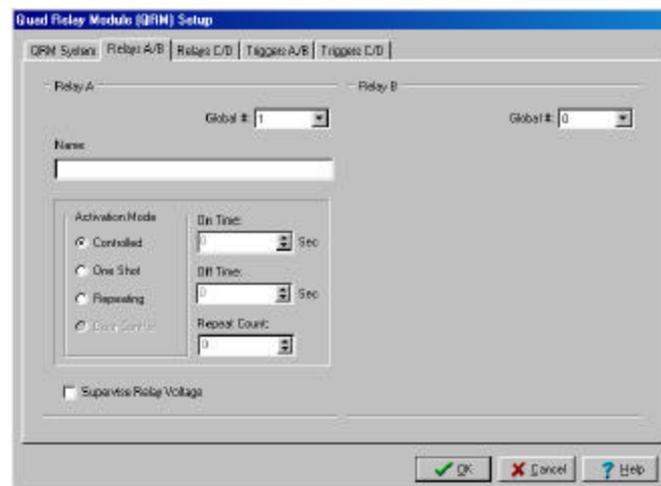
Nome modulo – E' possibile immettere un nome per il modulo, che verrà visualizzato sullo schermo come parte dell'informazione di identificazione del QRM.

Supervisione AC – Quando questo campo è attivato, il modulo informa il sistema quando si trova in una situazione di mancanza di alimentazione di rete. Viene registrato un evento quando l'alimentazione viene a mancare o quando viene ripristinata. Questa funzionalità dovrebbe essere attivata solo su uno dei moduli collegati a un alimentatore che non sia quello di un kit.

Supervisione batteria bassa – Quando questo campo è attivato, il modulo informa il sistema nel caso in cui la batteria di soccorso fosse scarica o guasta. Viene registrato un evento quando si individua una batteria bassa o quando viene ripristinata. Questa funzionalità dovrebbe essere attivata solo su uno dei moduli collegati a un alimentatore che non sia quello di un kit.

Etichette Relè

La finestra di dialogo ha due etichette Relè: una per i relè A/B e una per i relè C/D. Le etichette Relè di A/B e di C/D appaiono come nell'esempio qui sotto:



N. globale – Questo campo seleziona il numero di questa risorsa, da un numero di risorse disponibili. Utilizzare l'elenco per selezionare il valore disponibile. Il sistema mostra automaticamente solo i numeri disponibili. Ogni relè deve avere un numero di relè unico.

Nome – Utilizzare questo campo per immettere un nome per il relè da impostare.

Attivazione – Si può selezionare uno dei tre modi:

- **Fissa:** il sistema o un operatore possono attivare o disattivare il relè.
- **Un impulso:** Quando comandato dal sistema o da un operatore, il relè si attiva per un numero di secondi specifico, poi si disattiva. [1 - 65535 secondi]
- **Ripetuta:** Quando comandato dal sistema o da un operatore, il relè si attiva e si disattiva per un numero di secondi specifico. Questo ciclo si ripete per un numero di volte specifico o all'infinito, finché riceve un comando di arresto.
[Impulso = 1-65535 secondi] [Pausa = 1-65535 secondi]
[Numero di ripetizioni = 0 (Continuo) o 1-65535 ripetizioni]

Impulso – Questo campo è attivo solo se è stato selezionato *Un Impulso* o *Ripetuta* come attivazione. Immettere un periodo di tempo in secondi (1 - 65535) per impostare il tempo di attivazione del relè.

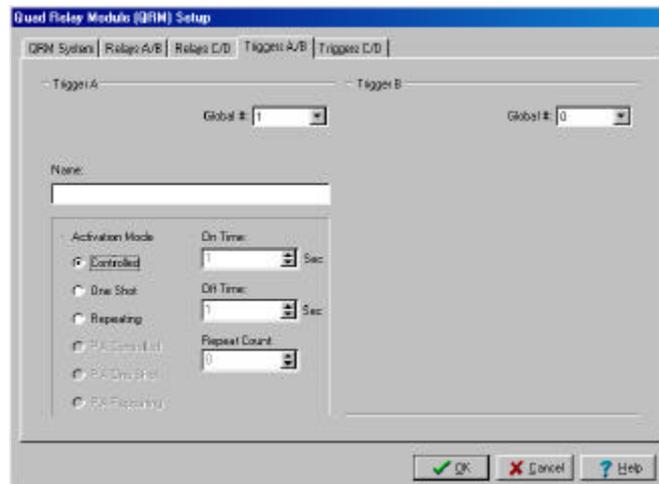
Pausa – Questo campo è attivo solo se è stato selezionato *Ripetuta* come attivazione. Immettere un periodo di tempo in secondi (1 - 65535) per impostare il tempo di disattivazione del relè, prima che esso si attivi di nuovo.

Numero di ripetizioni – Questo campo è attivo solo se è stato selezionato *Ripetuta* come attivazione. Immettere il numero di volte in cui il relè deve ripetere il ciclo attivazione/disattivazione. Si può scegliere un numero qualsiasi compreso tra 0 e 65535. Notare che con il valore 0 il relè ripete il ciclo all'infinito finché interviene un comando di arresto.

Tensione relè supervisionata – Selezionare questo campo se si desidera controllare la tensione collegata al morsetto comune del contatto del relè. Selezionando questo campo, il sistema controlla continuamente la tensione e ne visualizza lo stato su una finestra di stato separata.

Etichette Trigger

La finestra di dialogo ha due etichette Trigger: una per i trigger A&B e una per i trigger C&D. Le etichette Trigger per A/B e per C/D appaiono come nell'esempio qui sotto:



N. globale – Questo campo seleziona il numero di questa risorsa, da un numero di risorse disponibili. Utilizzare l'elenco per selezionare il valore disponibile. Il sistema mostra automaticamente solo i numeri disponibili. Ogni trigger, se non è utilizzato per fornire il preallarme di un varco, deve avere un numero unico.

Nome – Utilizzare questo campo per immettere un nome per il trigger da impostare.

Attivazione – Si può selezionare uno dei tre modi:

- **Fissa:** il sistema o un operatore possono attivare o disattivare il trigger.

- **Un impulso:** Quando comandato dal sistema o da un operatore, il trigger si attiva per un numero di secondi specifico, poi si disattiva. [1 - 65535 secondi]
- **Ripetuta:** Quando comandato dal sistema o da un operatore, il trigger si attiva e si disattiva per un numero di secondi specifico. Questo ciclo si ripete per un numero di volte specifico o all'infinito, finché riceve un comando di arresto.
[Impulso = 1-65535 secondi] [Pausa = 1-65535 secondi]
[Numero di ripetizioni = 0 (Continuo) o 1-65535 ripetizioni]

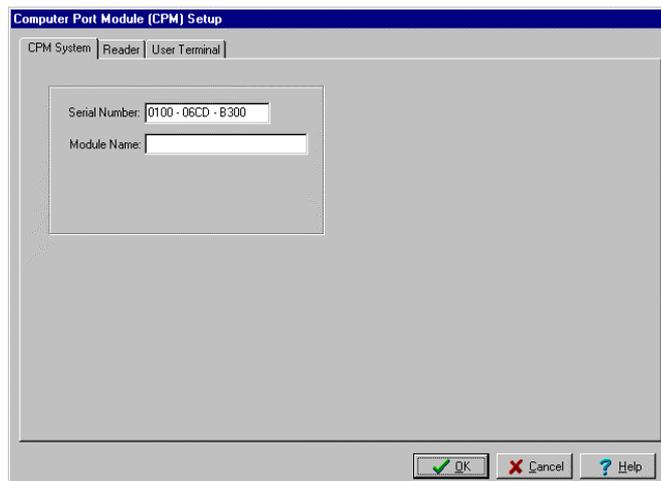
Impulso – Questo campo è attivo solo se è stato selezionato *Un Impulso* o *Ripetuta* come attivazione. Immettere un periodo di tempo in secondi (1 - 65535) per impostare il tempo di attivazione del trigger.

Pausa – Questo campo è attivo solo se è stato selezionato *Ripetuta* come attivazione. Immettere un periodo di tempo in secondi (1 - 65535) per impostare il tempo di disattivazione del trigger, prima che esso si attivi di nuovo.

Numero di ripetizioni – Questo campo è attivo solo se è stato selezionato *Ripetuta* come attivazione. Immettere il numero di volte in cui il trigger deve ripetere il ciclo attivazione/disattivazione. Si può scegliere un numero qualsiasi compreso tra 0 e 65535. Notare che con il valore 0 il relè ripete il ciclo all'infinito finché interviene un comando di arresto.

Finestra di dialogo impostazione CPM

La finestra di dialogo impostazione CPM appare come nell'esempio qui sotto:



La finestra di dialogo contiene tre etichette, ognuna con campi che descrivono le varie funzioni e impostazioni di controllo del CPM. Le etichette e i relativi campi sono descritti qui sotto.

Etichetta Sistema CPM

Numero di serie – Si può immettere il numero di serie del modulo, se lo si conosce già. Se il modulo fosse già stato acquisito, il relativo numero di serie sarà visualizzato in questo campo.

Nome modulo – E' possibile immettere un nome per il modulo, che verrà visualizzato sullo schermo come parte delle informazioni di identificazione del CPM.

Etichetta lettore

N. globale – Questo campo seleziona il numero di risorsa fra i numeri di risorse disponibili. Utilizzare l'elenco per selezionare fra i valori disponibili, gli unici indicati dal sistema. Ogni lettore utilizzato nel sistema deve avere un numero di lettore globale unico, se non è utilizzato per la gestione di un varco.

Nome – Utilizzare questo campo per immettere un nome per il lettore da impostare.

Tipo – Questo campo seleziona il tipo di tecnologia del lettore. Selezionare dal menu a tendina il tipo di lettore utilizzato. Le selezioni disponibili sono:

- **Badge Wiegand**
- **Prox Card**
- **Badge banda magnetica**
- **Solo tastiera**
- **Abbinamento Wiegand/tastiera**
- **Abbinamento Prox/tastiera**
- **Abbinamento banda magnetica /tastiera**

Notare che Solo tastiera e gli abbinamenti NON DEVONO essere usati da un lettore con funzioni di acquisizione.

Funzione – Questo campo seleziona la funzione del lettore non valido. Impostando questo campo come Lettore di acquisizione al Terminale operatore x, si imposta questo lettore per inviare i numeri di badge al Terminale operatore indicato. In questo modo il lettore può essere utilizzato come Stazione di acquisizione. Impostando questo comando a Lettore comando, il lettore viene impostato per accettare badges che attivano azioni all'interno del sistema. Le azioni possono essere programmate tramite le impostazioni eventi/azioni del sistema o attraverso le azioni attribuite ai singoli utenti.

Interfaccia – Le specifiche elettriche del lettore collegato a quest'interfaccia devono essere indicate in questo campo. La maggior parte delle unità sono conformi a Data1/Data0 o Wiegand, cablaggio standard, anche se il lettore non è un lettore di badges Wiegand. Molti lettori di badges a banda magnetica sono conformi all' interfaccia Clock/Dati. Specificare il tipo di

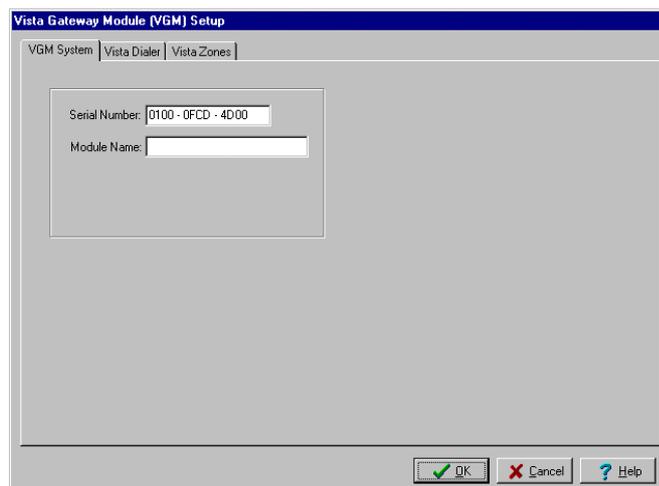
interfaccia elettrico utilizzato dai lettori installati, selezionando il tipo di interfaccia adatto.

Etichetta Terminale operatore

Le selezioni in questa etichetta non sono solitamente utilizzate e sono riservate a future versioni del prodotto.

Finestra di dialogo impostazione VGM

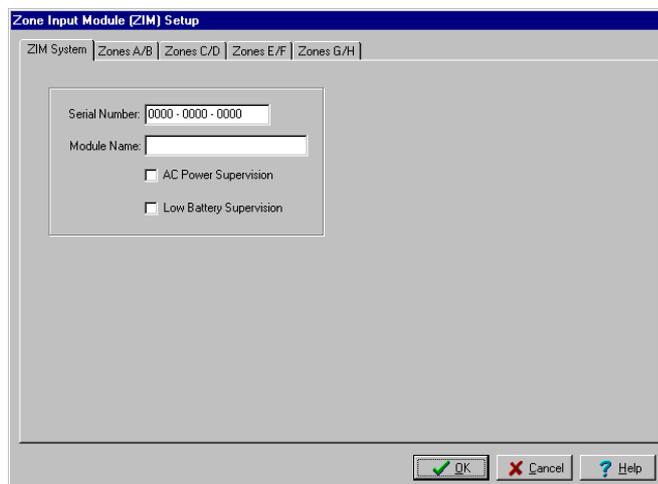
La finestra di dialogo impostazione VGM appare come nell'esempio qui sotto:



La finestra di dialogo contiene tre etichette, ognuna con campi che descrivono le varie funzioni e impostazioni di controllo del VGM. Vedere il capitolo 11 di questa guida per ulteriori informazioni su questi campi.

Finestra di dialogo impostazione ZIM

La finestra di dialogo impostazione ZIM appare come nell'esempio qui sotto:



La finestra di dialogo contiene cinque etichette, ognuna con campi che descrivono le varie funzioni e impostazioni di controllo dello ZIM. Ogni etichetta e i relativi campi sono descritti qui sotto.

Etichetta Sistema ZIM

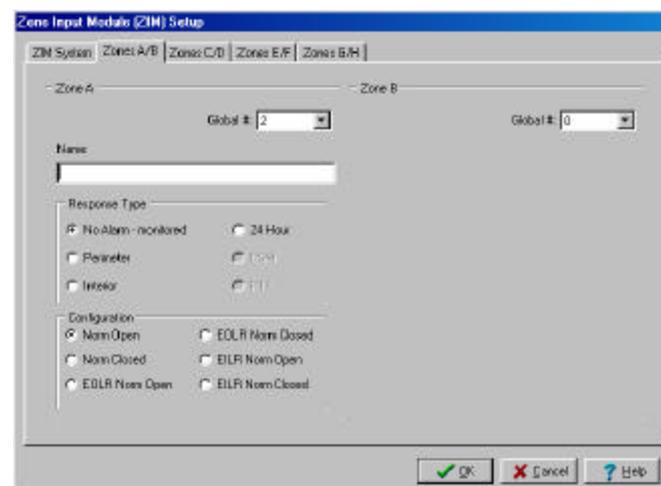
Numero di serie – Si può immettere il numero di serie del modulo, se lo si conosce già. Se il modulo fosse già stato acquisito, il relativo numero di serie sarà visualizzato in questo campo.

Nome modulo – E' possibile immettere un nome per il modulo. Il nome apparirà sullo schermo come parte delle informazioni di identificazione dello ZIM.

Supervisione AC - Quando questo campo è attivato, il modulo informa il sistema quando si trova in una situazione di mancanza di alimentazione di rete. Viene registrato un evento quando l'alimentazione viene a mancare o quando viene ripristinata. Questa funzionalità dovrebbe essere attivata solo su uno dei moduli collegati a un alimentatore che non sia quello di un kit.

Etichette Zone ZIM

La finestra di dialogo ha quattro etichette Zona e ognuna contiene informazioni su due diverse zone. Le etichette zona per A/B, C/D, E/F e G/H appaiono come nell'esempio qui sotto:



- Le zone del sistema PassPoint servono per funzioni supplementari, come la segnalazione di alcune condizioni. Non è stata testata la loro compatibilità UL e quindi non possono essere usati per funzioni di intrusione nelle installazioni UL.

N. globale – Questo campo seleziona il numero della risorsa dal numero totale di risorse disponibili. Utilizzare questo elenco per

selezionare fra i valori disponibili, gli unici indicati dal sistema. Ogni zona utilizzata nel sistema deve possedere un numero globale unico se non è utilizzata per il controllo dello stato di un varco.

Nome – Utilizzare questo campo per immettere un nome della zona che si sta impostando.

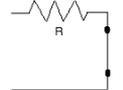
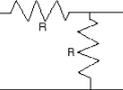
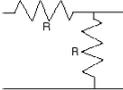
Tipo risposta – Selezionare un tipo di risposta per la zona. E' possibile scegliere fra quattro opzioni diverse:

- **No allarmi - monitorato:** In questo modo la zona può essere vista dal sistema e individuare aperture/ripristini. Questo tipo di zona viene utilizzata principalmente dalle correlazioni eventi/azioni e dagli script del sistema.
- **Perimetro:** Aperture/ripristini di questo tipo di zona sono sempre individuati, ma possono attivare un allarme solo quando il sistema anti intrusione è inserito **TOTALMENTE** o **PARZIALMENTE**. Una zona perimetrale si ripristina quando la zona ritorna nello stato normale.
- **Interno:** Aperture/ripristini di questo tipo di zona sono sempre individuati, ma possono attivare un allarme quando il sistema anti intrusione è inserito **TOTALMENTE**. Tutte le zone interne vengono ignorate temporaneamente per i primi 2 minuti seguenti l'inserimento **TOTALE**. Una zona Interna si ripristina quando la zona ritorna nello stato normale.
- **24 ore:** Aperture/ripristini di questo tipo di zona sono sempre individuati. Si attiva un allarme ogni volta che la zona è aperta indipendentemente dallo stato di inserimento o disinserimento del sistema di allarme. Una zona 24 ore si ripristina non appena la zona ritorna nello stato normale.

Configurazione – Selezionare una configurazione hardware per la zona. Sono disponibili le seguenti opzioni:

- Normalmente aperta
- Normalmente chiusa
- Normalmente aperta con resistenza di fine linea (singolo bilanciamento)
- Normalmente chiusa con resistenza di fine linea (singolo bilanciamento)
- Normalmente aperta con doppio bilanciamento
- Normalmente chiusa con doppio bilanciamento

NOTA: le zone a singolo e doppio bilanciamento necessitano di resistenze di terminazione da 2KOhm.

Stato sensore normale	STATI ZONA					
	ZONA A DUE STATI (non bilanciata)		ZONA A TRE STATI (bilanciata)		ZONA A QUATTRO STATI (doppio bilanciamento)	
	Norm. Aperta (N.O.)	Norm. Chiusa (N.C.)	Norm. Aperta (N.O.)	Norm. Chiusa (N.C.)	Norm. Aperta (N.O.)	Norm. Chiusa (N.C.)
0 (corto circuito)	APERTA	CHIUSA	APERTA	GUASTA	GUASTA (corto circuito)	GUASTA (corto circuito)
R	-	-	CHIUSA	CHIUSA	APERTA	CHIUSA
2R	-	-	-	-	CHIUSA	APERTA
infinito (circuito aperto)	CHIUSA	APERTA	GUASTA	APERTA	GUASTA (circuito aperto)	GUASTA (circuito aperto)
Connessioni sensore						
ZONE MLB	√	√	√	√		
ZONE DCM	√	√	√	√		
ZONE ZIM	√	√	√	√	√	√

Aggiornamento del Database

L'ultima fase nella registrazione del modulo è quella di aggiornare il database.

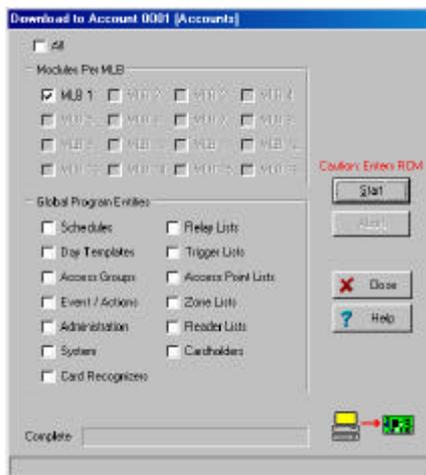
1. Chiudere la finestra di dialogo Configurazione Installatore.

Il sistema chiederà automaticamente se si vuole aggiornare il database.



2. Fare clic su Sì.

Appare la finestra di dialogo Aggiorna. Sulla parte superiore della finestra appare il numero cliente da aggiornare. Verificare che si tratti del cliente giusto. Alcune caselle che indicano le informazioni che saranno aggiornate. Queste caselle sono selezionate automaticamente, in base alle opzioni che sono state modificate.



Se si desidera aggiornare opzioni che non siano state selezionate automaticamente, è possibile selezionarle facendo clic nelle apposite caselle.

3. Fare clic su *Avvio*.

Comincia l'aggiornamento del database.

Appendice

A

Istruzioni di cablaggio

Installando il sistema PassPoint, è necessario prendere in considerazione diversi fattori cablaggio. Questa appendice spiega le varie topologie di cablaggio e fornisce i dettagli sulle varie specifiche.

Istruzioni di cablaggio

Prima di posizionare i diversi componenti del sistema, è importante capire le modalità di cablaggio del sistema stesso.

Tutti i moduli di sistema comunicano con la Main Logic Board attraverso una rete a doppino ritorto. Questo collegamento consente la comunicazione con un numero massimo di 126 moduli periferici. Ciascun modulo collegato in rete viene detto “nodo”. Quando si utilizza un pacchetto PassPoint Starter Kit, si hanno a disposizione due nodi: MLB e DCM, entrambi con numeri di serie propri. Il sistema può essere espanso con moduli aggiuntivi: ad esempio, è possibile aggiungere un altro modulo DCM per controllare due varchi supplementari.

Per il cablaggio del sistema e la scelta dei punti di installazione dei componenti, è necessario tenere conto di diversi fattori, descritti nelle pagine successive.

-
- -

Il metodo di cablaggio e le posizioni di installazione consigliati nel manuale sono conformi al National Electrical Code ANSI/NFPA 70.

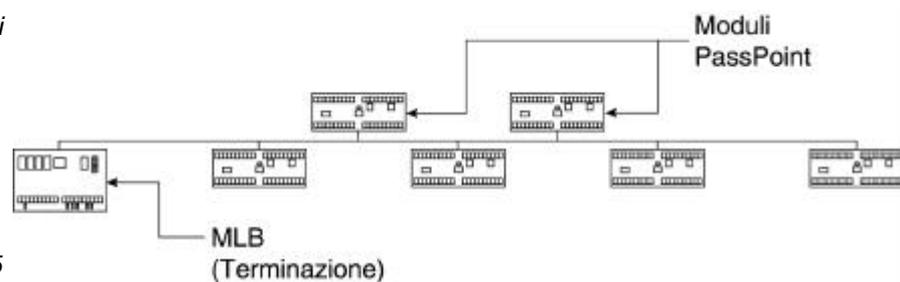
Topologia

La tecnologia di cablaggio con doppino ritorto non schermato è concepita per offrire la massima libertà di cablaggio, potendo gestire topologie di collegamento in cascata, a stella, ad anello e le relative combinazioni. I moduli PassPoint possono essere posizionati in qualsiasi punto lungo il cablaggio di rete.

Questa funzionalità semplifica l'installazione e l'aggiunta di moduli per eventuali espansioni del sistema. Le cinque diverse topologie di cablaggio sono illustrate nelle figure successive.

Questa topologia di cablaggio viene terminata in corrispondenza della MLB utilizzando una resistenza da 52,3 ohm applicata sui terminali di rete (15 & 16) della scheda MLB.

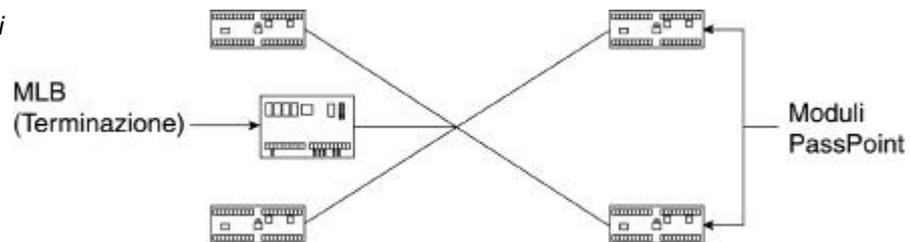
NOTA: lunghezza cavo totale \leq 500 metri



Topologia in cascata a terminazione singola

Questa topologia di cablaggio viene terminata in corrispondenza del modulo MLB utilizzando una resistenza da 52,3 ohm applicata sui terminali di rete (15 & 16) della scheda MLB.

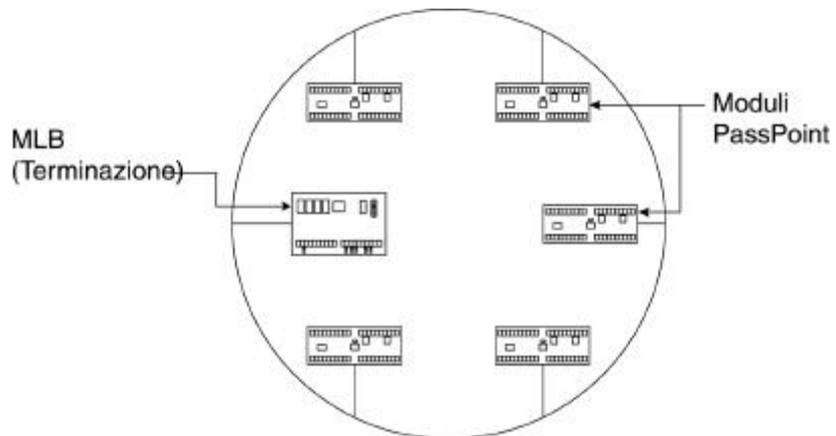
NOTA: lunghezza cavo totale \leq 500 metri



Topologia a stella

Questa topologia di cablaggio viene terminata in corrispondenza del modulo MLB utilizzando una resistenza da 52,3 ohm applicata sui terminali di rete (15 & 16) della scheda MLB.

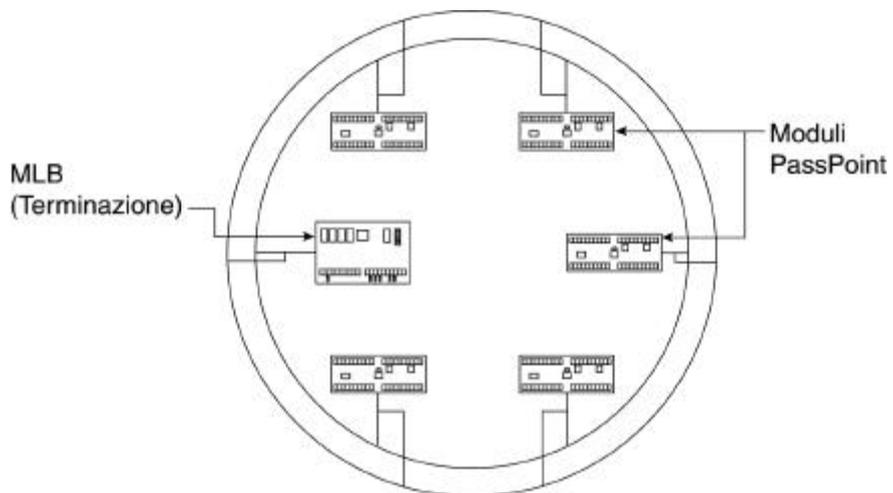
NOTA: lunghezza cavo totale ≤ 500 metri



Topologia ad anello

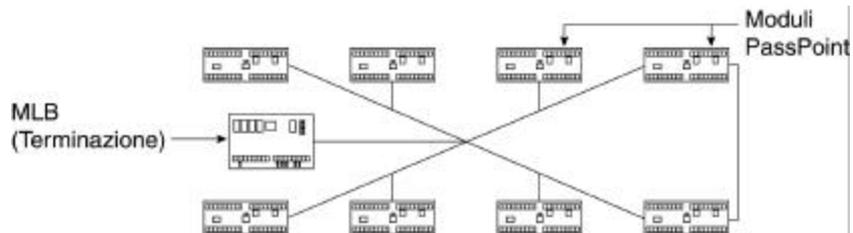
Questa topologia di cablaggio viene terminata in corrispondenza del modulo MLB utilizzando una resistenza da 52,3 ohm applicata sui terminali di rete (15 & 16) della scheda MLB.

NOTA: lunghezza cavo totale ≤ 500 metri



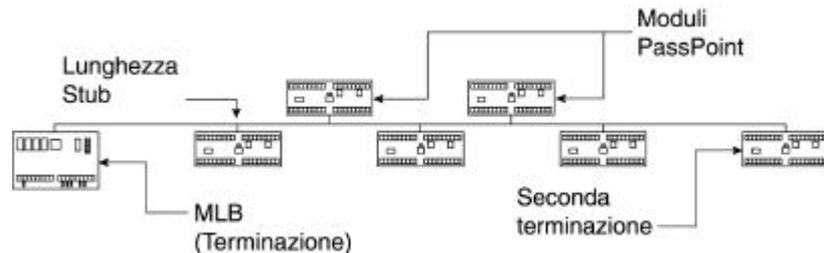
Topologia ad anello ridondante

Questa topologia di cablaggio viene terminata in corrispondenza del modulo MLB utilizzando una resistenza da 52,3 ohm applicata sui terminali di rete (15 & 16) della scheda MLB.
 NOTA: lunghezza cavo totale <= 500 metri



Tecnologia combinata anello/cascata

Questa topologia di cablaggio viene terminata utilizzando una resistenza da 105 ohm applicata sui terminali di rete dei due moduli più lontani. La scheda MLB non deve essere necessariamente uno dei punti terminali.
 NOTA: lunghezza cavo totale <= 500 metri



Topologia in cascata a terminazione doppia

Specificata a topologia libera:

(terminazione singola in cascata, a stella, ad anello o combinata ad anello/cascata)

Tabella 1:

Tipo di cavo	Distanza max. nodo-nodo	Lunghezza max. cavo totale
Belden 85102	500 metri	500 metri
Belden 8471	500 metri	500 metri

Level IV, 22 AWG 500 metri 500 metri
(0,32 mmq)

Specifiche bus a terminazione doppia:

Tipo di cavo	Lunghezza bus max.
Belden 85102	2.700 metri
Belden 8471	2.700 metri
Level IV, 22 AWG (0,32 mmq)	1.350 metri

-
- Quando si definisce lo schema di cablaggio, è importante ricordare che l'uso di cavi schermati riduce drasticamente le lunghezze massime consentite.

Cablaggio RS-232:

Cavo standard null-modem, 9 poli, schermato, 22 AWG (0,32 mmq), 15 metri massimo

-
- Consultare gli schemi di cablaggio nel Capitolo 3 se è necessario l'utilizzo di un cavo RS-232 più lungo.

Cablaggio tastiera:

22 AWG (0,32 mmq), 1 metro
(La tastiera deve essere installata esclusivamente sull'armadio e non cablata attraverso i locali.)

Cavo di rete:

Utilizzare un cavo di rete a tre conduttori con sezione minima 1 mmq

Potenza dell'elettroserratura:

Dipende dalla sezione del cavo e dai requisiti del chiavistello o della serratura magnetica. Solitamente circa 150 metri di cavo 16 AWG (1,3 mmq) per 350mA di corrente.

Interfacce lettori:

70 metri di cavo sezione 22
100 metri di cavo sezione 20
150 metri di cavo sezione 18

Codice cromatico delle resistenze di terminazione:

52.3 Ohm - Verde, Rosso, Arancio, Oro, Marrone
105 Ohm - Marrone, Nero, Verde, Nero, Marrone
2 kOhm – Rosso, Nero, Marrone

Note di cablaggio

Mantenere i cablaggi di lettori, bus Echelon e RS-232 distanti da qualsiasi cablaggio con corrente elevata. Questo vale in particolare per le serrature delle porte e per qualsiasi cablaggio dell'edificio che fornisce potenza a carico "rumoroso" (gruppi elettrogeni, frigoriferi, ecc.).

-
-

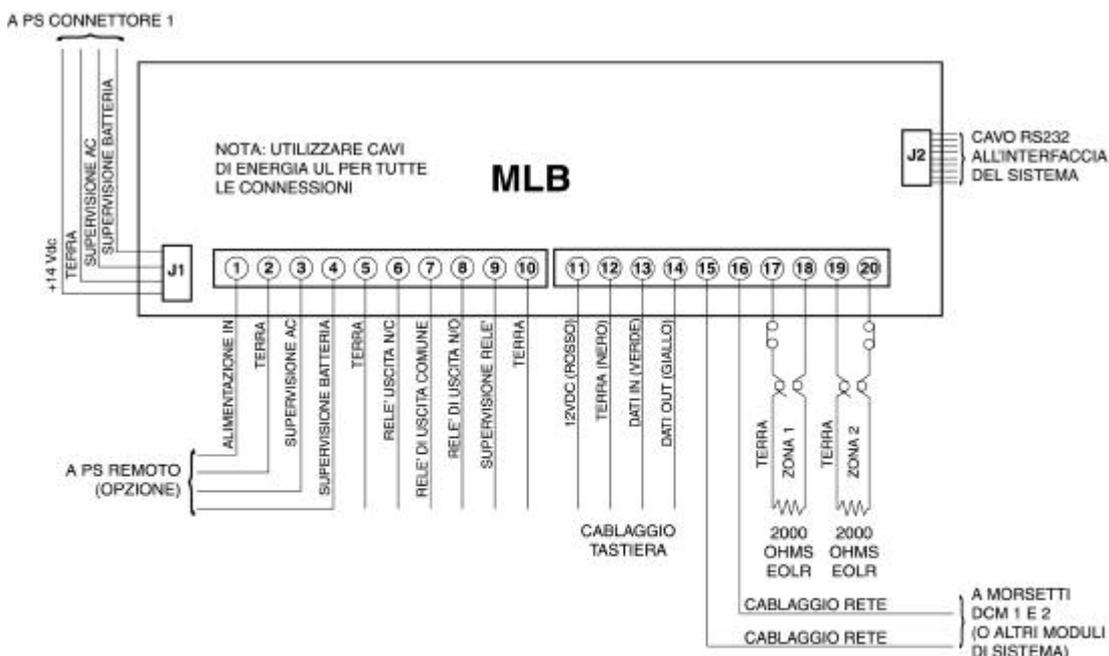
Si consiglia di utilizzare un soppressore elettrico (mod. ANS4) per proteggere le serrature delle porte e i contatti dei relè da eventuali transitori. Installare un soppressore il più vicino possibile alla serratura ed un secondo soppressore sui terminali del relè di comando della serratura.

Specifiche dei cavi

Tipo di cavo	Diametro cavo/sezione	R. loop Ohm/km	C nF/km	Vprop % di c
Belden 85102 Doppino ritorto singolo, trefoli 9/29, non schermato, plenum	1,3mm/16AWG (1,3 mmq)	28	56	62
Belden 8471 Doppino ritorto singolo, trefoli 9/29, non schermato, non- plenum	1,3mm/16AWG (1,3 mmq)	28	72	55
Level IV 22AWG (0,32 mmq) Doppino ritorto singolo, tipicamente compatto e non schermato	0,65mm/22AWG (0,32 mmq)	106	98	41
JY (St) Y 2x2x0.8 4 poli ritorto a elica, compatto, schermato	0,8mm/20AWG (0,5 mmq)	73	98	41

Cablaggio della Main Logic Board

Cablare la MLB come mostrato nello schema seguente:



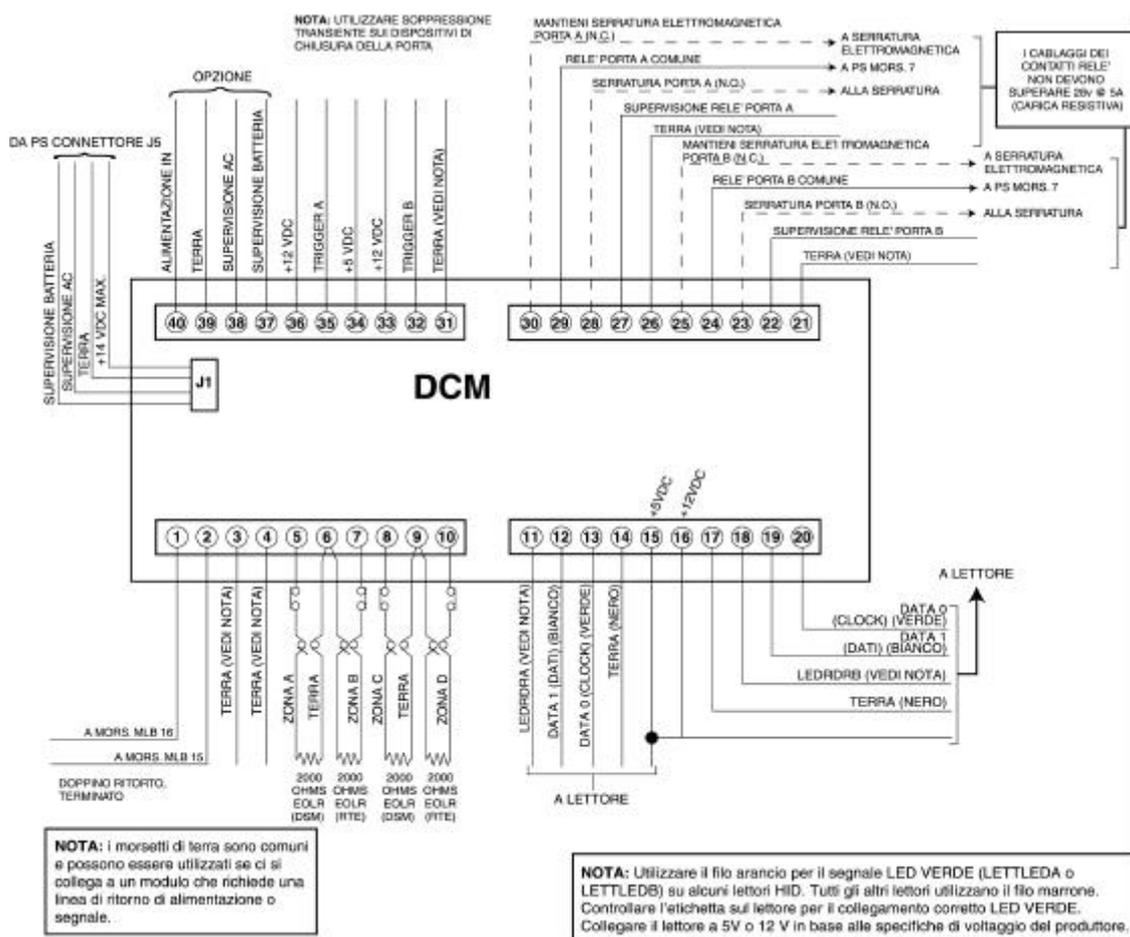
Supporto batteria MLB ADEMCO N. N7673. Batteria litio 3V, durata in standby: 10 anni.

ATTENZIONE - Pericolo di esplosione se la batteria viene sostituita in modo sbagliato. Sostituire solo con una batteria uguale o equivalente, consigliata dal produttore. Gettare le batterie usate secondo le istruzioni del produttore. Tipo di batteria: batteria litio 2025.

QUESTE ATTREZZATURE DEVONO ESSERE INSTALLATE IN CONFORMITA' CON LE NORME ANTINCENDIO 70 & 74 (NATIONAL FIRE PROTECTION ASSOC., BATTERY MARCH PARK, QUINCY, MA. 02269). QUESTA ATTREZZATURA DEVE ESSERE FORNITA CON TUTTE LE INFORMAZIONI RIGUARDANTI LA CORRETTA INSTALLAZIONE, OPERAZIONE, TEST, MANUTENZIONE, PIANO DI EVACUAZIONE E SERVIZIO DI RIPARAZIONE.

Cablaggio del Door Control Module

Cablare il modulo DCM come mostrato nello schema seguente:



Specifiche di alimentazione

Trasformatore (codice prodotto ADAT18C): 220VAC PRIM. (60 Hz)
18VAC 50VA SEC.

Nota: Collegare il trasformatore ad un interruttore differenziale magnetotermico dedicato.

Uscita regolatore di commutazione: 13,3V +/- 1.2Vcc
con tensione di ingresso: 200-240Vca
ripple 600mVpp

Regolatore lineare per uscita potenza locale: 13,7Vcc @ 450mA

Corrente di uscita totale alimentatore: 1,8A +/- 200mA

Corrente max. serratura: 900mA

Uscita potenza logica locale J1: 450mA max.

Uscita potenza logica J5: 450mA max.

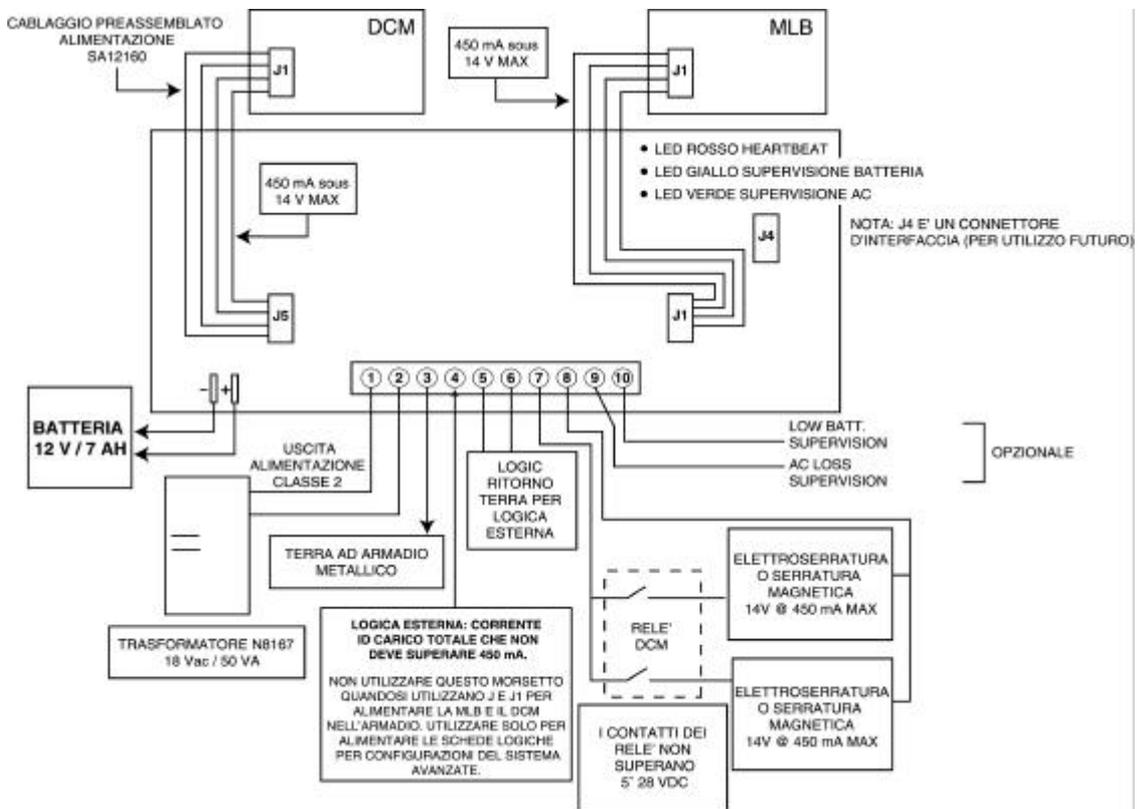
Batteria tampone: 12Vcc/7Ah



Il collegamento ai terminali 9 e 10 non è necessario per la supervisione della tensione di rete e della batteria se si utilizzano i cavi in dotazione collegati ai connettori J1 e J5. In caso contrario, collegare i morsetti di supervisione Low Battery e AC Loss dell'alimentatore ai morsetti di supervisione Low Battery e AC Loss dei moduli di sistema. Sono disponibili uscite di supervisione AC Loss e Low Battery per la supervisione di due moduli PassPoint.

Indicatori stato di sistema:

- LED Mancanza rete: Verde
- LED Batteria bassa: Giallo
- LED Heartbeat: Rosso



Appendice

B

Aggiornamento del Firmware

Grazie alla Flash Eprom installata sulla MLB, è possibile eseguire aggiornamenti del firmware, purchè il vecchio firmware sia compatibile con la versione più recente del software PassPoint. Questa appendice fornisce tutte le procedure per aggiornare il firmware della MLB di PassPoint.

IMPORTANTE: Non sostituire mai il firmware della MLB a meno che non venga richiesto specificatamente.

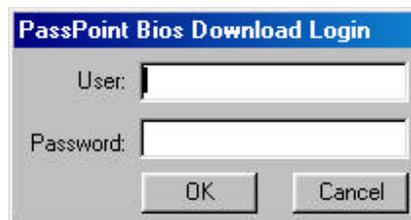
Aggiornamento Firmware MLB

Quando è necessario aggiornare un firmware di un'installazione, i nuovi dati MLB verranno forniti in un file con estensione .MLB. Nel caso in cui il firmware facesse parte di un aggiornamento del programma PassPoint, il firmware è contenuto in una sottocartella PassPoint chiamata Aggiornamenti.

Per aggiornare nuovi firmware MLB, seguire la procedura descritta qui sotto:

- 1. Chiudere PassPoint Plus.**
- 2. Fare clic sul pulsante Avvio di Windows.**
- 3. In Programmi, andare in PassPoint Plus e selezionare Aggiornamento firmware MLB.**

L'aggiornamento firmware MLB si carica e appare lo schermo seguente:

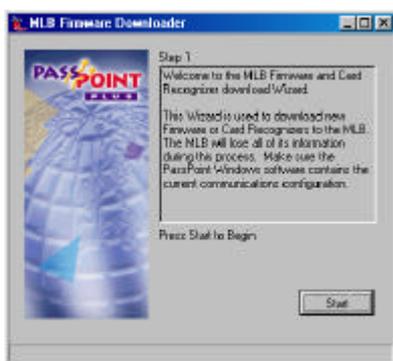


- 4. Immettere il nome operatore e la password.**

Il nome operatore e la password sono quelli impostati come nome operatore e password dell'Installatore in PassPoint Plus.

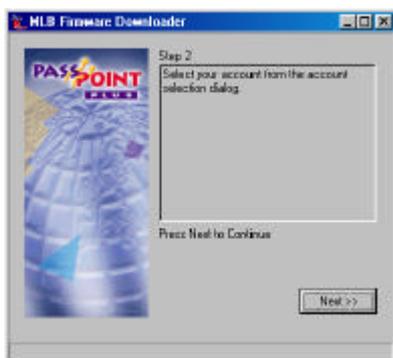
- 5. Fare clic su OK.**

Appare lo schermo seguente Aggiornamento firmware MLB:



6. Fare clic su *Avvio*.

Appare il seguente schermo Aggiornamento firmware MLB:



7. Fare clic su *Successivo*.

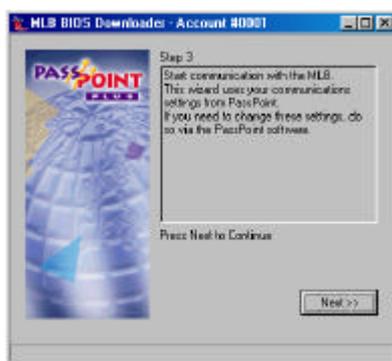
Appare il seguente schermo Navigatore clienti:



- 8. Selezionare il cliente della MLB che deve ricevere l'aggiornamento del firmware con il metodo a. o b.:**
- Se nel computer è stata impostata una sola MLB, il cliente viene selezionato automaticamente.**
 - Se il computer controlla diverse MLB (clienti), si possono individuare i clienti nel modo seguente:**
 - Fare clic sulla freccia in basso che si trova a destra del campo *Trova per*. Appare un elenco, nel quale selezionare se cercare per nome o numero cliente.**
 - Selezionare il metodo di ricerca che si desidera.**
 - Nel campo *Trova*, immettere il nome o numero cliente desiderato. Quando si inseriscono i dati, il sistema visualizza il termine che più si avvicina nel database. Quando viene visualizzato il cliente corretto nella finestra *Trova*, smettere di immettere i dati.**

9. Fare clic su *OK*.

Si apre il cliente selezionato, il computer si collega alla MLB, e appare il seguente schermo Aggiornamento Firmware MLB:



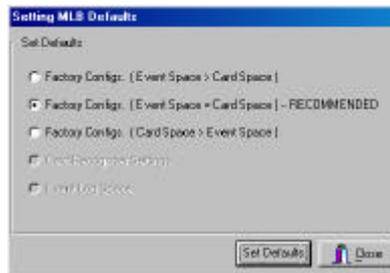
10. Fare clic su *Successivo*.

Appare il seguente schermo Aggiornamento firmware MLB:



11. Fare clic su *Successivo*.

Appare il seguente schermo Impostazione MLB a default:

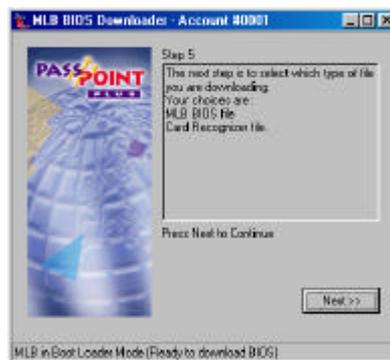


12. Fare clic sulle *Config. di fabbrica desiderate.*

NOTA: Consigliamo di utilizzare le Configurazioni di fabbrica già selezionate.

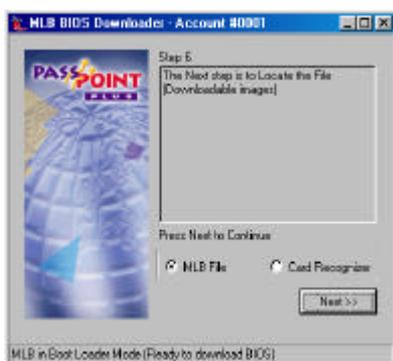
13. Fare clic su *Imp. default.*

La MLB si resetta alle impostazioni di default selezionate. Dopo che la MLB si è resettata (2 minuti circa), appare il seguente schermo Aggiornamento firmware MLB:



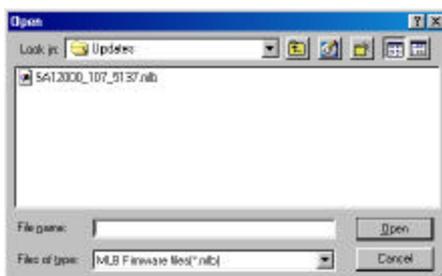
14. Fare clic su *Successivo.*

Appare il seguente schermo Aggiornamento firmware MLB:



- 15. Lo schermo ha già selezionato *File MLB*. Lasciare questa selezione tale e quale e premere *Successivo*.**

Appare il seguente schermo Apri:



La directory è già impostata su Aggiorna. Se questa directory non corrisponde a quella nella quale si trova l'aggiornamento firmware MLB, modificare con i dati corretti.

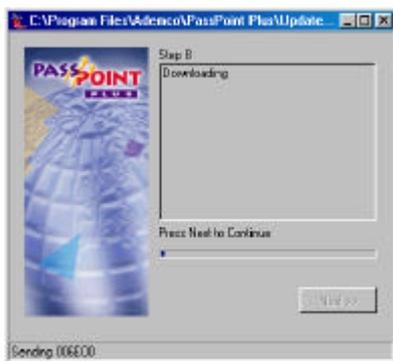
- 16. Fare clic sul nome del file di aggiornamento del firmware MLB e fare clic su *Apri*.**

Appare il seguente schermo Aggiornamento firmware MLB:

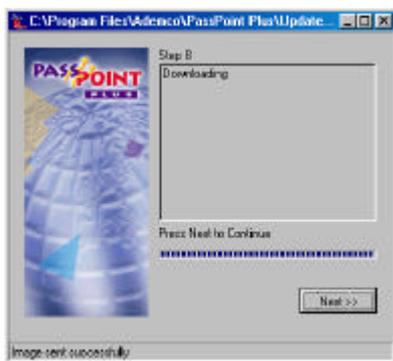


17. Fare clic su *Successivo*.

Comincia l'aggiornamento del firmware MLB e appare il seguente schermo Aggiornamento firmware MLB:

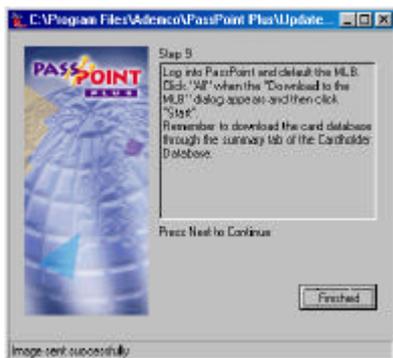


L'aggiornamento del firmware MLB impiega qualche minuto. Al termine dell'aggiornamento, lo schermo Aggiornamento firmware MLB appare come nell'esempio:



18. Fare clic su *Successivo*.

Appare il seguente schermo Aggiornamento Firmware MLB:



19. Fare clic su *Fine*.

Il firmware nella MLB è stato aggiornato.

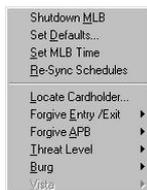
La MLB è stata impostata con i valori di default di fabbrica durante l'aggiornamento del firmware. Tutte le informazioni del cliente devono essere ora ricaricate nella MLB utilizzando le procedure descritte nel paragrafo seguente.

Aggiornamento delle informazioni cliente

Dopo l'aggiornamento del firmware MLB, è necessario riportare la MLB ai valori di default e ricaricare il database utenti.

Per cancellare la MLB e aggiornare i database richiesti, seguire la procedura seguente:

1. **Caricare PassPoint *Plus* e collegarsi al cliente al quale è stato aggiornato il firmware.**
2. **Nel menu PassPoint *Plus Control* indicato qui sotto, selezionare *Imp. default*.**

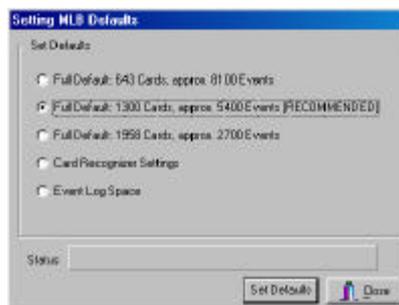


Appare la finestra di Login.



3. **Immettere la Password "installer" e fare clic su *OK*.**

Appare lo schermo Impostazione MLB a default:



4. Fare clic sul **Default** desiderato in base al numeri di utenti gestiti dal sistema. Poi fare clic su **Imp. default**.

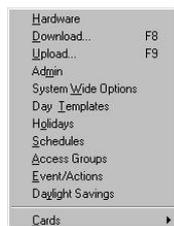
Appare lo schermo Conferma:



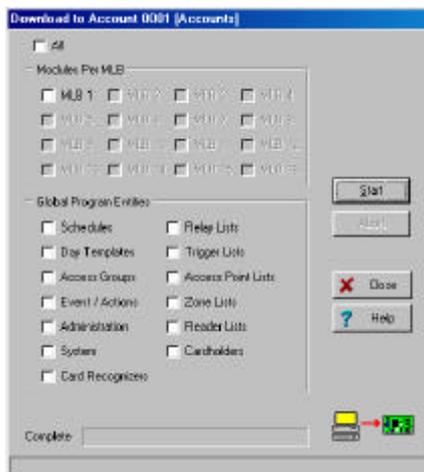
5. Fare clic su **Sì**.

I valori di default sono caricati nella MLB.

6. Nel menu **Config**, selezionare **Aggiorna**.

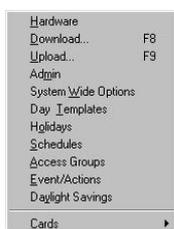


Appare lo schermo seguente:

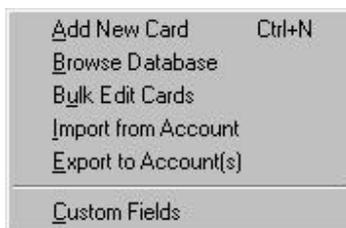


7. Fare clic nella casella *Tutti* e fare clic su *Avvio*. Il computer aggiorna la MLB.

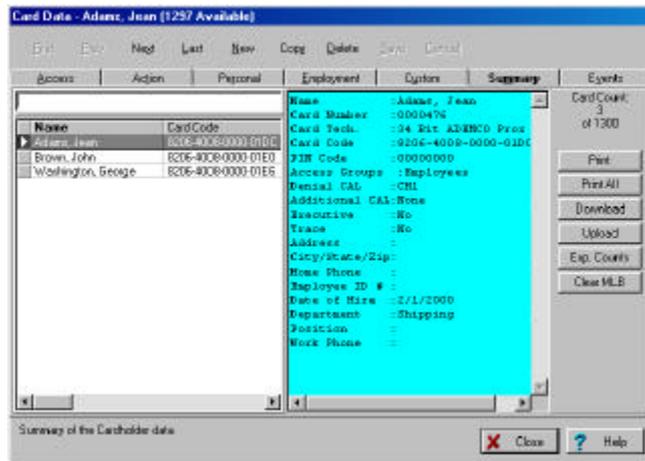
8. Nel menu *Config*, selezionare *Badges*.



Appare lo schermo seguente:



9. Selezionare *Esplora database*. Quando appare lo schermo *Dati badge*, fare clic sull'etichetta *Sommario*.



10. Fare clic su *Canc. MLB*.

Appare lo schermo Conferma.



11. Fare clic su *Sì*.

Il database utenti viene cancellato dalla MLB e appare il seguente schermo:



12. Fare clic su *Sì*. Viene ricreato il database dei badge nella MLB.



Tutti i database necessari sono stati scaricati sulla MLB e il sistema è pronto per l'uso.

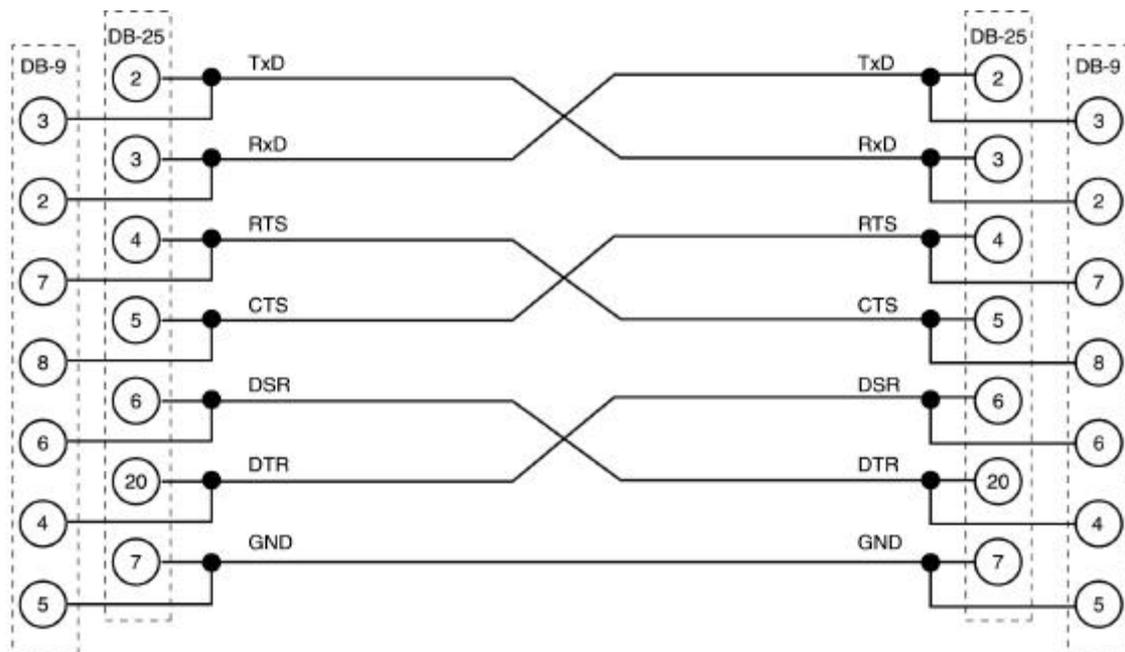
Appendice

C

Schemi di cablaggio

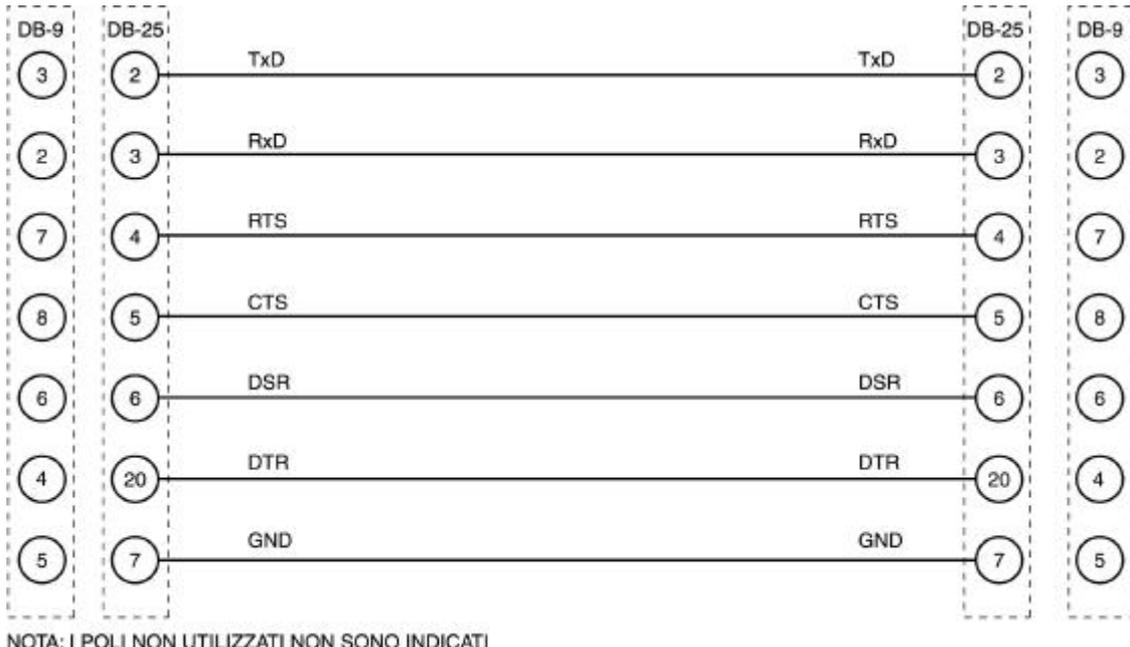
Questo documento fornisce i diagrammi di cablaggio e di connessione dei moduli, con le relative procedure d'installazione. Quest'appendice riprende tutti i diagrammi per una consultazione rapida.

Cavo null-modem

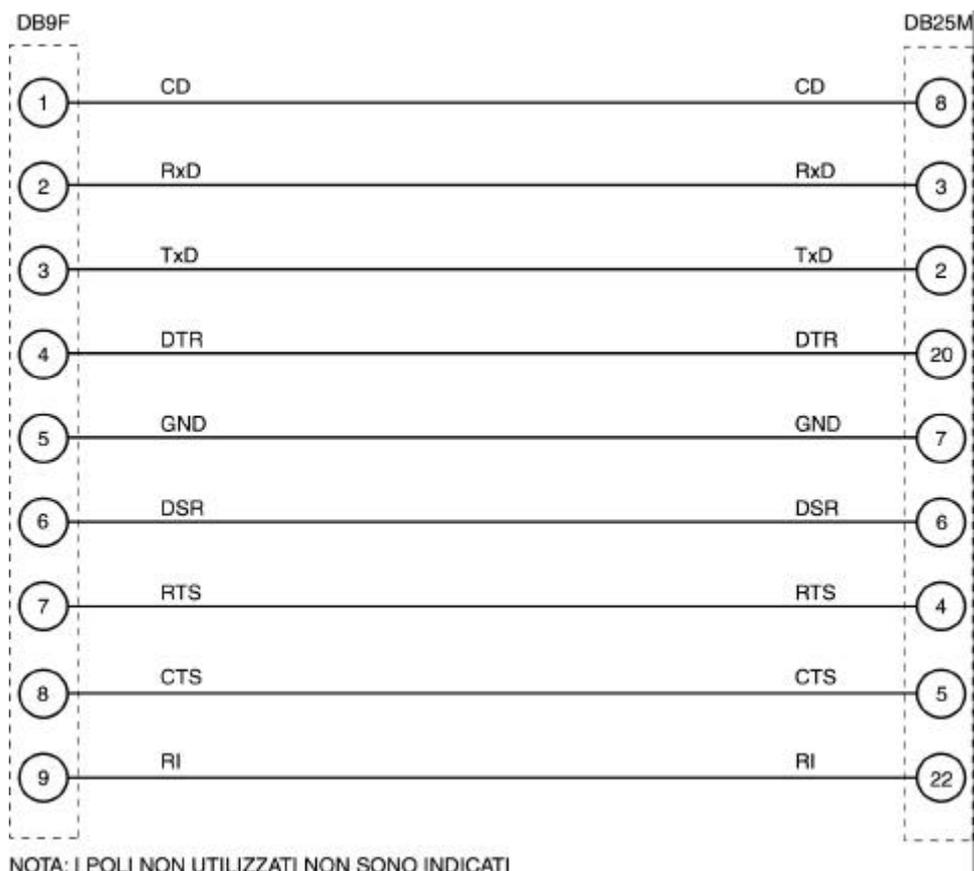


NOTA: I POLI NON UTILIZZATI NON SONO INDICATI

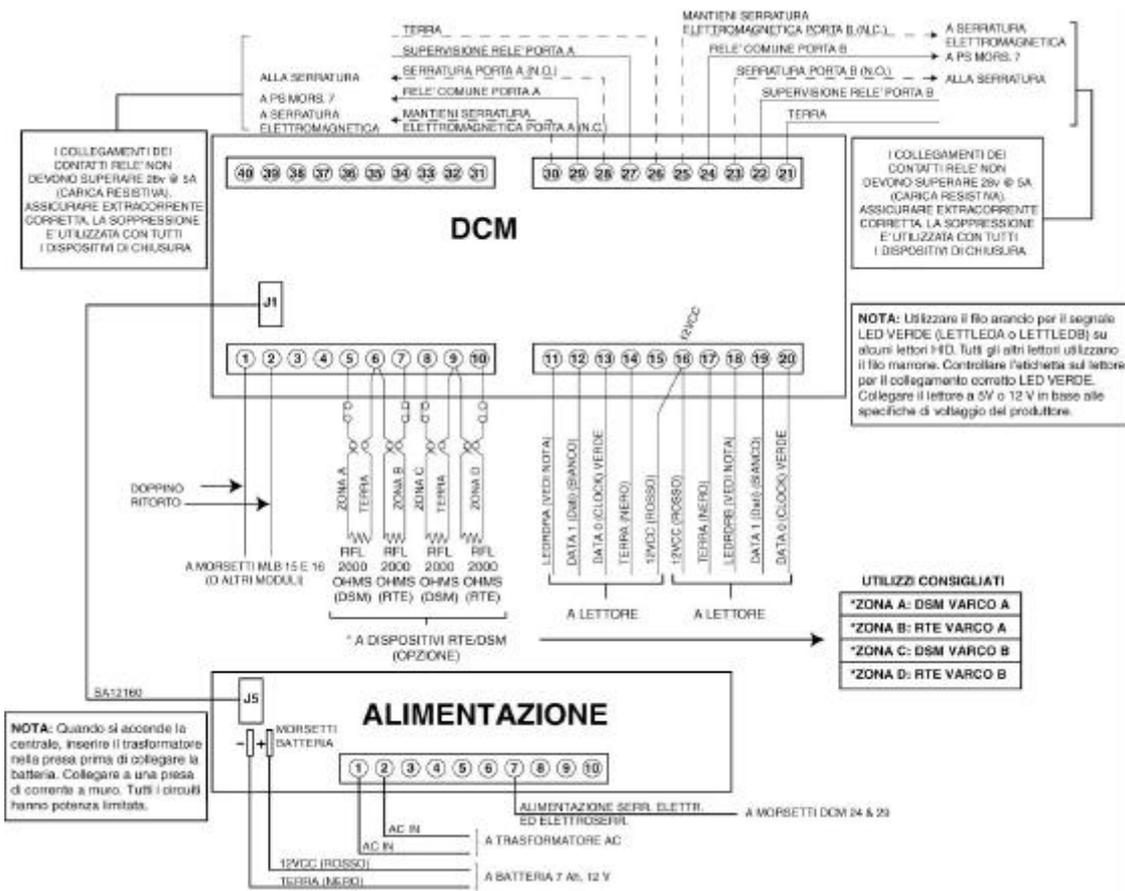
Cavo per prolunga RS-232



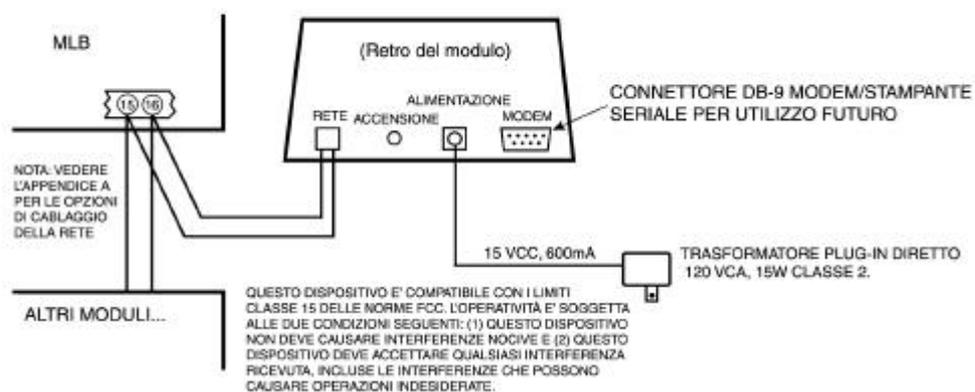
Cavo modem



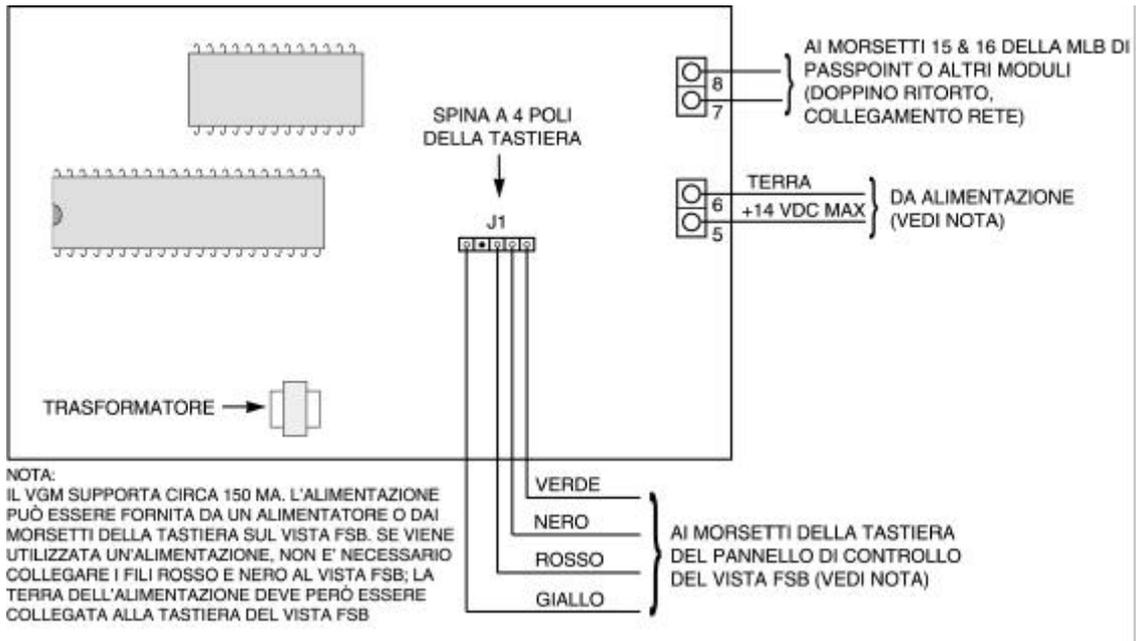
Door Expansion Kit



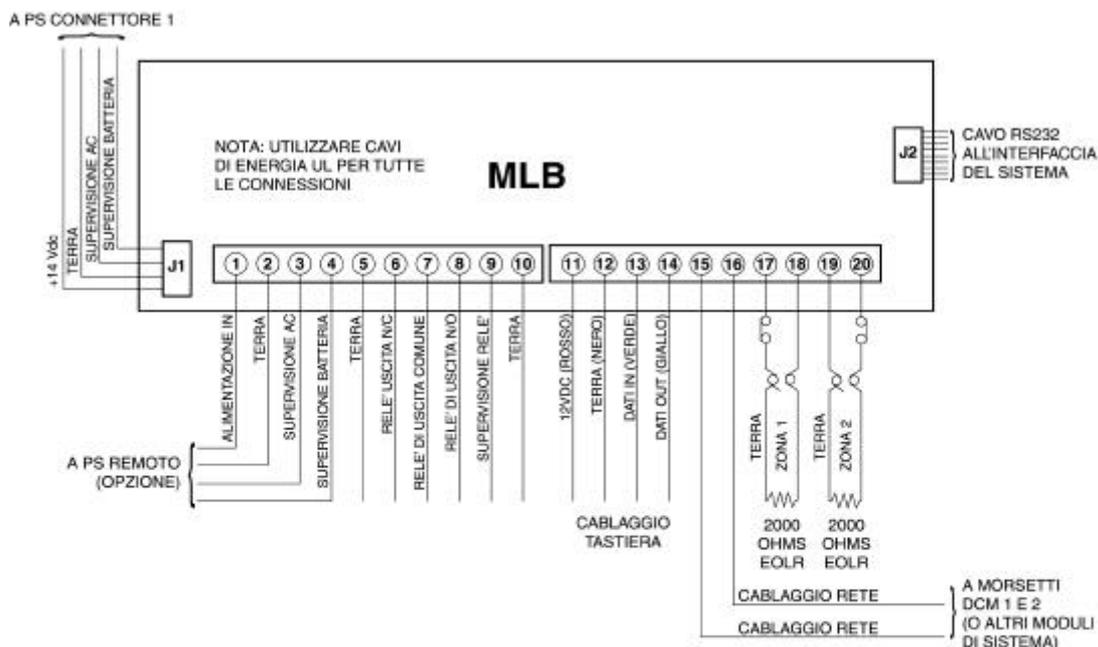
Card Enrollment Kit



VISTA Gateway Module



Main Logic Board

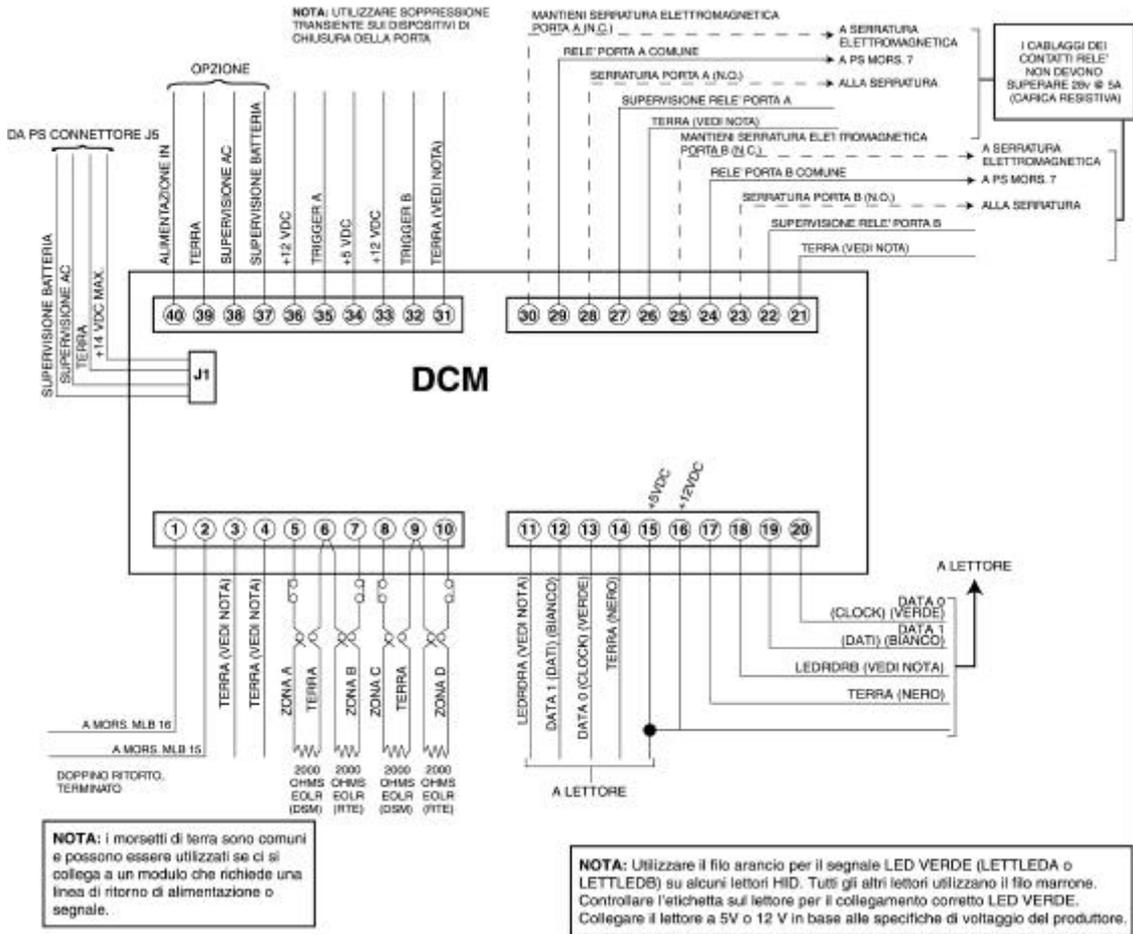


Supporto batteria MLB ADEMCO N. N7673. Batteria litio 3V, durata in standby: 10 anni.

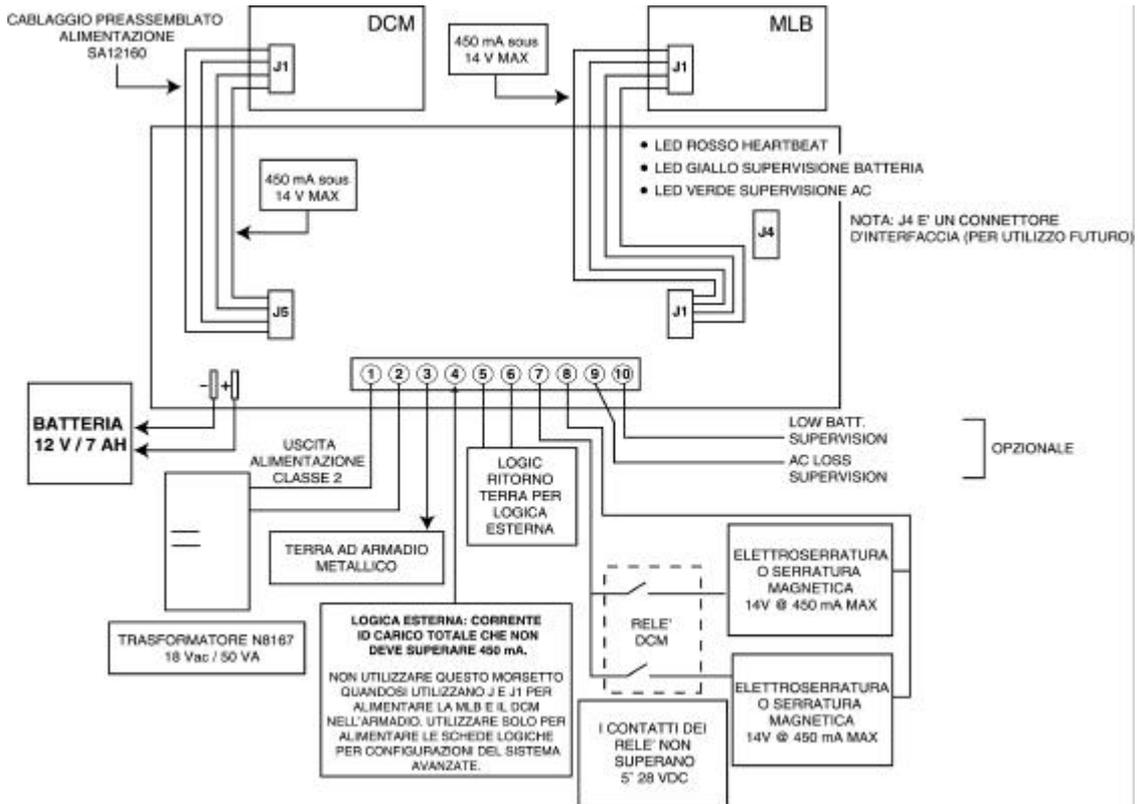
ATTENZIONE - Pericolo di esplosione se la batteria viene sostituita in modo sbagliato. Sostituire solo con una batteria uguale o equivalente, consigliata dal produttore. Gettare le batterie usate secondo le istruzioni del produttore. Tipo di batteria: batteria litio 2025.

QUESTE ATTREZZATURE DEVONO ESSERE INSTALLATE IN CONFORMITA' CON LE NORME ANTINCENDIO 70 & 74 (NATIONAL FIRE PROTECTION ASSOC., BATTERY MARCH PARK, QUINCY, MA, 02269). QUESTA ATTREZZATURA DEVE ESSERE FORNITA CON TUTTE LE INFORMAZIONI RIGUARDANTI LA CORRETTA INSTALLAZIONE, OPERAZIONE, TEST, MANUTENZIONE, PIANO DI EVACUAZIONE E SERVIZIO DI RIPARAZIONE.

Door Control Module



Alimentatore



Appendice

G

Glossario controllo di accesso

A

Accesso libero – Vedere Esclusione (Varco)

Alimentatore (Controllo di accesso) – Apparato che fornisce tutta l'alimentazione necessaria alla MLB e al DCM. E' collegato alla rete elettrica tramite un trasformatore 18Vca, 50VA.

L'alimentatore fornisce una uscita caricabatteria e supporta una batteria di 7 amperora. Inoltre è in grado di monitorare e di testare l'ingresso dell'alimentazione di rete e lo stato della batteria. I risultati del test vengono inviati ai moduli ad esso collegati e in seguito alla MLB.

Anti-Passback (APB) – Una funzionalità del controllo di accesso, secondo la quale un utente non può "passare" il proprio badge a un'altra persona, perché quest'ultima acceda alla stessa area. Un ottimo esempio per spiegare la situazione è un direttore che cerca di passare il proprio badge alla segretaria per farla accedere al parcheggio riservato, perché entrambi possano lasciare la macchina nei posti riservati agli Executive. Naturalmente, l'anti-passback funziona se l'edificio è dotato di lettori di entrata e di uscita. L'utente deve alternare l'utilizzo ai lettori di entrata e di uscita. Se il badge viene presentato a un lettore di entrata dopo che è già stato autorizzato l'accesso a quel badge sullo stesso

lettore, si produce una violazione dell'anti-passback. Sulla base della configurazione del sistema di controllo di accesso, l'utente può vedersi rifiutare l'accesso a causa della violazione. Nella programmazione ADEMCO, una violazione anti-passback avviene quando si cerca di utilizzare lo stesso varco nella stessa direzione una seconda volta entro un periodo di tempo definito, senza aver prima utilizzato quel varco in senso opposto.

Anti-Passback hard – Una caratteristica che nega l'accesso a un utente che viola le regole di anti-passback.

Anti-Passback soft – Una caratteristica che autorizza l'accesso a un utente che viola regole di anti-passback, ma ne registra la violazione nello storico eventi.

Archivio – Un file memorizzato nel computer del sistema che contiene eventi caricati precedentemente. Gli archivi consentono di conservare e di organizzare tutti gli eventi registrati dal sistema.

B

Banda magnetica – La banda nera o marrone che si trova solitamente sul retro di una carta di credito o di un badge di accesso. La banda è codificata come la banda di una cassetta audio, vale a dire che le informazioni magnetiche sono impresse sul materiale in modo tale da poter essere lette da un lettore apposito.

Biometria – Una tecnologia di lettore che identifica gli attributi umani, come le impronte digitali, la geometria della mano, il riconoscimento vocale o la scansione della retina.

Bloccato (Varco) – Una modalità che blocca la porta del varco, disattivando le funzioni di controllo di accesso dei lettori. Il varco non consente nessun ingresso e nessuna uscita quando è bloccato.

Blocco tentativi PIN – Una funzionalità che disattiva la tastiera di un lettore d'ingresso per un certo numero di volte dopo che è stato

digitato un numero specifico o codici PIN errati. Il blocco tentativi PIN protegge i locali da intrusi che tentano di manomettere un varco controllato da una tastiera. Rallenta il processo di tentare tutte le possibili combinazioni di codici. Il sistema registra un evento quando viene attivato il blocco tentativi PIN a un varco.

C

Codice di sistema – Un valore codificato (all'interno del badge di accesso) che può essere utilizzato per identificare il sito o il punto che ha emesso un gruppo di badges specifico. Questa informazione può essere utilizzata in un luogo che non richieda molta sicurezza, poiché viene ignorato il numero di badge specifico, mentre chiunque provenga da quel "sito" è autorizzato ad entrare.

Codice operatore – Il codice di identificazione utilizzato da un operatore per accedere al sistema. I codici operatori sono immessi tramite l'interfaccia di sistema.

Codici residenti (o Badges residenti) – I codici utilizzati per sbloccare i varchi nelle operazioni di modo RCM (Reduced Capability Mode). Sono utilizzati solo quando la comunicazione fra la MLB e i suoi DCM è interrotta. In queste condizioni, il DCM utilizza questi codici residenti come piccolissimi database dei badges. Quando viene ripristinata la comunicazione e il sistema esce dal modo RCM, il database dei codici residenti non viene più utilizzato.

Controllo di accesso – Consente alla persona giusta di passare attraverso le porte giuste alle ore autorizzate sulla base di 1) Cosa possiedono, 2) Cosa sono, e/o 3) Cosa fanno

Controllo ingresso/uscita – Un mezzo per controllare e monitorare il flusso di utenti da un edificio. Viene utilizzato in abbinamento ai gruppi di accesso per autorizzare o negare ai membri del gruppo l'accesso ad aree specifiche, sulla base dell'utilizzo direzionale del varco.

Costrizione – Una condizione nella quale un utente viene obbligato da un intruso ad accedere a un'area protetta. L'utente può segnalare in modo discreto alla vigilanza che è costretto ad accedere all'area protetta.

CPM (Computer Port Module) – Il CPM serve da stazione di acquisizione. La stazione di acquisizione non può essere utilizzata per la gestione di un varco.

D

DCM (Door Control Module) – Il DCM fornisce tutti gli ingressi e le uscite necessarie per gestire uno o due varchi (porte). Si può trattare di un solo varco, dove è necessaria la funzione anti-passback.

Disattivazione (Varco) – Una funzione che disattiva la zona MSP o il varco. Il varco opera allora come se non avesse zone MSP installate. Questa funzione è utile in casi di guasti dell'hardware, quando un cattivo contatto della porta può impedire le operazioni del varco. Il varco può operare in esclusione finché viene riparato.

Disattivazione (Zona) – Una funzione uguale all'Esclusione zona, con una eccezione. Mentre l'esclusione zona individua i cambiamenti negli stati delle zone senza attivare allarmi, con la funzione Disattivazione zona, questa non è più controllata. Può essere utile in caso di zona difettosa su un modulo periferico. Il modulo periferico può riempire la rete di comunicazione con messaggi di cambiamento di stato. Disattivando la zona, si comunica al modulo periferico di ignorare la zona e di non inviare più messaggi di cambiamento di stato. La zona può restare disattivata finché viene riparata.

Disinserimento – Si tratta di una funzionalità del sottosistema intrusione del sistema PassPoint. Disinserendo il sistema, le zone non attivano più un allarme intrusione.

MSP (Door Status Monitor) – Una zona in un sistema di controllo di accesso vincolata al monitoraggio di un sensore della porta. Il sensore riflette lo stato della porta (aperta o chiusa) e consente anche a PassPoint di stabilire se la porta è stata forzata o tenuta aperta per troppo tempo.

E

Elettromagnetico (Blocco Elettromagnetico) – Un elettromagnete di grande capacità installato sullo stipite della porta che, quando alimentato, crea un forte campo magnetico. Viene fissata alla porta una piastra in metallo, che verrà tenuta saldamente contro il magnete dal campo magnetico. La porta può essere liberata (o “sbloccata”) interrompendo il flusso di corrente nel magnete, neutralizzando così il forte campo magnetico.

Elettroserratura – Un dispositivo di chiusura elettromeccanico, installato solitamente nello stipite di una porta, utilizzato per aprire e chiudere una porta con mezzi elettrici o elettronici. All'interno, il dispositivo è composto da un solenoide che viene alimentato, in modo tale che il pulsante sposti il collegamento che libera il meccanismo di chiusura.

Esclusione (Varco) – Quando un varco viene posto in modalità Esclusione, il meccanismo di chiusura è sbloccato, non viene generato nessun allarme porta forzata o porta aperta per troppo tempo, e tutte le richieste di uscita sono ignorate (la porta è già sbloccata). L'industria del controllo di accesso lo definisce anche “accesso libero”.

Esclusione (Zona) – Quando una zona di allarme viene posta in modalità Esclusione, non invia più allarmi all'operatore quando avviene una modifica di stato della zona. Si può escludere una zona interna (come un corridoio) durante il giorno, quando c'è attività ma nessun pericolo di sicurezza.

Esplorazione eventi – Lo strumento di PassPoint per visualizzare gli eventi aggiornati. L'esplorazione eventi organizza tutti gli eventi aggiornati per data e li visualizza sullo schermo.

- F** **Fascia oraria** – La parte di un programma orario utilizzata per specificare gli intervalli di tempo durante i quali un'azione si produce. Le fasce orarie contengono periodi che definiscono le ore alle quali le azioni iniziano e finiscono. Ad esempio, una fascia oraria può contenere i seguenti intervalli di tempo: 07:00-08:30, 12:00-13:00, 17:00-17:30. In seguito, questa fascia oraria può essere attribuita ai giorni della settimana, da lunedì a venerdì, di un programmatore orario, e il programmatore può essere attribuito a un'azione programmata, che si produce durante questo intervallo di tempo. Quest'azione potrebbe essere l'esclusione di un varco durante i giorni lavorativi della settimana (Vedere anche: Programmatore orario)
- G** **Gruppo di accesso** – Un gruppo di persone con gli stessi privilegi di accesso per quanto riguarda i varchi associati (porte) e gli orari. Il gruppo di accesso imposta i privilegi di accesso delle persone. Tutti i membri di un gruppo di accesso hanno privilegi di accesso identici.
- Guasto** – Una situazione che indica solitamente una linea problematica (cavo o connessione) per una zona controllata.
- H** **Hardware di controllo porta** – Le attrezzature installate ad un varco per controllare l'entrata e l'uscita degli utenti. Il tipo di hardware di controllo porta da scegliere dipende in parte dal livello di sicurezza che si desidera per ogni varco. Si possono avere porte con un solo lettore di badges, o con una combinazione lettore/tastiera, alle quali bisogna immettere un codice PIN dopo aver passato il badge. Ci sono molti tipi di hardware di controllo porta disponibili, e ci sono molti modi di configurarli.
- I** **Ingresso/Uscita Hard** – Una caratteristica che nega l'accesso a un utente che viola le regole d'ingresso/uscita.
- Ingresso/Uscita Soft** – Una caratteristica che autorizza l'accesso a un utente che viola le regole d'ingresso/uscita, ma registra la violazione nello storico eventi.

Inserimento parziale - E' una funzione del sottosistema intrusione del sistema PassPoint. Inserendo il sistema le zone possono attivare un allarme intrusione. Inserendo il sottosistema intrusione in modalità parziale, significa che si è ancora all'interno dei locali e si attivano solo i tipi di zona Perimetro e 24 ore.

Inserimento parziale forzato – Una funzionalità che inserisce il sistema anti intrusione in modalità parziale. Tutte le zone aperte vengono ignorate automaticamente.

Inserimento totale – E' una funzione del sottosistema intrusione del sistema PassPoint. Inserendo il sistema, le zone possono attivare un allarme intrusione. Inserendo il sottosistema intrusione in modalità totale, significa che si è fuori dai locali e i tipi di zona Interno e Perimetro attivano un allarme quando vengono aperti

Inserimento totale forzato – Una funzionalità che inserisce il sistema anti intrusione in modalità totale. Tutte le zone aperte vengono ignorate automaticamente.

Intervallo (Tempo) – Un intervallo di tempo durante il giorno nel quale si verificano alcune azioni. Un modello di giorno può contenere fino a otto intervalli di tempo.

L

Letto – Un dispositivo al quale un utente presenta il proprio badge, che legge i dati codificati sul badge e li trasmette a una centrale di controllo di accesso. La centrale decide poi quale azione intraprendere in seguito alla lettura del badge (attivare un relè, ecc.).

Letto di acquisizione badge – Un lettore di badges (collegato a un CPM) che può essere utilizzato per acquisire i badges nel sistema di controllo di accesso.

Letto di ingresso – Un dispositivo d'ingresso installato dal lato entrata di una porta. A questo dispositivo, le persone devono identificarsi a PassPoint, in modo tale che il sistema possa

esaminare i privilegi di accesso e determinare se può accedere all'area protetta. Il termine è “lettore d'ingresso” perché nella maggior parte dei casi il dispositivo è un lettore di badges, al quale la persona deve presentare il proprio badge di identificazione. Il dispositivo può essere comunque una tastiera, alla quale la persona deve digitare il proprio codice di identificazione personale (codice PIN). In alcuni casi, se è necessaria la massima sicurezza, può essere una combinazione di tastiera e lettore di badges.

Lettore di badge – Un dispositivo utilizzato dagli utenti per identificarsi al sistema PassPoint. Il lettore legge il badge di accesso dell'utente, in modo tale che il sistema possa analizzare i privilegi di accesso e determinare se può autorizzare l'ingresso nell'area protetta.

In alcuni casi, il dispositivo utilizzato per l'identificazione può essere una tastiera, invece di un lettore. Invece di presentare un badge alla tastiera, l'utente digita un numero di identificazione personale (codice PIN). In alcuni casi, dove è richiesta la massima sicurezza, il lettore di entrata può essere una combinazione di tastiera e lettore di badges.

Lettore di uscita – Un dispositivo installato sul lato uscita di una porta. A questo dispositivo, le persone devono identificarsi in modo tale che il sistema possa esaminare i loro privilegi di accesso e decidere se autorizzare l'uscita dall'area protetta (Vedere anche: Lettore di ingresso)

Livello di accesso – Il tipo di autorizzazioni di accesso attribuite a un utente.

Livello di pericolo – Una condizione che può essere impostata dall'operatore del sistema per definire uno stato di emergenza. Esistono sei livelli di pericolo, da TL0 a TL5. TL5 è il massimo livello di pericolo.

I livelli di pericolo possono essere impostati anche per singole azioni, indicando il livello di pericolo globale al quale l'azione dovrà prodursi. Se il livello di pericolo globale supera l'impostazione dell'azione, questa non avverrà

Livello di precedenza – Un tipo di livello di autorità che informa il sistema quando alcune risorse possono essere controllate. In parole semplici, i livelli di precedenza determinano se un'operazione deve avvenire o meno prima di una qualsiasi azione iniziata in precedenza.

M

Memorizzazione eventi (o Storico eventi) – Un elenco degli eventi che indica le azioni realizzate da e all'interno del sistema PassPoint. Ogni memorizzazione evento contiene l'ora, la data e tutte le altre informazioni che definiscono l'evento.

MLB (Main Logic Board) – L'unità di controllo principale del sistema di controllo di accesso. Contiene il database dei badges, la memorizzazione eventi e le informazioni di configurazione del sistema. Controlla anche lo stato del sistema. La MLB riceve corrente dall'alimentatore del controllo di accesso e comunica con il Door Control Module (descritto precedentemente) per determinare se autorizzare l'accesso a un determinato varco. Coordina anche le attività di altri moduli di sistema, come il QRM o lo ZIM.

Modem – Un dispositivo che converte le informazioni digitali in informazioni analogiche perché possano essere trasmesse tramite linea telefonica; i dati analogici ricevuti vengono convertiti in dati digitali dall'altro lato da un altro modem.

N

Nomi comuni – Una raccolta di nomi, attribuiti da un operatore, che possono essere applicati a oggetti del sistema (relè, lettori, ecc.) Possono esserci al massimo sessanta nomi, ognuno di quindici caratteri al massimo.

- O** **Operatore (sistema)** – Una persona che agisce sul sistema attraverso un'interfaccia di sistema. Può controllare i lettori, impostare le programmazioni orarie, acquisire i badges d'identificazione, ecc. Esistono quattro livelli di operatore: Installatore, Master, Manager, Operatore.
- Output** – Dispositivi ausiliari in un sistema di controllo di accesso, che controllano i dispositivi esterni, come le serrature elettroniche, i segnali piezoelettrici o led. Si può trattare di relè (contatti puliti) o uscite transistorizzate.
- P**
- PIN (Numero di identificazione personale)** – Un numero attribuito a una persona. Quando la persona lo digita su una tastiera, il sistema di controllo di accesso autorizza l'accesso a un'area protetta. I PIN possono essere abbinati anche a badges codificate e dispositivi biometrici per garantire maggior sicurezza.
- PIR (Infrarossi passivi)** – Una tecnologia di rivelazione che individua il movimento all'interno di un'area specifica e cambia lo stato dei contatti interni impostati. Questi contatti possono essere poi collegati alla zona Richiesta di uscita su un sistema di controllo di accesso per un'uscita automatizzata, quando una persona si avvicina a un varco dall'interno dell'area protetta.
- Privilegi di accesso** – I diritti attribuiti a un individuo che ne impostano le capacità. I privilegi di accesso sono le specifiche sugli orari e i punti ai quali la persona può avere accesso o può uscire da un'area controllata.
- Privilegi Executive** – Un'opzione per garantire agli utenti accesso totale a tutti i varchi del sistema.
- Programmazione oraria** – Un elenco di intervalli di tempo che definiscono quando un evento o una situazione può cominciare, finire o prodursi. Ad esempio, la programmazione oraria controlla quando alcuni gruppi di accesso possono accedere ai locali. Le programmazioni orarie sono costituite da Fasce orarie.

Prossimità – Una tecnologia di lettore che si basa su un collegamento a frequenza radio fra il lettore e il badge (prox reader e prox card). Le informazioni codificate passano fra il badge e il lettore, solitamente su un modello unico che identifica l'utente.

Protetto – Lo stato di operazione normale di un varco. Quando un varco è protetto, possono accedervi solo gli utenti autorizzati.

Protezione guasto – Un dispositivo di chiusura che si blocca automaticamente in caso di interruzione di corrente.

Q **QRM (Quad Relay Module)** – Un modulo che può essere installato sulla rete di controllo di accesso per fornire altri quattro output controllati di forma C, oltre ai quattro trigger output.

R **Rapporto evento/azione** – Un'opzione programmata dall'operatore, che consente nel collegare le funzioni del sistema a un evento. In base all'evento del sistema, si produce l'azione.

RCM (Reduced Capability Mode) – Una modalità in cui si trova il DCM (Door Control Module), nel caso improbabile in cui dovesse “scollegarsi” dal resto del sistema PassPoint. In questa modalità si può dire al DCM come operare mentre non ha più contatti con la MLB (Main Logic Board).

Relè di controllo porta - Un interruttore elettromeccanico utilizzato per controllare il flusso di elettricità al meccanismo di chiusura della porta. Il relè di controllo della porta è un contatto “forma C” impostato per un'uscita. In questo modo può essere utilizzato per introdurre o eliminare il flusso di corrente a un dispositivo esterno.

Relè forma C – Una configurazione di terminale Comune, un terminale Normalmente aperto e un terminale Normalmente chiuso. Quando il relè non è attivato, i punti Comune e Normalmente chiuso sono collegati fra loro, e i punti Comune e

Normalmente aperto sono scollegati fra loro. Quando il relè si attiva, i punti Comune e Normalmente chiuso si scollegano, e i punti Comune e Normalmente aperto si collegano fra loro.

Risorsa vincolata – Una risorsa, come un lettore o un relè, attribuita direttamente a un Varco. La risorsa vincolata non può più essere controllata o monitorata come elemento singolo. Un relè vincolato, ad esempio, è utilizzato per controllare la porta alla quale è attribuito.

RDU (Richiesta di uscita) – Una condizione generata da un dispositivo (pulsante, barra, PIR, dispositivo a terra, ecc.) che indica al sistema PassPoint che qualcuno sta uscendo dall'area protetta. Non è necessaria nessun badge e non si produce nessun evento porta aperta. Può anche sbloccare la porta. E' conosciuto anche con altri nomi: REX, Uscita e Esclusione. Nota: non confondere questo uso di Esclusione con quello di ADEMCO. (Vedere Esclusione.)

S

Badge di accesso – Un badge, solitamente delle stesse dimensioni e con la stessa forma di una carta di credito, che contiene dati codificati. I dati possono essere codificati in moltissimi modi, e talvolta comprendono più di una tecnologia di codificazione. (Vedere Banda magnetica, Wiegand, Prossimità)

Settore/area di accesso – Uno spazio completamente chiuso per il quale si controllano entrate e uscite. Solitamente, PassPoint nota quando una persona passa nell'area. In questo modo, il sistema può tenere traccia facilmente della posizione delle persone all'interno di un edificio. Notare, comunque, che sia le entrate sia le uscite di un'area devono essere memorizzate dal sistema PassPoint perché questa opzione funzioni. Vale a dire che se solo l'entrata in un'area è controllata da PassPoint, ma non l'uscita, il sistema non riceve nessuna informazione quando la persona esce dall'area. In questo modo non si può conoscere esattamente l'occupazione dei luoghi.

Sicurezza guasto – Un dispositivo di chiusura che si apre in caso di interruzione di corrente.

Solo uscita – Uno dei modi di configurazione del varco. In questo modo, il varco accetta solo richieste di uscita. Le richieste di entrata vengono ignorate.

Soppressione transiente – Un processo secondo il quale brevi getti improvvisi di alta energia possono essere limitati per salvaguardare i livelli con l'uso di componenti elettroniche specializzate. Lo scopo è quello di proteggere i componenti elettronici delicati collegati sulle linee telefoniche particolarmente lunghe.

Sospendi (Ingresso/Uscita, Anti-Passback) – Una funzione che consente all'amministratore di "sospendere" le violazioni anti-passback e ingresso/uscita in modo tale che l'utente non venga bloccato sul posto dove viene individuata la violazione se viene negato il passaggio del badge. Quando viene utilizzata questa funzione, il meccanismo e le registrazioni di anti-passback e/o ingresso/uscita del sistema vengono risincronizzate in modo tale che l'utente possa continuare a muoversi nei locali.

Sospensione rifiuto – Questa funzionalità consente di autorizzare l'accesso a tutti i badges. Quando il sistema viene installato, questa funzionalità consente a tutti di passare dalle porte. In seguito, si può rivedere lo storico eventi e precisare la configurazione. Dopo circa una settimana di monitoraggio particolareggiato, la funzionalità può essere disattivata e può essere instaurato un controllo standard.

Supervisione – Il procedimento secondo il quale un dispositivo viene monitorato per tenere sotto controllo un eventuale guasto nelle operazioni. Viene utilizzato particolarmente per il controllo del voltaggio o della resistenza. (Vedere anche: Supervisione RF e Supervisione relè.)

Supervisione relè – Il controllo del polo comune del relè forma C per la presenza di tensione. Viene attivato un allarme se la tensione non è corretta. Può essere utilizzato per individuare un guasto su un alimentatore esterno (utilizzato per blocco alimentazione).

Supervisione RF (Supervisione Resistenza finale) – Una modalità utilizzata per individuare se qualcuno ha tagliato o mandato in corto circuito un cavo che controlla una zona, come un sensore di una porta. Si può posizionare una resistenza nel circuito della zona al punto protetto, in modo tale che il dispositivo di controllo possa individuare un problema sulla linea, oltre a condizioni normali e di errore.

Supervisione RP (Supervisione Resistenza passante) – Una modalità utilizzata per individuare se qualcuno ha tagliato o mandato in corto circuito un cavo che controlla una zona, come un sensore di una porta. Si può posizionare una resistenza nel circuito della zona al punto protetto, in modo tale che il dispositivo di controllo possa individuare un problema di linea, oltre a condizioni normali e di errore.

T **Tastiera** – Solitamente un sistema a 12 tasti sul quale si premono i pulsanti per inviare un codice al sistema, sulla base di una serie di caratteri specifici. La tastiera assomiglia generalmente alla tastiera di un telefono, con le stesse posizione e attribuzioni dei tasti.

Temporizzatore – Un circuito interno al sistema che ripristini l'elettronica di controllo nel caso improbabile che si blocchi in un circolo infinito di qualsiasi tipo. Il sistema può così continuare ad operare anche se esiste un problema che in altre situazioni avrebbe bloccato il sistema.

Temporizzazione porta – Il periodo di tempo in cui una porta può restare aperta dopo che è stata sbloccata, prima che il sistema di controllo di accesso attivi l'allarme.

Temporizzazione trigger di preallarme (Temporizzazione P-A)

– L'intervallo di tempo, in secondi, prima che si attivi l'allarme Porta aperta di un varco, dove è stato attivato il dispositivo di preallarme.

Ad esempio, se è stato impostato che la porta resti aperta 30 secondi, un preallarme adeguato sarà di 10 secondi. Dopo che la porta è rimasta aperta per 20 secondi, il sistema avvisa per 10 secondi la persona che sta tenendo la porta aperta. Se la porta è ancora aperta allo scadere dei 30 secondi, si verifica un Evento allarme temporizzazione porta aperta. Il dispositivo di preallarme resta attivato (in base al modo configurato) finché la porta si richiude, azzerando l'Allarme temporizzazione porta aperta.

Timer minuti XX – Un timer programmato sulla centrale di allarme VISTA che scade dopo un numero di minuti predefinito. Solitamente, si può configurare un relè output VISTA perché lavori durante la durata del timer. Questo timer può essere programmato in posizione 1*74 sulla centrale VISTA.

Timer secondi YY - Un timer programmato sulla centrale di allarme VISTA che scade dopo un numero di secondi predefinito. Solitamente, si può configurare un relè output VISTA perché lavori durante la durata del timer. Questo timer può essere programmato in posizione 1*75 sulla centrale VISTA.

Transazione – Un evento che si produce all'interno del sistema di controllo di accesso e che genera un record nel database memorizzato.

Trigger Output – Interruttori digitali (transistor) che possono essere configurati come risorse valide o non valide. Possono essere usati per illuminare i LED, attivare segnali piezoelettrici o un relè esterno, o segnalare un trasmettitore radio a lunga portata.

TWAIN – Un programma che consente di scansionare un'immagine (utilizzando una videocamera o uno scanner)

direttamente nell'applicazione nella quale si desidera lavorare con l'immagine. Può essere utilizzato, ad esempio, per inserire una foto d'identità nei file dipendenti di PassPoint *Plus*.

- U** **Utente** – Un occupante dei luoghi, che ha ricevuto un badge di accesso o un codice di accesso (o codice PIN, Personal Identification Number) utilizzati per chiedere l'autorizzazione di passare attraverso varchi protetti all'interno dei locali.
- V** **Vacanza** – Un componente della programmazione che imposta la settimana lavorativa quando il programma lavorativo “normale” non può essere applicato ai locali. Ad esempio, il giorno di Natale è considerato vacanza.
- Varco** – Una serie di lettori di badges, zone, trigger e relè per il controllo e il monitoraggio dell'hardware di controllo della porta a un solo punto di passaggio.
- Verificazione visiva** – Un'opzione che chiede al sistema di fare appello a un operatore per controllare visivamente l'identità di tutti gli utenti dopo che il sistema ha già controllato il badge e il codice PIN dell'utente.
- VGM (VISTA Gateway Module)** – Il componente di PassPoint che fornisce un'interfaccia fra la Centrale VISTA di ADEMCO e il sistema di controllo di accesso di ADEMCO.
- W** **Wiegand** – Una tecnologia di lettura di badges che si basa su una serie di cavi incastrati in un badge in vinile. Il badge Wiegand viene passata in un lettore Wiegand per comunicare un determinato modello di uno e zero al sistema di controllo di accesso per identificare un utente particolare.
- Z** **ZIM (Zone Input Module)** – Un modulo che può essere posizionato sulla rete di controllo di accesso per fornire altri otto input di zona, che possono essere configurati come supervisionati o non supervisionati.

Zona – Un'area o un oggetto protetto da un circuito elettronico.

Indice

I

Indice controllo di accesso

Access Starter Kit.....	1-2, 1-6	Aggiornamento del database	10-15
Acquisizione		Aggiunta	10-1
CEK.....	10-5	Collegamento	10-3
DCM	9-14	Configurazione del lettore	10-12
Moduli, Auto.....	5-9	Installazione.....	10-3
Moduli di sistema	12-3	Modifica configurazione	10-12
VGM	11-6	Presentazione.....	10-2
Aggiornamento		Centrale sistema, Montaggio	3-4
Firmware MLB	B-1	Cliente	
Aggiornam. Database	5-13, 9-19, 10-15, 11-22	Creazione di un nuovo	4-9
Aggiunta di un CEK	10-1	Presentazione.....	4-10
Aggiunta di un DEK	9-1	Collegamenti MLB	A-9, A-10
Aggiunta di un VGM	11-1	Comunicazioni, collegamenti	5-7
Aggiunta di moduli di sistema	12-1	Configurazione DCM	9-20
Aggiunta utenti	6-2	Creazione nuovo cliente	4-9
Alimentazione	1-8	Database	
Specifiche	A-11	Aggiornamento 5-13, 9-19, 10-15, 11-22	
Area di stato	4-14	Utenti, aggiunta	6-2
Auto acquisizione dei moduli.....	5-9	Utenti, gestione.....	6-1
Avviamento di PassPoint <i>Plus</i>	4-8	Utenti, informazioni	6-2
Barra dei menu.....	4-14	DCM	1-8
Barra delle priorità.....	4-14	Acquisizione	9-8, 9-14
Barra degli strumenti controllo risorse ..	4-14	Collegamento	9-5
Basic Starter Kit.....	1-2	Collegamento alimentatore	3-6
Card Enrollment Kit	1-2	Collegamento MLB	3-6
CEK		Configurazione	9-20
Acquisizione.....	10-5	Etichetta lettori.....	9-35
		Etichetta RCM residente	9-43

Etichetta relè.....	9-36	Collegamento pulsante uscita	3-12
Etichetta sistema.....	9-22	Collegamento serrature magnetiche..	3-11
Etichetta trigger.....	9-38	Collegamento tastiera	3-18
Etichetta varco A.....	9-22	Collegamento terminale remoto	3-15
Etichetta varco B.....	9-22	DEK.....	9-3
Etichetta zone A/B	9-40	Lettoce, Collegamento.....	3-7
Etichetta zone C/D	9-40	Lettoce, Montaggio.....	3-7
Modifica configurazione.....	9-20	Montaggio elettroserrature	3-11
DEK	1-2	Montaggio serrature magnetiche.....	3-11
Aggiunta	9-1	Montaggio centrale del sistema.....	3-4
Installazione.....	9-3	PassPoint Plus	4-7
Montaggio.....	9-3	Sistema	3-1
Presentazione.....	9-2	VGM.....	11-3
Door Control Module	1-8	Installazione, Preparazione a	2-1
Door Expansion Kit.....	1-2	Configurazione DCM.....	2-13
Elenchi risorse.....	8-1	Hardware di controllo porta	2-4
Elenchi risorse		Mappa	2-5
Impostazione	8-2	Selezione varchi	2-8
Utilizzo	8-11	Tipi di lettori	2-15
Finestra eventi.....	4-14	Presentazione dei varchi.....	2-3
Finestra logica.....	4-14	Installazione del sistema	3-1
Finestra risorse.....	4-14	Interfaccia del sistema.....	1-9
Firmware		Istruzioni di cablaggio.....	A-1
Aggiornamento.....	B-1	Cablaggio DCM	A-10
Gerarchia del sistema.....	1-3	Cablaggio MLB	A-9
Impostazione CPM	12-17	Note di cablaggio	A-8
Impostazione liste risorse	8-2	Specifiche alimentatore.....	A-11
Impostazione opzioni generali		Specifiche dei cavi	A-7
del sistema	7-1	Topologia.....	A-2
Impostazione QRM.....	12-12	Kit	
Impostazione software	4-1	Access Starter	1-2, 1-6
Installazione		Basic Starter	1-2
Accensione del sistema.....	3-18	Card Enrollment.....	1-2
CEK.....	10-3	Door Expansion	1-2
Collegamento alimentatore/DCM.....	3-6	Main Logic Board	1-8
Collegamento alimentatore/MLB	3-6	MLB	1-8
Collegamento cavi computer	3-13	Collegamento alimentatore	3-6
Collegamento cavo RS-232 MLB	3-7	Collegamento cavo RS-232	3-7
Collegamento DCM/MLB.....	3-6	Modifica blocco badges	6-24
Collegamento MSP	3-12	Moduli	
Collegamento elettroserrature	3-11	Auto Acquisizione	5-9

Moduli di sistema			
Aggiornamento Database.....	12-24	Modifica configurazione	12-10
Aggiunta	12-1	Requisiti di sistema	4-5
Aggiunta e acquisizione	12-3	Requisiti di sistema, Computer	4-5
Configurazione.....	12-10	Ricerca veloce	4-14
Impostazione CPM.....	12-17	Riferimenti cablaggio	C-1
Impostazione QRM	12-12	Badges	
Installazione.....	12-3	Aggiunta lotto.....	6-9
Presentazione.....	12-2	Aggiunta manuale.....	6-9
Impostazione ZIM	12-21	Aggiunta singola	6-5
Monitor badge	6-33	Etichetta accesso.....	6-10
Montaggio MLB	3-4	Etichetta azione	6-14
Opzioni generali del sistema.....	7-2	Etichetta campi personalizzati.....	6-19
Etichetta Beep/Video varco	7-32	Etichetta eventi	6-23
Etichetta modem	7-33	Etichetta impiego	6-17
Etichetta predefiniti.....	7-3	Etichetta personale	6-16
Etichetta priorità.....	7-38	Etichetta personalizzazione.....	6-18
Etichetta residenti	7-16	Etichetta sommario	6-20
Etichetta rete/ID	7-36	Gestione	6-1
Etichetta sistema intrusione.....	7-28	MagStripe ABA	7-8
Etichetta selezionatore.....	7-33	Modifica blocco.....	6-24
Etichetta tecnologia badge	7-6	Monitor	6-33
Impostazione	7-1	Badges Magstripe ABA.....	7-8
PassPoint <i>Plus</i>		Setup Wizard	5-4
Area di stato.....	4-14	Tasti rapidi	4-15
Avviamento.....	4-8	Utilizzo elenco risorse	8-11
Barra dei menu	4-14	VGM	
Barra delle priorità.....	4-14	Acquisizione	11-6
Barra degli strumenti controllo risorse.....	4-14	Aggiornamento Database	11-22
Finestra eventi	4-14	Aggiunta	11-1
Finestra risorse	4-14	Collegamento	11-4
Finestra visualizzazione logica	4-14	Configurazione	11-13
Installazione.....	4-7	Installazione.....	11-3
Login.....	4-8	Modifica configurazione	11-13
Principali componenti dello schermo	4-13	Wizard	
Ricerca rapida.....	4-14	Badges	6-4
Tasti rapidi	4-15	Impostazione	5-4
QRM		ZIM	
Impostazione	12-12	Modifica configurazione	12-10
		Impostazione ZIM.....	12-21



5007 South Howell Avenue
Milwaukee, WI 53207
www.nciaccess.com

ÊK4879ÂŠ

K4879 3/00

ADEMCO
GROUP
INTEGRATED SYSTEMS

Copyright © 2000 PITTHWAY CORPORATION