# TruPortal™

## GUIDA DELL'UTENTE DEL SOFTWARE

P/N 460864001A • REV 01.03 • ISS 25LUG13

Guida dell'utente del software Interlogix® TruPortal™ prodotto versione 1.5.
Guida numero 460864001A, lugio 2013.



**Marchi commerciali e brevetti**

Interlogix, TruPortal, TruVision e logos sono marchi registrati di United Technologies. Microsoft, Internet Explorer e Windows sono marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri paesi. Apple e iTunes sono marchi registrati di Apple Inc. Gli altri marchi utilizzati in questo documento potrebbero essere marchi o marchi registrati del produttore o del rivenditore dei rispettivi prodotti.

**Produttore**

Interlogix
3211 Progress Drive, Lincolnton, NC 28092, USA

Rappresentante autorizzato per l'Europa:
UTC Climate Controls & Security B.V.
Kelvinstraat 7, 6003 DH Weert, Netherlands

**Versione**

Il presente documento si applica alla TruPortal versione 1.5.

**Certificazione**

CE N4131

**Conformità FCC**

Questo dispositivo è conforme alla regolamentazione FCC parte 15. L'utilizzazione è subordinata alle due condizioni seguenti: (1) Il dispositivo non deve causare un'interferenza nociva (2) il dispositivo deve accettare le interferenze ricevute, incluse le interferenze che potrebbero causare un funzionamento indesiderato..

**Classe A:** L'attrezzatura è stata verificata ed è conforme ai limiti dei dispositivi digitali di classe A, conformemente alla regolamentazione FCC parte 15. Tali limiti sono stati stabiliti per fornire una ragionevole protezione dall'interferenza nociva in caso di utilizzazione dell'attrezzatura in ambito commerciale. L'attrezzatura genera, utilizza e trasmette energia a radiofrequenza e se non installata ed utilizzata come descritto nel manuale, potrebbe causare interferenze nocive alle comunicazioni radio. L'utilizzazione dell'apparecchiatura in zone residenziali potrebbe causare un'interferenza nociva ed in questo caso l'utente dovrà rettificare l'interferenza a proprie spese.

**Classe B:** L'attrezzatura è stata verificata ed è conforme ai limiti dei dispositivi digitali di classe B, conformemente alla regolamentazione FCC parte 15. Tali limiti sono stati stabiliti per fornire una ragionevole protezione dall'interferenza nociva in installazioni residenziali. L'attrezzatura genera, utilizza e trasmette energia a radiofrequenza e se non installata ed utilizzata come descritto nelle istruzioni, potrebbe causare interferenze nocive alle comunicazioni radio.

Non esistono garanzie che non si verifichino interferenze in particolari tipi di installazione. Se l'apparecchiatura dovesse causare interferenza nociva alla ricezione radiofonica o televisiva, che può essere determinata attivando e disattivando l'apparecchiatura, l'utente dovrebbe cercare di correggere l'interferenza con una delle seguenti misure:

- Riorientare o spostare l'antenna ricevente.
- Aumentare lo spazio tra l'apparecchiatura ed il ricevitore.
- Collegare l'apparecchiatura ad una presa su un circuito differente da quello al quale è collegato il ricevitore.
- Consultare un rivenditore o un tecnico esperto in radio/TV.

**Conformità ACMA**

**Notifica!** Questo è un prodotto di classe A. In ambito residenziale il prodotto potrebbe causare un'interferenza radio per la quale potrebbe essere necessario intraprendere misure adeguate.

**Canada**

La presente apparecchiatura di classe A è conforme alla regolamentazione canadese ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-0330 du Canada.

**Direttive dell'Unione Europea**

1**2004/108/EC (direttiva EMC):** United Technologies dichiara che questa apparecchiatura è conforme ai requisiti essenziali e alle disposizioni della Direttiva 2004/108/EC.

**2002/96/EC (direttiva WEEE):** I prodotti contrassegnati da questo simbolo non possono essere eliminati in discariche municipali senza raccolta differenziata nell'ambito dell'Unione Europea. Per il riciclaggio corretto del prodotto, contattare il rivenditore locale al momento dell'acquisto di nuova apparecchiatura, o eliminarlo in punti di raccolta designati. Per ulteriori informazioni consultare: www.recyclethis.info.

**2006/66/EC (direttiva batteria):** Il prodotto contiene una batteria che non può essere eliminata in discariche municipali senza raccolta differenziata nell'ambito dell'Unione Europea. Per informazioni specifiche sulla batteria, consultare la documentazione del prodotto. La batteria è contrassegnata con questo simbolo che potrebbe includere lettere che indicano cadmio (Cd), piombo (Pb), o mercurio (Hg). Per un riciclaggio corretto, restituire la batteria al produttore, oppure in un centro di raccolta designato. Per ulteriori informazioni consultare: www.recyclethis.info.

**Contatto:**

www.interlogix.com

**Assistenza clienti**

www.interlogix.com/support

## Licenze pubbliche GNU

Linux Kernel 2.6.30, Pthreads, Larry DooLittle, Flex Builder e Buildroot sono rilasciati sotto licenza pubblica generica GNU, versione 2. Una copia della licenza è disponibile all'indirizzo http://www.gnu.org/licenses/gpl-2.0.html.

YAFFS2 e GNU tar sono rilasciati sotto licenza pubblica generica GNU, versione 3. Una copia della licenza è disponibile all'indirizzo http://www.gnu.org/licenses/gpl-3.0.html.

uClibc, iClibc locale, GPG Gnu Privacy Guard, gpgme GnuPG Made Easy sono rilasciati sotto licenza pubblica generica GNU attenuata, versione 3. Una copia della licenza è disponibile all'indirizzo http://www.gnu.org/licenses/gpl-3.0.html.

## OpenSSL, AstraFlex Componenti e LIGHTTPD sono rilasciati sotto una licenza modificata BSD



QUESTO SOFTWARE È FORNITO DAI PROPRIETARY DEL COPYRIGHT NELLO STATO DI FATTO IN CUI SI TROVA ED ESPRESSAMENTE ESCLUDE QUALSIASI ALTRA GARANZIA, IMPLICITA, ESPLICITA O STATUTORIA DI COMMERCIABILITÀ, L'IDONEITÀ A UN PARTICOLARE USO. IL TITOLARE DEL COPYRIGHT ED SUOI AFFILIATI NON SARANNO IN NESSUN CASO RESPONSABILI PER QUALSIASI PERDITA DI PROFITTI O OPPORTUNITÀ COMMERCIALI, PERDITE DI DATI, INCLUSO QUALSIASI DANNO INDIRETTO, CONSEQUENZIALE, OVVERO INCIDENTALE, RISULTANTE DA INTERRUZIONE DELL'ATTIVITÀ COMMERCIALE, LESIONE PERSONALE OVVERO VIOLAZIONE DI OBBLIGHI DI DILIGENZA DERIVATA DALL'USO DEL SOFTWARE, ANCHE SE AVVISATO DELLA POSSIBILITA DI TALI DANNI.

## CMockery e Google Protocol Buffers (C) sono rilasciati sotto una licenza Apache, versione 2.0 (la “Licenza”)

Il file può essere utilizzato solo in accordo con i termini della licenza. Una copia della licenza è disponibile all'indirizzo http://www.apache.org/licenses/LICENSE-2.0

Fatta eccezione per i limiti stabiliti dalla legge applicabile o accettati per iscritto, il software è fornito NELLO STATO DI FATTO IN CUI SI TROVA ED ESPRESSAMENTE ESCLUDE QUALSIASI ALTRA GARANZIA, implicita o esplicita. Consultare la licenza per le disposizioni specifiche che regolano le autorizzazioni ed i limiti della licenza.

## Flex-IFrame

L'utente in possesso di una copia del software Flex-IFrame e dei file di documentazione associati (il "software"), ha il diritto, gratuitamente, utilizzare il software senza restrizioni, incluso ma non limitato il diritto di utilizzare, copiare, modificare, integrare, pubblicare, fornire in sottolicenza e/o vendere copie del software e di attribuire agli utenti al quale è fornito gli stessi diritti.

## Google Protocol Buffers (C++) è rilasciato sotto licenza New BSD.

QUESTO SOFTWARE È FORNITO DAI PROPRIETARY DEL COPYRIGHT NELLO STATO DI FATTO IN CUI SI TROVA ED ESPRESSAMENTE ESCLUDE QUALSIASI ALTRA GARANZIA, IMPLICITA, ESPLICITA O STATUTORIA DI COMMERCIABILITÀ, L'IDONEITÀ A UN PARTICOLARE USO. IL TITOLARE DEL COPYRIGHT ED SUOI AFFILIATI NON SARANNO IN NESSUN CASO RESPONSABILI PER QUALSIASI PERDITA DI PROFITTI O OPPORTUNITÀ COMMERCIALI, PERDITE DI DATI, INCLUSO QUALSIASI DANNO INDIRETTO, CONSEQUENZIALE, OVVERO INCIDENTALE, RISULTANTE DA INTERRUZIONE DELL'ATTIVITÀ COMMERCIALE, LESIONE PERSONALE OVVERO VIOLAZIONE DI OBBLIGHI DI DILIGENZA DERIVATA DALL'USO DEL SOFTWARE, ANCHE SE AVVISATO DELLA POSSIBILITA DI TALI DANNI.

## gSOAP è rilasciato sotto licenza pubblica gSOAP (licenza modificata MPL)



QUESTO SOFTWARE È FORNITO IN PARTE DA GENIVIA INC ED ESPRESSAMENTE ESCLUDE QUALSIASI ALTRA GARANZIA, IMPLICITA, ESPLICITA O STATUTORIA DI COMMERCIABILITÀ, L'IDONEITÀ A UN PARTICOLARE USO. L'AUTORE NON È IN NESSUN CASO RESPONSABILE PER QUALSIASI PERDITA DI PROFITTI O OPPORTUNITÀ COMMERCIALI, PERDITE DI DATI, INCLUSO QUALSIASI DANNO INDIRETTO, CONSEQUENZIALE, OVVERO INCIDENTALE, RISULTANTE DA INTERRUZIONE DELL'ATTIVITÀ COMMERCIALE, LESIONE PERSONALE OVVERO VIOLAZIONE DI OBBLIGHI DI DILIGENZA DERIVATA DALL'USO DEL SOFTWARE, ANCHE SE AVVISATO DELLA POSSIBILITA DI TALI DANNI.

## mini_httpd è rilasciato sotto licenza freeware Acme Labs.

La ridistribuzione e l'uso in formato sorgente e binario di mini_httpd con o senza modifiche, è concessa alle seguenti condizioni:

1. La ridistribuzione del codice sorgente deve contenere l'avviso di copyright qui sopra, l'elenco delle condizioni e la dichiarazione di non responsabilità di seguito.
2. La ridistribuzione del codice binario deve contenere l'avviso di copyright qui sopra, l'elenco delle condizioni e la dichiarazione di non responsabilità di seguito nella documentazione e/o altro materiale fornito con la distribuzione.

QUESTO SOFTWARE È FORNITO DAGLI AUTORI E DAI CONTRIBUTORI NELLO STATO DI FATTO IN CUI SI TROVA ED ESPRESSAMENTE ESCLUDE QUALSIASI ALTRA GARANZIA, IMPLICITA, ESPLICITA O STATUTORIA DI COMMERCIABILITÀ, L'IDONEITÀ A UN PARTICOLARE USO. L'AUTORE ED I CONTRIBUTORI NON SONO IN NESSUN CASO RESPONSABILI PER QUALSIASI PERDITA DI PROFITTI O OPPORTUNITÀ COMMERCIALI, PERDITE DI DATI, INCLUSO QUALSIASI DANNO INDIRETTO, CONSEQUENZIALE, OVVERO INCIDENTALE, RISULTANTE DA INTERRUZIONE DELL'ATTIVITÀ COMMERCIALE, LESIONE PERSONALE OVVERO VIOLAZIONE DI OBBLIGHI DI DILIGENZA DERIVATA DALL'USO DEL SOFTWARE, ANCHE SE AVVISATO DELLA POSSIBILITA DI TALI DANNI.

## Apache log4Net è rilasciato sotto licenza Apache versione 2.0.

Una copia della licenza è disponibile all'indirizzo http://logging.apache.org/log4net/license.html.

Le versioni in lingua diversa dall'inglese della documentazione Interlogix sono un servizio offerto per le udienze globali. Si è tentato di fornire una traduzione accurata del testo, tuttavia il testo originale è il testo in lingua inglese e qualsiasi tipo di differenza nella traduzione non è vincolante e non ha alcun valore legale.

Il software incluso con il prodotto contiene software fornito di copyright e sottoposto a licenza GPL. È possibile richiedere il codice sorgente corrispondente per un periodo non superiore a tre anni dall'ultimo invio del prodotto, non prima del 2013-08-30, inviando un vaglia o un assegno di $5 al seguente indirizzo:

Interlogix
1212 Pittsford-Victor Road
Pittsford, NY 14534-3820

Il pagamento deve essere all'ordine di "sorgente per TruPortal" Una copia della sorgente è disponibile all'indirizzo http://www.interlogix.com. L'offerta è valida per chiunque sia in possesso di questa informazione.

# CAPITOLO 1 *Introduzione*

TruPortal™ è una soluzione di controllo dell'accesso basata su web dall'uso semplice, ma sofisticato. È compatibile con una gamma di componenti hardware per il controllo dell'accesso quali:

- Dispositivi d'ingresso che rilevano condizioni o eventi quali campanelli o allarmi.
- Dispositivi d'uscita quali luci e serrature che rispondono ai dispositivi d'ingresso e/o alle azioni.
- TruVision™ Digital Video Recorders (DVRs) e Network Video Recorders (NVRs).

L'interfaccia utente TruPortal fa parte del controller del sistema e può essere utilizzata per:

- Controllare l'accesso ad un massimo di 64 porte in base ad una programmazione definita dall'utente.
- Configurare la programmazione per includere i giorni festivi ricorrenti.
- Aggiungere fino a 10000 utenti e badge al sistema.
- Aggiungere programmazioni del lettore per facilitare l'automazione del sistema.
- Applicare l'anti-passback (APB).
- Creare gruppi di lettori.
- Controllare gli eventi a distanza e collegare automaticamente gli eventi ai video registrati.
- Aprire, chiudere, bloccare e ripristinare le porte a distanza.

**Notare:** Per un'installazione approvata s319 Underwriters Laboratories of Canada (ULC), le funzioni di accesso remoto sono supplementari.

Le versioni mobili dell'interfaccia utente sono anche disponibili per i dispositivi iOS6 e Android™. Gli app possono essere utilizzati per il monitoraggio del sistema e per effettuare semplici operazioni amministrative. Per ulteriori informazioni, consultare le *Note di rilascioTruPortal.*

Oltre all'interfaccia utente, il sistema include i seguenti programmi:

- L' **Installation Wizard** può essere utilizzata per rilevare il controller del sistema su una rete, sincronizzare l'ora del controller del sistema con l'ora sulla stazione di lavoro client locale e configurare le impostazioni della rete. Se l'indirizzo IP è stato modificato, l' Installation Wizard può anche essere utilizzato per determinare il nuovo indirizzo IP di un controller del sistema. Consultare Utilizzazione dell'installazione guidata a pagina 9.
- L' **upgrade guidata** può essere utilizzata per aggiornare il controller del sistema da una versione precedente. *Gli utenti TruPortal 1.0 e goEntry 3.0 esistenti possono utilizzare l'upgrade guidato invece dell'installazione guidata per aggiornare il controller guidata.* Consultare Utilizzazione dell' installazione guidata a pagina 11.
- L' **importazione/esportazione guidata** può essere utilizzata per importare dati relativi a persone e credenziali da un database esistente in formato CSV (Comma Separated Values) e per esportare dati. Può essere utilizzata anche per eliminare persone e credenziali in modalità batch e per esportare eventi. Per informazioni dettagliate, consultare la *Guida utente di importazione/esportazione guidata* inclusa nel disco utilità.

## Convenzioni utilizzate in questa documentazione

La documentazione TruPortalè inclusa nel disco del prodotto e il testo del manuale è formattato in modo tale da rendere facilmente identificabile il soggetto trattato.

- Se il termine è definito, la parola è rappresentata in *italico*.
- Il nome dei campi sono rappresentati in **grassetto**.
- I menù e gli elementi del menù sono presentati in ***grassetto italico***. Tutti gli elementi del menù sono associati ad un tasto di scelta che può essere utilizzato per selezionarli utilizzando la tastiera. La lettera sottolineata rappresenta il tasto di scelta per un determinato elemento del menù. I tasti di scelta sono indicati ad esempio, <Alt>, <C>.
- I tasti della tastiera sono rappresentati in parentesi ad angolo. Ad esempio: <Tab>, <Ctrl>.
- Le combinazioni di tasti sono presentate in due modi:

  <Ctrl> + <Z> significare mantenere premuto il primo tasto e premere il secondo.

  <Alt>, <C> significa premere il primo tasto, quindi il secondo.
- I pulsanti sullo schermo sono rappresentati dalle parentesi quadre; ad esempio: [Modificare], [Annullare].

Fare clic sul pulsante **Visualizzare aiuto** (  ) nell'angolo in alto a destra TruPortal dell'interfaccia utente, per accedere alla versione elettronica della *Guida dell'utente del software TruPortal* tramite il sistema di aiuto in linea.

Fare clic sul pulsante **Mostrare descrizione dei comandi** (  ) per visualizzare informazioni relative al contesto al passaggio sui campi e le icone TruPortal nell'interfaccia utente. La descrizione dei comandi può essere attivata e disattivata facendo clic sullo stesso pulsante. Ingrandire la finestra del browser per visualizzare le descrizioni dei comandi; se la finestra è troppo piccola, le descrizioni dei comandi potrebbero non essere visualizzate.

CAPITOLO 2

# *Installazione dell'hardware*

Il primo passo per l'impostazione del sistema è l'installazione dei componenti hardware che saranno utilizzati per il sistema (ingressi, uscite, lettori, telecamere, ecc.) secondo le istruzioni del produttore. Assicurarsi di annotare i dati relativi alle configurazioni della porta che saranno utilizzati in seguito per denominare i dispositivi, i gruppi di lettori e le aree quando i dispositivi sono configurati nell'interfaccia utente.

**Notare:** I clienti TruPortal 1.0 or goEntry 3.0 esistenti con hardware già installato e configurato, possono ignorare questo passaggio ed utilizzare l' **Upgrade guidata** per effettuare l'upgrade del controller del sistema. Consultare Utilizzazione dell' installazione guidata a pagina 11.

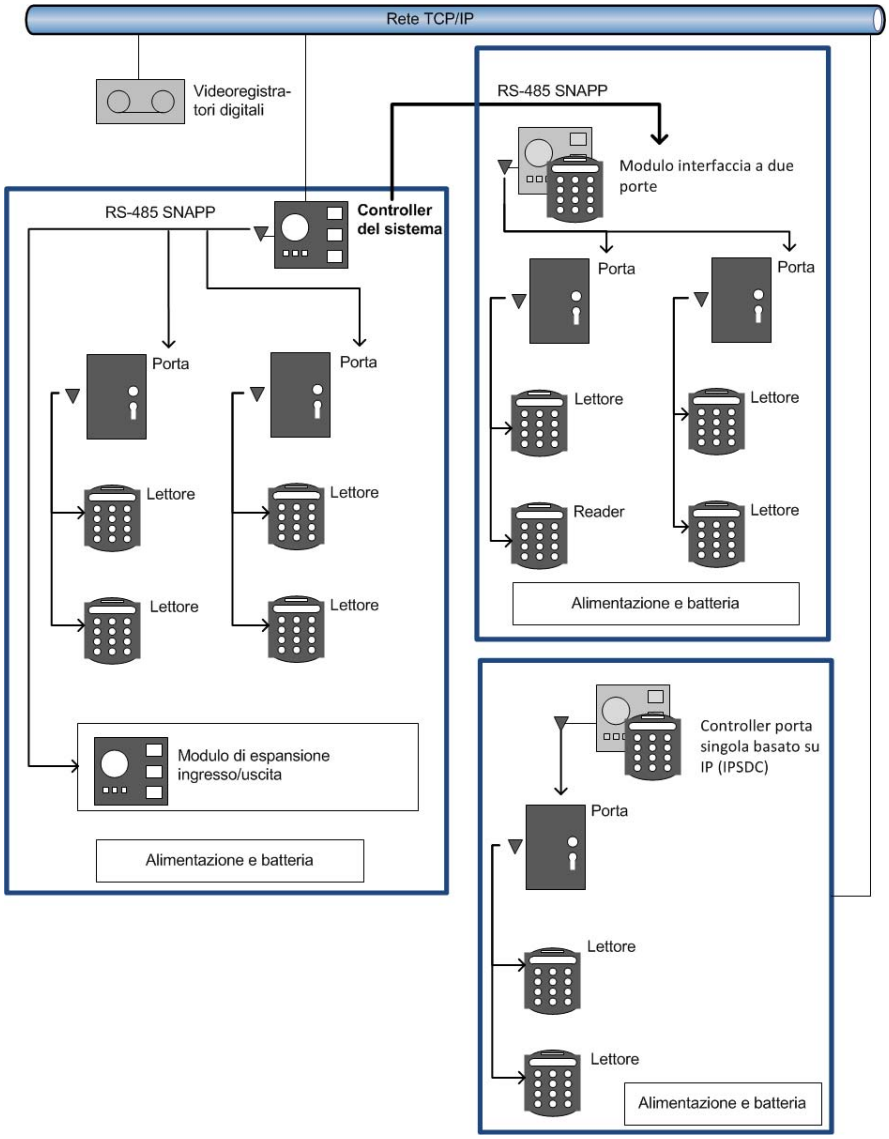
Dopo aver installato i componenti hardware, collegare il controller del sistema ad una stazione di lavoro locale o al Local Area Network (LAN), quindi utilizzare l'installazione guidata per rilevare il controller del sistema nella rete, come descritto in Preparazione della configurazione a pagina 7.

Gli argomenti del capitolo includono:

## Panoramica dell'architettura del sistema

Il controller del sistema può essere considerato il cervello del sistema poiché riceve ed invia informazioni. Contiene il database, che memorizza tutti i dati dei dispositivi, delle programmazioni, delle persone, ecc., oltre all'interfaccia utente accessibile tramite un browser web.

Al controller del sistema possono essere collegati diversi componenti quali controller della porta, lettori, moduli di espansione ingresso/uscita, relay sonori, relay luminosi e relay chiusura. Questi componenti possono essere considerati le braccia del sistema; immettono dati nel sistema e intraprendono le azioni richieste dal sistema.




Oltre ai componenti cablati al sistema, il controller del sistema può comunicare con il protocollo proprietario Internet controller porta singola basati su IP (IPSDC) Inoltre le app iPad®, iPhone® e Android™ consentono agli utenti di monitorare in remoto le attività del sistema ed effettuare semplici operazioni amministrative, quali aggiungere o eliminare utenti.

## Documentazione della posizione fisica di ciascun dispositivo

Man mano che si installano i dispositivi sulle porte (serrature, sensori, lettori), fornire una descrizione per ciascun dispositivo ed elencare i numeri di serie dei dispositivi associati a ciascuna porta in uno schema simile a quello illustrato qui sotto. I dati potranno essere utilizzati in seguito, al momento della configurazione dei dispositivi nell'interfaccia utente.

| Descrizione della porta | Lettore seriale Numeri | Controller porta Numeri di serie | Espansione I/O Numero di serie | Telecamera collegata |
|---|---|---|---|---|
| | Ingresso: | | | |
| | Uscita: | | | |
| | Ingresso: | | | |
| | Uscita: | | | |
| | Ingresso: | | | |
| | Uscita: | | | |
| | Ingresso: | | | |
| | Uscita: | | | |
| | Ingresso: | | | |
| | Uscita: | | | |
| | Ingresso: | | | |
| | Uscita: | | | |
| | Ingresso: | | | |
| | Uscita: | | | |
| | Ingresso: | | | |
| | Uscita: | | | |
| | Ingresso: | | | |
| | Uscita: | | | |
| | Ingresso: | | | |
| | Uscita: | | | |
| | Ingresso: | | | |
| | Uscita: | | | |
| | Ingresso: | | | |
| | Uscita: | | | |

| Descrizione della porta | Lettore seriale Numeri | Controller porta Numeri di serie | Espansione I/O Numero di serie | Telecamera collegata |
|---|---|---|---|---|
| | Ingresso: | | | |
| | Uscita: | | | |
| | Ingresso: | | | |
| | Uscita: | | | |
| | Ingresso: | | | |
| | Uscita: | | | |
| | Ingresso: | | | |
| | Uscita: | | | |
| | Ingresso: | | | |
| | Uscita: | | | |

## Collegamento alla stazione di lavoro client locale o LAN

Il controller del sistema può essere collegato direttamente alla stazione di lavoro client locale o a un Local Area Network (LAN). Ci sono due connettori Ethernet RJ-45 100BaseT sul controller del sistema. La porta 1 è configurabile, la porta 2 ha un indirizzo IP (Internet Protocol) fisso, 169.254.1.200. Per identificare i connettori, consultare la Guida rapida di riferimento del controller del sistema.

Se si collega il controller del sistema direttamente alla stazione di lavoro client locale, utilizzare il connettore Ethernet ed un cavo Ethernet categoria 6 (CAT6). Se si effettua il collegamento al LAN, utilizzare il connettore Ethernet configurabile ed un cavo Ethernet CAT6. Per ulteriori informazioni sulla configurazione del controller del sistema, consultare l'amministratore di rete del sito, come discusso in Determinare le impostazioni della rete a pagina 8.

**Notare:** Se diverse apparecchiature di rete utilizzano un unico nodo di rete tramite un commutatore o un piccolo router, assicurarsi che non ci sia più di un commutatore o router tra il controller del sistema ed nodo di rete.

## Installazione di un lettore di iscrizione

Se si intende utilizzare il lettore di iscrizione USB opzionale (TP-RDR-LRN) per leggere i dati della credenziale, installare e configurare il lettore su una stazione di lavoro client secondo le istruzioni del produttore. Per ulteriori informazioni, consultare Utilizzazione di un lettore iscrizione a pagina 70.

CAPITOLO 3

# *Preparazione della configurazione*

Dopo l'installazione dei dispositivi, effettuare i passaggi descritti di seguito prima di avviare l'interfaccia utente per effettuare la configurazione completa del  sistema:

1. Per assistenza con la configurazione delle impostazioni di rete, consultare l'amministratore di rete del sito. Consultare Determinare le impostazioni della rete a pagina 8.
2. *Per i clienti TruPortal 1.0 o goEntry 3.0 esistenti con hardware già installato e configurato*, utilizzare l'aggiornamento guidato per aggiornare il controller del sistema invece di utilizzare l'installazione guidata. Consultare Utilizzazione dell' installazione guidata a pagina 11.

   *Per i nuovi TruPortal utenti*, utilizzare i passaggi in Utilizzazione dell'installazione guidata a pagina 9 per:

   - Rilevare il controller del sistema sulla rete locale.
   - Per aumentare la sicurezza, modificare la password predefinita dell'account amministratore principale.
   - Sincronizzare la data e l'ora del controller del sistema con la stazione di lavoro locale del client.
   - Configurare le impostazioni di rete del controller del sistema.
3. Configurare i IPSDC installati per riconoscere l'indirizzo IP del controller del sistema *prima* di configurare l'IPSDC nell'interfaccia utente. Questo tipo di collegamento alla rete assicura la rilevazione di IPSDC durante la scansione per le modifiche hardware effettuata dal controller del sistema. Per ulteriori informazioni consultare Configurazione dei controller porta singola basati su IP a pagina 109.

## Determinare le impostazioni della rete

Prima di utilizzare l'installazione guidata per effettuare la configurazione iniziale del Controller del sistema, consultare l'amministratore di rete del sito per rispondere alle domande seguenti:

- **L'indirizzo IP del controller del sistema deve essere statico o dinamico?** Gli operatori accederanno all'interfaccia utente immettendo l'indirizzo IP del controller del sistema nel campo indirizzo del browser. Se l' indirizzo IP del Controller del sistema utilizza il protocollo di configurazione IP dinamica (DHCP), gli operatori devono utilizzare un URL virtuale o un altro alias per accedere al Controller del sistema. Se l'indirizzo assegnato è modificato dalla rete, l'operatore non sarà in grado di trovarlo.
- **La porta del servizio deve essere modificata?** La porta del servizio predefinita per un collegamento HTTPS è 443; il valore predefinito per un collegamento HTTP è 80. In genere questa porta deve essere modificata solo in caso di conflitto con una porta esistente utilizzata in rete. Se la porta è modificata, gli utenti devono aggiungere il numero di porta all'indirizzo IP del Controller del sistema per collegarsi al sistema (ad esempio, https://IPaddress:*porta*).

**Notare:** Le porte da 0 a 1024 (ad esempio *porte conosciute*) sono riservate ai servizi privilegiati. Si raccomanda di non utilizzare queste porte come porte del servizio.

- **In caso di utilizzazione di un indirizzo IP statico, quali sono i valori per la rete della maschera di sottorete, del gateway predefinito e del Domain Name Server (DNS)?** Si tratta di un'informazione necessaria per la configurazione delle proprietà della rete del Controller del sistema.
- **Si deve utilizzare un collegamento Hypertext Transfer Protocol Secure (HTTPS)?** HTTPS è altamente raccomandato per prevenire l'accesso non autorizzato al sistema. Questo protocollo di sicurezza effettua la cifratura dei pacchetti tra il browser ed il Controller del sistema, impedendo la raccolta delle informazioni relative ai clienti spiando il traffico di rete. In alcune circostanze potrebbe essere necessario utilizzare HTTP non sicuro. Ad esempio se l'accesso al Controller del sistema è effettuato tramite un server Web proxy che non supporta HTTPS, l'unica opzione è disattivare HTTPS.

  Dopo l'installazione, il sistema può essere configurato per l'utilizzazione di un collegamento Secure Shell (SSH) che verifica le stazioni di lavoro remote e consente agli utenti remoti (incluso il personale di supporto tecnico) di collegarsi al sistema. Consultare Configurazione della sicurezza del sistema a pagina 16.

# Utilizzazione dell'installazione guidata

Questa sezione descrive l'utilizzazione dell'installazione guidata per:

- Rilevare il controller del sistema sulla rete locale.
- Per aumentare la sicurezza, modificare la password predefinita dell'account amministratore principale.
- Sincronizzare la data e l'ora del controller del sistema con la stazione di lavoro locale del client.
- Configurare le impostazioni di rete del controller del sistema.

**Notare:** Per gli utenti TruPortal o goEntry esistenti, utilizzare **l'aggiornamento guidato** per aggiornare il controller del sistema invece di utilizzare l'installazione guidata. Consultare Utilizzazione dell' installazione guidata a pagina 11.

Se l'indirizzo IP è stato modificato, l' può anche essere utilizzato per determinare il nuovo indirizzo IP di un controller del sistema.

**Notare:** L'installazione guidata non è compatibile con Microsoft® Windows® XP.

Per utilizzare l'installazione guidata:

1. Verificare che il controller del sistema sia collegato alla rete locale per poter essere rilevato da .
2. Inserire il disco del prodotto nel lettore CD/DVD della stazione di lavoro locale del cliente.

**Notare:** Se l'immagine del disco è stata scaricata nel disco rigido della stazione di lavoro del cliente, aprire Windows Explorer, percorrere l'immagine del disco e fare doppio clic sull'applicazione **start.hta** per avviare l'utilità software.

   L'utilità software determinerà se la stazione di lavoro include i programmi necessari per il funzionamento dell'interfaccia utente.

3. Se richiesto, fare clic su **.NET 4.5 Framework** e/o **Bonjour** per installare il software.
4. Fare clic sull'icona **installazione guidata**.
5. Nella pagina introduzione, selezionare una **Lingua** e fare clic su [Successivo].

   L'installazione guidata cercherà i controller del sistema sulla rete.
6. Selezionare il controller del sistema dall'elenco e fare clic su [Successivo].
7. Nella pagina di login, immettere la **password** corrente dell'account amministratore.

   Il **nome utente** predefinito dell'account amministratore è `admin`.

   La **password** predefinita dell'account amministratore è `demo`.

**IMPORTANTE:** L'account amministratore ha accesso a tutti gli aspetti del sistema. Non modificare la password potrebbe essere pericoloso. Gli utenti che hanno già utilizzato il prodotto potrebbero essere a conoscenza della password predefinita.

8. Immettere la nuova password nei campi **nuova password** e **conferma password** e fare clic su [Successivo].
9. Nella pagina data/ora, selezionare il **fuso orario del controller del sistema**.
10. Se i valori **data e ora pannello** e **data e ora cliente** sono visualizzati in rosso, il fuso orario del controller del sistema è diverso da quello della stazione di lavoro del cliente, oppure la differenza dell'ora dei due dispositivi è superiore a 10 secondi.

Fare clic su [Sincronizzare ora] per sincronizzare il fuso orario o l'ora del controller del sistema con il fuso orario o l'ora della stazione di lavoro del cliente.

**Notare:** Al termine della configurazione iniziale, il sistema può essere sincronizzato con un server Network Time Protocol (NTP). Consultare Impostare la data e l'ora a pagina 15.

11. Fare clic su [Successivo] per passare alla pagina configurazione della rete.
12. Selezionare il tipo di collegamento **statico** o **dinamico** per il controller del sistema.

    Per configurare un indirizzo IP statico:

    a. Immettere l' **indirizzo IP** del controller del sistema che gli utenti immettono in un browser per collegarsi al sistema.
    b. (Opzionale) Modificare la **porta del servizio** del controller del sistema.

**Notare:** La porta del servizio predefinita per un collegamento HTTPS è 443; il valore predefinito per un collegamento HTTP è 80. Le porte da 0 a 1024 (ad esempio *porte conosciute*) sono riservate ai servizi privilegiati. Si raccomanda di non utilizzare queste porte come porte del servizio. Se la porta è modificata, gli utenti devono aggiungere il numero di porta all'indirizzo IP del Controller del sistema per collegarsi al sistema (ad esempio, https://IPaddress:*porta*).

    c. Immettere la **Maschera di subnet** della rete alla quale il controller del sistema è collegato.
    d. Immettere il **gateway predefinito** della rete.
    e. Immettere il **server DNS** della rete.
13. Selezionare **attivare il collegamento HTTPS** per utilizzare un protocollo ipertestuale sicuro.

**IMPORTANTE:** HTTPS è altamente raccomandato per prevenire l'accesso non autorizzato al sistema.

14. Fare clic su [Applicare] per salvare la configurazione di rete.
15. Per sperimentare configurazioni di rete differenti, fare clic su [Riavviare controller del sistema].

    Sarà visualizzata la pagina rilevamento pannello e rileverà nuovamente il controller del sistema. Se necessario, spostarsi alla pagina configurazione di rete per modificare le impostazioni.
16. Per accedere all'interfaccia utente principale ed iniziare la configurazione del sistema, fare clic sul collegamento ipertestuale dell'indirizzo IP del controller del sistema. Per ulteriori informazioni, consultare Configurazione del sistema a pagina 13.
17. Fare clic su [Finire] per chiudere l'installazione guidata.
18. Se IPSDC è installato, configurarlo per riconoscere l'indirizzo IP del controller del sistema *prima* di configurare IPSDC nell'interfaccia utente. Consultare Configurazione dei controller porta singola basati su IP a pagina 109.
19. Passare a Configurazione del sistema a pagina 13.

# Utilizzazione dell' installazione guidata

Gli utenti TruPortal 1.0 o goEntry 3.0 esistenti possono utilizzare **l'aggiornamento guidato** per aggiornare il controller del sistema a distanza da una stazione client locale da una versione del prodotto ad un'altra (ad esempio dalla versione 1.0 alla versione 1.5). Questo processo consiste nello scaricare i dati dal sito web del prodotto e poi utilizzare l'aggiornamento guidato per effettuare il backup dei dati, aggiornare il firmware ed il codice core del controller del sistema, quindi ripristinare i dati.

Prima di utilizzare l'aggiornamento guidato, si notino i seguenti dettagli:

**IMPORTANTE:** Non spegnere ed accendere (ad esempio spegnere e scollegare l'alimentazione elettrica) durante un aggiornamento.

**IMPORTANTE:** *L'upgrade* è differente rispetto all'*aggiornamento del firmware*. L'aggiornamento del firmware ha un impatto solo sul firmware, mentre l'upgrade ha un impatto sul firmware e sul codice core del controller del sistema. Non utilizzare la pagina ***Amministrazione del sistema > Aggiornamento Firmware*** per l'upgrade del controller del sistema, utilizzare invece l'aggiornamento guidato.

- Dopo un'upgrade il controller del sistema non può essere riportato alla versione precedente.
- L'aggiornamento guidato non è compatibile con Microsoft Windows XP.
- **(Raccomandato)** Eseguire l'aggiornamento guidato direttamente dal TruPortal DVD, invece che dall'immagine ISO.
- Anche se l'aggiornamento guidato offre l'opzione di effettuare il backup dei dati, è possibile creare un file di backup supplementare per precauzione (consultare Creare un file di backup a pagina 90). È possibile anche effettuare il backup delle impostazioni di configurazione (consultare Salvare e ripristinare le impostazioni predefinite a pagina 92). Per salvare un record cronologico degli eventi, utilizzare l'importazione/esportazione guidata per esportare gli eventi in formato CSV.
- Se si aggiorna da goEntry a TruPortal, le informazioni relative al formato della tessera saranno preservate.
- Prima di utilizzare l'aggiornamento guidato assicurarsi che non ci si ano utenti collegati al sistema.
- Assicurarsi che i processi di backup e ripristino siano terminati.
- Se il controller del sistema utilizza un indirizzo IP statico, l'aggiornamento sarà più rapido ed affidabile. (Per modificare queste impostazioni, consultare Configurare le impostazioni di rete a pagina 17.) Se si utilizza un indirizzo IP dinamico, l'indirizzo IP potrebbe cambiare durante l'upgrade causando l'arresto del processo. In questo caso utilizzare l'installazione guidata per ottenere un nuovo indirizzo IP, quindi riavviare l'aggiornamento guidato.
- Sulla maggior parte delle pagine della procedura guidata appare un pulsante [Fine]; utilizzarlo, se necessario, per arrestare l'aggiornamento.

Per utilizzare l'aggiornamento guidato:

1. Collegarsi al sito web del prodotto e scaricare i file seguenti nella stazione di lavoro client locale:
   - L'immagine ISO dell'ultima versione del disco utilità.
   - Il file NGP.bin utilizzato per aggiornare il firmware.

**IMPORTANTE:** Non modificare i  nomi dei file scaricati.

2. Utilizzare un'applicazione terze parti per installare (ad es. aggiungere) l'immagine ISO scaricata nella stazione di lavoro client.
3. In Windows Explorer, spostarsi nella cartella \PanelUpgradeWizard dell'immagine ISO.
4. Fare doppio clic su **PanelUpgradeWizard.exe**.

   La procedura guidata creerà la cartella \<*documenti locali*>\PanelUpgradeWizard che include due sottocartelle: \Backups e \Logs.
5. Nella pagina introduzione, selezionare una **Lingua** e fare clic su [Successivo].
6. Collegarsi come utente con autorizzazione di esecuzione per la funzione aggiornamento del firmware e fare clic su [Successivo].

   La pagina File sorgente contiene dettagli del firmware sul controller del sistema.
7. Fare clic su [...] per spostarsi nella cartella contenente il file NGP.bin.
8. Nella finestra di dialogo Apri, fare clic sul file NGP.bin per selezionarlo, quindi fare clic su [Apri].

   Il file sorgente contiene dettagli sul file NGP.bin.
9. Fare clic su [Successivo].
10. Nella pagina Backup immettere il percorso nel quale sarà salvato il backup dei dati, oppure spostarsi sulla posizione appropriata.

**Notare:** La casella **Creare file di backup** può essere deselezionata per evitare il backup dei dati, tuttavia si consiglia di lasciare la casella selezionata per effettuare il backup dei dati prima di un upgrade. Si tratta di un'opzione riservata al produttore.

**IMPORTANTE:** Se non si crea un file di backup durante l'utilizzazione dell'aggiornamento guidato, le foto non saranno salvate e dovranno essere ripristinare da un backup precedente.

11. Fare clic su [Backup].
12. All'apparizione del messaggio "Backup riuscito", fare clic su [Successivo].
13. Nella pagina successiva, fare clic su [Upgrade del firmware].

    Sarà visualizzato l'avanzamento dell'aggiornamento guidato. Questa operazione potrebbe durare dai cinque ai dieci minuti. In caso di errori saranno visualizzati quadrati rossi accanto all'errore.
14. Al termine dell'upgrade, fare clic su [Successivo].
15. Se è stato effettuato il backup dei dati nel gradino 11, la pagina Ripristino indicherà la posizione nella quale i file sono stati salvati.
    a. Fare clic su [Ripristinare] per caricare i dati salvati nel controller del sistema.
    b. All'apparizione del messaggio "Ripristino riuscito", fare clic su [Successivo] per verificare il successo dell'upgrade nella pagina Risultati dell'upgrade.
16. Dopo aver visualizzato la pagina Risultati dell'upgrade, fare clic su [Fine] per chiudere la procedura guidata.
17. In caso di aggiornamento dal sistemagoEntry a TruPortal, controllare le descrizioni del formato di tessera nella pagina ***Amministrazione del sistema > formati di tessera*** e, se necessario aggiornarli. (Le descrizioni del formato di tessera sono aggiornate solo in inglese).
18. Se IPSDC è installato, configurarlo per riconoscere l'indirizzo IP del controller del sistema *prima* di configurare IPSDC nell'interfaccia utente. Consultare Configurazione dei controller porta singola basati su IP a pagina 109.

CAPITOLO 4

# *Configurazione del sistema*

TruPortal è stato ideato per consentire, una volta configurato, di aggiungere ed eliminare rapidamente persone e credenziali e di gestire l'accesso ad un edificio. Durante la configurazione saranno definite le seguenti informazioni:

- Le aree, le porte, i lettori di credenziali, la telesorveglianza  e i sistemi di sicurezza ausiliari di un sito.
- I livelli si accesso necessari per i vari gruppi di persone che lavorano nel sito.
- La programmazione dell'accesso per i giorni feriali e per i giorni festivi.
- I ruoli operatore per il personale addetto alla gestione e alla sorveglianza del sistema.

Questo capitolo è organizzato in maniera sequenziale, con le attività presentate nell'ordine in cui devono essere completate per configurare il sistema.

**IMPORTANTE:** Se IPSDC è installato, configurarlo per riconoscere l'indirizzo IP del controller del sistema *prima* di configurarli nell'interfaccia utente. Consultare Configurazione dei controller porta singola basati su IP a pagina 109.

1. **Collegamento al sistema**.
2. **Impostare la data e l'ora**.
3. **Creare una richiesta di registrazione del certificato**.
4. **Importare un certificato di sicurezza**.
5. **Configurare le impostazioni di rete**.
6. **Configurare la sicurezza del sito**.
7. **Impostare la lingua del sistema**.
8. **Aggiungere un formato di scheda**.
9. **Scansione per le modifiche hardware**.
10. **Assegnare nomi significativi all'hardware**.
11. **Configurare il Controller del sistema**.
12. Opzionale: **Configurare i moduli di espansione I/O**.
13. **Configurare un controller della porta**.
14. **Configurare una porta**.
15. **Configurare i lettori**.
16. Opzionale: **Aggiungere un DVR/NVR**.
17. Opzionale: **Aggiungere una telecamera.**.
18. Opzionale: **Collegare le telecamere ai dispositivi per tracciare i video degli eventi.**.
19. Opzionale: **Aggiungere un area**.
20. Opzionale: **Configurare un anti-passback**.
21. Opzionale: **Assegnare i lettori alle aree**.
22. Opzionale: **Aggiungere un gruppo vacanze**.
23. Opzionale: **Aggiungere una programmazione.**.
24. Opzionale: **Aggiungere un gruppo lettori.**.
25. **Aggiungere un livello di accesso**.
26. Opzionale: **Aggiungere un ruolo operatore**.
27. Opzionale: **Configurare un Email Server**.
28. Opzionale: **Aggiungere un elenco email**.
29. Opzionale: **Aggiungere campi definiti dall'utente**.
30. Opzionale: **Programmazione del comportamento della porta e del lettore**.
31. **Importare persone e credenziali da un file CSV**.
32. Opzionale: **Configurare i trigger azione**.
33. Opzionale: **Configurare una condivisione di rete**.
34. **Creazione di un backup e di un punto di ripristino**.
35. Opzionale: **Aggiungere un record di trigger azione.**.
36. Opzionale:**Aggiungere un pacchetto lingue**.

## Collegamento al sistema

1. Avviare un browser Internet.
2. Immettere l'indirizzo IP del sistema nella barra dell'indirizzo del browser.

**Notare:** Se la porta del servizio del sistema è stata modificata, aggiungere il numero di porta all'indirizzo IP (es. https://IPaddress:*porta*).

3. Se si utilizza Internet Explorer® e viene visualizzato un avviso sul certificato di sicurezza, selezionare **continuare al sito web (sconsigliato)**.
4. Immettere un **Nome utente**.
5. Immettere una **Password**.
6. (Opzionale) Selezionare una **Lingua** differente per l'interfaccia utente.

   Per impostazione predefinita, il sistema include cinque lingue, inglese, spagnolo, francese, olandese e portoghese, ma possono esserne aggiunte altre. Consultare Gestione dei pacchetti lingue a pagina 95.
7. Fare clic su [Collegamento]
8. Se si utilizza l'interfaccia utente per la prima volta sulla stazione di lavoro del cliente, fare clic su **accettare** nella pagina dell'accordo di licenza.

La pagina ***Home*** contiene diverse procedure guidate per aggiungere rapidamente persone, credenziali, livelli d'accesso, programmazioni e vacanze. Fare clic sulla procedura guidata e seguire le istruzioni sullo schermo per aggiungere nuovi elementi oppure consultare le sezione appropriata di questo documento per le istruzioni passo a passo.

Per terminare il collegamento in seguito, fare clic sull'icona **Logout** in alto a destra dell'interfaccia utente.

## Impostare la data e l'ora

Il sistema supporta la sincronizzazione dell'ora con un server NTP (Network Time Protocol). Questa opzione, se attivata per l'interfaccia utente ed il DVR/NVR consente di mantenere la sincronizzazione dell'ora del DVR/NVR e del sistema. Senza questa opzione l'ora del sistema potrebbe variare rispetto all'ora del DVR/NVR, causare problemi di programmazione e l'utilizzazione di orari incorretti per la ricerca di video relativi ad un evento di accesso.

Si notino i dettagli seguenti sulla sincronizzazione dell'ora NTP.

- Il client NTP tenterà la sincronizzazione ogni ora.
- Per utilizzare questa opzione, il controller del sistema deve essere in grado di accedere al server NTP tramite UDP (User Datagram Protocol), porta 123. Se la porta non è accessibile, il sistema non sarà in grado di effettuare la sincronizzazione con il server NTP e sarà registrato un evento "Fallimento sinc. NTP". Consultare l'amministratore di rete del sito.
- Se l'ora del sistema è modificata manualmente entro un minuto dall'inizio di una programmazione assegnata ad una porta, la programmazione avrà un effetto immediato.

Per impostare la data e l'ora:

1. Selezionare ***Amministrazione del sistema > Impostazioni del sistema***.
2. Fare clic sulla scheda **Data e ora**.
3. Selezionare un **Fuso orario**.
4. Selezionare la **Data e ora** locale.
5. (Opzionale) Sincronizzare l'ora:
   a. Selezionare la casella **Sincronizzare con il server NTP**.
   b. Fare clic [Accettare le modifiche].
   c. Immettere l'indirizzo IP per il server NTP.
   d. Fare clic [Accettare le modifiche].
   e. Fare clic [Sinc subito].
6. Fare clic [Accettare le modifiche].

## Configurazione della sicurezza del sistema

La scheda Configurazione di rete della pagina ***Amministrazione del sistema > Impostazioni del sistema*** presenta diverse impostazioni di rete e può essere utilizzata per assegnare un certificato di sicurezza e configurare le proprietà della rete inclusa la navigazione sicura.

### Creare una richiesta di registrazione del certificato

SSL (Secure Sockets Layer) è una tecnologia di cifratura che protegge i dati trasmessi tra il server web e gli utenti del browser per prevenire l'intercettazione, la manomissione dei dati, ecc. L'utilizzazione di SSL in un sito web è in genere indicata da un'icona a forma di lucchetto nel browser, ma può anche essere indicata dalla barra dell'indirizzo verde.

Per attivare SSL nel sistema, creare una richiesta di registrazione del certificato (detta anche *CSR* o *richiesta di certificazione*), inviarla a una autorità di certificazione ed importare il certificato registrato. È possibile anche installare un certificato autofirmato. Questo blocco di testo cifrato è generato nel server sul quale il certificato è utilizzato; contiene informazioni quali il nome dell'azienda, il nome comune (ad es. il nome di dominio), la località ed il paese.

Per creare una richiesta di registrazione del certificato:

1. Selezionare ***Amministrazione del sistema > Impostazioni del sistema.***
2. Fare clic sulla scheda **Configurazione della rete**.
3. Fare clic su [Creare richiesta registrazione certificato].
   Sarà visualizzata la finestra di dialogo Creare richiesta registrazione certificato.
4. Immettere le informazioni necessarie e fare clic su [Generare].

**Notare:** Immettere l'indirizzo IP oppure il nome di dominio completo (FQDN) del server nel campo **Nome comune**. Se il pannello è configurato per l'utilizzazione di un indirizzo IP assegnato da DHCP, si raccomanda fortemente di configurare il server DHPC per l'assegnazione sempre dello stesso indirizzo IP al pannello. Altrimenti ogni volta che viene assegnato al pannello un indirizzo IP differente, sarà necessario generare ed installare un nuovo certificato.

Il testo della richiesta di registrazione del certificato (CSR) è visualizzato nella casella di testo sul lato destro della finestra di dialogo.

5. Per utilizzare un certificato autofirmato, fare clic su [Installare un certificato autofirmato].

   Il controller del sistema sarà riavviato automaticamente.

6. Per utilizzare un certificato registrato:
   a. Copiare il testo del CSR e salvarlo in un file locale per l'invio ad un'autorità di certificazione.
   b. Chiudere la finestra di dialogo Richiesta registrazione certificato.
   c. Vedere **Importare un certificato di sicurezza a pagina 17.**

## Importare un certificato di sicurezza

1. Selezionare ***Amministrazione del sistema > Impostazioni del sistema***.
2. Fare clic sulla scheda **Configurazione della rete**.
3. Fare clic su [Importare certificato]. Sarà visualizzata la finestra di dialogo Caricare certificato.
4. Fare clic su [Selezionare file].
5. Sfogliare e selezionare il file del certificato.
6. Fare clic su [Aprire]
7. Fare clic su [Caricare]

   Il controller del sistema sarà riavviato automaticamente.

## Configurare le impostazioni di rete

Le impostazioni della rete sono inizialmente impostate con l'Installation Wizard, ma possono essere aggiornate nella scheda Configurazione di rete della pagina ***Amministrazione del sistema > impostazioni del sistema***, come descritto di seguito. Per ulteriori informazioni sulle opzioni di configurazione, consultare Determinare le impostazioni della rete a pagina 8.

1. Collegarsi come utente con autorizzazione di modifica per la funzione configurazione di rete.
2. Selezionare ***Amministrazione del sistema > Impostazioni del sistema***.
3. Fare clic sulla scheda **Configurazione della rete**.
4. Fare clic su [Configurare].

   Sarà visualizzata la finestra di dialogo Proprietà della rete.

5. Per utilizzare un collegamento dinamico, selezionare **Ottenere un indirizzo IP automaticamente tramite DHCP**.
6. Per utilizzare un collegamento statico, selezionare **Utilizzare il seguente indirizzo IP** ed immetterlo.

   Per configurare un indirizzo IP statico:
   a. Immettere **l'indirizzo IP** del controller del sistema.
   b. Immettere la **maschera di sottorete**.
   c. Immettere il **gateway predefinito**.
   d. Immettere il **Server DNS**.
7. (Opzionale) Modificare la **porta del servizio** del controller del sistema.

**Notare:** La porta del servizio predefinita per un collegamento HTTPS è 443; il valore predefinito per un collegamento HTTP è 80. Le porte da 0 a 1024 (ad esempio *porte conosciute*) sono riservate ai servizi privilegiati. Si raccomanda di non utilizzare queste porte come porte del servizio.

In caso di modifica della porta, comunicare l'informazione agli utenti poiché sarà necessario aggiungere il numero di porta all'indirizzo IP del Controller del sistema (ad esempio, https://IPaddress:*porta*) per ricollegarsi dopo il riavvio del sistema.

8. Selezionare **attivare il collegamento HTTPS** per utilizzare un protocollo ipertestuale sicuro.

**IMPORTANTE:** HTTPS è altamente raccomandato per prevenire l'accesso non autorizzato al sistema.

9. In caso di modifica delle impostazioni HTTPS, svuotare la cache del browser, soprattutto se si utilizzano Firefox o Chrome.
10. Per utilizzare un collegamento SSH che verifica le stazioni di lavoro remote e consente agli utenti remoti (incluso il personale di supporto tecnico) di collegarsi al sistema, selezionare **Attivare collegamento SSH**.

**Notare:** Consultare Configurazione della sicurezza a pagina 18 per informazioni sull'impostazione di una password per un account SSH.

11. Fare clic su [Salvare] per accettare le modifiche della configurazione di rete.

    Sarà visualizzato un messaggio che indica che il controller del sistema deve essere riavviato per applicare le modifiche della configurazione della rete.
12. Fare clic su [Salvare le modifiche].

    Il sistema sarà riavviato. Gli utenti collegati perderanno la connessione e dovranno ricollegarsi. Se l'indirizzo IP del controller del sistema è stato modificato, aggiornare tutti i IPSDC del sistema per riconoscere il nuovo indirizzo IP. Consultare Utilizzazione dell' ICT per configurare gli IPSDC a pagina 112.

## Configurazione della sicurezza

La scheda Sicurezza della pagina ***Amministrazione del sistema > impostazioni del sistema*** può essere utilizzata per configurare alcuni aspetti della sicurezza fisica dell'impianto.

### Codici PIN

Il sistema può essere configurato per l'accesso solo con credenziale oppure con credenziale e Personal Identification Number (PIN). Richiedere agli utenti la presentazione di un badge (credenziale) e di immettere un PIN fornisce una sicurezza supplementare evitando l'accesso con un badge trovato o rubato. Il lettore può essere configurato come solo credenziale oppure credenziale e PIN in base alla pianificazione. (Vedere **Programmazione del comportamento della porta e del lettore a pagina 51.**)

#### Lunghezza massima del PIN

I PIN possono essere costituiti da 4, 6 o 9 cifre.

#### Numero massimo di tentativi PIN

Consente alle persone di impostare il numero massimo di tentativi per immettere correttamente il PIN.

**Durata blocco PIN:**
Se la persona immette il PIN incorretto diverse volte, l'ID della credenziale sarà bloccato dal lettore per la durata indicata in questa opzione. Alla scadenza del blocco, i privilegi dell'ID della credenziale saranno ripristinati.

### Modalità fallback porta

Le informazioni relative alle credenziali sono salvare nel controller del sistema. Se il controller doppia porta perde la comunicazione con il controller del sistema, le credenziali presentate al lettore non potranno essere verificate. In questo caso, il controller della porta deve verificare la richiesta d'accesso per chiunque acceda all'impianto.

**Notare:** Gli IPSDC hanno una modalità fallback separata.

### Immettere terminazioni EOL

Le porte possono essere cablate per rilevare se sono aperte o chiuse, forzate e manomesse. Questo tipo di porta è detta *controllata*. Una porta sprovvista di questo tipo di circuiti di rilevazione è detta non controllata anche se è provvista di un lettore e di una serratura oppure una chiusura magnetica. Per le porte controllate, questa opzione descrive i tipi di resistenza utilizzati e la cablatura del circuito. Sono controllati due tipi principali: Circuiti 1,000 Ohm e 4,700 Ohm. Questi sono cablati con resistenze doppie o con una singola resistenza cablata in serie o parallela rispetto al sensore della porta.

**Notare:** IPSDC supporta solo 1K/supervisione doppia, come configurato con l'impostazione degli interruttori del pannello. Per ulteriori informazioni consultare la *Guida rapida ai controller porta singola basati su IP.*

### Impostare la password SSH per l'account del servizio

Un collegamento SSH può essere attivato nella scheda **Sicurezza** della pagina ***Amministrazione del sistema > Impostazioni del sistema*** per verificare gli utenti remoti (incluso il personale di supporto tecnico) che si collegano al sistema. Utilizzare il pulsante [Impostare la password SSH per l'account del servizio] per impostare la password.

### Modalità fallback IPSDCU

Le informazioni relative alle credenziali sono salvare nel controller del sistema. Se un IPSDC perde la comunicazione con il controller del sistema, le credenziali presentate al lettore non potranno essere verificate. Selezionare **Utilizzare la tabella cache locale** per consentire l'accesso se la tessera presenta una delle ultime 50 credenziali utilizzate per l'accesso salvate nella cache locale IPSDC.

Si notino i dettagli seguenti sulla modalità fallback IPSDCU:

- Per i primi 40/60 secondi dopo la perdita del collegamento di rete, IPSDA continuerà a tentare di verificare le credenziali tramite il controller del sistema. Se il controller del sistema non può essere contattato, le credenziali saranno rifiutate fino all'avvio della modalità fallback IPSDC.
- Qualsiasi modifica o eliminazione delle credenziali causerà la perdita delle informazioni della cache su IPSDC.

### Criptare comunicazioni IPSDC

Per impostazione predefinita, la casella è selezionata per cifrare le comunicazioni tra il Controller del sistema e le IPSDC per migliorare la sicurezza dei dati.

## Configurare la sicurezza del sito

1. Selezionare ***Amministrazione del sistema > Impostazioni del sistema***.

2. Fare clic sulla scheda **Sicurezza**.
3. Selezionare la **Lunghezza massima del PIN**.

**IMPORTANTE:** Quando viene salvata una nuova lunghezza massima per il PIN ed esistono credenziali con numeri PIN che superano la lunghezza massima, sarà visualizzato un avviso indicante che i numeri PIN esistenti saranno troncati per adattarli alla nuova lunghezza. Il messaggio consentirà all'utente di continuare oppure di annullare l'operazione di salvataggio.

4. Selezionare il numero **massimo di tentativi PIN**.
5. Selezionare una **durata del blocco PIN**.
6. Selezionare una **modalità fallback della porta**:
   - **Nessun accesso**: Non è consentito alcun tipo di accesso.
   - **Accesso codice sito**: L'accesso è consentito se la tessera presenta uno dei formati definiti nella pagina ***Amministrazione del sistema > Formati tessera*** ed il codice del sito sulla tessera corrisponde al codice del sito indicato nel formato.
   - **Accesso completo**: L'accesso è consentito se la tessera presenta uno qualsiasi dei formati definiti nella pagina ***Amministrazione del sistema > Formati tessera***.
7. Selezionare un'opzione per le **Immissione terminazioni EOL**.
8. Se è stato attivato un collegamento SSH nella scheda Configurazione di rete, fare clic su **Impostare password SSH per l'account del servizio** per impostare una password per il collegamento degli utenti remoti al sistema.
9. Selezionare una **Modalità fallbackIPSDCU**.
   - **Nessun accesso**: Non è consentito alcun tipo di accesso
   - **Accesso codice sito**: L'accesso è consentito se la tessera presenta uno dei formati definiti nella pagina ***Amministrazione del sistema > Formati tessera*** ed il codice del sito sulla tessera corrisponde al codice del sito indicato nel formato.
   - **Accesso completo**: L'accesso è consentito se la tessera presenta uno qualsiasi dei formati definiti nella pagina ***Amministrazione del sistema > Formati tessera***.
   - **Utilizzare la tabella cache locale**: L'accesso è consentito se la tessera presenta una delle ultime 50 credenziali utilizzata per l'accesso.
10. (Consigliato) Mantenere la casella **Criptare le terminazioni IPSDCU** per criptare le comunicazioni tra il controller del sistema ed i vari IPSDC e migliorare la sicurezza dei dati
11. Fare clic su [Accettare le modifiche].

## Configurare la lingua principale del sistema

La lingua principale del sistema può essere definita nella scheda Opzioni del sistema della pagina ***Amministrazione del sistema > Impostazioni del sistema*** per determinare la lingua utilizzata per le funzioni effettuate dal sistema, quali l'assegnazione di nomi predefiniti per il dispositivo, i backup pianificati e email automatici.

La lingua del sistema è anche utilizzata per gli utenti che si collegano e selezionano una lingua non disponibile oppure se un utente effettua un'operazione linguistica (ad esempio caricare un evento nella pagina ***Eventi*** ) e la lingua utilizzata dall'utente per il collegamento non è disponibile. Questo si verifica se il pacchetto lingue è eliminato durante il collegamento dell'utente al sistema.

### Impostare la lingua del sistema

1. Selezionare ***Amministrazione del sistema > Impostazioni del sistema***.
2. Fare clic sulla scheda **Opzioni del sistema** .
3. Selezionare una **lingua del sistema**.
4. Fare clic su [Accettare le modifiche].

## Configurazione dei formati tessera predefiniti

Le credenziali (badge di identificazione) utilizzate per il controllo dell'accesso elettronico memorizzano i dati in diversi formati. Per leggere i dati correttamente il formato della tessera deve essere aggiunto alla configurazione. L'ID della credenziale memorizzato nella tessera include il numero di tessera, il codice dell'edificio e il codice di emissione.

Per poter riconoscere una credenziale, il sistema deve essere configurato per riconoscere il formato di tessera — la formattazione dei dati nel badge dell'ID. Sono forniti quattro formati di tessera predefiniti e ne possono essere aggiunti altri. Tuttavia, il sistema dovrebbe essere configurato per riconoscere solo i formati utilizzati attivamente.

I formati di tessera predefiniti includono:

- Wiegand 26 Bit (H10301) codice impianto 200
- 32 Bit 14443 sovrapporre 1
- 37 Bit (I10304) impianto 40
- 40 Bit CASI 4002

Si notino i dettagli seguenti sui formati della scheda:

- Se il sistema è aggiornato da una versione precedente, i formati di tessera esistenti saranno conservati.
- Il sistema è configurato con diversi formati commerciali di tessera e supporta fino a otto formati di tessera attivi contemporaneamente. Se si intende utilizzare un formato di tessera non elencato, può essere aggiunto come tipo personalizzato.
- Un *formato di tessera grezzo* non include il codice dell'impianto, ma tratta tutte le informazioni della tessera come parte della credenziale d'accesso. Per questo motivo le tessere di credenziali in formato grezzo sono più facili da configurare rispetto alle tessere che includono il codice dell'impianto.
- La maggior parte dei formati di tessera standard includono il codice dell'impianto come parte dell'ID della credenziale. Questo consente una maggiore complessità nella configurazione della sicurezza del sito, ma allo stesso tempo complica la configurazione. Ad esempio, se si utilizza il codice dell'impianto ed una porta entra in modalità fallback perché non riesce a comunicare con il controller del sistema, la porta può essere configurata per l'apertura con un codice impianto valido presentato al lettore. Questo si verifica perché il controller della porta non conserva il database completo della persona, ma può salvare il codice dell'impianto.

### Aggiungere un formato di scheda

1. Selezionare ***Amministrazione del sistema > Formati di tessera***.
2. Fare clic su [Aggiungere].
3. Immettere un nome descrittivo nel campo **Nome del formato** .
4. Selezionare un **Tipo di formato**.
5. Se necessario, immettere il **Codice dell'impianto**.
6. Per un formato personalizzato, immettere i dati necessari.
7. Fare clic su [Accettare le modifiche].

### Eliminare un formato di tessera

1. Selezionare ***Amministrazione del sistema > Formati di tessera***.
2. Selezionare il formato di tessera da eliminare.
3. Fare clic su [Eliminare].
   Sarà visualizzata la finestra di dialogo Eliminare elemento.
4. Fare clic su [Eliminare].

## Configurazione dei dispositivi

Questa sezione descrive la configurazione dei seguenti dispositivi:

- Controller del sistema
- Ingressi e uscite
- Controller della porta
- Porte
- Lettori
- Moduli di espansione ingressi/uscite

Per ulteriori informazioni sulla configurazione dei DVR/NVR e delle telecamere, consultare Configurazione dei dispositivi video a pagina 34.

### Prima di iniziare

Prima di configurare i dispositivi nella pagina ***Amministrazione del sistema > Dispositivi***, completare i passaggi seguenti:

1. Se IPSDC è installato, configurarlo per riconoscere l'indirizzo IP del controller del sistema *prima* di configurare IPSDC nell'interfaccia utente. Questo tipo di collegamento alla rete assicura la rilevazione di ciascun IPSDC durante la scansione per le modifiche hardware effettuata dal controller del sistema. Consultare Configurazione dei controller porta singola basati su IP a pagina 109.
2. Utilizzare il pulsante [Scansione per le modifiche hardware] per rilevare i dispositivi come indicato di seguito.
3. (Opzionale ma consigliato) Modificare i nomi generici dei dispositivi. Consultare Assegnare nomi significativi all'hardware a pagina 23.

## Scansione  per le modifiche hardware

Prima di configurare i dispositivi, fare clic sul pulsante [Scansione per le modifiche hardware] nella pagina ***Amministrazione del sistema > Dispositivi*** per rilevare i seguenti tipi di dispositivi proprietari situati downstream dal controller del sistema ed aggiungerli automaticamente alla struttura del dispositivo:

- I moduli interfaccia a due porte
- I moduli di espansione ingressi/uscite
- IPSDC già configurati per la rilevazione del controller del sistema

I controller della porta possono anche essere aggiunti alla pagina ***Dispositivi*** selezionando il controller del sistema e facendo clic su [Aggiungere]. Selezionare il tipo di controller da aggiungere, completare i campi restanti e fare clic su [Accettare le modifiche].

Il sistema assegna ai dispositivi nomi generici predefiniti che potranno essere modificati in un secondo momento (consultare Assegnare nomi significativi all'hardware a pagina 23) e visualizza i dispositivi in una struttura gerarchica nella pagina ***Amministrazione del sistema > Dispositivi***. Alcuni dei nomi predefiniti sono sequenziali (ad es. Input11, Input12, ecc.). Le porte ed i lettori ereditano il numero di serie del controller della porta parente. Ad esempio se il controller della porta ha un numero di serie 1234, le porte posizionate downstream rispetto al controller della porta saranno denominate Porta 1234-1, Porta 1234-2, ecc.

**Notare:** Se il numero di serie del controller della porta è modificato (ad esempio in caso di sostituzione), tutti gli oggetti dipendenti (porte e lettori) che utilizzano i nomi predefiniti devono essere aggiornati per riflettere il nuovo numero di serie del controller della porta parente. Consultare Sostituire un controller della porta a pagina 25.

Per rilevare i dispositivi hardware nel sistema:

**IMPORTANTE:** I controller della porta non sono in linea durante la scansione che in genere dura diversi minuti.

1. Selezionare ***Amministrazione del sistema > Dispositivi***.
2. Selezionare il Controller del sistema.
3. Fare clic su [Scansione per le modifiche hardware].
4. Fare clic su [Accettare le modifiche].

   Se il sistema rileva un problema (ad esempio nessuna batteria di backup installata), sarà visualizzata una notifica in una finestra nera nella parte superiore dell'interfaccia utente; fare clic all'interno della finestra per aprire la pagina ***Amministrazione del sistema > Diagnostica*** per ulteriori informazioni sul problema. Consultare Diagnostica a pagina 98.

## Assegnare nomi significativi all'hardware

Indipendentemente dal numero e dal tipo di dispositivi del sistema, convenzioni di  denominazione efficaci sono essenziali per la riuscita dell'implementazione. L'utilizzazione di nomi significativi e ben strutturati per gli ingressi, le uscite, i controller della porta, i lettori, ecc. aiuta a:

- Identificare la posizione e la funzione di ciascun dispositivo.
- Organizzare i dispositivi in gruppi significativi.
- Aiutare nel monitoraggio degli eventi d'accesso.

Invece di utilizzare i nomi generici assegnati ai dispositivi dall' Installation Wizard (ad esempio, *Controller porta 8888*), utilizzare elementi pertinenti per ciascuno dei dispositivi fornendo un

riferimento al tipo di dispositivo, alla posizione o altra categoria significativa per l'installazione, quale *Ingresso principale, porta muro Est*del controller della porta.

**Notare:** Se i nomi predefiniti non sono personalizzati, tenere presente che qualsiasi modifica al nome di un oggetto principale deve essere rispecchiata negli oggetti secondari (ad esempio, le porte ed i lettori collegati ad un controller della porta) per evitare nomi di dispositivi inconsistenti.

Prima di procedere, consultare la mappa dell'installazione creata all'installazione dei dispositivi, come descritto in Documentazione della posizione fisica di ciascun dispositivo a pagina 5.

1. Selezionare ***Amministrazione del sistema > Dispositivi***.
2. Selezionare il Controller del sistema.
3. Immettere un **Nome di dispositivo descrittivo**.
4. Fare clic su [Accettare le modifiche].
5. Selezionare il primo controller della porta dell'elenco.
6. Per confermare la selezione del dispositivo corretto nell'Interfaccia utente, paragonare il **Numero di serie** allo schema dell'installazione.
7. Immettere un **Nome di dispositivo descrittivo**.
8. Fare clic su [Accettare le modifiche].
9. Ripetere per tutti i dispositivi della gerarchia.

## Configurare il Controller del sistema

Il controller del sistema può accettare quattro ingressi ausiliari di uso generale e produrre due segnali in uscita di uso generale che devono essere attivati manualmente. Gli ingressi possono essere utilizzati per accessori quali un rilevatore di movimento per la stanza oppure per ingressi da altri sistemi quali un sistema d'allarme antincendio. Si tratta di configurazioni opzionali da attivare solo se installate. Gli ingressi di uso generale possono essere configurati, se attivati, per sbloccare automaticamente tutte le porte, in caso ad esempio di allarme antincendio o altre situazioni di emergenza.

1. Selezionare ***Amministrazione del sistema > Dispositivi***.
2. Selezionare il Controller del sistema.
3. Fare clic sulla scheda **Generale**.
4. Selezionare una **Telecamera collegata** se ne esiste una configurata per controllare la posizione fisica del controller del sistema.
5. Fare clic sulla scheda **Ingressi** .
6. Per ognuno degli ingressi ausiliari generali collegati:
   a. Selezionare **Attivato**.
   b. Immettere un nome significativo.
   c. Selezionare il **Tipo**.
   d. (Opzionale) Selezionare **Sbloccare tutte le porte** in caso di ingresso di un allarme o di un sistema d'emergenza.
   e. (Opzionale) Selezionare una **telecamera collegata** se ne esiste una associata all'origine dell'ingresso (ad esempio una telecamera associata al rilevatore di movimento).
7. Fare clic sulla scheda **Uscite** .
8. Per ognuna delle uscite ausiliarie generali collegate:
   a. Selezionare **Attivata**.

b. Immettere un nome significativo.
c. Selezionare **Attivo On/Off** se il relay deve essere alimentato quando l'uscita è disattivata, altrimenti deselezionare la casella.
d. (Opzionale) Selezionare una **telecamera collegata**se ne esiste una associata all'uscita.

9. Fare clic su [Accettare le modifiche].
10. Fare clic su [Riavviare controller] per riavviare il controller del sistema.

## Configurare gli ingressi e le uscite

Gli ingressi e le uscite sono opzioni ad uso generale che possono essere configurate a seconda dei bisogni del sito. Ad esempio un ingresso potrebbe essere un segnale da un rilevatore di movimento. L'uscita è un impulso elettrico dal Controller ad alcuni dispositivi.

Per configurare gli ingressi e le uscite, utilizzare la pagina ***Amministrazione del sistema > Dispositivi***. Gli ingressi e le uscite possono essere controllati nella pagina ***Controllo > ingressi/ uscite*** e le uscite possono essere attivate manualmente in questa pagina. Le uscite possono essere controllate anche dai trigger azione.

## Configurare un controller della porta

**Notare:** Se IPSDC è installato, configurarlo per riconoscere l'indirizzo IP del controller del sistema *prima* di configurarli nell'interfaccia utente. Consultare Configurazione dei controller porta singola basati su IP a pagina 109.

I controller doppia porta possono essere collegati fino a quattro lettori sulle due porte. IPSDC può essere collegato a due lettori su una porta. Ogni porta può avere due lettori, uno per l'ingresso e uno per l'uscita, in genere utilizzato con Anti-passback.

1. Selezionare ***Amministrazione del sistema > Dispositivi***.
2. Espandere la struttura sotto il controller del sistema.
3. Selezionare il controller della porta.
4. Selezionare il **numero di porte** collegate al controller.
5. (Opzionale) Selezionare una **telecamera collegata** se ne esiste una configurata per controllare la posizione fisica del controller del sistema.
6. Fare clic su [Accettare le modifiche].

**Notare:** Se tutte le porte sono bloccate e viene aggiunto un nuovo controller, il nuovo controller della porta resterà sbloccato. Per bloccarlo, tutte le porte devono essere ripristinate, quindi bloccate ancora una volta.

## Sostituire un controller della porta

**IMPORTANTE:** In caso di sostituzione del controller della porta, assicurarsi di aggiornare gli oggetti secondari con il nuovo numero di serie prima di utilizzare il pulsante [Scansione modifiche hardware] nella pagina ***Amministrazione del sistema > Dispositivi*** come descritto di seguito. Altrimenti le informazioni di configurazione saranno sovrascritte.

Per sostituire un controller della porta e conservarne la configurazione, consultare:

1. Effettuare il backup del database, come descritto in Creare un file di backup a pagina 90.
2. Sostituire il pannello del controller della porta.
3. (SOLO PER IPSDC) Utilizzare lo strumento di configurazione integrato (ITC) per configurare il nuovo IPSDC per rilevare l'indirizzo IP del controller del sistema. Consultare Configurazione dei controller porta singola basati su IP a pagina 109.
4. Aggiornare il numero di serie dell'IPSDC nella pagina ***Amministrazione del > sistema Dispositivi*** .
5. Se gli oggetti secondari (porte e lettori) utilizzano ancora i nomi predefiniti, devono essere aggiornati con il nuovo numero di serie del controller della porta principale.
6. Riavviare il controller del sistema Consultare Riavviare il controller del sistema a pagina 98.
7. Dopo il riavvio, collegarsi nuovamente al controller del sistema.

   Il controller della porta apparirà non in linea fino al collegamento al controller del sistema.
8. (Raccomandato) Una volta online con il nuovo numero di serie, effettuare il backup del database e salvare la configurazione aggiornata del controller della porta. Consultare Creazione del backup dei dati a pagina 89 e Salvare e ripristinare le impostazioni predefinite a pagina 92.

## Configurare le porte

Ogni porta deve essere configurata per:

- Il periodo di tempo durante il quale deve essere sbloccata alla presentazione di una credenziale valida.
- Il periodo di tempo durante il quale può essere tenuta aperta senza far scattare l'allarme.
- Il tipo di serratura utilizzata (serratura standard o magnetica).
- Se necessita  il lettore solo per l'ingresso o per l'ingresso e l'uscita.
- Il tipo di eventi e allarmi monitorati dalla circuiteria.
- Gli ingressi e relay ausiliari. Ad esempio una porta può essere configurata con apertura automatica o una richiesta di uscita estesa (RTE) per facilitare l'accesso da parte dei portatori di handicap.

### Configurare una porta

1. Selezionare ***Amministrazione del sistema > Dispositivi***.
2. Espandere la struttura sotto il controller del sistema.
3. Espandere la struttura sotto il controller della porta.
4. Selezionare la porta da configurare.

**Notare:** Alcuni campi non appariranno nella pagina ***Dispositivi*** se la porta è collegata ad un IPSDC che non supporta tipi di ingresso/uscita ausiliari o i punti d'ingresso tamper. Consultare *Guida rapida controller porta singola basato su IP* per ulteriori informazioni sulla modifica delle impostazioni dell'interruttore DIP per i tipi di ingresso. Dopo la modifica delle impostazione dell'interruttore DIP, riavviare IPSDC.

5. Selezionare un **orario regolare di ingresso autorizzato**.
6. (Opzionale) Selezionare un **orario ingresso autorizzato esteso**.
7. Selezionare una **Durata porta lasciata aperta**.
8. (Opzionale) Selezionare una **durata estesa porta lasciata aperta**.

9. Selezionare **modalità apriporta**:
   - **Sblocco temporizzato**
   - **Bloccare alla chiusura**
10. (Opzionale) Selezionare una **telecamera collegata** se ne esiste una associata per il controllo della porta.
11. Selezionare una **Modalità accesso**.
12. (Opzionale) Selezionare una **Richiesta di uscita attivata** se la porta è cablata per questa opzione.
13. (Opzionale) Se **Richiesta di uscita attivata** è selezionata, selezionare **Non attivare sblocco su RTE** per prevenire l'attivazione del fermaporta alla chiusura del contatto Richiesta di uscita.
14. (Opzionale) Selezionare gli allarmi collegati alla porta per:
    - **Apertura prolungata**
    - **Apertura forzata**
    - **Tamper**
15. (Opzionale) Se la porta è collegata ad un allarme luminoso o sonoro, selezionare “Porta trattenuta/forzata” dall'elenco **Relay aus** .
16. Configurare il sensore **Tipi di ingresso** per:
    - Il sensore**Contatto porta**
    - Il pulsante o sensore**Richiesta di uscita**
    - Ingresso**Aus** da Richiesta di uscita estesa o sensore contatto serratura magnetica
    - Circuiteria**Tamper**

**Notare:** Gli ingressi aus e tamper elencati qui sopra non si applicano alle porte collegate a IPSDC.

17. Fare clic su [Accettare le modifiche].
18. Ripetere per ciascuna porta.

## Configurare una porta per l'accesso ai portatori di handicap.

Gli eventi sono registrati quando una porta resta aperta troppo a lungo e in caso di accesso consentito ma la porta non è aperta. Con un allarme luminoso o sonoro, il sistema è in grado di attivare un allarme fisico in caso di porta forzata o di apertura prolungata.

Per accomodare i bisogni di coloro che necessitano più tempo per aprire o passare attraverso la porta, il sistema consente agli utenti di identificare le credenziali ottenute con questo tipo di autorizzazione e consente agli utenti di configurare funzioni supplementari quali l'apertura automatica della porta e più tempo per i sensori di Richiesta di uscita. Si tratta di una configurazione a livello della credenziale per preservare la sicurezza del sito, poiché più la porta rimane aperta, più facile è l'ingresso senza presentare credenziali. Vedere **Aggiungere una credenziale a pagina 70.**

1. Selezionare ***Amministrazione del sistema > Dispositivi***.
2. Espandere la struttura sotto il controller del sistema.
3. Espandere la struttura sotto il controller della porta.
4. Selezionare la porta da configurare.

**Notare:** Alcuni campi non appariranno nella pagina ***Dispositivi*** se la porta è collegata ad un IPSDC che non supporta tipi di ingresso/uscita ausiliari o i punti d'ingresso tamper. Consultare la *Guida rapida controller porta singola basato su IP* per ulteriori informazioni sulla modifica delle impostazioni dell'interruttore per i tipi di ingresso.

5. Selezionare un **orario regolare di ingresso autorizzato**.
6. Selezionare un **orario ingresso autorizzato esteso**.

   Si tratta della durata di sblocco della porta per consentirne l'apertura.
7. Selezionare una **Durata porta lasciata aperta**.
8. Selezionare una **durata estesa porta lasciata aperta**.

   Si tratta della durata di apertura della porta per consentire l'ingresso.
9. Selezionare **modalità apriporta**:
   - **Sblocco temporizzato**
   - **Bloccare alla chiusura**
10. (Opzionale) Selezionare una **telecamera collegata** se ne esiste una associata per il controllo della porta.
11. Selezionare una **Modalità accesso**.
12. (Opzionale) Selezionare una **Richiesta di uscita attivata** se la porta è cablata per questa opzione.
13. (Opzionale) Se **Richiesta di uscita attivata** è selezionata, selezionare **Non attivare sblocco su RTE** per prevenire l'attivazione del fermaporta alla chiusura del contatto Richiesta di uscita.
14. (Opzionale) Selezionare gli allarmi collegati alla porta per:
    - **Apertura prolungata**
    - **Apertura forzata**
    - **Tamper**
15. Se la porta è cablata per un apriporta:
    a. Selezionare “RTE esteso” dall'elenco **Ingresso aus.**
    b. Selezionare “**Apriporta**” dall'elenco **Relay aus**.
    c. Selezionare un **Relay aus in orario**.
16. Configurare il sensore **Tipi di ingresso** per:
    - Sensore **contatto porta**
    - Pulsante o sensore**Richiesta di uscita**
    - Ingresso**Aus** da Richiesta di uscita estesa o sensore contatto serratura magnetica
    - Circuiteria**Tamper**

**Notare:** Gli ingressi aus e tamper elencati qui sopra non si applicano alle porte collegate a IPSDC.

17. Fare clic su [Accettare le modifiche].
18. Ripetere per ciascuna porta.

## Configurare una porta per le serrature magnetiche

***• AVVERTIMENTO! •*** Quando si configura una porta con una chiusura magnetica, è importante utilizzare l'opzione "sensore chiusura elettromagnete" per prevenire l'attivazione prematura dei magneti della porta e la chiusura inaspettata della porta, che potrebbe causare infortuni.

1. Selezionare ***Amministrazione del sistema > Dispositivi***.
2. Espandere la struttura sotto il controller del sistema.
3. Espandere la struttura sotto il controller della porta.
4. Selezionare la porta da configurare.

**Notare:** Alcuni campi non appariranno nella pagina ***Dispositivi*** se la porta è collegata ad un IPSDC che non supporta tipi di ingresso/uscita ausiliari o i punti d'ingresso tamper. Consultare *Guida rapida controller porta singola basato su IP* per ulteriori informazioni sulla modifica delle impostazioni dell'interruttore per i tipi di ingresso.

5. Selezionare un **orario regolare di ingresso autorizzato**.
6. Selezionare un **orario ingresso autorizzato esteso**.

   Si tratta della durata di sblocco della porta per consentirne l'apertura.
7. Selezionare una **Durata porta lasciata aperta**.
8. Selezionare una **durata estesa porta lasciata aperta**.

   Si tratta della durata di apertura della porta per consentire l'ingresso.
9. Selezionare **modalità apriporta**:
   - **Sblocco temporizzato**
   - **Bloccare alla chiusura**
10. (Opzionale) Selezionare una **telecamera collegata** se ne esiste una associata per il controllo della porta.
11. Selezionare una **Modalità accesso**.
12. (Opzionale) Selezionare una **Richiesta di uscita attivata** se la porta è cablata per questa opzione.
13. (Opzionale) Se **Richiesta di uscita attivata** è selezionata, selezionare **Non attivare sblocco su RTE** per prevenire l'attivazione del fermaporta alla chiusura del contatto Richiesta di uscita.
14. (Opzionale) Selezionare gli allarmi collegati alla porta per:
    - **Apertura prolungata**
    - **Apertura forzata**
    - **Tamper**
15. Selezionare "**Sensore blocco elettromagnete**" dall'elenco the **Ingressoaus.**
16. (Opzionale) Se la porta è collegata ad un allarme luminoso o sonoro, selezionare "Porta trattenuta/forzata" dall'elenco **Relay aus** .
17. Configurare il sensore **Tipi di ingresso** per:
    - Sensore **Contatto porta**
    - Pulsante o sensore**Richiesta di uscita**
    - Ingresso**Aus** da Richiesta di uscita estesa o sensore contatto serratura magnetica
    - Circuiteria**Tamper**

**Notare:** Gli ingressi aus e tamper elencati qui sopra non si applicano alle porte collegate a IPSDC.

18. Fare clic su [Accettare le modifiche].
19. Ripetere per ciascuna porta.

## Opzioni configurazione porta

**Orario regolare di ingresso autorizzato**
Quando il lettore effettua la scansione di una credenziale valida, la porta sarà bloccata per la durata selezionata qui.

**Notare:** Le serrature wireless Schlage AD-400 ignorano queste impostazioni. Configurare il valore **Chiudere nuovamente in seguito** nell'utilità del software Schlage. Per informazioni dettagliate, consultare la *TruPortal Guida rapida alle serrature wireless*.

**Orario ingresso autorizzato esteso:**
Quando il lettore effettua la scansione di una credenziale valida con l'opzione **Utilizzare durata di sblocco/attesa estesi** (configurata nella pagina ***Gestione dell'accesso > Persone*** ), la porta sarà sbloccata per la durata **Orario regolare di ingresso autorizzato** e **Orario ingresso autorizzato esteso**. Questo consente agli utenti di configurare il sistema in conformità con la legislazione che regola l'accesso da parte dei portatori di handicap.

**Notare:** Le serrature wireless Schlage AD-400 ignorano queste impostazioni. In alternativa, configurare questa funzione nel software Schlage . Per informazioni dettagliate, consultare la *TruPortal* Guida rapida alle serrature wireless.

**Tempo lasciata aperta:**
Quando il lettore effettua la scansione di una credenziale valida, la porta sarà aperta per la durata **Orario regolare di ingresso autorizzato** e **Apertura prolungata**. Sarà registrato un evento se la porta è aperta più a lungo e l'opzione **Apertura prolungata** è selezionata.

**Tempo apertura prolungata esteso**
Quando il lettore effettua la scansione di una credenziale valida con l'opzione **Utilizzare durata di sblocco/attesa** estesi (configurata nella pagina ***Gestione dell'accesso > Persone*** ), la porta potrà restare aperta per la durata **Orario regolare di ingresso** autorizzato e **Apertura prolungata estesa**. Sarà registrato un evento se la porta è aperta più a lungo e l'opzione **Apertura prolungata** è selezionata. Questo consente agli utenti di configurare il sistema in conformità con la legislazione che regola l'accesso da parte dei portatori di handicap.

**Richiesta di uscita attivata**
Se la porta è dotata d'allarme per l'apertura forzata, per l'apertura prolungata o e per la manomissione, Richiesta di uscita (RTE) deve essere utilizzata con un pulsante da premere per uscire, con un lettore utilizzato per l'uscita oppure con sensore che rileva un individuo che si avvicina alla porta dall'interno. Altrimenti, ogni volta che qualcuno esce, sarà attivato l'allarme porta forzata.

**Non attivare sblocco su RTE**
Un contatto Richiesta di uscita è in genere un pulsante situato accanto alla porta associata. Selezionare questa opzione per evitare l'alimentazione dell'apriporta alla chiusura del contatto RTE. Quando un titolare di tessera preme il pulsante, viene inviata una RTE al controller del sistema. (RTE detti anche REX.)

Se la casella è selezionata, l'apriporta NON sarà alimentato alla chiusura di un contatto RTE. Se la casella non è selezionata, l'apriporta sarà alimentato alla chiusura del contatto RTE.

## Modalità apriporta

**Sblocco temporizzato**
Quando l'accesso è consentito, la porta resterà aperta fino alla scadenza dell' **orario regolare di ingresso autorizzato.**

Se l'**ingresso aus** della porta è configurato su sensore blocco elettromagnete, il relay dell'apriporta resterà attivo finché il sensore magnetico del contatto è attivo, il contatto della porta è chiuso, indipendentemente dalla durata dello sblocco.

**Notare:** Gli IPSDC non supportano gli ingressi e le uscite ausiliarie. Le serrature wireless Schlage AD-400 ignorano queste impostazioni.

#### Bloccare alla chiusura

Quando l'accesso è consentito, la porta resterà aperta fino alla scadenza dell'**orario regolare di ingresso autorizzato**, oppure se la porta è aperta e chiusa, a seconda di quale delle due si verifichi per prima.

Se l'ingresso **AUS della porta** è configurato su *sensore blocco elettromagnete*, il relay dell'apriporta resterà attivo finché il sensore magnetico del contatto è attivo, il contatto della porta è chiuso, indipendentemente dalla durata dello sblocco.

**Notare:** Gli IPSDC non supportano gli ingressi e le uscite ausiliarie. Le serrature wireless Schlage AD-400 ignorano queste impostazioni.

### Modalità di accesso

#### Lettore solo ingresso

La porta è dotata di un lettore che effettua la scansione solo delle credenziali d'ingresso, ma non richiede la presentazione delle credenziali per uscire.

#### Lettore ingresso lettore uscita

La porta è dotata di lettori che effettuano la scansione delle credenziali di ingresso e di uscita. Si tratta di un'opzione obbligatoria per le configurazioni anti-passback.

### Allarme attivato

#### Apertura prolungata

Selezionare questa opzione se la porta è cablata per la rilevazione dell'apertura. Se la porta è mantenuta aperta oltre la durata selezionata in **Durata apertura prolungata**, sarà registrato un evento nella pagina ***Eventi***.

#### Apertura forzata

Selezionare questa opzione se la porta è cablata per la rilevazione dell'ingresso forzato. Se una persona apre la porta senza presentare una credenziale d'accesso, sarà registrato un evento nella pagina ***Eventi***. Configurare con un allarme luminoso o sonoro collegato al **Relay aus** se è necessario un allarme fisico in caso di forzatura della porta.

#### Tamper

Selezionare questa opzione se la porta è cablata per la rilevazione della manomissione del lettore. In caso di manomissione, sarà registrato un evento nella pagina ***Eventi***.

**Notare:** La casella **Tamper** controlla solo la manomissione dell'ingresso, non il contatto porta, la richiesta d'uscita o i punti d'ingresso ausiliare. Inoltre, l'opzione non apparirà nella pagina ***Sistema Amministrazione > Dispositivi*** se la porta è collegata ad un IPSDC che non supporta l'ingresso tamper lettore.

### Ingresso ausiliario

**Notare:** Alcuni campi non appariranno nella pagina ***Sistema Amministrazione > Dispositivi*** se la porta è collegata ad un IPSDC che non supporta tipi di ingresso/uscita ausiliari o i punti d'ingresso tamper. Consultare *Guida rapida controller porta singola basato su IP* per ulteriori informazioni sulla modifica delle impostazioni dell'interruttore per i tipi di ingresso.

#### Nessuno

Indica che l'ingresso non è utilizzato e non è controllato.

**RTE esteso**
Da utilizzarsi solo con l'opzione Apriporta selezionato per **Relay aus**.

**Sensore elettromagnete**
Da utilizzarsi per le porte che utilizzano la chiusura magnetica invece della serratura. Rileva la segnalazione della serratura magnetica e indica l'adesione della porta al magnete. Il sistema non attiverà il magnete fino alla segnalazione del sensore di chiusura della porta indicante il contatto della porta al magnete ed il sensore del contatto porta indica che la porta è chiusa. Questo impedisce l'attivazione prematura del magnete che potrebbe causare la chiusura inaspettata della porta.

Se "Sblocco temporizzato" è selezionato per **Modalità apriporta**, il magnete resterà inattivo fino alla scadenza del tempo prestabilito. Tuttavia, non sarà attivato fino alla ricezione dei segnali provenienti dal sensore di chiusura magnetica ed il sensore di contatto porta indicanti la chiusura della porta ed il contatto con il magnete.

### Relay ausiliario

**Notare:** Alcuni campi non appariranno nella pagina ***Sistema Amministrazione > Dispositivi*** se la porta è collegata ad un IPSDC che non supporta tipi di ingresso/uscita ausiliari o i punti d'ingresso tamper. Consultare *Guida rapida controller porta singola basato su IP* per ulteriori informazioni sulla modifica delle impostazioni dell'interruttore per i tipi di ingresso.

**Nessuno**
Indica che l'ingresso non è utilizzato e non è alimentato.

**Apertura prolungata/forzata**
Questa opzione in genere è utilizzata con un allarme fisico quale una sirena o una luce, azionato quando la porta è trattenuta o forzata.

**Apriporta**
Utilizzato in genere con una porta configurata con un singolo lettore per l'ingresso ed il rilascio manuale per la richiesta di uscita (RTE), ed un pulsante per l'apriporta automatico RTE esteso. Il segnale RTE mantiene sbloccata la porta per la durata dello sblocco manuale per consentire l'uscita. L'ingresso ausiliario (RTE esteso) attiva il relay ausiliare per il Relay ausiliare in orario indicato. L'uscita relay attiva un apriporta che automaticamente sblocca e apre la porta per una persona che ha bisogno d'aiuto.

Si tratta di un'impostazione utile solo se **Ingresso ausiliare**è configurato per RTE esteso.

### Tipi di ingresso

**NO (aperto normalmente)**
Il sensore dell'interruttore è aperto normalmente.

**NC (chiuso normalmente)**
Il sensore dell'interruttore è chiuso normalmente.

**Senza supervisione**
Il circuito non è cablato con un circuito continuato per rilevare la manomissione.

**Controllato**
Il circuito è cablato con un circuito continuato per rilevare la manomissione.

**Notare:** Per gli IPSDC, consultare la *Guida rapida ai controller porta singola basati su IP* per informazioni sulla configurazione delle impostazioni degli interruttori in base al tipo di ingresso selezionato.

## Configurare i lettori

1. Selezionare ***Amministrazione del sistema > Dispositivi***.
2. Espandere la struttura sotto il controller del sistema.
3. Espandere la struttura sotto il controller della porta.
4. Espandere la struttura sotto la porta.
5. Selezionare il lettore da configurare.
6. Selezionare una **Modalità accesso**.
   - **Solo credenziale**
   - **Credenziale e PIN**
7. Selezionare **Telecamera collegata** se ne esiste una per il controllo di una determinata porta e lettore.
8. Fare clic [Accettare le modifiche].
9. Ripetere per gli altri lettori.

## Opzioni di configurazione del lettore

**Solo credenziale**
La persona deve essere dotata di una credenziale valida (tessera ID) per l'accesso.

**Credenziale e PIN**
La persona deve presentare una credenziale valida per l'accesso ed immettere un PIN (Personal Identification Number). Evitando in tal modo l'accesso con una credenziale trovata o rubata. Alcuni edifici utilizzano **Solo credenziale** durante il giorno e **Credenziale e PIN** durante le ore di chiusura dell'edificio.

### Configurare i moduli di espansione I/O

1. Selezionare ***Amministrazione del sistema > Dispositivi***.
2. Selezionare espansore I/O.
3. Fare clic sulla scheda **Generale**.
4. Selezionare una **Telecamera collegata** se ne esiste una configurata per controllare ila posizione fisica del controller del sistema.
5. Selezionare **Allarme tamper attivato** se il varco è cablato per la rilevazione del tamper.
6. Fare clic sulla scheda **Ingressi**.
7. Per ognuno degli ingressi ausiliari generali collegati:
   a. Selezionare **Attivato**.
   b. Immettere un nome significativo.
   c. Selezionare il **Tipo**.
   d. (Opzionale) Selezionare **Sbloccare tutte le porte** in caso di ingresso di un allarme o di un sistema d'emergenza.
   e. (Opzionale) Selezionare una **telecamera collegata** se ne esiste una associata all'origine dell'ingresso (ad esempio una telecamera associata al rilevatore di movimento).
8. Per ognuna delle uscite ausiliarie generali collegate:
   a. Selezionare **Attivato**.
   b. Immettere un nome significativo.
   c. Selezionare **Attivo On/Off** se il relay deve essere alimentato quando l'uscita è disattivata, altrimenti deselezionare la casella.
   d. (Opzionale) Selezionare una **telecamera collegata**se ne esiste una associata all'uscita.
9. Fare clic [Accettare le modifiche].

## Configurazione dei dispositivi video

I record video possono essere visualizzati accedendo ai video registrati sul DVR/NVR dalle telecamere associate con un dispositivo collegato al controller del sistema. Se il dispositivo rileva un evento, il sistema registrerà la data e l'ora dell'evento. Se la telecamera è collegata al dispositivo, il sistema utilizzerà la data e l'ora dell'evento per creare un collegamento ipertestuale al video registrato sul DVR/NVR collegato alla telecamera.

Il collegamento di una telecamera al dispositivo, consente al sistema di associare un evento rilevato nel dispositivo con il video registrato dalla camera nell'intervallo di tempo dell'evento. Il sistema non controlla direttamente la telecamera o il DVR/NVR, ma utilizza l'informazione per indicare al DVR/NVR la data e l'ora e la telecamera che ha registrato l'evento da riprodurre.

Esistono due tipi di telecamera di sorveglianza: fisse o con capacità panoramica, inclinazione e zoom (PTZ). Gli utenti possono controllare le telecamere PTZ se:

- Il browser utilizzato è Internet Explorer,
- È installatoMicrosoft .NET Framework 4.5 (o successivo),
- I controlli ActiveX sono attivati per il browser e
- la telecamera è collegata a un DVR/NVR.

## Aggiungere un DVR/NVR

Prima di aggiungere un DVR/NVR, consultare le note di rilascio per determinare i requisiti minimi del firmware. Consultare la documentazione relativa al DVR/NVR per le istruzioni di aggiornamento del firmware.

1. Selezionare ***Amministrazione del sistema > Dispositivi > Telecamere***.
2. Fare clic su [Aggiungere] e selezionare il modello DVR/NVR.
3. Immettere un nome descrittivo per il dispositivo nel campo **Nome dispositivo** .
4. Immettere l'**indirizzo IP** del dispositivo.
5. Immettere il **nome utente** per collegarsi al dispositivo.
6. Immettere la **password** per collegarsi al dispositivo.
7. Fare clic su [Accettare le modifiche].
8. Fare clic sul collegamento qui sotto **Configurazione e controllo del web browser** per confermare il collegamento e verificare la configurazione delle telecamere collegate al dispositivo.

## Aggiungere una telecamera.

Prima di effettuare questa operazione, il DVR/NVR deve essere aggiunto al sistema.

1. Selezionare ***Amministrazione del sistema > Dispositivi > Telecamere***.
2. Selezionare il DVR/NVR con la telecamera da aggiungere
3. Selezionare ***Aggiungere > Telecamera.***
4. Immettere un nome descrittivo per la telecamera nel campo **Nome dispositivo** .

   Ad esempio, "telecamera ingresso principale".
5. Selezionare **l'ingresso DVR** appropriato.

   Si tratta del canale DVR/NVR al quale la telecamera è collegata fisicamente.
6. Selezionare una **Larghezza di banda dello stream video**.

   Se non si conosce la larghezza di banda, collegarsi all'interfaccia web del DVR/NVR e consultare le impostazioni della telecamera.
7. Immettere la **Durata della riproduzione pre-evento**.

   È l'intervallo di tempo che precede l'evento che apparirà nella riproduzione. Ad esempio un evento di apertura forzata della porta sarà registrato nel sistema al momento dell'apertura forzata, tuttavia, la persona che ha forzato la porta ha probabilmente impiegato diversi secondi per la manomissione della porta prima dell'apertura.

Una telecamera può anche essere impostata per controllare la posizione fisica del controller del sistema. Consultare Configurare il Controller del sistema a pagina 24.

## Aggiungere layout video

I layout video determinano il numero di ingressi della telecamera che possono essere controllati su uno schermo di computer contemporaneamente.

1. Selezionare ***Controllo > Layout video.***
2. Fare clic su [Aggiungere].
3. Immettere un nome descrittivo nel campo **Nome layout video** .

   Se ad esempio sono installate quattro telecamere per il controllo della piattaforma di carico, creare un layout 2x2 e chiamarlo "Telecamere piattaforma di carico."
4. Selezionare un **Tipo di layout video**.
5. Selezionare una telecamera per ogni cella del layout.
6. Fare clic su [Accettare le modifiche].

## Collegare le telecamere ai dispositivi per tracciare i video degli eventi.

I lettori creano un evento per gli accessi consentiti e gli accessi rifiutati e se una telecamera è collegata al lettore, gli utenti disporranno di una registrazione di chiunque sia passato (o meno) attraverso un determinato varco.

Le porte creeranno eventi in caso di apertura forzata, apertura prolungata e sblocco temporaneo e se una telecamera è collegata alla porta, gli utenti avranno un record degli incidenti di sicurezza.

Gli ingressi e le uscite ausiliarie sono dispositivi opzionali collegati al controller del sistema o al modulo di espansione I/O. Per collegare una telecamera a questi dispositivi, utilizzare la scheda Ingresso o Uscita del controller del sistema.

1. Collegare il sistema (tramite rete TCP/IP) al DVR/NVR e alla telecamera.
   a. Vedere **Aggiungere un DVR/NVR a pagina 35.**
   b. Vedere **Aggiungere una telecamera. a pagina 35.**
2. Selezionare ***Amministrazione del sistema > Dispositivi***.
3. Selezionare il dispositivo dalla struttura gerarchica.
4. Selezionare la telecamera dall'elenco **Telecamera collegata.**

# Configurare le aree

Le aree rappresentano gli spazi nella planimetria del piano fisico dell'edificio, in particolare gli ingressi e le uscite a tali spazi. La definizione delle aree consente agli utenti di identificare i lettori che danno accesso agli spazi e quelli che consentono di passare ad aree adiacenti. Le aree sono utilizzare per tracciare la posizione di un utente nell'edificio, visualizzabile nel  Report presenze e per la rilevazione Anti-Passback (APB) delle credenziali.

## Aggiungere un area

Prima di assegnare un lettore ad un'area, è necessario creare un'area.

1. Selezionare ***Gestione dell'accesso > Aree > Definire l'area***.
2. Fare clic su [Aggiungere].
3. Immettere un nome descrittivo nel campo **Nome dell'area** .
4. Selezionare un'opzione **Reimpostazione automatica anti-passback.**

   Se si seleziona "Mai", la violazione anti-passback deve essere reimpostata manualmente.
5. Fare clic su [Accettare le modifiche].

## Assegnare i lettori alle aree

Le aree nel sistema sono definite dall'assegnazione dei lettori a determinate aree. Il sistema registra il lettore che ha effettuato la scansione della credenziale e in base all'assegnazione dell'area, stabilisce l'area nella quale il titolare della credenziale deve trovarsi ed i lettori attraverso i quali deve transitare prima di spostarsi in un'altra area.

**IMPORTANTE:** Assicurarsi che l'assegnazione del lettore sia corretta. Se una credenziale è rilevata presso un lettore non contiguo all'ultimo lettore, sarà rilevata una violazione anti-passback. Se ad esempio il Lab A è adiacente al corridoio principale ed è impostato in modo tale che il Lettore 1 consente l'accesso ed il Lettore 2 consente l'uscita, ma l'utente assegna erroneamente il Lettore 3 come uscita, ogni persona che tenta di uscire dal Lab A causerà una violazione anti-passback.

1. Selezionare ***Gestione dell'accesso > Aree > Assegnazione lettori***.
2. Per ogni lettore:
   a. Selezionare **da area**. Si tratta dell'area nella quale si trova il lettore.
   b. Selezionare **all'area**. Si tratta dell'area alla quale l'utente avrà accesso quando il lettore avrà accettato le credenziali.
   c. Selezionare **Anti-Passback**:
      - **Nessuno**
      - **Soft**
      - **Hard**
3. Fare clic su [Accettare le modifiche].

### Eliminare un' area

**Notare:** L' area predefinita non può essere eliminata.

1. Selezionare ***Gestione dell'accesso > Aree > Definire l'area***.
2. Selezionare un'area da eliminare.
3. Fare clic su [Eliminare].
   Sarà visualizzata la finestra di dialogo Eliminare elemento.
4. Fare clic su [Eliminare].

## Configurare l'anti-passback

L'anti-passback necessita l'uso di una credenziale per l'ingresso e l'uscita da un'area per consentire al sistema di registrare l'area nella quale si trova il titolare della credenziale. Il sistema registra i movimenti del personale nelle aree sicure ed impedisce il passaggio ad aree logicamente impossibili.

Se un utente utilizza una credenziale per accedere ad un'area configurata per l'anti-Passback e poi esce dall'area (ad esempio attraverso una porta tenuta aperta da un altro utente), il sistema non registra l'uscita dell'utente dall'area. Di conseguenza, se il sistema è configurato per l'applicazione dell'anti-passback, impedirà l'utilizzazione della credenziale in un'area differente, inclusa quella nella quale si è appena transitato fino alla reimpostazione della posizione della credenziale ad un'area predefinita o neutra.

#### Opzioni anti-passback

Una violazione anti-passback si verifica quando una persona presenta una credenziale (badge id) per accedere ad un'area, ma in qualche modo lascia l'area senza presentare l'id. L'evento è registrato quando la persona tenta di accedere ad un'altra area non collegata fisicamente all'ultima posizione rilevata della persona.

**Nessuno**
L'anti-passback non è utilizzato.

**Soft**
Quando una credenziale non rispetta le regole anti-passback, viene registrato un evento.

**Hard**
La credenziale in violazione dell'anti-passback non consente l'accesso alle aree fino al ripristino della posizione della credenziale ad area neutrale o predefinita.

### Configurare un anti-passback

Per configurare l'anti-passback, aggiungere aree nel sistema che corrispondono alle aree del sito o alla planimetria, assegnare lettori alle aree ed aggiungere credenziali.

1. Vedere **Aggiungere un area a pagina 37.**
2. Vedere **Assegnare i lettori alle aree a pagina 37.**
3. Vedere **Aggiungere una credenziale a pagina 70.**

**Notare:** Il riquadro Credenziale della pagina ***Gestione dell'accesso > Persone*** consente agli utenti di esentare singole credenziali dall'applicazione dell'anti-passback.

## Creazione di gruppi di vacanze

Le vacanze sono eccezioni della programmazione del posto di lavoro. La creazione di un gruppo vacanze per questi giorni causerà la sovrascrittura della programmazione normale per quei giorni da parte del sistema. Se la vacanza non deve sovrascrivere una determinata programmazione, il gruppo vacanze deve essere incluso nella programmazione.

Ad esempio, un edificio è aperto dal lunedì al venerdì tranne durante alcuni giorni festivi, durante i quali l'accesso è consentito solo agli addetti alle pulizie ed agli amministratori di rete. Gli addetti alle pulizie effettuano una pulizia estensiva quando l'edificio è chiuso alle attività normali. Gli amministratori di rete potrebbero utilizzare i giorni festivi per operazioni di manutenzione estensiva oppure aggiornamenti che potrebbero disturbare una giornata normale di lavoro.

Per accomodare questi bisogni, creare un gruppo vacanze per i giorni in cui il personale non lavora. Poi creare due programmazioni e due livelli d'accesso, uno per il personale normale ed uno per il personale d'assistenza (ad esempio addetti alle pulizie e amministratori di rete). Includere il gruppo vacanze nella programmazione del personale di assistenza e non in quella del personale normale. Per impostazione predefinita. quando un gruppo vacanze è creato, è "escluso" automaticamente dalle programmazioni e la programmazione non funzionerà quel giorno.

Al momento della configurazione del livello d'accesso del personale di assistenza, assegnare la programmazione del personale di supporto ai lettori ed ai gruppi di lettori utilizzati dal personale di assistenza. (Ricordarsi di "includere" il gruppo vacanze selezionandolo nella programmazione, per consentire l'accesso a questo gruppo di persone durante i giorni festivi.) Al momento della configurazione del livello d'accesso del personale normale, assegnare la programmazione del personale normale ai lettori ed ai gruppi di lettori utilizzati dal personale normale.

Notare i dettagli seguenti sull'impatto dei giorni festivi sulla programmazione:

- Quando una data è contrassegnata come giorno festivo, il sistema fa un'eccezione a tutte le normali operazioni per quel giorno o gruppo di giorni, a meno che esista una programmazione personalizzata da utilizzare nella stessa data.

  Ad esempio, se una porta è programmata per l'apertura tutti i giorni dalle 8 alle 17, la porta rimarrà chiusa in un giorno festivo invece di sbloccarsi. Un altro esempio si verifica se una persona che accede ad una determinata porta il mercoledì ed un giorno festivo cade di mercoledì, la persona non potrà accedere alla porta quel giorno.
- Per fare un'eccezione per una persona che necessita l'acceso all'edificio durante un giorno festivo, la persona deve essere assegnata ad una programmazione esclusa dal gruppo di vacanze.

  Ad esempio, per consentire l'accesso ad una persona il giorno di Natale, modificare il livello d'accesso della persona (ad esempio, un accesso chiamato "personale di supporto"), collegare l'accesso ad una programmazione specifica (ad esempio una programmazione chiamata "24/7"), quindi modificare la programmazione 24/7 includendo il giorno di Natale.
- Per sbloccare una programmazione durante un giorno festivo, aggiungere il giorno festivo alla programmazione assegnata ad una determinata porta.

## Aggiungere un gruppo vacanze

**IMPORTANTE:** La creazione di un gruppo vacanze avrà un effetto immediato. Le vacanze aggiunte al gruppo saranno escluse da TUTTE le pianificazioni, di conseguenza la rimozione di determinati giorni dalle normali operazioni per una data o un intervallo di date causerà la sovrascrittura della normale programmazione. Per informazioni supplementari, consultare Creazione di gruppi di vacanze a pagina 39.

1. Selezionare ***Gestione dell'accesso > Vacanze.***
2. Fare clic su [Aggiungere].
3. Immettere un nome descrittivo nel campo **Nome gruppo vacanze**.

   Per impostazione predefinita, un nuovo gruppo vacanze contiene un giorno di vacanza.

   a. Scegliere la data ed una frequenza per il giorno di vacanza:
      - **Singolo**: un evento unico.
      - **Si ripete ogni anno**: un evento che si verifica alla stessa data ogni anno, ad esempio il 25 dicembre.
      - **Personalizzato**: un evento che si ripete ogni anno con una frequenza specifica, ad esempio il primo lunedì di maggio.

   b. Per un giorno di vacanza singolo o ricorrente, immettere la data d'inizio nel campo **Data** oppure fare clic sull'icona **Calendario** accanto al campo **Data** per selezionare una data dalla finestra pop-up Calendario.

   c. Immettere il numero di giorni che costituiscono la vacanza nel campo **Durata** . (Per impostazione predefinita, una nuova vacanza è costituita da un giorno. Valori validi sono da 1 a 366.)
4. Per aggiungere un'altra vacanza al gruppo, fare clic su [Aggiungere] nel riquadro elenco vacanze e ripetere da gradino a a gradino c.
5. Fare clic su [Accettare le modifiche].

## Aggiungere un giorno di vacanza al gruppo vacanze

1. Selezionare ***Gestione dell'accesso > Vacanze.***
2. Selezionare il gruppo di vacanze da modificare.
3. Per aggiungere un giorno di vacanza al gruppo:

   a. Fare clic su [Aggiungere] nel riquadro elenco vacanze.
4. Creare gli intervalli per la programmazione.

   a. Per creare intervalli supplementari, fare clic su [Aggiungere] nel riquadro Elenco intervallo.

   b. Fare clic sulla casella situata sopra ciascuno dei giorni da aggiungere all'intervallo.

   c. Immettere un valore per l'ora d'inizio e fine.

   d. Per un giorno di vacanza singolo o ricorrente, immettere la data d'inizio nel campo **Data** oppure fare clic sull'icona **Calendario** accanto al campo **Data** per selezionare una data dalla finestra pop-up Calendario.

   e. Immettere il numero di giorni che costituiscono la vacanza nel campo **Durata** .
5. Fare clic su [Accettare le modifiche].

### Copiare un gruppo vacanze

1. Selezionare ***Gestione dell'accesso > Vacanze.***
2. Selezionare il gruppo di vacanze da copiare.
3. Fare clic su [Copiare].
4. Immettere un nome descrittivo nel campo **Nome gruppo vacanze**.
5. Se necessario, modificare le vacanze nel gruppo copiato.
6. Fare clic su [Accettare le modifiche].

### Eliminare un gruppo ferie

**Notare:** Un gruppo vacanze in uso non può essere eliminato.

1. Selezionare ***Gestione dell'accesso > Vacanze.***
2. Selezionare il gruppo di vacanze da eliminare.
3. Fare clic su [Eliminare].
   Sarà visualizzata la finestra di dialogo Eliminare elemento.
4. Fare clic su [Eliminare].

## Creazione delle programmazioni

Le programmazioni determinano quando una persona può accedere a un lettore o il blocco e lo sblocco automatico della porta. Possono essere create ed utilizzate nel sistema fino a 64 programmazioni, incluse le seguenti programmazioni predefinite:

- Tutti i giorni 24/7
- Giorni feriali 8-17
- Giorni feriali 9-18
- Giorni feriali 7-19

Un *intervallo* è il periodo di tempo durante il quale la programmazione è attiva. Le programmazioni possono includere diversi intervalli. Ad esempio, se gli addetti alle pulizie passano l'aspirapolvere il mercoledì, ma gli altri giorni della settimana puliscono solo i  bagni e svuotano le pattumiere, necessiteranno di più ore d'accesso il mercoledì rispetto al resto della settimana. In questo caso può essere creato un intervallo il mercoledì ed un altro per gli altri giorni della settimana.

Si notino i dettagli seguenti sulle programmazioni:

- Le ore di programmazione sono espresse in ore e minuti, non in secondi, ma l'inizio dell'intervallo è relativo all'inizio del minuto (0 secondi) e la fine dell'intervallo è relativo alla fine del minuto (59 secondi) Nella programmazione predefinita 24/7, notare che l'ora d'inizio è le 12 e l'ora di fine è le 23.59. Espressa in secondi, l'ora d'inizio è 12:00:00 AM  e l'ora di fine è le 23:59:59 PM, un secondo di differenza. Una programmazione che passa la mezzanotte deve essere impostata in questo modo, perché se si utilizza 12.00 come ora di inizio e di fine, la programmazione resterebbe attiva solo 59 secondi (dalle 12.00.00 alle 12.00.59).
- I trigger azione, le programmazioni ed il controllo manuale possono avere un impatto sullo stato dei dispositivi e sono trattati allo stesso modo dal sistema. L'ultima operazione eseguita determina lo stato del dispositivo.

- Quando una data è contrassegnata come giorno festivo, il sistema fa un'eccezione a tutte le normali operazioni per quel giorno o gruppo di giorni, a meno che esista una programmazione personalizzata da utilizzare nella stessa data. Consultare **Creazione di gruppi di vacanze** per ulteriori informazioni sull'impatto dei giorni festivi sulla programmazione:
- Le programmazioni per controllare le ore d'accesso al lettore sono assegnate tramite la pagina ***Gestione dell'accesso > Livelli d'accesso*** .
- Le programmazioni per controllare la chiusura della porta sono assegnate nella pagina ***Controllo > Porte*** .

## Aggiungere una programmazione.

1. Selezionare ***Gestione dell'accesso > Programmazioni.***
2. Fare clic su [Aggiungere].
3. Immettere un nome descrittivo nel campo **Nome della programmazione** .
4. Fare clic su **Gruppi vacanze**.
5. Selezionare un gruppo di vacanze da includere nella programmazione.

**Notare:** Le vacanze sono eccezioni alla programmazione di accesso normale. L'aggiunta di un gruppo di vacanze in una programmazione evita che il gruppo di vacanze sovrascriva la programmazione. Ad esempio, se viene creato un gruppo di vacanze per una banca e l'ufficio è chiuso in quei giorni, il gruppo non dovrebbe essere selezionato per la programmazione del livello d'accesso dei dipendenti dell'ufficio. Tuttavia se il reparto spedizioni lavora durante il giorno festivo, il gruppo vacanze banca può essere selezionato per la programmazione degli addetti alla spedizione, impedendo al gruppo di vacanze banca di sovrascrivere la programmazione spedizioni.

6. Fare clic su [Accettare le modifiche].

## Aggiungere un intervallo ad una programmazione

1. Selezionare ***Gestione dell'accesso > Programmazioni.***
2. Selezionare la programmazione da modificare.
3. Creare gli intervalli per la programmazione.
   a. Per creare intervalli supplementari, fare clic su [Aggiungere] nel riquadro Elenco intervallo.
   b. Fare clic sulla casella situata sopra ciascuno dei giorni da aggiungere all'intervallo.
   c. Immettere un valore per l'ora d'inizio e fine.
4. Fare clic su [Accettare le modifiche].

## Eliminare un intervallo da una programmazione

1. Selezionare ***Gestione dell'accesso > Programmazioni.***
2. Selezionare la programmazione da modificare.
3. Selezionare un intervallo da eliminare.
4. Nel riquadro elenco intervallo, fare clic su [Eliminare].
5. Fare clic su [Accettare le modifiche].

### Copiare una programmazione

1. Selezionare ***Gestione dell'accesso > Programmazioni.***
2. Selezionare la programmazione da copiare.
3. Fare clic su [Copiare].
4. Immettere un nome descrittivo nel campo **Nome della programmazione** .
5. Aggiungere, eliminare o modificare gli intervalli a seconda delle proprie esigenze.
6. Fare clic su [Accettare le modifiche].

### Eliminare una programmazione

1. Selezionare ***Gestione dell'accesso > Programmazioni.***
2. Selezionare la programmazione da eliminare.
3. Fare clic su [Eliminare].
   Sarà visualizzata la finestra di dialogo Eliminare elemento.
4. Fare clic su [Eliminare].

## Creazione di gruppi di lettori

I gruppi di lettori sono utili quando nell'edificio esistono un gran numero di lettori e porte. I gruppi di lettori consentono agli utenti di riunire diversi lettori in base ad una caratteristica comune e di assegnarli come gruppo ai livelli di accesso. Ad esempio, tutti i lettori del seminterrato di un edificio possono essere aggiunti ad un gruppo.

Il raggruppamento tuttavia non è limitato ad un'area fisica. Ad esempio un gruppo di lettori chiamato pulizie potrebbe consentire l'accesso a tutti i ripostigli protetti di materiale per le pulizie .

Il gruppo lettori appare nella pagina ***Gestione dell'accesso > Livelli d'accesso*** consentendo agli utenti di consentire l'accesso a tutti i lettori in un gruppo con una sola selezione, invece che un lettore alla volta.

### Aggiungere un gruppo lettori.

1. Selezionare ***Gestione dell'accesso > Gruppi di lettori***.
2. Fare clic su [Aggiungere].
3. Immettere un nome descrittivo nel campo **Nome gruppo di lettori** .
4. Selezionare tutti i lettori del gruppo.
5. Fare clic su [Accettare le modifiche].

### Copiare un gruppo vacanze

1. Selezionare ***Gestione dell'accesso > Gruppi di lettori***.
2. Selezionare il gruppo di lettori da copiare.
3. Fare clic su [Copiare].
4. Immettere un nome descrittivo nel campo **Nome gruppo di lettori** .
5. Aggiungere o modificare l'assegnazione dei lettori a seconda delle esigenze.

6. Fare clic su [Accettare le modifiche].

### Eliminare un gruppo lettori

1. Selezionare ***Gestione dell'accesso > Gruppi di lettori***.
2. Selezionare il gruppo di lettori da eliminare.
3. Fare clic su [Eliminare].
   Sarà visualizzata la finestra di dialogo Eliminare elemento.
4. Fare clic su [Eliminare].

## Configurare i livelli di accesso

I livelli di accesso determinano le porte alle quali le credenziali danno accesso e quando. Ad esempio, se l'impianto ha un ufficio e un magazzino ed i dipendenti dell'ufficio non devono avere accesso al magazzino, saranno creati per i dipendenti dell'ufficio livelli d'accesso che includono solo le porte situate nell'area uffici.

La pagina ***Gestione dell'accesso > Livelli di accesso*** è utilizzata per assegnare le pianificazioni ai lettori ed ai gruppi di lettori. Ai livelli di accesso sono poi assegnate le credenziali che determinano i giorni e le ore durante i quali il titolare della credenziale può avere accesso e attraverso quali lettori.

### Aggiungere un livello di accesso

1. Selezionare ***Gestione dell'accesso*** > ***Livelli di accesso***.
2. Fare clic su [Aggiungere].
3. Immettere un nome descrittivo nel campo **Nome livello di accesso**.
4. Selezionare i lettori e i gruppi di lettori da includere nel livello di accesso.
5. Selezionare una programmazione per ogni lettore selezionato.
6. Fare clic su [Accettare le modifiche].

### Copiare un livello di accesso.

Per un gran numero di lettori, la creazione di nuovi livelli di accesso potrebbe richiedere molto tempo. Copiare un livello di accesso consente agli utenti di riutilizzare una configurazione simile ed effettuare solo le modifiche necessarie al nuovo livello d'accesso.

1. Selezionare ***Gestione dell'accesso*** > ***Livelli di accesso***.
2. Fare clic sul livello d'accesso da copiare.
3. Fare clic su [Copiare].
4. Immettere un nome descrittivo nel campo **Nome livello di accesso**.
5. Effettuare le modifiche necessarie al lettore e al gruppo di lettori nel livello d'accesso.
6. Deselezionare la casella accanto ai lettori che non devono essere inclusi nel livello d'accesso.
7. Fare clic su [Accettare le modifiche].

### Eliminare un livello di accesso.

1. Selezionare ***Gestione dell'accesso*** > ***Livelli di accesso***.

2. Fare clic sul livello d'accesso da eliminare.
3. Fare clic su [Eliminare].
   Sarà visualizzata la finestra di dialogo Eliminare elemento.
4. Fare clic su [Eliminare].

## Configurazione dei ruoli operatore

Un ruolo operatore è un gruppo di policy di autorizzazione. Quando una persona è aggiunta e autorizzata a collegarsi e ad gestire il sistema, tale operatore avrà l'autorizzazione di modificare, eseguire o solo visualizzare funzioni e dati. Invece di configurare manualmente le singole funzioni o dati per ciascun operatore, la funzione ruolo operatore consente agli utenti di assegnare autorizzazioni d'accesso comuni per ogni tipo di operatore a seconda della mansione svolta.

Si notino i dettagli seguenti sui ruoli operatore:

- Per il ruolo amministratore non è possibile modificare le impostazioni predefinite.
- Solo un amministratore può modificare le impostazioni per i ruoli operatore, custode, solo visualizzazione e distributore.
- Il ruolo amministratore non può essere eliminato.
- Il ruolo operatore non può essere eliminato se è assegnato a una o più persone

Esempi dei diversi ruoli operatore includono:

- **Amministratore** L'utente principale responsabile per la gestione del sistema.
- **Operatore** Esperto in informatica che utilizza il sistema per attività quali il backup del database, l'assegnazione dei livelli d'accesso, ecc.
- **Custode**: Personale di sicurezza responsabile del controllo dell'impianto che utilizza il sistema per la gestione delle telecamere PTZ, le porte, gli ingressi, ecc. ma anche per visualizzare video, generare report ed eseguire manualmente record di azioni.
- **Solo visualizzazione**: Supervisori che necessitano l'accesso in sola lettura al sistema a scopo di gestione.
- **Distributore** Rivenditori e consulenti responsabili per l'impostazione iniziale del sistema.

I vari livelli di autorizzazione includono:

- **Nessuno** L'operatore non può accedere o visualizzare la pagina.
- **Visualizzazione** L'operatore è in grado di visualizzare la pagina o i dati, ma non può effettuare modifiche o eseguire comandi.
- **Modifica** L'operatore può modificare le impostazioni.
- **Esecuzione** L'operatore può eseguire comandi.

Per visualizzare un elenco dei livelli di autorizzazione assegnati ai ruoli operatore, consultare Autorizzazioni ruolo operatore predefiniti a pagina 114.

## Aggiungere un ruolo operatore

1. Selezionare ***Amministrazione del sistema > Ruoli operatore***.
2. Fare clic su [Aggiungere].
3. Immettere un nome descrittivo nel campo **Nome ruolo**.
4. Selezionare una **Autorizzazione** per ciascuna delle funzioni.
5. Fare clic su [Accettare le modifiche].

## Modificare un ruolo operatore

**Notare:** Il ruolo amministratore non può essere modificato.

1. Selezionare ***Amministrazione del sistema > Ruoli operatore***.
2. Per ridenominare, immettere un nome descrittivo per il ruolo nel campo **Nome ruolo**.
3. Modificare l'**Autorizzazione** per ciascuna funzione, a seconda delle necessità.
4. Fare clic su [Accettare le modifiche].

## Copiare un ruolo operatore

Copiare un ruolo operatore consente agli utenti di riutilizzare una configurazione simile ed effettuare solo le modifiche necessarie al nuovo ruolo.

1. Selezionare ***Amministrazione del sistema > Ruoli operatore***.
2. Selezionare il ruolo da copiare.
3. Fare clic su [Copiare].
4. Immettere un nome descrittivo nel campo **Nome ruolo**.
5. Modificare l'**Autorizzazione** per ciascuna funzione, a seconda delle necessità.
6. Fare clic su [Accettare le modifiche].

## Eliminare un ruolo operatore

**Notare:** I ruoli assegnati agli utenti non possono essere eliminati.

1. Selezionare ***Amministrazione del sistema > Ruoli operatore***.
2. Selezionare il ruolo da eliminare.
3. Fare clic su [Eliminare].
   Sarà visualizzata la finestra di dialogo Eliminare elemento.
4. Fare clic su [Eliminare].

# Configurazione dell'email

Il sistema può essere configurato per l'invio automatico di email al verificarsi di eventi quali il backup del database o all'esecuzione di un trigger azione.

Il sistema include un elenco di email predefiniti al quale possono essere aggiunti destinatari per l'invio automatico di email. Possono essere creati fino a dieci elenchi email, ciascuno dei quali può contenere fino a dieci destinatari, per l'invio di email automatici.

Per utilizzare la funzione email automatici, configurare il sistema per l'utilizzazione di un server Simple Mail Transfer Protocol (SMTP) interno o esterno e aggiungere almeno un destinatario nell'elenco predefinito, come descritto in questa sezione.

## Configurare un Email Server

Il sistema può essere configurato per accedere un email server interno, enterprise SMTP oppure un server SMTP esterno (ad es. Gmail) per inviare email automatiche.

Consultare il provider del servizio Internet (ISP) o il provider del servizio email per determinare l'indirizzo IP o l'hostname per il server email ed il numero di porta. Inoltre, chiedere se il server email utilizza il protocollo Secure Sockets Layer (SSL) per la cifratura dei dati.

**Notare:** Alcuni provider ISP e di servizio email, limitano il numero di email inviati ogni giorno e potrebbero richiedere un pagamento supplementare per quantità superiori. In alcuni casi il provider potrebbe bloccare l'account se la quantità viene superata. Se queste condizioni rappresentano un problema, considerare un servizio relay SMTP a pagamento oppure considerare l'implementazione di un server email interno.

1. Selezionare ***Amministrazione del sistema > Email > Server Impostazioni***.
2. Selezionare **Attivare le notifiche email**.
3. In caso di collegamento ad un server email sicuro, selezionare la casella **Attivare autenticazione.**
   a. Immettere l'indirizzo IP o l'hostname del server email nel campo **Server email**.
   b. Immettere il numero di porta del server email nel campo **Porta.**

      Se il server email utilizza SSL, il valore predefinito è 465; altrimenti il valore predefinito è 25.
   c. Se il server email utilizza SSL, selezionare la casella **Necessita SSL.**
   d. Immettere il nome utente per il server email nel campo **Utente.**
   e. Immettere la password per il server email nel campo **Password.**
4. Se il collegamento al server email non richiede un nome utente e una password, no selezionare la casella **Attivare autenticazione.**
   a. Immettere l'indirizzo IP o l'hostname del server email nel campo **Server email** .
   b. Immettere il numero di porta del server email nel campo **Porta.**

      Se il server email utilizza SSL, il valore predefinito è 465; altrimenti il valore predefinito è 25.
   c. Se il server email utilizza SSL, selezionare la casella **Necessita SSL.**
   d. Immettere il nome che apparirà negli email automatici nel campo **Nome del mittente** .
   e. Immettere l'indirizzo che apparirà negli email automatici nel campo **Email del mittente** .

Se i destinatari non devono rispondere agli email automatici, creare un account "nessuna risposta", ad esempio “noreply@yourdomainname.com” da utilizzare come indirizzo del mittente.

5. Fare clic su [Accettare le modifiche].
6. Fare clic su [Verificare server email] per verificare le impostazioni del server email.

## Modificare un elenco email

È possibile aggiungere e eliminare destinatari dall'elenco email ed il nome dell'elenco può essere modificato, come descritto nei passaggi di seguito. Il sistema include un elenco email predefinito, al quale deve essere aggiunto almeno un destinatario per gli email automatici.

1. Selezionare ***Amministrazione del sistema > Email > Elenchi email***.
2. Fare clic sull'elenco email per selezionarlo.
3. Per rinominare un elenco email, immettere un nome descrittivo per l'elenco nel campo **Nome elenco email** .
4. Per aggiungere una persona all'elenco:
   a. Immettere il nome della persona nel campo **Nome visualizzato.**
   b. Immettere l'indirizzo email della persona nel campo **Indirizzo email.**
   c. Fare clic su [Aggiungere].
5. Per eliminare una persona all'elenco:
   a. Fare clic sul nome della persona per selezionarlo.
   b. Fare clic su [Eliminare].
6. Fare clic su [Accettare le modifiche].

## Aggiungere un elenco email

Il sistema include un elenco email predefinito, al quale deve essere aggiunto almeno un destinatario per gli email automatici. Possono essere creati fino a dieci elenchi email, ciascuno dei quali può contenere fino a dieci destinatari. È possibile anche copiare un elenco email esistente e modificarlo a seconda delle proprie esigenze.

1. Selezionare ***Amministrazione del sistema > Email > Elenchi email***.
2. Fare clic su [Aggiungere].
3. Immettere un nome descrittivo per l'elenco email nel campo **Nome elenco email** .
4. Per ogni persona aggiunta all'elenco email:
   a. Fare clic su [Aggiungere].
   b. Immettere il nome della persona nel campo **Nome visualizzato.**
   c. Immettere l'indirizzo email della persona nel campo **Indirizzo email.**
5. Una volta terminata l'aggiunta dei destinatari all'elenco email, fare clic su [Accettare le modifiche].

### Eliminare un elenco email

**Notare:** Non è possibile eliminare un elenco email utilizzato dal sistema.

1. Selezionare ***Amministrazione del sistema > Email > Elenchi email***.
2. Fare clic sull'elenco email per selezionarlo.
3. Fare clic su [Eliminare].
   Sarà visualizzata la finestra di dialogo Eliminare elemento.
4. Fare clic su [Eliminare].

### Disattivare le notifiche email

Per disattivare rapidamente tutte le notifiche email, deselezionare la casella **Attivare notifiche email** nella pagina ***Impostazioni del server***. Si noti che questa operazione avrà un impatto sulle azioni trigger che generano email automatici.

1. Selezionare ***Amministrazione del sistema > Email > Impostazioni del server***.
2. Deselezionare la casella **Attivare notifiche email.**
3. Fare clic su [Accettare le modifiche].

## Configurare i campi definiti dall'utente

I record della persona nel database  possono essere associati a campi definiti dall'utente utilizzati per immettere dati relativi al personale, quali la targa del veicolo o il numero di telefono della residenza. Per essere visualizzato nella pagina ***Gestione dell'accesso  > Persone***, il campo deve essere attivato. Quando un campo è disattivato, sarà eliminato dal database ed i dati associati alla persona verranno perduti.

Ogni database deve poter distinguere un record dall'altro. Alcuni nomi sono molto comuni, quindi l'utilizzazione del database come unico elemento d'identificazione non funziona. Per questa ragione in genere le aziende assegnano ad ogni impiegato o membro un numero di identificazione unico.

**IMPORTANTE:** L'ideale è utilizzare un identificatore del record della persona, quale il numero di impiegato, unico per ogni persona nell'azienda. Se non è possibile identificare ogni record come unico, gli aggiornamenti, le importazioni ed altre operazioni di manutenzione del database, potrebbero essere applicate al record sbagliato.

I campi definiti dall'utente creati possono essere designati come protetti. Le impostazioni per questa opzione determinano se i campi definiti dall'utente con la funzione Protetto selezionata sono visibili o modificabili dai diversi ruoli operatore. Questo consente un maggiore livello di protezione per informazioni riservate quali il numero di telefono della residenza. Ad esempio, se gli utenti con un ruolo Operatore possono visualizzare tutte le informazioni personali e gli utenti con il ruolo Custode possono visualizzare solo le informazioni personali non protette, modificare le impostazioni del ruolo operatore come illustrato nella tabella qui sotto:

| Ruolo | Impostazioni campi definiti dall'utente | Impostazioni campi utente protetti |
|---|---|---|
| **Operatore** | Solo visualizzazione | Solo visualizzazione |
| **Protezione** | Solo visualizzazione | Nessuno |

## Aggiungere campi definiti dall'utente

I campi definiti dall'utente fanno parte dei record della persona nel database. Per essere visualizzato nella pagina ***Gestione dell'accesso > Persone***, il campo deve essere attivato.

1. Selezionare ***Amministrazione del sistema > Impostazioni del sistema***.
2. Fare clic sulla scheda **Campi definiti dall'utente.**
3. Per ogni campo:
   a. Selezionare **Attivato**.
   b. Immettere un' **Etichetta**.
   c. (Opzionale) Selezionare **Obbligatorio**.
   d. (Opzionale) Selezionare **Protetto**.
4. Fare clic su [Accettare le modifiche].

## Riorganizzare i campi definiti dall'utente

I campi definiti dall'utente fanno parte dei record della persona nel database. Per essere visualizzato nella pagina ***Gestione dell'accesso > Persone***, il campo deve essere attivato. Se un campo è disattivato, sarà eliminato dal database ed i dati associati alla persona verranno perduti.

**IMPORTANTE:** Non tentare di riorganizzare i campi modificandone il nome. I dati sono associati al campo, non all'etichetta. La modifica dell'etichetta non ne modifica l'ordine, ma i dati saranno etichettati in modo errato.

1. Selezionare ***Amministrazione del sistema > Impostazioni del sistema***.
2. Fare clic sulla scheda **Campi definiti dall'utente.**
3. Utilizzare la freccia Ordina per spostare i campi su o giù.

   L'ordine dei campi in questa scheda corrisponde all'ordine dei campi nella pagina ***Gestione dell'accesso  Persone***.

### Eliminare un campo definito dall'utente

Per essere visualizzato nella pagina ***Gestione dell'accesso > Persone***, il campo deve essere attivato. Se un campo è disattivato, sarà eliminato dal database ed i dati associati alla persona verranno perduti.

1. Selezionare ***Amministrazione del sistema > Impostazioni del sistema***.
2. Fare clic sulla scheda **Campi definiti dall'utente.**
3. Disattivare la casella **Attivato** del campo e dei dati da eliminare.
4. Fare clic su [Accettare le modifiche].

## Programmazione del comportamento della porta e del lettore

La scheda Visualizzazione programmazione della pagina ***Monitoraggio > Porte*** è utilizzata per sovrascrivere il comportamento predefinito della porta e del lettore in base alla programmazione. Ad esempio, durante le ore di apertura una porta pubblica, quale la sala esposizione o l'area di vendita, sarà sbloccata. Dopo le ore d'apertura al pubblico alcuni lettori potrebbero richiedere una credenziale e un PIN (utile per prevenire l'accesso con credenziali perdute o rubate), il lettore può quindi essere configurato per richiedere solo una credenziale per impostazione predefinita (***Amministrazione del sistema > Dispositivi***) e richiedere una credenziale ed un PIN al termine dell'orario d'apertura (***Controllo > Porte > Visualizzazione programmazioni***).

**Notare:** Non confondere il comportamento della porta e del lettore con l'accesso. La pagina ***Gestione dell'accesso > Livelli di accesso*** è utilizzata per assegnare le pianificazioni ai lettori ed ai gruppi di lettori. Ai livelli di accesso sono poi assegnate le credenziali che determinano i giorni e le ore durante i quali il titolare della credenziale può avere accesso e attraverso quali lettori. La modalità di accesso, solo credenziale o credenziale e PIN, non è rilevante per il livello d'accesso. (Vedere **Configurazione della sicurezza a pagina 18.**)

1. Selezionare ***Controllo > Porte***.
2. Fare clic sulla scheda **Visualizzazione programmazione.**
3. Per ogni combinazione di porta e lettore:
   a. Selezionare una **Programmazione**.
   b. Selezionare una **Modalità programmazione**.

      Per le porte le modalità di programmazione sono:

      - **Sbloccata**
      - **Prima Tessera In**
      - **Bloccata**

      Per i lettori le modalità di programmazione sono:

      - **Solo credenziale**
      - **Credenziale e PIN**

## Importare persone e credenziali da un file CSV

L'importazione/esportazione guidata fornita con il disco utilità può essere utilizzata per aggiungere o eliminare diversi set di dati persone e credenziali di altra provenienza  in modalità batch, ad esempio il database dell'ufficio personale o un altro sistema di controllo dell'accesso.

**Notare:** Le persone possono anche avere un account utente nel sistema che consente loro di collegarsi al sistema ed utilizzarlo. Le informazioni relative all'account utente non sono trattate dall'importazione/esportazione guidata.

L'importazione/esportazione guidata può essere utilizzata per mappare i campi di un file CSV con la tabella del database del sistema ed importare le persone e le credenziali di altra provenienza, ad esempio il database dell'ufficio personale o un altro sistema di controllo dell'accesso. Per informazioni dettagliate, consultare la *Guida utente di importazione/esportazione guidata*.

**Notare:** Il record di una persona consiste in campi definiti dall'utente per le informazioni personali, le credenziali d'accesso (ID badge, PIN, livello d'accesso) e per le informazioni opzionali dell'account utente per consentire il collegamento al sistema. L'importazione e l'esportazione di dati relativi all'account utente non sono supportate. È possibile importare ed esportare solo dati personali e le credenziali definiti dall'utente.

I record delle persone possono anche essere aggiunti individualmente, come descritto in Gestione delle persone a pagina 67.

## Configurare i trigger azione

Con la funzione trigger azione, è possibile definire le condizioni del trigger e le azioni intraprese quando si verificano tali condizioni. Ad esempio, se una porta esterna è forzata tra le 19 e le 7, sarà eseguito un trigger azione che causerà un allarme acustico, visivo e un email automatico sarà inviato a tutti i gestori del sito.

La pagina ***Amministrazione del sistema > Trigger*** azione contiene due schede, **Trigger** e **Azioni**, come descritto di seguito.

### Comprendere i  trigger

Utilizzare la scheda **Trigger** della pagina ***Trigger azione*** per definire le condizioni di trigger che eseguiranno azioni. Un trigger è costituito da uno o più gruppi di condizioni ed un gruppo di condizioni è costituito da una o più definizioni di condizione.

La definizione di condizione include cinque elenchi a discesa nei quali è possibile:

- Indicare il tipo di entità, ad esempio **Porta** o **Programmazione**.
- Indicare un qualificatore relativo al tipo di entità selezionato. Se il tipo di entità selezionato è **Porta** le opzioni nell'elenco includeranno **Nessuna**, **Tutte** e un elenco di porte definite nel sistema.
- Indicare se la condizione è vera o falsa.
- Selezionare una condizione che potrebbe causare un'azione. Se il tipo di entità selezionato è **Porta** le opzioni includono **Protetta**, **Sbloccata**, **Bloccata**, **Trattenuta**, **Forzata**, **Manomessa**, **Aperta**, and **Magnetica Avaria sensore**.

La tabella che segue elenca i trigger disponibili per ciascun tipo di entità:

| Entità | Condizioni di trigger | Note |
|---|---|---|
| Area | Sbloccata - Qualsiasi porta | La porta appartiene ad un'area se i lettori sono configurati per accedere o uscire dall'area nella pagina ***Gestione dell'accesso > Aree > Assegnazioni lettore*** . L'unica eccezione è "Bloccata - qualsiasi porta" che prende in considerazione solo i lettori che consentono l'ingresso all'area selezionata.<br>Trigger vero quando le porte dell'area soddisfano la condizione. Trigger falso quando le porte dell'area non soddisfano la condizione. Non supportato all'esterno dell'area. Per ulteriori dettagli, leggere i trigger della porta corrispondenti.<br>Se un'area non è associata ad una porta, le condizioni "Tutte le porte" saranno sempre false e le condizioni "Tutte le porte" sempre vere. |
| | Bloccata - Qualsiasi porta | |
| | Trattenuta - Qualsiasi porta | |
| | Forzata aperta - Qualsiasi porta | |
| | Manomessa - Qualsiasi porta | |
| | Aperta - Qualsiasi porta | |
| | Proteggere - Tutte le porte | |
| | Avaria Sensore Magnete - Qualsiasi porta | |
| Porta | Sbloccata | Trigger vero quando la serratura è attivata. Trigger falso quando la serratura è disattivata. |
| | Bloccata | Trigger vero quando la porta è bloccata. Trigger falso quando il blocco della porta non è più attivo. |
| | Trattenuta | Trigger vero quando l'allarme porta trattenuta è attivo. Trigger falso quando l'allarme porta trattenuta è ripristinato. |
| | Forzata aperta | Trigger vero quando l'allarme porta forzata è attivo. Trigger falso quando l'allarme porta forzata è ripristinato. |
| | Tamper | Trigger vero quando l'allarme porta manomessa è attivo. Trigger falso quando l'allarme porta manomessa è ripristinato. Include la manomissione su Contatto porta, Richiesta di uscita, Ingresso ausiliario e Tamper. |
| | Aperta | Trigger vero quando la porta è aperta. Trigger falso quando la porta è chiusa. Include le condizioni porta forzata e trattenuta aperta. |
| | Protetta | Trigger vero quando l'apriporta è disattivato e la porta è chiusa. Trigger falso quando l'apriporta è attivato o la porta è aperta. |
| | Avaria Sensore magnete | Trigger vero quando l'allarme del sensore del magnete è attivo. Trigger falso quando l'allarme del sensore del magnete è ripristinato. |

| Entità | Condizioni di trigger | Note |
|---|---|---|
| Ingresso | Inattivo | Trigger vero quando l'ingresso è inattivo. Trigger falso quando l'ingresso è non è inattivo. |
| | Attivo | Trigger vero quando l'ingresso è attivo. Trigger falso quando l'ingresso è non è attivo. |
| | Manomessa | Trigger vero quando l'ingresso è manomesso. Trigger falso quando l'ingresso è non è manomesso. |
| Uscita | On | Trigger vero quando l'uscita è on. Trigger falso quando l'uscita non è on. |
| | Off | Trigger vero quando l'uscita è off. Trigger falso quando l'uscita non è off. |
| Modulo | Manomessa | Il trigger è vero quando la periferica riporta condizioni di manomissione. Il trigger è falso quando la periferica riporta condizioni di manomissione ripristinate. |
| | Errore di comunicazione | Trigger vero in caso di perdita della comunicazione con la periferica. Trigger falso quando la comunicazione è ripristinata. |

| Entità | Condizioni di trigger | Note |
|---|---|---|
| Lettore | Autorizzato | Trigger vero/falso per qualsiasi tipo di evento d'accesso autorizzato. Sarà seguito da un altro evento d'accesso autorizzato. |
| | Consentito - Nessun ingresso | Trigger vero/falso quando la porta non è aperta e non esiste una violazione APB. |
| | Consentito - Ingresso effettuato | Trigger vero quando la porta è aperta ed il lettore conduce in un'area non esterna. |
| | Consentito - Ingresso effettuato soft APB | Trigger vero/falso quando la porta è aperta ed il lettore conduce in un'area non esterna e violazione soft APB. |
| | Consentito - Nessun ingresso soft APB | Trigger vero/falso quando la porta non è aperta ed il lettore conduce in un'area non esterna e violazione soft APB. |
| | Consentito - Uscita effettuata | Trigger vero/falso quando la porta è aperta ed il lettore conduce in un'area esterna e non esiste una violazione APB. |
| | Consentito - Uscita effettuata soft APB | Trigger vero/falso quando la porta è aperta ed il lettore conduce in un'area esterna ed esiste una violazione soft APB. |
| | Consentito - Nessuna uscita soft APB | Trigger vero/falso quando la porta non è aperta ed il lettore conduce in un'area esterna e violazione soft APB. |
| | Negato - Qualsiasi ragione | Trigger vero/falso quando l'accesso è rifiutato per qualsiasi ragione. |
| | Negato - Credenziale non valida | Trigger vero/falso quando l'accesso è rifiutato a causa di una credenziale sconosciuta. |
| | Negato - Codice impianto | Trigger vero/falso quando l'accesso è rifiutato a causa di un codice impianto non valido. |
| | Negato - Codice emissione | Trigger vero/falso quando l'accesso è rifiutato a causa di un codice di emissione non valido. |
| | Negato - PIN | Trigger vero/falso quando l'accesso è rifiutato a causa di un PIN non valido. Non esiste un trigger specifico quando si raggiunge il numero massimo di tentativi e il titolare della tessera è bloccato. |
| | Negato - Non autorizzato | Trigger vero/falso quando l'accesso è rifiutato a causa dell'assenza di un livello d'accesso. |
| | Negato - Hard APB | Trigger vero/falso quando l'accesso è rifiutato a causa di una violazione hard APB. |
| | Negato - Porta bloccata | Trigger vero/falso quando l'accesso è rifiutato a causa di una porta bloccata. |
| | Negato - Inattivo | Trigger vero/falso quando l'accesso è rifiutato a causa di una credenziale attiva da/a fuori dall'intervallo. |

| Entità | Condizioni di trigger | Note |
|---|---|---|
| Programmazione | In vigore | Trigger vero quando la programmazione inizia. Trigger falso quando la programmazione finisce. |
| | Vacanza in vigore | Trigger vero quando la programmazione non è in vigore a causa di una vacanza. (L'ora di attivazione del trigger è basato sulla programmazione.)<br>Trigger falso quando quando la vacanza finisce. Consultare Considerazioni sui record trigger azioni basati su programmazione a pagina 57. |
| | 15 minuti prima dell'inizio | Trigger vero 15 minuti prima dell'inizio della programmazione. Trigger falso quando la programmazione inizia |
| | 15 minuti prima della fine | Trigger vero 15 minuti prima della fine della programmazione. Trigger falso quando la programmazione finisce. |
| Sistema | Bloccare tutte le porte - Comando | Trigger vero quando il blocco è attivo. Trigger falso quando il blocco non è più attivo. |
| | Sbloccare tutte le porte - Comando | Trigger vero quando lo sblocco è attivo. Trigger falso quando lo sblocco non è più attivo. |
| | Guasto | Trigger vero quando la manomissione esterna/muro è attiva. Trigger falso quando la condizione di trigger è inattiva. |
| | Batteria di backup scarica | Trigger vero quando il voltaggio della batteria è inferiore a 11.7 VDC. Trigger falso quando il voltaggio della batteria è superiore a 11.7 VDC. |
| | Memoria della batteria bassa | Trigger vero quando il voltaggio della batteria è inferiore a 2.0 VDC. Trigger falso quando il voltaggio della batteria è superiore a 2.0 VDC. Controllata solo ogni 6 ore. |
| | Guasto alimentazione aria condizionata | Trigger vero in caso di rimozione dell'alimentazione aria condizionata. Trigger falso in caso di ripristino dell'alimentazione aria condizionata. |
| | Fusibile scattato | Trigger vero in caso di fusibile scattato. Trigger falso quando il fusibile è ripristinato. |
| | Orario modificato | Trigger vero quando l'orario è modificato. Non sarà riattivato per un minuto. Dopo un minuto è automaticamente falso. |

Si notino i dettagli seguenti sui trigger:

- Possono essere creati fino a dieci gruppi di dichiarazioni di condizione, con fino a dieci condizioni per tutti i gruppi (ad esempio due gruppi potrebbero avere ciascuno cinque condizioni).
- Per iniziare un nuovo gruppo di condizioni, fare clic sul pulsante [+] situato sulla condizione di un gruppo esistente. Fare clic sul pulsante [-] per eliminare un gruppo di condizioni.
- Un secondo livello di pulsanti [+] e [-] sono situati accanto a ciascuna delle condizioni. Fare clic sul pulsante [+] per aggiungere una nuova condizione; fare clic sul pulsante [-] per eliminare una singola condizione.

- Per un gruppo specifico di condizioni o per tutti i gruppi, può essere selezionato **Deve verificarsi una qualsiasi** o **Devono verificarsi tutte.**
- Se sono selezionati **Qualsiasi** o **Tutte** per l'inclusione delle entità nella condizione, tutti gli oggetti aggiunti al sistema con lo stesso tipo di entità sono aggiunti automaticamente nella valutazione della condizione. Se ad esempio si crea una condizione per il controllo di tutti i lettori e viene installato un nuovo lettore, il nuovo lettore sarà aggiunto automaticamente al gruppo di lettori controllati.
- Le condizioni di trigger per i lettori saranno false immediatamente dopo essere vere. Inoltre le azioni di disattivazione non sono in genere utilizzate con le condizioni di trigger del lettore.
- Se un'entità del sistema (ad esempio un lettore) è definita in una dichiarazione di condizione e l'entità è in seguito eliminata dal sistema, la condizione corrispondente sarà anche eliminata. Se l'entità è ricreata, può essere creata una nuova condizione per l'entità.
- Quando lo stato della condizione trigger passa da vero a falso, sarà registrato un evento.
- Nello stesso gruppo di condizioni possono essere incluse condizioni duplicate.
- In una dichiarazione di trigger possono essere inclusi ingressi e uscite disattivati, ma non avranno alcun effetto sulla valutazione del trigger.
- I record del trigger azione può essere configurato per verificarsi quando il trigger è disattivato.
- I record delle azioni trigger possono includere condizioni senza nessuna azione associata.

Inoltre notare che le condizioni trigger sono presupposte in uno stato indeterminato e passeranno a vero o falso per eseguire le azioni corrispondenti:

- Per tutti i record all'avvio del sistema.
- Per ogni record quando un record è configurato e salvato.
- Per i record interessati in caso di eliminazione di un'entità referenziata.

## Considerazioni sui record trigger azioni basati su programmazione

Quando si creano le dichiarazioni di condizione per i record trigger azione che riguardano le programmazioni, tenere presente che il gruppo vacanze può essere incluso o escluso da una programmazione, a seconda della configurazione del gruppo vacanze nella pagina ***Gestione dell'accesso > Programmazioni***.

- Se un gruppo vacanze è *incluso* in una programmazione (la casella è selezionata), la programmazione sarà attiva nei giorni definiti nel gruppo vacanze durante le ore definite nella programmazione. Indipendentemente dai giorni della settimana selezionati per la programmazione.
- Se la casella gruppo vacanze è *esclusa* da una programmazione (la casella non è selezionata), la programmazione non sarà attiva durante i giorni e le ore definite nel gruppo vacanze. Indipendentemente dai giorni della settimana selezionati per la programmazione.
- Se lo stesso giorno fa parte di un gruppo vacanze *incluso* in una programmazione e fa anche parte di un altro gruppo vacanze *escluso* dalla stessa programmazione, il giorno sarà *incluso* nella programmazione.

Per garantire un'azione trigger indipendentemente dal fatto che un determinato giorno sia una vacanza o meno, creare una dichiarazione "o" nella condizione trigger utilizzando l'opzione "Deve verificarsi una qualsiasi". Ad esempio una condizione trigger sarà vera quando una programmazione settimanale dalle 9 alle 18 è in vigore ed una condizione trigger corrispondente sarà vera quando le vacanze sono in vigore.

L'esempio seguente illustra quando un trigger Vacanza in vigore è attivo se una vacanza ha un impatto negativo sulla programmazione, per una programmazione giorni feriali dalle 7 alle 17.

| | Mer. 13/2<br>7 -19 | Gio. 14/2<br>7 -19 | Ven. 15/2<br>7 -19 | Sab. 16/2<br>7 -19 | Dom. 17/2<br>7 -19 | Lun. 18/2<br>7 -19 | Mar. 19/2<br>7 -19 |
|---|---|---|---|---|---|---|---|
| Nessun giorno di vacanza definito | | | | | | | |
| nella finestra | Attivo | Attivo | Attivo | | | Attivo | Attivo |
| Vacanza in vigore | | | | | | | |
| | | | | | | | |
| Vacanza 1 (14/2-16/2) casella disattivata | | | | | | | |
| Vacanza 2 (15/2-18/2) casella disattivata | | | | | | | |
| nella finestra | Attivo | | | | | | Attivo |
| Vacanza in vigore | | Attivo | Attivo | | | Attivo | |
| | | | | | | | |
| Vacanza 1 (14/2-16/2) casella **selezionata** | | | | | | | |
| Vacanza 2 (15/2-18/2) casella disattivata | | | | | | | |
| nella finestra | Attivo | Attivo | Attivo | Attivo | | | Attivo |
| Vacanza in vigore | | | | | | Attivo | |

## Comprendere le azioni

Utilizzare la scheda **Azioni** della pagina ***Amministrazione del sistema > Trigger azione*** per definire le azioni da intraprendere quando una condizione di trigger diventa vera o falsa. (I trigger azione possono essere eseguiti nella pagina ***Monitoraggio > Trigger azione.*** Consultare Controllo dei trigger delle azioni a pagina 87.)

Ad esempio, può essere definita una condizione nella scheda Trigger indicante che si verificherà un'azione in caso di porta forzata. È possibile configurare un'azione nella scheda Azioni che stabilisce che quando la condizione diventa vera, sarà inviato un messaggio automatico a tutti i manager. Se la porta è forzata dopo la creazione del record trigger azione, sarà inviato un messaggio automatico a tutti i manager del sito.

Possono essere creati fino a 32 trigger azioni che risulteranno in due tipi di azioni:

- Azioni di attivazione che saranno eseguite quando una condizione di trigger diventa vera e
- Azioni di disattivazione che saranno eseguite quando una condizione di trigger diventa falsa.

Possono essere configurati diversi trigger azioni per eseguire la stessa azione o controllare la stessa entità del sistema. Ad esempio può essere configurato un record per attivare una sirena ed inviare un messaggio automatico quando uno dei diversi ingressi d'emergenza diventa attivo ed un altro record può essere configurato per disattivare la sirena ed inviare un messaggio quando il ripristino d'emergenza è attivo.

La tabella seguente elenca le azioni disponibili:

| Entità | Azioni | Note |
|---|---|---|
| Controller del sistema | Ripristino APB | Ripristinare l'anti-passback di tutte le credenziali ad uno stato neutro (ad esempio passaggio libero). |

| Entità | Azioni | Note |
|---|---|---|
| Porte /lettori | Bloccare | Blocca la porta.<br>**Nota:** Non influisce sulla modalità d'accesso del lettore. |
| | Sbloccare | Sblocca la porta.<br>**Nota:** Non influisce sulla modalità d'accesso del lettore. |
| | Aprire | Sblocca l'apriporta durante le normali ore d'ingresso.<br>**Nota:** Non influisce sulla modalità d'accesso del lettore. |
| | Aperta estesa | Sblocca l'apriporta dopo le normali ore d'ingresso.<br>**Nota:** Non influisce sulla modalità d'accesso del lettore. |
| | Prima Tessera In | Imposta la modalità porta su "In attesa del primo utente". |
| | Relay aus On | Attiva il relay ausiliare della porta. |
| | Relay aus Off | Disattiva il relay ausiliare della porta. |
| | Segnale acustico della porta attivato | Attiva il segnale acustico della porta.<br>**Nota:** IPSDC non supporta questa azione. |
| | Segnale acustico della porta disattivato | Disattiva il segnale acustico della porta.<br>**Nota:** IPSDC non supporta questa azione. |
| | Bloccaggio porta | Blocco porta (influisce sulla serratura ed i lettori ingresso/uscita). |
| | Ripristinare porta | Ripristina la porta (influisce sulla serratura ed i lettori ingresso/uscita). |
| | Lettore tessera+PIN | Imposta il lettore sulla modalità d'accesso "credenziale e PIN"<br>**Nota:** Non ha alcun effetto sull'apriporta. |
| | Tessera+PIN - Lettore uscita | Imposta il lettore sulla modalità d'accesso "credenziale e PIN"<br>**Nota:** Non ha alcun effetto sull'apriporta. |
| | Tessera+PIN - Lettore ingresso/uscita | Imposta il lettore sulla modalità d'accesso "credenziale e PIN"<br>**Nota:** Non ha alcun effetto sull'apriporta. |
| | Solo tessera - Lettore ingresso | Imposta il lettore sulla modalità d'accesso "credenziale e PIN"<br>**Nota:** Non ha alcun effetto sull'apriporta. |
| | Solo tessera - Lettore uscita | Imposta il lettore sulla modalità d'accesso "credenziale e PIN"<br>**Nota:** Non ha alcun effetto sull'apriporta. |
| | Solo tessera - Lettori ingresso/uscita | Imposta il lettore sulla modalità d'accesso "credenziale e PIN" **Nota:** Non ha alcun effetto sull'apriporta. |

| Entità | Azioni | Note |
|---|---|---|
| Uscita | Attiva | Attiva l'uscita. |
| | Off | Disattiva l'uscita. |
| | Impulso On | Impulso uscita attivato, quindi disattivato per la durata selezionata.<br>**Nota:** La precisione della durata dell'impulso varia in base alla lunghezza dell'impulso. Consultare Precisione della durata della pulsazione a pagina 118. |
| | Impulso Off | Impulso uscita disattivato, quindi attivato per la durata selezionata.<br>**Nota:** La precisione della durata dell'impulso varia in base alla lunghezza dell'impulso. Consultare Precisione della durata della pulsazione a pagina 118. |

| Entità | Azioni | Note |
|---|---|---|
| Area | Ripristino APB | Ripristina l'APB di tutte le credenziali dell'aria a neutrale (ad es. passaggio libero). |
| | Sbloccare - Porte | Vedere comando porta corrispondente. Influisce su tutte le porte dotate di lettori ingresso o uscita associati all'area. |
| | Bloccare - Porte | Vedere comando porta corrispondente. Influisce su tutte le porte dotate di lettori ingresso o uscita associati all'area. |
| | Relay aus On - Porte | Vedere comando porta corrispondente. Influisce su tutte le porte dotate di lettori ingresso o uscita associati all'area. |
| | Relay aus Off - Porte | Vedere comando porta corrispondente. Influisce su tutte le porte dotate di lettori ingresso o uscita associati all'area. |
| | Dispositivo acustico On - Porte | Vedere comando porta corrispondente. Influisce su tutte le porte dotate di lettori ingresso o uscita associati all'area. **Nota:** IPSDC non supporta questa azione. |
| | Dispositivo acustico Off - Porte | Vedere comando porta corrispondente. Influisce su tutte le porte dotate di lettori ingresso o uscita associati all'area. **Nota:** IPSDC non supporta questa azione. |
| | Prima tessera In - Porte | Vedere comando porta corrispondente. Influisce su tutte le porte dotate di lettori ingresso o uscita associati all'area. |
| | Bloccare - Porte | Vedere comando porta corrispondente. Influisce su tutte le porte dotate di lettori ingresso o uscita associati all'area. |
| | Ripristinare - Porte | Vedere comando porta corrispondente. Influisce su tutte le porte dotate di lettori ingresso o uscita associati all'area. |
| | Credenziale e PIN - Lettori ingresso | Vedere comando porta corrispondente. Influisce su tutti i lettori che possono accedere all'area. |
| | Solo Credenziale - Lettori uscita | Vedere comando porta corrispondente. Influisce su tutti i lettori che possono uscire dall'area. |
| | Solo Credenziale - Tutti i Lettori | Vedere comando porta corrispondente. Influisce su tutti i lettori che possono entrare o uscire dall'area. |
| | Solo Credenziale - Lettori ingresso | Vedere comando porta corrispondente. Influisce su tutti i lettori che possono accedere all'area. |
| | Solo Credenziale - Lettori uscita | Vedere comando porta corrispondente. Influisce su tutti i lettori che possono uscire dall'area. |
| | Solo Credenziale - Tutti i Lettori | Vedere comando porta corrispondente. Influisce su tutti i lettori che possono entrare o uscire dall'area. |
| Notifica email | Invia un email | Vedere requisiti specifici qui sotto. |

Notare i dettagli seguenti sui record delle azioni trigger:

- Possono essere incluse fino a 10 azioni per record azione trigger. Le azioni possono essere qualsiasi combinazione di azioni di attivazione e/o disattivazione.
- Le azioni possono essere configurate per verificarsi quando il trigger è disattivato.
- Utilizzare il campo **Stato** nella parte superiore della pagina ***Amministrazione del sistema > Trigger azione*** per attivare o disattivare il record azione trigger.
- I trigger azione possono essere anche attivati manualmente nella pagina ***Monitoraggio > Trigger azione.*** Consultare Controllo dei trigger delle azioni a pagina 87.

**Notare:** Per fornire una maniera rapida per proteggere tutte le porte di un edificio, creare un trigger azione per bloccare tutte le porte ed azionarlo manualmente, quando necessario, nella pagina ***Controllo > Triggers azione***.

- Gli ingressi e le uscite disattivate possono essere incluse come azione, ma non devono essere implementate fino all'attivazione dell'ingresso o dell'uscita.
- I trigger azione, le programmazioni ed il controllo manuale possono avere un impatto sullo stato dei dispositivi e sono trattati allo stesso modo dal sistema. L'ultima operazione eseguita determina lo stato del dispositivo.
- I trigger azione non sovrascrivono gli stati globali "Bloccare tutte le porte " o "sbloccare tutte le porte".
- Se un'entità (ad esempio un lettore) è definita in un trigger azione e l'entità è in seguito eliminata dal sistema, tutti i record di trigger azione corrispondenti saranno anche eliminati. Se l'entità è ricreata, può essere creato una nuovo record trigger azione per l'entità.
- Se il sistema è configurato per l'invio automatico di messaggi, può essere creato un record trigger azione per l'invio di una notifica ad un elenco di email quando una condizione trigger cambia. L'invio del messaggio sarà tentato per il numero di tentativi selezionato in Numero massimo di nuovi tentativi, per il trigger azione.
- IPSDC non supporta le azioni  Segnale acustico attivato e Segnale acustico disattivato.
- Se un trigger azione è diretto verso un'entità appartenente ad un modulo non in linea, l'azione non avrà alcun effetto sull'entità quando il modulo sarà nuovamente in linea. In altre parole le azioni non persistono e non restano in coda.
- Le azioni uscita non registreranno un evento Uscita attivata o Uscita disattivata a meno che l'uscita non cambi fisicamente stato. Ad esempio, se un'uscita è attivata e si verifica un trigger azione che attiva l'uscita, non sarà generato alcun evento Uscita attivata.

Inoltre notare che le condizioni trigger sono presupposte in uno stato indeterminato e passeranno a vero o falso per eseguire le azioni corrispondenti:

- Per tutti i record all'avvio del sistema.
- Per ogni record quando un record è configurato e salvato.
- Per i record interessati in caso di eliminazione di un'entità referenziata.

## Aggiungere un record di trigger azione.

1. Selezionare ***Amministrazione del sistema > Trigger azione***.
2. Fare clic su [Aggiungere].
3. Immettere un nome descrittivo per il record fino a 64 caratteri nel campo **Nome trigger azione** .
4. Selezionare i valori nei quattro elenchi a discesa per creare la prima condizione che creerà l'azione.
5. Per creare condizioni supplementari nello stesso gruppo:
   a. Fare clic sul pulsante [+] nella riga dell'ultima condizione impostata.
   b. Selezionare i valori dai quattro elenchi a discesa.
   c. Ripetere gradino a e gradino b per ogni nuova condizione.
   d. Se necessario, fare clic sul pulsante [-] per eliminare una condizione.
6. Per creare un nuovo gruppo di condizioni, fare clic sul pulsante [+] nella stessa riga dell'elenco a discesa **Deve verificarsi una qualsiasi** .
7. Modificare gli elenchi a discesa **Deve verificarsi una qualsiasi** per creare operatori logici (ad esempio dichiarazioni E/O) per le condizioni in ciascun gruppo.
8. Fare clic su [Accettare le modifiche].
9. Quindi fare clic su [Azioni] per configurare l'azione(i) che si verificheranno quando una o tutte (in base alla configurazione dei trigger) le condizioni sono vere.

   La scheda Azioni include due sezioni: Azioni d'attivazione e azioni di disattivazione. Se necessario, le azioni possono essere aggiunte ad una o entrambe le sezioni.
10. Per aggiungere azioni sistema, area, uscita o porta:
    a. Fare clic su [Aggiungere] sotto la sezione Attivazione azioni o Disattivazione azioni.
    b. Selezionare il tipo d'azione da aggiungere.
    c. Nella finestra di dialogo Configurare azioni, selezionare le entità e l'azione che deve verificarsi.
    d. Fare clic su [Ok] per chiudere la finestra di dialogo Configurare azioni.
11. Per aggiungere azioni email:

    **Notare:** Evitare di aggiungere grandi quantità di azioni email per evitare lo spamming dei destinatari.

    a. Fare clic su [Aggiungere] sotto la sezione Attivazione azioni o Disattivazione azioni.
    b. Selezionare **Azioni email**.
    c. Nella finestra di dialogo Configurare azioni, selezionare l'elenco di distribuzione email al quale il messaggio deve essere inviato quando una condizione trigger cambia. I messaggi possono anche essere inviati a tutti gli elenchi.
    d. Immettere il **contenuto dell'email**.
    e. Selezionare un valore **Nuovo tentativo scaduto**. Se il messaggio iniziale fallisce a causa di un errore di collegamento, il sistema tenterà di inviare nuovamente il messaggio raddoppiando la durata dell'attesa tra tentativi fino al raggiungimento del valore selezionato.
    f. Fare clic su [Ok] per chiudere la finestra di dialogo Configurare azioni.
12. Fare clic su [Accettare le modifiche].

### Copiare un record di trigger azione

1. Selezionare ***Amministrazione del sistema > Trigger azione***.
2. Fare clic sul trigger azione per selezionarlo.
3. Fare clic su [Copiare].
4. Se necessario, modificare il record.
5. Fare clic su [Accettare le modifiche].

### Eliminare un record di trigger azione

1. Selezionare ***Amministrazione del sistema > Trigger azione***.
2. Fare clic sul trigger azione per selezionarlo.
3. Fare clic su [Eliminare].
   Sarà visualizzata la finestra di dialogo Eliminare elemento.
4. Fare clic su [Eliminare].

## Configurare una condivisione di rete

Come descritto in Creazione del backup dei dati a pagina 89, i backup automatici possono essere pianificati per l'esecuzione automatica e con l'invio del file di backup ad una risorsa di rete condivisa detta *condivisione di rete*.

Le condivisioni di rete possono essere configurate per una cartella di rete o un file system remoto che utilizza uno dei seguenti protocolli di comunicazione:

- File Transfer Protocol (FTP)
- File Transfer Protocol Secure (FTPS)
- Common Internet File System (CIFS)

### Aggiungere una condivisione di rete

Per configurare una condivisione di rete per i backup programmati:

1. Selezionare ***Amministrazione del sistema > condivisione di rete***.
2. Fare clic su [Aggiungere].
3. Selezionare un protocollo di comunicazione nel campo **Protocollo** per collegarsi ad un file system remoto, oppure selezionare *Nessuno* per utilizzare una cartella di rete.

**Notare:** Man mano che si immettono i dati nei campi della pagina, il campo **Nome condivisione** cambierà per riflettere le nuove informazioni.

4. Se sono stati selezionati FTP o FTPS nel gradino 3, immettere il numero di porta del collegamento nel campo **Porta** .
5. Immettere l'indirizzo IP o l'hostname del server email nel campo **Host** .
6. Immettere la posizione della cartella della condivisione di rete nel campo **Host** .
7. Se è stato selezionato un protocollo di file system remoto nel gradino 3, immettere il nome utente necessario al collegamento al sistema nel campo **Utente**.

8. Se è stato selezionato un protocollo di file system remoto nel gradino 3, immettere la password necessaria al collegamento al sistema nel campo **Password**.
9. Fare clic [Accettare le modifiche].

### Copiare una condivisione di rete

1. Selezionare ***Amministrazione del sistema > condivisione di rete***.
2. Fare clic sulla condivisione di rete per selezionarla.
3. Fare clic su [Copiare].
4. Se necessario, modificare la condivisione di rete.
5. Fare clic su [Accettare le modifiche].

### Eliminare una condivisione di rete

1. Selezionare ***Amministrazione del sistema > condivisione di rete***.
2. Fare clic sulla condivisione di rete per selezionarla.
3. Fare clic su [Eliminare].

   Sarà visualizzata la finestra di dialogo Eliminare elemento.
4. Fare clic su [Eliminare].

## Creazione di un backup e di un punto di ripristino

Dopo la configurazione del sistema è importante:

- Creare un file di backup che includa tutti i record. le foto e le impostazioni configurate nel sistema. Consultare Creazione del backup dei dati a pagina 89.
- Creare un punto di ripristino che includa tutti i dati salvati nel file di backup e le impostazioni personalizzate del controller del sistema. L'informazione sarà salvata nel controller del sistema e può essere ripristinata in seguito per riportare il sistema allo stato operativo iniziale. Consultare Salvare e ripristinare le impostazioni predefinite a pagina 92.

# CAPITOLO 5 *Gestione dell'accesso*

L'accesso ad un edificio e l'interfaccia utente possono essere gestite:

- Aggiungendo o eliminando persone,
- Aggiungendo, disattivando, riattivando o eliminando credenziali e
- Aggiungendo o elimimando account utenti.

Gli argomenti del capitolo includono:



## Gestione delle persone

Gli individui che fanno parte di un'organizzazione possono accedere all'edificio ed al sistema. L'accesso all'edificio è controllato tramite le credenziali (dette anche badge di identificazione). L'accesso al sistema è controllato tramite l'account utente utilizzato per collegarsi al controller del sistema. Per organizzare gli account e le credenziali, il sistema li associa entrambi con un record per ogni individuo dell'organizzazione. Il record individuale nel database è chiamato "persona" poiché corrisponde effettivamente ad una persona.

La distinzione tra persone, credenziali e account utente è importante. Anzitutto chiunque debba accedere ad un edificio ha bisogno di una credenziale (un badge di identificazione con un numero codificato riconosciuto dal sistema). Tuttavia non tutti coloro che accedono all'edificio necessitano l'accesso al sistema tramite un account utente. Inoltre solo coloro che utilizzano e gestiscono il sistema necessitano un account utente. Infine, in alcuni casi, gli operatori lavorano in remoto e non necessitano di una credenziale per accedere all'edificio anche se hanno un account utente.

I record "persone" del database consentono agli utenti di gestire facilmente le credenziali e gli account utenti a partire da un solo record, invece di gestire database separati per gli utenti del sistema e le credenziali d'accesso all'edificio.

## Aggiungere una persona

Prima di aggiungere il record di una persona assicurarsi di:

- Assegnare ad ogni record persona un numero di identificazione unico. Ad esempio il numero dipendente.
- Aggiungere campi definiti dall'utente per immettere dati relativi al personale, quali la targa del veicolo o il numero di telefono della residenza. Consultare Configurare i campi definiti dall'utente a pagina 49.

Esistono diverse modalità per aggiungere record persone:

- Nella pagina ***Gestione dell'accesso > Persone*** come descritto di seguito.
- Utilizzando la procedura guidata Aggiungere persone, disponibile nella pagina ***Home***.
- Utilizzando l'importazione/esportazione guidata fornita con il disco utilità utilizzata per importare i record e le credenziali già esistenti in formato CSV (ad esempio in caso di dati esportati da un altro sistema di controllo dell'accesso o dal database del personale). Per informazioni dettagliate, consultare la *Guida utente di importazione/esportazione guidata*.
- Utilizzando il lettore opzionale Learn-In. Consultare Utilizzazione di un lettore iscrizione a pagina 70.

Per aggiungere il record di una persona nella pagina ***Gestione dell'accesso > Persone*** :

1. Fare clic su ***Gestione dell'accesso > Persone***.
2. Fare clic su [Aggiungere].
3. Immettere il **nome** e il **cognome**.
4. Fare clic sulla scheda **Dettagli**.
5. Immettere le informazioni necessarie nei campi definiti dall'utente.
6. Se la persona necessita l'accesso al sistema, fare clic sulla scheda **Account utente** per creare un account. Vedere **Aggiungere un account a pagina 72.**
7. Fare clic su [Accettare le modifiche].
8. Se la persona necessita di una credenziale per l'ascesso all'edificio, consultare Aggiungere una credenziale a pagina 70.

## Eliminare una persona

Il sistema può memorizzare fino a 10000 record di persone. Tuttavia le persone che non necessitano più l'accesso al sito o al sistema devono essere eliminate dal database.

**Notare:** Per eliminare diverse persone in blocco, utilizzare l'importazione/esportazione guidata fornita nel disco utilità.

1. Fare clic su ***Gestione dell'accesso > Persone***.
2. Selezionare la persona dall'elenco delle persone.
3. Fare clic su [Eliminare].

   Sarà visualizzata la finestra di dialogo Eliminare elemento.
4. Fare clic su [Eliminare].

## Caricare la foto di ientificazione di una persona

Le persone possono avere una foto di identificazione associata al record. Ad ogni evento d'accesso associato alla credenziale della persona, apparirà una miniatura della foto.

Si notino i dettagli seguenti sul caricamento delle foto:

- I file supportati sono GIF, JPG e PNG.
- Possono essere caricate foto fino a 200 KB, ma saranno automaticamente ridimensionate a 10 KB o meno, in formato JPG.
- La memoria disponibile per le foto è limitata a 40 KB.
- In caso di caricamento di foto di grandi dimensioni, i 40 KB potrebbero essere esauriti prima di raggiungere la capacità di 10000 persone.

Per caricare una foto:

1. Fare clic su ***Gestione dell'accesso > Persone***.
2. Selezionare la persona dall'elenco delle persone.
3. Fare clic sull'icona foto ID accanto al nome della persona.
   Sarà visualizzata la finestra di dialogo Caricare foto.
4. Fare clic su **Selezionare file**.
   Sarà visualizzata la finestra di dialogo Selezionare file.
5. Selezionare una foto e fare clic su **Aprire**
6. Fare clic su **Caricare**.
7. La finestra di dialogo Selezionare file sarà chiusa.
8. Fare clic su [Accettare le modifiche].

**Notare:** Per caricare una foto esistente, fare clic sulla foto e ripetere i passaggi.

## Eliminare la foto di ientificazione di una persona

1. Fare clic su ***Gestione dell'accesso > Persone***.
2. Selezionare la persona dall'elenco delle persone.
3. Fare clic sull'icona foto ID accanto al nome della persona.
   Sarà visualizzata la finestra di dialogo Caricare foto.
4. Fare clic su **Eliminare**.
5. Nel messaggio di conferma, fare clic su **Eliminare**.

# Gestione delle credenziali

Chiunque debba accedere ad un edificio ha bisogno di una credenziale (un badge di identificazione con un numero codificato riconosciuto dal sistema). Prima di assegnare una credenziale, aggiungere la persona al database. Vedere **Aggiungere una persona a pagina 68.**

**Notare:** In caso di modifica o eliminazione di una credenziale, la cache locale del IPSDC è svuotata per prevenire l'accesso non autorizzato in caso si utilizzazione del IPSDC in modalità fallback. Consultare Modalità fallback IPSDCU a pagina 19.

## Utilizzazione di un lettore iscrizione

Il lettore di iscrizione USB opzionale (TP-RDR-LRN) può essere collegato alla stazione di lavoro locale client e poi utilizzato per leggere le credenziali. I dati delle credenziali saranno automaticamente inseriti nel campo **ID credenziale** della pagina ***Gestione dell'accesso > Persone*** . Questo dispositivo può fare risparmiare tempo se si aggiungono diverse credenziali.

Installare e configurare il lettore nella stazione di lavoro client locale seguendo le istruzioni del produttore disponibili alla pagina www.rfideas.com. Scaricare l'utilità di configurazione pcProx, che include la documentazione del lettore pcProx Plus (ad esempio il TP-RDR-LRN).

Notare i seguenti dettagli sulla configurazione di un lettore di iscrizione:

- Se le credenziali sono utilizzate con un codice edificio, configurare il lettore per la separazione del codice edificio dalle credenziali del badge.
- L'utilità di configurazione pcProx Configuration utilizza file .hwg per configurare il lettore di iscrizione. Utilizzare il file di configurazione Casi_card.hwg per riconoscere i badge CASI Prox.

## Aggiungere una credenziale

Prima di creare una credenziale per una persona, creare la persona. Vedere **Aggiungere una persona a pagina 68.**

1. Selezionare ***Gestione dell'accesso > Persone***.
2. Selezionare la persona che necessita la credenziale.
3. Fare clic su [Credenziali].
4. Fare clic su [Aggiungere credenziali].
5. Fare clic sulla scheda **Generale**.
6. Immettere l' **ID credenziale**.

   Se il lettore opzionale iscrizione è collegato alla stazione di lavoro locale, fare clic nel campo **ID credenziale** e strisciare la tessera credenziale nel lettore per inserire i dati nel campo.
7. (Opzionale) Immettere il codice **PIN.**

**Notare:** Utilizzare il carattere cancelletto (#) alla fine di ciascun PIN, soprattutto se la lunghezza del PIN è inferiore alla **Lunghezza massima PIN** definita nella scheda Sicurezza della pagina ***Amministrazione del sistema > Impostazioni del sistema***. I caratteri cancelletto sono necessari per le PIN utilizzate su dispositivi collegati al IPSDC.

8. (Opzionale) Selezionare **Utilizzare sblocco/apertura prolungato** se il titolare della credenziale necessita più tempo per aprire e attraversare le porte.
9. (Opzionale) Selezionare **Esente da anti-passback** se si utilizza l'anti-passback e la credenziale non è tracciata.

10. (Opzionale) Selezionare una data **Attiva da** e **Attiva fino al** se la credenziale ha una durata limitata.
11. Fare clic sulla scheda **Livelli di accesso.**
12. Selezionare i livelli di accesso da applicare alla credenziale.
13. Fare clic su [Accettare le modifiche].

### Eliminare una credenziale

Per evitarne l'uso, una credenziale non deve essere eliminata. Se ad esempio un individuo smarrisce una credenziale, invece di eliminarla subito, può essere disattivata per consentire all'individuo di cercarla. Se la credenziale è definitivamente smarrita, quando l'individuo richiede una nuova credenziale, la credenziale smarrita sarà eliminata. Vedere **Prevenzione dell'uso delle credenziali rubate o perdute a pagina 71.**

1. Selezionare ***Gestione dell'accesso > Persone***.
2. Selezionare la persona titolare della credenziale da eliminare.
3. Fare clic su [Credenziali].
4. Fare clic sulla credenziale da eliminare.
5. Fare clic su [Eliminare credenziale].
6. Fare clic su [Eliminare].
7. Nella finestra di dialogo Eliminazione elementi, fare clic su [Eliminare].

## Gestione delle credenziali rubate o smarrite

Se un individuo smarrisce una credenziale, invece di eliminarla subito, può essere disattivata per consentire all'individuo di cercarla. Se la credenziale è definitivamente smarrita, quando l'individuo richiede una nuova credenziale, la credenziale smarrita sarà eliminata.

Esistono altri vantaggi per la disattivazione di una credenziale. Una credenziale non valida presentata al lettore genera un evento, ma se la credenziale è ancora assegnata ad una persona, l'evento indicherà che la persona sta tentando di utilizzare una credenziale non valida. Se gli eventi porta e lettore sono controllati da una telecamera, sarà registrata un'immagine della persona che tenta di utilizzare la credenziale rubata. La ricerca nel database degli eventi della persona che ha smarrito la credenziale, mostrerà tutti gli incidenti associati alla persona prima e dopo lo smarrimento della credenziale. In questo modo potrebbe essere stabilita una relazione tra la vittima del furto e l'autore.

### Prevenzione dell'uso delle credenziali rubate o perdute

Utilizzare i  passaggi seguenti per disattivare una credenziale invece di eliminarla.

1. Selezionare ***Gestione dell'accesso > Persone***.
2. Selezionare la persona titolare della credenziale da disattivare.
3. Fare clic su [Credenziali].
4. Fare clic sulla credenziale da disattivare.
5. Fare clic nel campo **Attiva fino al**

   Sarà visualizzato un calendario popup.
6. Selezionare una data passata.
7. Fare clic su [Accettare le modifiche].

### Ripristinare una credenziale trovata

1. Selezionare ***Gestione dell'accesso > Persone***.
2. Selezionare la persona titolare della credenziale da disattivare.
3. Fare clic su [Credenziali].
4. Fare clic sulla credenziale da riattivare.
5. Fare clic nel campo **Attiva fino al**
6. Fare clic su [Accettare le modifiche].

## Gestione degli account utente

Gli account utente consentono alle persone di collegarsi al sistema. L'account utente è associato con il record del database della persona, esattamente come la credenziale. Tuttavia una persona non ha bisogno di avere un account utente per accedere all'impianto con una credenziale.

### Aggiungere un account

Prima di creare una credenziale per un account utente, creare un record per la persona. Vedere **Aggiungere una persona a pagina 68.**

1. Collegarsi come amministratore o rivenditore. (Gli altri ruoli operatore non hanno l'autorizzazione per la modifica degli 'account utente.)
2. Selezionare ***Gestione dell'accesso > Persone***.
3. Selezionare la persona da modificare.
4. Fare clic sulla scheda **account utente.**
5. Selezionare **Collegamento consentito**.
6. Immettere un **Nome utente**.
7. Fare clic su [Impostare la password].
8. Immettere la nuova password nei campi **nuova password** e **conferma password**.
9. Fare clic su [OK].
10. Selezionare un **ruolo**.
11. Fare clic su [Accettare le modifiche].

### Modificare un nome utente ed una password

1. Collegarsi come amministratore o rivenditore. (Gli altri ruoli operatore non hanno l'autorizzazione per la modifica degli 'account utente.)
2. Selezionare ***Gestione dell'accesso > Persone***.
3. Selezionare la persona da modificare.
4. Fare clic sulla scheda **account utente.**
5. Immettere un nuovo **Nome utente**.
6. Fare clic su [Impostare la password].
7. Immettere la nuova password nei campi **nuova password** e **conferma password**.
8. Fare clic su [OK].
9. Fare clic su [Accettare le modifiche].

### Disattivare un account utente

1. Collegarsi come amministratore o rivenditore. (Gli altri ruoli operatore non hanno l'autorizzazione per la modifica degli 'account utente.)
2. Selezionare ***Gestione dell'accesso  Persone***.
3. Selezionare la persona da modificare.
4. Fare clic sulla scheda **account utente.**
5. Deselezionare la casella **Can log on**
6. Fare clic su [Accettare le modifiche].

## Creazione di reports

I cinque report predefiniti consentono agli utenti di visualizzare informazioni memorizzate nel server del database.

**Cronologia accesso**
Un riepilogo dei tentatici di accesso di una persona filtrati per data, nome della persona (carattere jolly), lettore, area risposta consentito o rifiutato.

**Credenziale**
Un elenco di credenziali assegnate filtrato per nome della persona (carattere jolly), lD credenziale (carattere jolly), livelli di accesso,  risposta consentito o rifiutato.

**Accesso lettore**
Un elenco di persone con accesso a ciascun lettore, filtrato per nome della persona (carattere jolly) e lettore.

**Appello nominale**
Un elenco di persone per area corrente o ultimo lettore, filtrato per nome della persona (carattere jolly), lettore e eventi. Selezionare **Includere eventi "Accesso/Uscita Consentita - Nessun Ingresso"** per includere eventi per i quali l'accesso o l'uscita è stata consentita, ma non è possibile stabilire se si siano verificati .

**Elenco**
Un elenco di persone nel database filtrato per nome della persona (carattere jolly) e privilegi di login.

Si notino i dettagli seguenti sui report:

- I report sono visualizzati in formato HTML in una finestra del browser Internet. Se si utilizza Internet Explorer 7 o precedente, il logo del prodotto nell'angolo in alto a destra non sarà visualizzato correttamente. Si tratta di un problema con le vecchie versioni di Internet Explorer.
- In caso di modifica dei nomi dell'entità (ad esempio nomi di dispositivi, nomi di persone), il nome aggiornato dell'entità sarà riportato nel report successivo.

### Creare un report

1. Selezionare ***Report***.
2. Selezionare il tipo di report da creare.
3. Se necessario, compilare i campi specifici del report.
4. Fare clic su [Visualizzare] per visualizzare il report in una finestra del browser.
5. Per esportare un report:
   a. Fare clic su [Esportare].
   b. Quando richiesto, fare clic su [Salvare].
   c. Nella finestra di dialogo visualizzata, spostarsi sulla posizione nella quale il report deve essere salvato in formato CSV.
   d. Fare clic su [Salvare].

**Notare:** Se la notifica "Creazione report" continua ad apparire e l'interfaccia utente principale è offuscata, il livello di memoria della stazione di lavoro client locale potrebbe essere basso. Chiudere la finestra del browser per terminare la sessione, chiudere tutti i programmi non utilizzati, ricollegarsi e cercare nuovamente di creare il report.

## Ricerca di persone

La funzione di ricerca filtra il database per record con campi che corrispondono completamente o in parte alla richiesta.

### Cercare persone

1. Selezionare ***Gestione dell'accesso > Persone***.
2. Fare clic su [Ricerca] e selezionare un campo per la ricerca.

   Il pulsante [Ricerca] appare accanto al riquadro di testo Ricerca ed ha la forma di una lente d'ingrandimento. Facendo clic sul pulsante, scenderà un elenco di campi da ricercare.
3. Immettere il termine di ricerca.
4. Fare clic su <Invio>.

### Annullare una ricerca

I risultati della ricerca continueranno a filtrare il database, anche se l'utente passa ad un'altra pagina e ritorna alla pagina ***Persone***, fino all'annullamento della ricerca.

1. Selezionare ***Gestione dell'accesso > Persone***.
2. Fare clic sulla **X** per svuotare il campo ricerca.

CAPITOLO 6

# *Controllo dell'accesso*

Durante le normali operazioni, l'accesso all'edificio può essere gestito e controllato tramite:

- La visualizzazione degli eventi.
- In presenza di telecamere, visualizzando i video di sicurezza.
- Interventi sul comportamento programmato della porta per aprire, sbloccare, bloccare, ripristinare o proteggere le porte.
- La risposta agli allarmi.

Gli argomenti del capitolo includono:

# Controllo degli eventi e degli allarmi

La pagina ***Eventi*** registra record riguardanti:

- Problemi relativi all'accesso
  - Accesso non autorizzato
  - Le violazioni anti-passback
  - Apertura prolungata della porta
  - Gli utenti collegati al sistema
- I messaggi di stato del sistema e del dispositivo
  - Modifiche dello stato del sistema quali aggiornamenti della data e dell'ora
  - Modifica delle modalità dei dispositivi
  - Modifica dello stato dei trigger azioni
  - Il database ed il backup
- Allarmi
  - Il sabotaggio della porta
  - L'apertura forzata della porta
  - Fallimenti o problemi del sistema

Si notino i dettagli seguenti sulla pagina ***Eventi***:

- Gli eventi associati ad un dispositivo collegato ad una telecamera registreranno un record video dell'evento.
- Per ordinare gli eventi, fare clic sull'intestazione di colonna.
- Per eventi ordinati per data e ora, la pagina ***Eventi*** sarà riordinata automaticamente al verificarsi di un nuovo evento, con il più recente in cima (ad esempio l'elenco è mostrato dall'inizio).
- Per visualizzare informazioni dettagliate su un dispositivo, fare clic sul dispositivo nella colonna Dispositivo per accedere alla pagina ***Controllo > Porte*** .

Fare clic su un evento per visualizzare nel riquadro dettagli la data, l'ora e la descrizione dell'evento. Saranno inoltre forniti dettagli supplementari sull'evento a seconda che si tratti di un evento relativo alla persona (ad esempio accesso autorizzato) o relativo al dispositivo (ad esempio porta sbloccata).

- Per eventi relativi alla persona, il riquadro dettagli includerà anche il nome della persona, la credenziale e, se disponibile, una foto. Fare doppio clic su una foto per accedere alla pagina ***Gestione dell'accesso > Persone*** e visualizzare dettagli sull'individuo.
- Per eventi relativi ad un dispositivo, il riquadro dettagli includerà la descrizione dell'evento, la data, l'ora e, se disponibile, il video dell'evento.

Una volta terminato, fare clic su [Chiudere] sul riquadro dettagli.

## Visualizzare gli eventi più recenti

Gli eventi più recenti sono visualizzati nell'angolo in basso a sinistra della pagina. Se si verifica un evento mentre si lavora un un'altra  pagina, un riassunto dell'evento, inclusa una miniatura della foto della persona associata all'evento , potrà essere visualizzato spostando il cursore del mouse sull'evento.

La finestra popup visualizzerà la data e l'ora dell'evento, una descrizione e la credenziale. Nella parte inferiore sarà visualizzata la foto ed il nome della persona.

## Caricare altri eventi

La pagina ***Eventi*** visualizza gli eventi più recenti. Per visualizzare gli eventi precedenti, caricarli nel browser dal sistema. Il comando Caricare altri eventi, carica i 500 eventi successivi (o meno se ne esistono meno di 500).

1. Selezionare ***Eventi***.
2. Fare clic sul pulsante circolare [Eventi].
3. Selezionare **Caricare altri eventi**.
4. (Opzionale) Per bloccare l'operazione, fare clic su **Annullare** .

## Caricare tutti gli eventi

La pagina ***Eventi*** visualizza gli eventi più recenti. Per visualizzare gli eventi precedenti, caricarli nel browser dal sistema. Il comando Caricare tutti gli eventi, trasferirà tutti gli eventi del controller del sistema nel browser, l'operazione potrebbe richiedere diversi minuti.

1. Selezionare ***Eventi***.
2. Fare clic sul pulsante circolare [Eventi].
3. Selezionare **Caricare altri eventi**.
4. (Opzionale) Per bloccare l'operazione, fare clic su **Annullare** .

## Cercare eventi

Utilizzare la funzione di ricerca per filtrare l'elenco degli eventi visualizzati secondo uno o più criteri.

1. Selezionare ***Eventi***.
2. Fare clic sull'icona **Filtrare** nella parte destra della pagina.
3. Immettere i criteri di ricerca nei campi appropriati.

   Per ottenere i migliori risultati, immettere diversi criteri di ricerca.
4. Fare clic su <Invio>.

## Esportare eventi

Il sistema può memorizzare fino a 65.535 record di persone. Una volta raggiunto il limite, gli eventi più vecchi saranno eliminati per recuperare spazio. Utilizzare il comando Esportare eventi per salvare il record degli eventi in un file in formato CSV.

1. Selezionare ***Eventi***.
2. Fare clic sul pulsante circolare [Eventi].
3. Selezionare **Esportare eventi**.
4. Scegliere la posizione nella quale salvare il file nella stazione di lavoro client.
5. Immettere un nome descrittivo e l'estensione .**csv**.
6. Fare clic su **Salvare**.

# Controllo dei video degli eventi

Il sistema è in grado di visualizzare il video live o registrato da telecamere specifiche ed associare il video registrato con gli eventi di determinati dispositivi, quali lettori o porte. (Consultare Configurazione dei dispositivi video a pagina 34.)

Il collegamento a video relativi a eventi specifici si trova nella pagina ***Eventi***. Utilizzare la pagina ***Controllo > Video*** per controllare il flusso video da una o più telecamere. I videoclip di video live o registrati possono essere scaricati nella stazione di lavoro client locale.

## Prima di iniziare

Prima di riprodurre un video nella pagina ***Eventi*** o ***Controllo > Video***, verificare che le impostazioni di sicurezza si Internet Explorer siano impostate correttamente, come descritto di seguito.

1. Aprire Internet Explorer.
2. Nel menù Strumenti, fare clic su **Opzioni Internet**.
3. Passare alla scheda Sicurezza e fare clic su [Livello personalizzato...].

**Notare:** Se il pulsante **Livello personalizzato...** non è attivato, potrebbero esistere policy di sicurezza per impedire agli utenti di modificare le impostazioni di Internet Explorer. Contattare l'amministratore di rete oppure eseguire Internet Explorer come amministratore.

4. vScorrere l'elenco Impostazioni di sicurezza per visualizzare le impostazioni Controlli ActiveX e plug-ins.
5. Per *Richieste di conferma automatiche per i controlli ActiveX*, fare clic su **Attivare**.
6. Per *Scaricare controlli ActiveX* verificati, fare clic su **Attivare** o **Richiedere conferma**.
7. Per *Inizializzare e elaborare controlli ActiveX* non contrassegnati come sicuri per la programmazione, fare clic su **Attivare** o **Richiedere conferma**.
8. Per *Eseguire controlli ActiveX e plug-ins*, fare clic su **Attivare** o **Richiedere conferma**.
9. Per *Elaborare controlli ActiveX contrassegnati come sicuri per la programmazione*, fare clic su **Attivare** o **Richiedere conferma**.
10. Scorrere l'elenco Impostazioni di sicurezza per visualizzare le impostazioni varie.
11. Per *Programmazione attiva*, fare clic su **Attivare** o **Richiedere conferma**.
12. Scorrere l'elenco Impostazioni di sicurezza per visualizzare le impostazioni di programmazione.
13. Per *Utilizzare blocco pop-up*, fare clic su **Disattivare**.
14. Click **OK**, quindi ancora una volta su **OK** per salvare le impostazioni.

Inoltre, quando si accede ad un video per la prima volta, apparirà un messaggio indicante che è necessaria l'installazione di un riproduttore video proprietario. Per installare il software, fare clic su [Scaricare e installare]. (Se le policy di sicurezza della rete bloccano lo scaricamento, contattare l'amministratore di rete oppure eseguire Internet Explorer come amministratore.) Dopo il messaggio indicante il successo dell'installazione del riproduttore video, terminare il collegamento e ricollegarsi per accedere al video.

**IMPORTANTE:** Gli utenti delle versioni TruPortal 1.0 o goEntry 3.0 devono disinstallare (se necessario) la versione corrente del TruPortal controllo ActiveX tramite l'opzione **Pannello di controllo > Programmi e funzioni > Disinstallare un programma** prima di installare una versione aggiornata del lettore video proprietario.

## Riprodurre il video dell'evento

Gli eventi con un video registrato associato, presentano un'icona telecamera collegata ( ) alla descrizione dell'evento nella pagina ***Eventi***.

1. Selezionare ***Eventi***.
2. Scorrere o cercare un evento.
3. Fare clic sull'icona **Telecamera** accanto alla Descrizione dell'evento.

   Sarà visualizzato il riquadro Dettaglio evento ed un fotogramma del video nella parte inferiore della pagina
4. Fare clic su [Riprodurre video dell'evento].
5. Passare sulla parte inferiore del fotogramma video per visualizzare i controlli per la riproduzione e la registrazione del video. Consultare Referenza dei controlli video a pagina 80.

## Controllare i video

La pagina ***Eventi*** visualizza i video registrati degli eventi relativi ad un determinato dispositivo, la pagina ***Monitoraggio > Video*** invece consente agli utenti di gestire la sicurezza dell'intero sito. Se ad esempio un individuo sospetto si aggira nel parcheggio, non sarà generato nessun evento porta o lettore, tuttavia se esiste una telecamera nel parcheggio, la persona potrebbe essere notata da un utente che guarda la telecamera.

**Notare:** Prima di poter controllare un video live o registrato, aggiungere almeno un layout video. Consultare Aggiungere layout video a pagina 36.

Per controllare il video:

1. Selezionare ***Controllo > Video***.

**Notare:** Se il messaggio indica che il riproduttore video deve essere installato, fare clic su [Scaricare ed installare]. Al termine dell'installazione, terminare il collegamento e ricollegarsi per riprodurre il video dell'evento. Per ulteriori informazioni, consultare Prima di iniziare a pagina 78.

2. Selezionare un **Layout**.
3. Per visualizzare un video live, fare clic sul pulsante [Live].
4. Per visualizzare i video registrati, fare clic su [Riproduzione] e selezionare un'opzione dal menù.
5. (Opzionale) Per riposizionare una telecamera PTZ, fare clic sul pulsante **PTZ** per aprire e regolare i controlli PTZ.

## Scaricare un videoclip

I videoclip possono essere scaricati dalle pagine ***Eventi*** e ***Monitoraggio > Video*** come descritto di seguito.

1. Passare sulla parte inferiore del fotogramma video per visualizzare i controlli per la riproduzione e la registrazione del video. Consultare Referenza dei controlli video a pagina 80.
2. Per scaricare un videoclip live:
   a. Fare clic su [Riproduzione].
   b. Dal menù visualizzato, selezionare **Live**.
   c. Fare clic sul pulsante **Registrare video Live/Registrati** .

d. Spostarsi su una cartella nella finestra di dialogo visualizzata, quindi fare clic su **OK**.

e. Fare clic ancora una volta sul pulsante **Registrare video Live/Registrati** per terminare la registrazione del video live.

**Nota:** Il passaggio alla modalità riproduzione durante lo scaricamento del video causerà l'arresto dello scaricamento.

Il videoclip è scaricato nella cartella selezionata.

3. Per scaricare una porzione di un videoclip registrato:

a. Fare clic sul pulsante **Riproduzione**.

b. Dal menù riproduzione visualizzato selezionare *2 minuti*.

c. Attendere 30 secondi.

d. Fare clic sul pulsante **Registrare video Live/Registrati**.

Sarà visualizzata una barra d'avanzamento sul fotogramma.

e. Spostare il cursore su 1 minuto e fare clic su **OK**.

f. Spostarsi su una cartella nella finestra di dialogo visualizzata, quindi fare clic su **OK**.

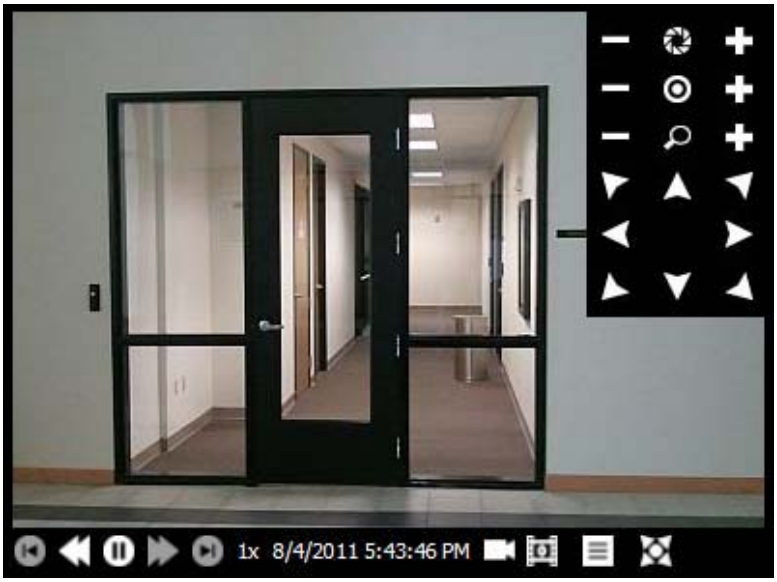
Il videoclip è scaricato nella cartella selezionata.

**Notare:** Se il video non può essere scaricato da una telecamera collegata ad un TVR31, tentare di regolare la limitazione della larghezza di banda sul TVR31.

Per visualizzare i videoclip scaricati, utilizzare il lettore TruVision Navigator fornito con il disco del prodotto nella cartella \VideoPlayer.

## Referenza dei controlli video

**FIGURA 1. Controlli video**



| Icona | Caratteristica | Funzione |
|---|---|---|
|  | Controllo iride | Apre o chiude l'iride della telecamera per regolare la quantità di luce disponibile |
|  | Controllo focalizzazione | Regola la focalizzazione dell'immagine. |
|  | Controllo zoom | Regola lo zoom della pagina. |
|  | Controlli panoramica e inclinazione | Sposta la telecamera nella direzione(i) indicata dalle frecce. |
|  | Controllo riavvolgimento passo a passo | Sposta il video registrato indietro di un fotogramma. |
|  | Controllo riavvolgimento | Sposta il video all'indietro. |
|  | Controllo riproduzione | Riproduce il flusso video (live o registrato). |
|  | Controllo pausa | Interrompe il flusso video (live o registrato). |
|  | Controllo avanzamento | Sposta il video in avanti in avanzamento rapido. |
|  | Controllo un passo in avanti | Sposta il video registrato in avanti di un fotogramma. |
|  | Controllo live | Passa dalla riproduzione di un video registrato alla visualizzazione di un video live. |

| Icona | Caratteristica | Funzione |
|---|---|---|
|  | Controllo video registrato | Fornisce un menù di opzioni di riproduzione, da live fino a diversi minuti indietro. |
|  | Controllo impostazioni predefinite | Sposta rapidamente la telecamera nella posizione predefinita. |
|  | Attivare controllo PTZ | Apre i controlli panoramica, inclinazione e zoom (funziona solo con telecamere PTZ). |
|  | Controllo registrazione video live/registrato | Registra video. |

## Controllo delle porte

La pagina ***Monitoraggio > Porte*** contiene lo stato delle porte, i lettori assegnati, gli eventi recenti relativi alle porte e le pianificazioni assegnate. La pagina consente agli operatori di bloccare, aprire, ripristinare e sbloccare le porte.

### Aprire una porta

Utilizzare il comando Aprire porta per consentire l'accesso ad un individuo sprovvisto di credenziali.

1. Selezionare ***Controllo > Porte***.
2. Fare clic sulla scheda **Visualizzazione evento.**
3. Fare clic sul pulsante **Comandi singola porta** per aprire la porta.
4. Selezionare **Aprire porta**.

### Sbloccare una porta

Utilizzare il comando Sbloccare porta per disattivare la sicurezza della porta, consentendo a chiunque di entrare o uscire senza presentare una credenziale valida.

1. Selezionare ***Controllo > Porte***.
2. Fare clic sulla scheda **Visualizzazione evento.**
3. Fare clic sul pulsante **Comandi singola porta** per sbloccare la porta.
4. Selezionare **sbloccare porta**.

## Ripristinare una porta

Utilizzare il comando Ripristinare porta per riportare la porta al funzionamento normale dopo uno sblocco.

1. Selezionare ***Controllo > Porte***.
2. Fare clic sulla scheda **Visualizzazione evento.**
3. Fare clic sul pulsante **Comandi singola porta** per ripristinare la porta.
4. Selezionare**Ripristinare porta**.

## Bloccare una porta

Utilizzare il comando Bloccare porta per bloccare una porta e modificare l'impostazione del lettore per prevenire l'utilizzazione delle credenziali per accedere alla porta.

1. Selezionare ***Controllo > Porte***.
2. Fare clic sulla scheda **Visualizzazione evento.**
3. Fare clic sul pulsante **Comandi singola porta** per bloccare la porta.
4. Selezionare **Bloccare porta**.

## Proteggere una porta

Utilizzare il comando Proteggere porta per bloccare una porta.

1. Selezionare ***Controllo > Porte***.
2. Fare clic sulla scheda **Visualizzazione evento.**
3. Fare clic sul pulsante **Comandi singola porta** per proteggere la porta.
4. Selezionare **Proteggere porta**.

**Notare:** Per fornire una maniera rapida per proteggere tutte le porte di un edificio, creare un trigger azione per bloccare tutte le porte ed azionarlo manualmente, quando necessario, nella pagina ***Controllo > Triggers azione***. Consultare Configurare i trigger azione a pagina 52.

## Ripristinare tutte le porte

Utilizzare il comando Ripristinare tutte le porte per riportare i lettori collegati alle porte allo stato normale di funzionamento dopo aver sbloccato o bloccato tutte le porte, a meno che non esista uno sblocco **ingresso** attivo. L'ingresso sbloccato è configurato nella pagina ***Amministrazione del sistema > Dispositivi > Controller.***

1. Selezionare ***Controllo > Porte***.
2. Fare clic sul pulsante **Comandi globali porta** situato nella parte superiore della pagina.
3. Selezionare **Ripristinare tutte le porte**.

Sarà generato un evento Lettore ripristinato per ciascun lettore in stato bloccato in precedenza e un evento singolo Tutte le porte ripristinate per il contoller del sistema. Inoltre sarà generato un evento lettore modalità solo tessera o un evento modalità Tessera + PIN  per ciascuna porta, in base alla configurazione del lettore nella pagina ***Amministrazione del sistema > Dispositivi*** .

## Bloccare tutte le porte

Utilizzare il comando Bloccare tutte le porte per bloccare tutte le porte e modificare l'impostazione del lettore per prevenire l'utilizzazione delle credenziali per accedere alle porte. Tutte le azioni che potrebbero avere un impatto sull'elettroserratura non avranno effetto fino all'esecuzione del comando Ripristinare tutte le porte.

1. Selezionare ***Controllo > Porte***.
2. Fare clic sul pulsante **Comandi globali porta** situato nella parte superiore della pagina.
3. Selezionare **Bloccare tutte le porte**.

Sarà generato un evento "Lettore bloccato" per ciascun lettore in stato bloccato in precedenza e un evento singolo "Tutte le porte bloccate" per il contoller del sistema.

**Notare:** Se tutte le porte sono bloccate, se viene aggiunto un nuiovo controller, il nuovo controller della porta resterà sbloccato. Per bloccarlo, tutte le porte devono essere ripristinate, quindi bloccate ancora una volta.

## Sbloccare tutte le porte

Utilizzare il comando Sbloccare tutte le porte per disattivare la sicurezza di tutto il sito, consentendo a chiunque di entrare o uscire senza presentare una credenziale valida. Tutte le azioni che potrebbero avere un impatto sull'elettroserratura non avranno effetto fino all'esecuzione del comando Ripristinare tutte le porte.

1. Selezionare ***Controllo > Porte***.
2. Fare clic sul pulsante **Comandi globali porta** situato nella parte superiore della pagina.
3. Selezionare **Sbloccare tutte le porte**.

Sarà generato un evento "Lettore ripristinato" per ciascun lettore in stato bloccato in precedenza e un evento singolo "Tutte le porte sbloccate" per il contoller del sistema.

## Menù dei comandi della porta

A volte è necessario disattivare la programmazione normale di una determinata porta (ad esempio se la porta deve essere aperta per la consegna di un pacco) o per tutto il sito (ad esempio durante un'esercitazione antincendio). In caso di catastrofe o emergenza nei pressi dell'edificio, potrebbe essere necessario bloccare tutte le porte. Le singole porte possono essere controllate nella scheda **Visualizzazione evento** della pagina ***Controllo > Porte*** . I comandi globali porta consentono all'utente di modificare lo stato di tutte le porte del sito con un solo clic.

### Menù comandi globali porta

**Notare:** Dopo aver sbloccato o bloccato tutte le porte, utilizzare il comando **Ripristinare tutte le porte** prima di cercare di controllare le porte individualmente.

**Sbloccare tutte le porte**
Sblocca tutte le serrature, consentendo libero accesso e uscita. Sarà registrato come evento 14644. Dopo aver eseguito questo comando, ripristinare tutte le porte per poter controllare le singole porte direttamente.

**Bloccare tutte le porte**
Blocca tutte le porte ed ignora le credenziali, impedendo l'ingresso e l'uscita. Sarà registrato come evento 14646. Dopo aver eseguito questo comando, ripristinare tutte le porte per poter controllare le singole porte direttamente.

**Ripristinare tutte le porte**
Ripristina tutte le porte allo stato normale a meno che non esista uno sblocco **ingresso** attivo. L'ingresso sbloccato è configurato nella pagina ***Amministrazione del sistema > Dispositivi > Controller.***

### Menu comandi globali porta

**Aprire porta.**
Sblocca la porta per la durata indicata in **Orario regolare di ingresso autorizzato** nella pagina ***Amministrazione del sistema > Dispositivi*** .

**Sbloccare porta.**
Sblocca la serratura della porta consentendo l'ingresso e l'uscita libera, fino alla modifica dello stato della porta da parte della pianificazione del lettore oppure all'esecuzione del comando globale ("tutte le porte").

**Ripristinare porta.**
Ripristina la porta alle impostazioni predefinite in base alla programmazione.

**Bloccare porta**
Blocca la porte ed ignora le credenziali, impedendo l'ingresso e l'uscita.

**Proteggere porta**
Blocca la porta.

## Scheda visualizzazione evento

La scheda **Visualizzare eventi** della pagina ***Controllo > Porte*** contiene gli eventi recenti della porta ed i lettori associati e lo stato corrente di ciascuna porta e dei lettori associati. Per controllare le singole porte, utilizzare la scheda **Visualizzare eventi** della pagina ***Controllo > Porte*** .

## Scheda visualizzazione programmazione

La scheda **Visualizzazione programmazione** della pagina ***Controllo > Porte*** può essere utilizzata per modificare il comportamento della porta e del lettore in base alla programmazione, invece di tentare la modifica manuale nella scheda **Visualizzare eventi** .

Come nel caso di una sala d'esposizione con una porta d'ingresso dal parcheggio che deve rimanere chiusa a chiave durante la chiusura e aperta durante le ore d'apertura per consentire ai clienti l'accesso all'edificio. In questo caso, selezionare una fascia oraria dalle 9:00 alle 17:00 e la **Modalità programmazione** "Prima tessera ingresso" se la sala esposizioni deve restare aperta dopo l'ingresso con credenziale del venditore.

**Programmazione**
Selezionare una pianificazione dall'elenco (le pianificazioni sono create in ***Gestione accesso > Pianificazioni***) per indicare il periodo di attività della modalità pianificazione.

### Modalità programmazione (porta)

Selezionare un'opzione dell'elenco per impostare il comportamento di una determinata porta durante la fascia oraria selezionata.

**Sbloccata**
La porta è sbloccata ed accessibile senza presentazione delle credenziali durante la pianificazione selezionata.:

**Prima Tessera In**
La porta è bloccata all'inizio della pianificazione resterà in questo stato fino all'utilizzazione della prima credenziale valida. A quel punto, la porta passerà allo stato sbloccato.:

**Bloccata**
La porta sarà bloccata e necessita una credenziale valida per l'ingresso durante la fascia oraria selezionata.

### Modalità programmazione (lettore)

Selezionare un'opzione dell'elenco per impostare il comportamento di un determinato lettore durante la fascia oraria selezionata.

**Solo credenziale**
La persona deve essere dotata di una credenziale valida (tessera ID) per l'accesso.

**Credenziale e PIN**
La persona deve presentare una credenziale valida per l'accesso ed immettere un PIN Personal Identification Number). Evitando in tal modo l'accesso con una credenziale trovata o rubata. Alcuni edifici utilizzano **Solo credenziale** durante il giorno e **Credenziale e PIN** durante le ore di chiusura dell'edificio.

## Modalità fallback porta

Le informazioni relative alle credenziali sono salvare nel controller del sistema. Se il controller della porta non è in grado di comunicare con il -Controller per determinare se consentire l'accesso (ad es. cattiva connessione) le porte del controller delle porte funzioneranno in modalità fallback:

**Limitato**
Non è consentito alcun tipo di accesso.

**Codice sito**
L'accesso è consentito se la tessera presenta uno dei formati definiti nella pagina ***Amministrazione del sistema > Formati tessera*** ed il codice del sito sulla tessera corrisponde al codice del sito indicato nel formato. L'ID della credenziale non è controllato.

**Tutte**
L'accesso è consentito se la tessera presenta uno dei formati definiti nella pagina ***Amministrazione del sistema > Formati di tessera*** indipendentemente dal codice del sito o dall'ID della credenziale.

# Controllo degli ingressi e delle uscite

Gli ingressi e le uscite possono essere controllati nella pagina ***Controllo > ingressi/uscite*** e le uscite possono essere attivate o disattivate manualmente in questa pagina. Le uscite possono essere controllate anche dai trigger azione. Per ulteriori informazioni sugli ingressi e le uscite, consultare Configurare gli ingressi e le uscite a pagina 25

## Attivare o disattivare un'uscita

1. Selezionare ***Controllo > Ingressi/uscite***.
2. Fare clic sul pulsante **Attivare/disattivare** per l'uscita.

   Lo stato dell'uscita cambia.

# Controllo dei trigger delle azioni

Nella pagina ***Amministrazione del sistema > Trigger azione*** i trigger azione possono essere configurati per il controllo di una o più condizioni di trigger con le azioni corrispondenti da intraprendere quando si verificano le condizioni di trigger, come descritto in Configurare i trigger azione a pagina 52.

In base alla configurazione, i record dei trigger azione possono risultare in:

- Azioni di disattivazione che saranno eseguite quando una condizione di trigger diventa vera e
- Azioni di disattivazione che saranno eseguite quando una condizione di trigger diventa falsa.

Una volta creati, i trigger azione possono essere eseguiti manualmente nella pagina ***Controllo > Trigger azione*** per intraprendere l'azione corrispondente.

Si notino i dettagli seguenti sui trigger azione:

- I trigger azioni non associati a un'azione non saranno visualizzati nella pagina ***Controllo > Trigger azione*** .
- I trigger manuali con hanno priorità rispetto ai trigger del sistema e lo stato del trigger non è persistente. Per le azioni eseguite manualmente, qualsiasi modifica dello stato successiva della condizione trigger del sistema causerà una nuova esecuzione dell'azione.
- Per fornire una maniera rapida per proteggere tutte le porte di un edificio, creare un trigger azione per bloccare tutte le porte ed azionarlo manualmente, quando necessario, nella pagina ***Controllo > Triggers azione***.

## Eseguire manualmente un record di trigger azione

1. Selezionare ***Controllo > Trigger azione***.
2. Fare clic sul pulsante **Trigger manuale** per il record triggere azione.
3. Selezionare **Eseguire azioni di attivazione** o **Eseguire azioni di disattivazione**.

## Reimpostazione dell'anti-passback

Anti-Passback necessita una credenziale per accedere o uscire da un'area. In questo modo il sistema traccia le aree occupare dal titolare della credenziale, registra i movimenti del personale nelle aree protette e previene il passaggio ad aree logicamente impossibili. Se un utente utilizza una credenziale per accedere ad un'area configura per Anti-Passback e poi esce dall'area senza utilizzare la credenziale (ad esempio attraverso una porta tenuta aperta da un altro utente), il sistema non registra l'uscita dell'utente dall'area. Di conseguenza, se il sistema è configurato per l'applicazione dell'anti-passback, impedirà l'utilizzazione della credenziale in un'area differente, inclusa quella nella quale si è appena transitato fino alla reimpostazione della posizione della credenziale ad un'area predefinita o neutra.

1. Selezionare ***Controllo > Reimpostazione Anti-Passback***.
2. Per impostare tutte le persone:
   a. Fare clic su [Reimpostare tutto].
   b. Selezionare un'area dall'elenco.
3. Per reimpostare le persone selezionate:
   a. Selezionare un intervallo di persone facendo clic sul primo nome dell'elenco, mantenendo premuto <Maiusc> e facendo clic sull'ultima persona. L'intervallo di nomi è evidenziato.
   b. Selezionare gli individui facendo clic sul primo nome, mantenendo premuto <Ctrl> e facendo clic sugli altri nomi per selezionarli.
   c. Fare clic su [Reimpostare selezioni].
   d. Selezionare un'area dall'elenco.

# CAPITOLO 7 Manutenzione

Sono sufficienti alcune semplici operazioni di manutenzione per garantire il funzionamento efficiente del sistema, senza problemi ed interruzioni Queste includono il backup del database e l'aggiornamento del firmware.

Gli argomenti del capitolo includono:



## Creazione del backup dei dati

Si raccomanda fortemente di effettuare periodicamente il backup del sistema per garantire un recupero rapido delle condizioni di sicurezza in caso di guasto. Il sistema salva il backup nella stazione di lavoro client, per creare una copia supplementare rispetto a quella del controller del sistema. Il file di backup criptato contiene tutti i record, le foto e le impostazioni configurate nel sistema con le seguenti eccezioni:

- Stati della porta/lettore impostati manualmente nella pagina ***Monitoraggio > Porte*** e
- gli eventi.

I backup del database possono essere programmati per l'esecuzione automatica e con l'invio di email indicanti il successo o il fallimento del backup. Gli eventi possono essere salvati in un file CSV.

## Creare un file di backup

Questa sezione descrive la creazione di un file di backup e come scaricarlo sulla stazione di lavoro locale del client. I dati del sistema possono essere salvati sulla stazione di lavoro client (come descritto di seguito) oppure programmati per l'esecuzione automatica come descritto nella sezione seguente. (Per effettuare il backup degli eventi, consultare Effettuare il backup degli eventi a pagina 91.)

1. Collegarsi al sistema come utente con autorizzazione di esecuzione per la funzione backup del database.
2. Selezionare ***Amministrazione del sistema > backup/ripristino***.
3. Fare clic su [Scaricare il file di backup].

   Sarà visualizzata la finestra di dialogo Database backup.
4. Fare clic su [Scaricare il file di backup].
5. Selezionare una posizione per il file di backup.
6. Fare clic su [Salvare].

**IMPORTANTE:** Il nome del file di backup del database contiene un checksum di verifica necessario per il ripristino del sistema (ad esempio, backup_1926651153.bak). Non modificare i caratteri dopo il carattere sottolineato (_) del nome del file.

## Programmazione dei backup automatici

I backup automatici possono essere pianificati per l'esecuzione fino a sette volte alla settimana e con l'invio del file di backup ad una risorsa di rete condivisa. (consultare Configurare una condivisione di rete a pagina 65). Se il sistema è configurato per l'invio automatico di email, sarà inviata una notifica al termine del backup programmato.

**Notare:** I backup programmati devono essere almeno 30 minuti l'uno dall'altro.

1. Collegarsi al sistema come utente con autorizzazione di esecuzione per la funzione backup programmato.
2. Selezionare ***Amministrazione del sistema > backup/ripristino***.
3. Fare clic su [Programmare backup].
4. Per creare una programmazione per il backup del database:
   a. Nella sezione Configurazione della programmazione del database, selezionare **Programmazione attivata**.
   b. Selezionare il giorno del backup della programmazione.
   c. Selezionare l'ora per il backup.
   d. Selezionare la posizione nella quale sarà salvato il file di backup nel campo **Condivisioni di rete** .
   e. (Opzionale) Fare clic su [Effettuare backup subito] per iniziare il backup immediatamente.
5. Per creare una programmazione per un evento backup:
   a. Nella sezione Configurazione della programmazione evento, selezionare **Programmazione attivata**.
   b. Selezionare **Programmazione incrementale** per effettuare il backup di eventi verificatisi dall'ultimo backup.
   c. Selezionare il giorno del backup della programmazione.
   d. Selezionare l'ora per il backup.

e. Selezionare la posizione nella quale sarà salvato il file di backup nel campo **Condivisioni di rete** .
f. (Opzionale) Fare clic su [Effettuare backup subito] per iniziare il backup immediatamente.

6. (Opzionale) Per inviare un messaggio automatico al termine del backup programmato:
   a. Selezionare la casella **Inviare se riuscito**, **Inviare se fallito**, o entrambe.
   b. Selezionare un **Elenco email**.
7. Fare clic su [Accettare le modifiche].

## Effettuare il backup degli eventi

Si notino i dettagli seguenti sugli eventi:

- Gli eventi non possono essere ripristinati dal file di backup. Il file è creato solo a scopo di archiviazione.
- Gli eventi possono essere esportati tramite l'importazione/esportazione guidata fornita nel disco utilità, come descritto nella *Guida utente importazione/esportazione guidata*.

Per effettuare il backup degli eventi:

1. Collegarsi al sistema come utente con autorizzazione di esecuzione per la funzione backup del database.
2. Selezionare ***Amministrazione del sistema > backup/ripristino***.
3. Fare clic su [Programmare backup].
4. Nella sezione Configurazione della programmazione evento, fare clic su [Effettuare backup subito].

   I risultati saranno visualizzati nella finestra di dialogo Esecuzione backup programmato.

## Ripristino dal backup

**IMPORTANTE:** Il ripristino del backup sovrascrive il database e tutte le modifiche apportate a partire dalla data del backup saranno perdute.

1. Collegarsi al sistema come utente con autorizzazione di esecuzione per la funzione ripristino del database.
2. Selezionare ***Amministrazione del sistema > backup/ripristino***.
3. Fare clic su [Sfogliare]
4. Spostarsi sul file di backup.
5. Selezionare il file e fare clic su [Aprire].
6. Fare clic su [Caricare il file di backup].

# Salvare e ripristinare le impostazioni predefinite

Utilizzare la pagina ***Amministrazione del sistema > Salvare/Ripristinare impostazioni*** per creare un punto di ripristino che includa tutti i dati salvati nel file di backup e le impostazioni personalizzate del controller del sistema. Si tratta di uno stato predefinito personalizzato.

Invece di reimpostare il controller del sistema ai predefiniti di fabbrica, che dovranno poi essere riconfigurati a seconda dei requisiti specifici, la configurazione di base del sito può essere salvata come impostazione personalizzata e, in caso si necessità, ripristinata. L'informazione è archiviata nel controller del sistema e può essere ripristinata in un secondo momento utilizzando una frase di sicurezza pre-impostata.

## Salvare i dati e le impostazioni personalizzate

Questa operazione crea un file contenente tutti i dati e le impostazioni di configurazione correnti salvati nel controller del sistema.

1. Selezionare ***Amministrazione del sistema > salvare/reimpostare le impostazioni.***
2. Selezionare **Salvare impostazioni personalizzate**.
3. Immettere un **Nome utente**.
4. Immettere una **Password**
5. Immettere la frase di sicurezza, esattamente come visualizzata (rispetta maiuscole/minuscole).
6. Fare clic su **Salvare impostazioni personalizzate**.

## Ripristinare le impostazioni personalizzate

**IMPORTANTE:** L'utilizzazione di questa funzione rimuove tutte le impostazioni ed i dati e ripristina il sistema alle impostazioni ed i dati salvati nel file delle impostazioni personalizzate. Assicurarsi di creare un backup corrente prima di ripristinare le impostazioni personalizzate.

**IMPORTANTE:** Dopo il ripristino delle impostazioni personalizzate, il controller del sistema sarà riavviato. Durante il riavvio, il sistema non sarà disponibile per alcuni minuti. Per questo motivo si raccomanda di utilizzare questa funzione in periodi di accesso limitato, in caso contrario i titolari di credenziali dovranno attendere per l'ingresso se la **Modalità fallback della porta** non è stata configurata per consentire l'accesso in caso di non funzionamento del controller del sistema.

1. Selezionare ***Amministrazione del sistema > salvare/reimpostare le impostazioni.***
2. Selezionare **Ripristinare le impostazioni personalizzate**.
3. Immettere un **Nome utente**.
4. Immettere una **Password**
5. Immettere la frase di sicurezza, esattamente come visualizzata (rispetta maiuscole/minuscole).
6. Fare clic su **Ripristinare le impostazioni personalizzate**.

   Sarà visualizzato un avviso: “Riavvio del dispositivo in corso” e una barra di avanzamento.

   Al completamento della barra di avanzamento, il server non sarà in linea ed il browser visualizzerà la pagina predefinita poiché non può collegarsi all'indirizzo web.
7. Svuotare la cache del browser. (In Internet Explorer 8+, premere <Ctrl>+<Shift>+<Delete>.)

## Reimpostare le impostazioni di fabbrica

**IMPORTANTE:** Questa funzione cancellerà tutte le impostazioni ed i dati (tranne le impostazioni della configurazione di rete) e ripristina il controller del sistema ai valori predefiniti di fabbrica. Assicurarsi di creare un backup corrente prima di ripristinare le impostazioni di fabbrica.

1. Selezionare ***Amministrazione del sistema > salvare/reimpostare le impostazioni.***
2. Selezionare **Reimpostare le impostazioni di fabbrica**.
3. Immettere un **Nome utente**.
4. Immettere una **Password**.
5. Immettere la frase di sicurezza, esattamente come visualizzata (rispetta maiuscole/minuscole).
6. Fare clic su **Reimpostare le impostazioni di fabbrica**.

   Sarà visualizzato un avviso: “Riavvio del dispositivo in corso” e una barra di avanzamento.

   Al completamento della barra di avanzamento, il server non sarà in linea ed il browser visualizzerà la pagina predefinita poiché non può collegarsi all'indirizzo web.
7. Svuotare la cache del browser. (In Internet Explorer 8 o successivo, premere <Ctrl>+<Shift>+<Delete>.)

   Quando il server ritorna in linea, sarà visualizzato il formulario di accettazione della licenza software utente finale (EULA).
8. Fare clic su **Accetto**.

# Aggiornamento del firmware

I miglioramenti delle funzioni sono periodicamente disponibili nel sito web del prodotto sotto forma di aggiornamenti del firmware da scaricare e sono applicati al controller del sistema ed a tutte le IPSDC installate.

**Notare:** L'*aggiornamento* del controller del sistema è differente dall'*upgrade* del sistema che ha un impatto oltre che sul firmware, anche sul codice core del controller del sistema. Per passare da una versione di TruPortal ad una versione successiva (ad esempio dalla versione 1.0 alla versione 1.5) o per l'upgrade da goEntry a TruPortal, consultare Utilizzazione dell' installazione guidata a pagina 11.

## Prima di iniziare

Prima di effettuare l'aggiornamento del firmware, si notino i seguenti dettagli:

**IMPORTANTE:** Prima di aggiornare il firmware, collegare una batteria di backup carica al controller del sistema. Il controller del sistema potrebbe diventare inutilizzabile e necessitare la sostituzione in caso si perdita di corrente durante l'aggiornamento del firmware. Per informazioni sulla batteria, consultare *Guida rapida al controller del sistema*.

**IMPORTANTE:** Non reimpostare o riavviare IPSDC durante l'aggiornamento del firmware perché IPSDC potrebbe diventare non operativo.

- Effettuare il backup del database prima di aggiornare il firmware del controller del sistema. Consultare Creazione del backup dei dati a pagina 89.
- Durante l'aggiornamento del firmware gli eventi memorizzati nel controller del sistema saranno rimossi. Per conservare gli eventi esistenti, effettuare il backup degli eventi (consultare Effettuare il backup degli eventi a pagina 91) oppure esportarli (consultare la *Guida importazione/ esportazione guidata*).
- Una volta iniziato, l'aggiornamento del firmware non può essere annullato.
- Il firmware non può essere ripristinato dopo l'aggiornamento.
- Durante l'aggiornamento del firmware del controller del sistema, per due brevi periodi le credenziali non potranno essere utilizzate per accedere alle porte. Al termine dell'aggiornamento e dopo il riavvio del controller del sistema, si potranno riprendere le normali operazioni.

## Ricerca degli aggiornamenti del firmware

1. Scaricare il file di aggiornamento del firmware dal sito web del prodotto.
   - I file di aggiornamento del firmware del controller hanno l'estensione LFF.
   - I file di aggiornamento del firmware IPSDC utilizzano il seguente nome di file: IPSDCU.bin.
2. Collegarsi al sistema come utente con autorizzazione di esecuzione per la funzione aggiornamento del firmware.
3. Paragonare gli aggiornamenti del firmware disponibili sul sito web con i numeri di revisione del firmware del controller del sistema e degli IPSDC elencati nella pagina ***Amministrazione del sistema > impostazioni del sistema***.
4. Scaricare gli aggiornamenti più recenti rispetto al firmware sul controller del sistema e gli IPSDC.

5. Selezionare ***Amministrazione del sistema > Aggiornamento firmware***.
6. Selezionare **Aggiornare TruPortal Firmware** oppure **Aggiornare firmware ID Controller porta**.
7. Nel campo **Nuovo file firmware** navigare e selezionare il file di aggiornamento del firmware.
8. Fare clic su [Successivo].
9. Fare clic su [Aggiornare].

Dopo l'aggiornamento del firmware del controller del sistema, il controller del sistema sarà riavviato. Ricollegarsi e passare alla pagina ***Monitoraggio > Diagnostica*** (consultare Diagnostica a pagina 98) per assicurarsi che non ci siano problemi con le porte, i controller ed altro hardware appena installato.

## Gestione dei pacchetti lingue

Nell'ambito dell'approccio alle lingue, il sistema fornisce la flessibilità seguente:

- La lingua principale del sistema determina la lingua utilizzata per le funzioni effettuate dal sistema, quali l'assegnazione di nomi predefiniti per il dispositivo, i backup pianificati e email automatici.
- Gli utenti possono selezionare una lingua differente a livello utente durante il collegamento al sistema.

Il sistema fornisce cinque lingue: inglese, spagnolo, francese, olandese e portoghese e gli utenti possono selezionare una lingua differente per l'interfaccia utente durante il collegamento. (Consultare Collegamento al sistema a pagina 15.)

Altre lingue sono offerte come *pacchetti lingue* disponibili nel sito web del prodotto. I pacchetti lingue possono essere scaricati ed aggiunti al sistema. I pacchetti di lingue possono anche essere rimossi.

Si notino i dettagli seguenti sui pacchetti lingue:

- Possono essere attive solo cinque lingue contemporaneamente.
- Prima di aggiungere una nuova lingua ad una nuova installazione, deve essere eliminata una lingua esistente.

**Notare:** L'inglese e la lingua del sistema non possono essere eliminati.

- Dopo l'aggiunta di una lingua, quest'ultima sarà disponibile al collegamento successivo da parte dell'utente.
- In caso di rimozione della lingua attiva (ad esempio lo spagnolo), l'utente deve scollegarsi dal sistema e ricollegarsi per selezionare la nuova lingua.
- I pacchetti di lingue sono creati per versioni specifiche del firmware del controller del sistema. I primi due numeri del numero di versione del pacchetto lingue (ad esempio *3.5x*.xxxx) devono corrispondere ai primi due numeri della versione del firmware corrente, indicato nella pagina ***Amministrazione del sistema > pacchetti lingue***.
- All'aggiornamento del firmware del controller del sistema, l'inglese ed i pacchetti lingue predefiniti (spagnolo, francese, olandese e portoghese) installati saranno aggiornati. Per aggiornare gli altri pacchetti lingue, scaricare ed installare il pacchetto lingua appropriato dal sito web del prodotto.
- Gli aggiornamenti del pacchetto servizio non influiscono sui pacchetti lingue.

## Aggiungere un pacchetto lingue

1. Avviare un browser Internet supportato.
2. Scaricare il pacchetto lingua desiderato dal siti web del prodotto in una stazione di lavoro client locale o su un file system condiviso.
3. Collegarsi al sistema come utente con autorizzazione di modifica.
4. Selezionare ***Amministrazione del sistema > pacchetti lingue***.
5. Fare clic su [Aggiungere].

**Notare:** Il pulsante [Aggiungere] è attivo solo se sono installati meno di cinque pacchetti lingue. Se necessario, eliminare un pacchetto lingua (tranne l'inglese ed il pacchetto lingua utilizzato dal sistema) prima di aggiungere un nuovo pacchetto lingue. Vedere **Eliminare un pacchetto lingue a pagina 96.**

6. Nella finestra di dialogo Apri, spostarsi nella cartella nella quale è stato scaricato il pacchetto lingua (il file ha l'estensione NLS), selezionare il file, quindi fare clic su [Apri}.
7. Nella finestra Pacchetto lingua aggiuntivo fare clic su [Installare].
8. Al termine dell'installazione, fare clic su [Fine].
9. Per iniziare ad utilizzare una nuova lingua:
   a. Terminare il collegamento al sistema facendo clic sull'icona **Logout** in alto a destra dell'interfaccia utente.
   b. Seguire i passaggi in Collegamento al sistema a pagina 15 e selezionare la nuova lingua nel campo **Lingua**.

## Eliminare un pacchetto lingue

**Notare:** L'inglese e il pacchetto lingue utilizzato a livello del sistema non possono essere eliminati.

1. Selezionare ***Amministrazione del sistema > pacchetti lingue***.
2. Fare clic sul pacchetto lingue per selezionarlo.
3. Fare clic su [Eliminare].

   Sarà visualizzata la finestra di dialogo Eliminare elemento.
4. Fare clic su [Eliminare].

# CAPITOLO 8 *Risoluzione dei problemi*

Gli argomenti del capitolo includono:



## Risoluzione dei problemi relativi al browser

Svuotare la cache e riavviare il browser può risolvere diversi problemi, ad esempio il cattivo funzionamento dell'interfaccia utente. Interventi specifici dipendono dal tipo e dalla versione del browser.

1. Scollegarsi dal sistema, ricollegarsi e ritornare alla ***pagina iniziale***.
2. Svuotare la cronologia e la cache del browser.
3. Chiudere il browser e riaprirlo.
4. Collegarsi al sistema.

**Notare:** Dopo aver attivato o disattivato HTTPS/SSL assicurarsi di svuotare la cache del browser, soprattutto se si utilizza Firefox o Chrome.

Di seguito sono elencati altri suggerimenti per risolvere i problemi del browser:

- Se il controller del sistema è reimpostato o il database ripristinato, Internet Explorer potrebbe visualizzare temporaneamente una pagina XML invece della pagina di login. In questo caso, aggiornare la pagina del browser fino all'apparizione della pagina di login.
- Il sistema supporta l'utilizzazione del pulsanti [Precedente] e [Successivo] del browser, ma di tanto in tanto potrebbe essere visualizzata una pagina vuota durante la navigazione. In questo caso, aggiornare la pagina del browser.

- Per altri browser i pulsanti [Precedente] e [Successivo] potrebbero non funzionare per la navigazione da una scheda all'altra della pagina (ad esempio, quando si vuole passare tra le schede Dettagli e Account utente della pagina ***Gestione dell'accesso > Persone*** ). In questo caso servirsi del mouse per fare clic sulla scheda.
- Ingrandire la finestra del browser per visualizzare le descrizioni dei comandi. Se la finestra è troppo piccola, le descrizioni dei comandi potrebbero non essere visualizzate.
- Se la sicurezza HTTPS è attivata o disattivata nella pagina ***Impostazioni del sistema > Configurazione di rete,*** la pagina di login dovrebbe essere visualizzata automaticamente. Se la pagina di login non è visualizzata, svuotare manualmente la cache del browser e riavviare il browser per accedere alla pagina di login.
- Le impostazioni proxy del browser potrebbero influire sul collegamento al controller del sistema (che utilizza le porte 80 e 443) quando HTTPS è disattivato. Per risolvere questo problema, configurare i server proxy per consentire il traffico HTTP attraverso la porta 443 in maniera esplicita (1) specificando la porta 443 nella URL del pannello (ad esempio, http://192.168.1.10:443), (2) aggiungendo un'eccezione alle impostazioni proxy sul client, oppure (3) configurando una porta peril servizio non bloccata dal firewall. Consultare Configurare le impostazioni di rete a pagina 17.

## Riavviare il controller del sistema

1. Selezionare ***Amministrazione del sistema > Dispositivi***.
2. Selezionare il controller del sistema dalla struttura gerarchica del dispositivo.
3. Fare clic su [Riavviare controller].

Quando il controller del sistema funziona solo a batteria ed il voltaggio scende al di sotto di 10.2 V la scheda si spegne fino al ripristino dell'alimentazione AC/DC.

## Diagnostica

Gli errori rilevati dal sistema sono visualizzati nella pagina ***Monitoraggio > Diagnostica***, insieme alle statistiche del sistema, quale il numero di ingressi. Tutte le informazioni sono ricercate al momento del login ed ogni minuto. Per aggiornare manualmente i dati, fare clic su [Aggiornare].

Per accedere alla pagina ***Diagnostica***:

- Selezionare ***Monitoraggio> Diagnostica***, oppure
- Fare clic sull'indicatore di stato nella parte superiore dell'interfaccia utente in caso di errori o avvisi.

Si notino i dettagli seguenti sulla pagina ***Diagnostica***:

- L'ombreggiatura rossa indica il funzionamento incorretto, ad esempio un dispositivo non collegato. L'ombreggiatura gialla inca un avviso, ad esempio una condizione di manomissione.
- La presenza di punti di sospensione (...) indica la disponibilità di informazioni supplementari in una descrizione di comando, visualizzata al passaggio sui punti di sospensione.
- Il sistema non include azioni per l'esecuzione di test di diagnostica specifici.
- Fare clic su [Scaricare file di diagnostica] per creare un file cifrato contenente una serie di informazioni sul sistema, quali i dati relativi alla configurazione ed i log. Il file non conterrà

nessuna informazione specifica riguardante il personale (ad esempio i nomi o i codici fiscali); Per ulteriori informazioni, consultare le Note di rilascio. Il file può essere salvato localmente ed inviato all'assistenza tecnica per la risoluzione dei problemi.

- La rilevazione precisa dell'alimentazione DC non può essere visualizzata se il controller del sistema è alimentato da una sorgente DC. Le informazioni sull'alimentazione DC possono essere visualizzate solo il controller del sistema è alimentato da una sorgente AC.

| Diagnostica | Valore visualizzato | Stato |
|---|---|---|
| Alimentazione AC | OK \| Brownout \| Fallimento | INF = OK<br>AVV = Brownout<br>ERR = Fallimento |
| Alimentazione DC | Voltaggio, corrente | INF >= 10.0<br>AVV < 10.0 V<br>AVV = Sovraccarico corrente |
| Batteria di backup | Voltaggio, corrente, caricamento \| scarico | INF >= 11.7<br>AVV < 11.7 V<br>ERR < 11.4 V, nessuna batteria |
| Batteria memoria | Voltaggio | INF >= 2.3 V<br>AVV < 2.3 V<br>ERR < 2.0 V |
| Fusibili | OK \| *Nome fusibile,…* | INF = tutto OK<br>ERR = Se non OK |
| Controller | OK \| *Problemi*,… | INF = OK<br>AVV = Se non OK |
| Moduli | OK \| *ModuleName problema*,… | INF = tutto OK<br>WRN = Se manomesso<br>ERR = Se non in linea |
| Porte | OK \| *DoorName problema*,… | INF = tutto OK<br>AVV = Se trattenuta, apertura prolungata, manomissione<br>ERR - Se non in linea |
| Ingressi digitali | OK \| *InputName problema*,… | INF = tutto OK<br>WRN = Se manomesso<br>ERR - Se non in linea |
| Operatività | Ultimo riavvio, giorni operatività | INF = sempre |
| Media carico CPU | 1m, 5m, 15m | INF 15m < 0.80<br>WRN 15m >= 0.80<br>ERR 15m >= 0.95 |

| Diagnostica | Valore visualizzato | Stato |
|---|---|---|
| Utilizzazione memoria | Utilizzato, totale | INF < 95%<br>WRN >= 95%<br>ERR = 100% |
| Memoria principale | Percentuale | INF < 90%<br>WRN >= 90%<br>ERR = 100% |
| Foto e memorizzazione backup | Utilizzato, totale | INF < 50%<br>WRN >= 50%<br>ERR = 95% |
| Schede ADP | Utilizzato, totale | INF = sempre |
| Porte | Utilizzato, totale | INF = sempre |
| Lettori | Utilizzato, totale | INF = sempre |
| Schede EIO | Utilizzato, totale | INF = sempre |
| Ingressi | Utilizzato, totale | INF = sempre |
| Uscite | Utilizzato, totale | INF = sempre |
| DVR | Utilizzato, totale | INF = sempre |
| Telecamere | Utilizzato, totale | INF = sempre |
| Persona | Utilizzato, totale | INF = sempre |
| Credenziali | Utilizzato, totale | INF = sempre |
| Livelli di Accesso | Utilizzato, totale | INF – sempre |
| Pianificazioni | Utilizzato, totale | INF – sempre |
| Gruppo vocanze | Utilizzato, totale | INF – sempre |
| Vacanze | Utilizzato, totale | INF = sempre |
| Aree | Utilizzato, totale | INF = sempre |
| Gruppi Lettori | Utilizzato, totale | INF = sempre |
| Ruoli operatore | Utilizzato, totale | INF = sempre |
| Video Layout | Utilizzato, totale | INF = sempre |
| Formati tessera | Utilizzato, totale | INF = sempre |

## Fusibili

I fusibili proteggono l'alimentazione DC fornita dalla scheda del controller del sistema alle periferiche esterne.

| Fusibile | +V | 0V |
|---|---|---|
| Aus 1 | CN3.1 | CN3.2 |
| Aus 2 | CN3.3 | CN3.4 |
| Controller porta | CN10.2<br>CN17.2 | CN11.4<br>CN18.4 |
| Ingresso ausiliario | CN21.1 | CN21.3<br>CN22.2 |

## Stato problemi hardware

Gli elementi hardware possono presentare i seguenti problemi:

### Controller

- Manomissione

### Moduli

- Non in linea
- Manomissione

### Porte

- Non in linea
- Forzata
- Apertura prolungata
- Tamper RTE
- Tamper contatto porta
- Tamper aus porta
- Manomissione porta

### Ingresso digitale

- Non in linea
- Manomissione

## Risoluzione dei problemi lettori

Se il lettore non risponde come previsto, utilizzare il pulsante [Scansione per le modifiche hardware] (consultare Scansione per le modifiche hardware a pagina 23), verificare che il lettore sia presente nella struttura gerarchica nella pagina ***Amministrazione del sistema > Dispositivi*** e verificarne la configurazione. Consultare Configurare i lettori a pagina 33.

In caso di eventi inattesi per le porte o i lettori collegati ad un IPSDC, verificare le impostazioni degli interruttori e dei commutatori IPSDC, per assicurarsi che l'hardware sia configurato correttamente. Ad esempio, la porta d'ingresso del dispositivo (DI) del lettore, J2, comporta due ingressi digitali utilizzati per i dispositivi di stato della porta (contatti porta e ingresso richiesta di uscita) e possono essere configurati come ingressi digitali controllati o senza supervisione. Gli ingressi configurati come controllati nell'interfaccia utente TruPortal necessitano resistenze EOL. Per informazioni supplementari, consultare la *Guida rapida IPSDC*.

### Risoluzione dei problemi Programmazioni

Se una programmazione non funziona come previsto, controllare le sezioni seguenti:

- Creazione di gruppi di vacanze a pagina 39
- Creazione delle programmazioni a pagina 41
- Considerazioni sui record trigger azioni basati su programmazione a pagina 57

## Messaggi d'errore, avviso e evento

### Stati di manomissione

Al momento della registrazione di un evento manomissione, il controller del sistema non è in grado di distinguere quale dei quattro ingressi della porta è in stato manomissione. Lo stato degli ingressi in tamper in tempo reale può essere visualizzato nella pagina ***Monitoraggio > Diagnostica***.

### Eventi alimentazione e batteria

#### Spegnimento del controller del sistema alimentato da batteria

Se il controller del sistema è alimentato solo da batteria ed il voltaggio della batteria scende al di sotto dei 10,5 volt, il controller del sistema si spegnerà fino al ripristino dell'alimentazione AC.

### Eventi batteria di backup

Gli eventi batteria di backup si verificano quando il voltaggio della batteria di backup scende al di sotto di una determinata soglia.

| Codice evento | Descrizione evento | Causa |
|---|---|---|
| Evento 14612 | Batteria di backup critica | Voltaggio inferiore a 11.4V, o superiore a 10.2V |
| Evento 14613 | Batteria di backup disconnessa | Voltaggio inferiore a 10.2V, o superiore a 9.0V |
| Evento 14624 | Batteria di backup bassa | Voltaggio inferiore a 11.7V o superiore a 11.4V |
| Evento 14625 | Batteria di backup ripristinata | Voltaggio superiore a 11.7V |
| Evento 14649 | Batteria di backup non rilevata | Voltaggio inferiore a 9.0V |

**Notare:** Se il controller del sistema è alimentato esclusivamente con la batteria di backup, sarà spento a 10.2 V e gli eventi Disconnessione e Non rilevato non saranno generati.

### Eventi memoria della batteria

| Codice evento | Descrizione evento |
|---|---|
| Evento 14618 | Batteria di backup memoria scarica |

### Eventi fusibile

| Codice evento | Descrizione evento |
|---|---|
| Evento 14651 | Fusibile scattato |
| Evento 14652 | Fusibile ripristinato |

## Dispositivo eventi

| Codice evento | Descrizione evento | Dispositivo |
|---|---|---|
| Evento 4105 | Comunicazioni con il dispositivo fallite | Controller porta, espansione I/O |
| Evento 4106 | Comunicazioni con il dispositivo ripristinate | Controller porta, espansione I/O |
| Evento 4107 | Allarme manomissione* | Controller, controller porta, espansione I/O |
| Evento 14622 | Problema del sistema | Controller |
| Evento 14623 | Sistema ripristinato | Controller |
| Evento 14628 | Dispositivo fallito | Controller |
| Evento 14629 | Dispositivo ripristinato | Controller |
| Evento 14643 | Tamper ripristinato* | Controller, controller porta, espansione I/O |

* Non applicabile al controller della porta incorporato

**Comunicazioni con il dispositivo fallite/ripristinate**
Utilizzato per indicare errori di comunicazione con i dispositivi downstream. Si verifica quando la comunicazione tra il bus RS-485 SNAPP ed un dispositivo configurato downstream è perduta o stabilita. Il dispositivo mostrerà sempre il modulo interessato.

**Dispositivo fallite/ripristinate**
Utilizzato per indicare errori di generici con i dispositivi downstream. Si verifica quando l'ingresso tamper di qualsiasi dispositivo cambia stato (incluso il tamper esterno/perimetro, ma non la porta tamper) o quando è rilevato un errore di comunicazione VBUS. Dispositivo indicherà sempre il controller. Per gli eventi tamper, esisterà un evento tamper corrispondente per il dispositivo. Per gli eventi errore VBUS, non è possibile indicare quale dispositivo presenta l'errore VBUS, perciò non esiste un evento corrispondente per indicare il dispositivo con l'errore VBUS.

**Problemi/ripristino del sistema**
Utilizzato per indicare errori di generici del sistema. Si verifica quando **Tamper esterno/ perimetro** cambia stato. **Dispositivo** indicherà sempre il controller del sistema. L'evento potrà essere utilizzato in futuro per indicare altre condizioni d'errore.

## Eventi tamper porta

| Codice evento | Descrizione evento |
|---|---|
| Evento 14633 | Tamper porta ripristinata |
| Evento 14632 | Allarme tamper porta |

**Tamper porta Allarme/ripristinata**
Utilizzato per indicare una condizione di tamper di una delle quattro porte d'uscita - DR, RTE, TR, AUX. L'evento allarme tamper è generato in caso di rilevazione di una condizione tamper su una delle uscite o quando TR è attivo. Non saranno creati altri eventi allarme tamper per RTE, TR e AUX fino alla risoluzione di tutte le condizioni tamper, tuttavia altri eventi allarme tamper saranno creati per DR anche se esistono altre condizioni tamper. L'evento tamper ripristinato è creato solo alla risoluzione della condizione tamper sui quattro ingressi e TR è attivo.

## Eventi ingresso ausiliario

| Codice evento | Descrizione evento |
|---|---|
| Evento 14640 | Ingresso attivo |
| Evento 14641 | Allarme tamper ingresso |
| Evento 14642 | Ingresso inattivo |
| Evento 4170 | Ingresso disattivato |

## Eventi uscita ausiliaria

| Codice evento | Descrizione evento |
|---|---|
| Evento 10240 | Uscita attiva |
| Evento 11264 | Uscita disattivata |

## Avviso “Oggetti modificati”

Talvolta la cache del browser locale può perdere la sincronizzazione con il sistema. In questo caso, l'interfaccia utente è disattivata e sarà visualizzato un messaggio d'avviso. Fare clic sul testo dell'avviso per ricaricare la pagina.

## Evento "Sincronizzazione NTP fallita"

La sincronizzazione del sistema con un server  NTP, come discusso in Impostare la data e l'ora a pagina 15, è possibile solo se il sistema è in grado di accedere al server NTP tramite UDP porta 123.

Se la porta non è aperta (ad esempio è bloccata da un firewall) sarà registrato un evento "Sinc. NTP fallita" Per risolvere il problema, rivolgersi all'amministratore di rete del sito.

# Errori del lettore video

Se si verificano problemi di visualizzazione del video, oltre alle informazioni seguenti, consultare Prima di iniziare a pagina 78.

## Nessun collegamento video attivo

Questo messaggi appare nella pagina ***Monitoriaggio > Video*** e nella scheda Dettagli dell'evento della pagina ***Eventi.***

Il messaggio significa che:

- La telecamera non è configurata,
- Il sistema ha perduto il collegamento con il DVR/NVR oppure
- Il lettore video non è installato o non è aggiornato. Consultare Prima di iniziare a pagina 78.

**Notare:** Il video può essere visualizzato solo con Internet Explorer. Per ulteriori informazioni, consultare le *Note di rilascio.*

### Se il messaggio d'errore è visualizzato quando si fa clic sull'icona telecamera accanto all'evento:

1. Fare clic su [Riprodurre video dell'evento].
2. Il video è visualizzato oppure il lettore video non è installato. Consultare Prima di iniziare a pagina 78.
3. Se non si verifica nessuna delle condizioni, verificare il funzionamento del DVR/NVR o della telecamera:
   a. Vedere **Configurazione dei dispositivi video a pagina 34.**
   b. Vedere **Collegare le telecamere ai dispositivi per tracciare i video degli eventi. a pagina 36.**.

### Se il messaggio d'errore è visualizzato alla selezione di *Monitoraggio > Video*:

1. Fare doppio clic nel riquadro nel quale è visualizzato il messaggio d'errore.
2. Se non è visualizzato il video:
   a. Selezionare ***Monitoraggio > Layout video***.
   b. Selezionare il layout video da visualizzare.
   c. Assicurarsi di selezionare la telecamera corretta in ciascun elenco a discesa in ciascun riquadro del layout video.
3. Se la telecamera non si trova nell'elenco, verificare che la telecamera si trovi nella pagina ***Amministrazione del sistema > Dispositivi*** e che funzioni correttamente:
   a. Vedere **Configurazione dei dispositivi video a pagina 34.**
   b. Vedere **Aggiungere una telecamera. a pagina 35.**
   c. Vedere **Aggiungere layout video a pagina 36.**

# CAPITOLO 9 *Consultazione*

Gli argomenti del capitolo includono:

## Capacità del sistema

| Attributo | Capacità |
|---|---|
| Numero di persone | 10.000 |
| Numero di credenziali uniche | 10.000 |
| Credenziali per persona | 5 |
| Livelli di accesso | 64 |
| Livelli di accesso per credenziale | 8 |
| Pianificazioni | 64 |
| Intervalli orari per programmazione | 6 |
| Gruppi ferie per programmazione | 8 |
| Gruppi ferie | 8 |
| Vacanze per gruppo di vacanze | 32 |
| Vacanze (totale) | 255 |
| Aree | 64 |
| Gruppi Lettori | 64 |
| Ruoli operatore | 32 |
| Campi definiti dall'utente | 10 |
| Layout video | 64 |
| Formati tessera | 8 |
| Elenchi email | 10 |
| Trigger azione | 32 |
| Numero degli eventi conservati nel log eventi | 65.000 |
| **Capacità del dispositivo** | |
| Numero di porte (scheda madre e controller a doppia porta) con lettori ingresso / Numero di porte con lettori ingresso e uscita | 64 / 32 |
| Numero totale di moduli interfaccia a due porte (incluso built in) | 32 |
| Numero totale di controller porta singola basati su IP (IPSDC) | 62 |
| Lettori (totale) | 64 |
| Ingressi/Uscite | |
| Numero totale di ingressi del sistema (incluso il controller del sistema) | 132 |
| Numero totale delle uscite del sistema (incluso il controller del sistema) | 66 |
| Numero totale di espansioni add-ons ingresso/uscita o di espansioni scheda add-ons ingresso/uscita | 8 |

| Attributo | Capacità |
|---|---|
| DVR/NVR | 4 |
| Telecamere | 64 |
| Porte Ethernet | 2 |
| Porte bus RS-485 SNAPP | 4 |

## Configurazione dei controller porta singola basati su IP

Prima di configurare i controller porta singola basati su IP (IPSDC) nell'interfaccia utente, ciascun IPSDC deve essere configurato per rilevare l'indirizzo IP del controller del sistema. L'impostazione di un collegamento di rete consente la rilevazione IPSDC tramite il pulsante [Scansione modifiche hardware] nella pagina ***Amministrazione del sistema > Dispositivi.***

Di seguito è presentata una panoramica generale dei passaggi necessari alla configurazione di un IPSDC:

1. Installare l'IPSDC. Per ulteriori informazioni consultare la *Guida rapida ai controller porta singola basati su IP TruPortal*.
2. Seguire i passaggi in Preparazione delle stazioni di lavoro client per l'utilizzazione dello Strumento di configurazione integrato (ITC) a pagina 110. Prima di poter configurare un IPSDC, l'indirizzo IP della stazione di lavoro client locale deve essere modificata in modo tale da essere sulla stessa sottorete dell'IPSDC.
3. Per ulteriori informazioni su ICT, consultare Prima di iniziare a pagina 111 .
4. Seguire i passaggi in Utilizzazione dell' ICT per configurare gli IPSDC a pagina 112.
5. Collegarsi all'interfaccia utente TruPortal ed accedere alla pagina ***Amministrazione del sistema > Dispositivi*** .
6. Utilizzare il pulsante [Scansione modifiche hardware] per consentire al controller del sistema di rilevare l'IPSDC ed aggiungerlo alla struttura del dispositivo. Consultare Scansione per le modifiche hardware a pagina 23.
7. Configurare l'IPSDC nell'interfaccia utente TruPortal . Consultare Configurare un controller della porta a pagina 25.

Di seguito sono indicati alcune informazioni supplementari su IPSDC:

- I miglioramenti funzionali degli IPSDC sono periodicamente disponibili nel sito web del prodotto sotto forma di aggiornamenti del firmware. Consultare Aggiornamento del firmware a pagina 94.
- Gli IPSDC possono essere configurati per l'utilizzazione della modalità fallback in caso di perdita del collegamento al controller del sistema. La cache locale che memorizza le ultime 50 credenziali riuscite può consentire l'accesso. Consultare Configurazione della sicurezza a pagina 18.
- Gli IPSDC non supportano le azioni Segnale acustico attivato e Segnale acustico disattivato configurate peri trigger azione, i punti d'ingresso tamper o i tipi d'ingresso ausiliari. Consultare *Guida rapida controller porta singola basato su IP TruPortal* per ulteriori informazioni sulla modifica delle impostazioni dell'interruttore per i tipi di ingresso.
- Per sostituire un IPSDC, consultare Sostituire un controller della porta a pagina 25.

## Preparazione delle stazioni di lavoro client per l'utilizzazione dello Strumento di configurazione integrato (ITC)

Lo *Strumento di configurazione integrato (ICT)* è un programma basato su browser incorporato in ciascun IPSDC che può essere utilizzato per configurare un IPSDC per la rilevazione del controller del sistema.

L'indirizzo IP predefinito di un IPSDC è 192.168.6.6. Prima di utilizzare l'ICT per la configurazione dell'IPSDC, la stazione di lavoro client locale deve essere modificata in modo tale da essere sulla stessa sottorete dell'IPSDC. I passaggi necessari variano a seconda del sistema operativo utilizzato, come descritto di seguito.

Per preparare una stazione di lavoro client Windows XP:

1. Fare clic su **Avvio**, **Pannello di controllo**, quindi **Collegamenti di rete**.
2. Fare clic con il tasto destro del mouse su **Collegamento locale**. Se la prima opzione dell'elenco a discesa è:
   - **Disattivare**, significa che il collegamento è attivato. Spostarsi su gradino 3.
   - **Attivare**, selezionarlo per attivare il collegamento. Ritornare a gradino 1.
3. Selezionare **Proprietà** dall'elenco a discesa
4. Nella sezione **Questo collegamento utilizza:**, selezionare **Protocollo Internet TCP/IP**.
5. Selezionare **Proprietà**.
6. Se il computer è impostato per:
   - **DHCP**, **Ottenere automaticamente indirizzo IP** è già selezionato. Selezionare **Utilizzare il seguente indirizzo IP**.
   - **Statico**, quindi annotare l'indirizzo IP ed il numero di sottorete. Al termine della configurazione del controller, reimpostare il computer a questi valori.
7. Immettere l'indirizzo IP `192.168.6.1` o un indirizzo IP simile valido (ad esempio `192.168.6.`*x* laddove *x* è un numero tra 1 e 254 tranne 6).
8. Modificare la sottorete con `255.255.255.0`.

   Il gateway predefinito non deve essere modificato.
9. Fare clic su **OK** fino alla chiusura di tutte le finestre aperte.
10. Prima di avviare l'ITC, se la stazione di lavoro client dispone di un firewall, disattivarlo.
11. Passare a Utilizzazione dell' ICT per configurare gli IPSDC a pagina 112.

Per preparare una stazione di lavoro client Windows 7:

1. Fare clic sul pulsante **Avvio**, selezionare **Panello di controllo**, **Rete e Internet**, quindi **Centro connessioni di rete e condivisioni**.
2. Nella sezione **Visualizzare reti attive** del modulo, fare clic sul collegamento **Collegamento locale** .
3. Nella finestra di dialogo **Collegamento locale**, fare clic su **Proprietà**.
4. Nella finestra di dialogo Proprietà collegamento locale, selezionare **Protocollo Internet versione 4 (TCP/IPv4)** o **Protocollo Internet versione 6 (TCP/IPv6)**.
5. Fare clic su **Proprietà**.
   - Se **Ottenere un'indirizzo automaticamente IPvx** è già selezionato, selezionare **Utilizzare il seguente Indirizzo IPv*x***, laddove *x* è la versione del protocollo Internet utilizzata (4 o 6).

- Se si tratta di un collegamento statico, annotare l'indirizzo IP ed il numero della maschera di sottorete. Al termine della configurazione del controller, reimpostare il computer a questi valori.

6. Immettere l'indirizzo IP `192.168.6.1` o un indirizzo IP simile valido (ad esempio`192.168.6.x` laddove *x* è un numero tra 1 e 254 tranne 6).
7. Cambiare il valore della lunghezza del prefisso di sottorete a `255.255.255.0`.

   Il gateway predefinito non deve essere modificato.
8. Fare clic su **OK** e **Chiudere** fino alla chiusura di tutte le finestre aperte.
9. Prima di avviare l'ITC, se la stazione di lavoro client dispone di un firewall, disattivarlo.
10. Passare a Utilizzazione dell' ICT per configurare gli IPSDC a pagina 112.

Per preparare una stazione di lavoro client Windows 8:

1. Fare clic sull'icona **Rete** per aprire il Centro connessioni di rete e condivisioni.
2. Fare clic su **Modificare impostazioni dell'adattatore**.
3. Nella finestra collegamenti di rete, fare clic con il pulsante destro del mouse sull'icona **Collegamento locale** e selezionare **Proprietà** dal menu.
4. Nella finestra di dialogo Proprietà collegamento locale, selezionare **Protocollo Internet versione 4 (TCP/IPv4)** o **Protocollo Internet versione 6 (TCP/IPv6)**.
5. Fare clic su **Proprietà**.
   - Se **Ottenere un'indirizzo automaticamente IPvx** è già selezionato, selezionare **Utilizzare il seguente Indirizzo IPv*x***, laddove *x* è la versione del protocollo Internet utilizzata (4 o 6).
   - Se si tratta di un collegamento statico, annotare l'indirizzo IP ed il numero della maschera di sottorete. Al termine della configurazione del controller, reimpostare il computer a questi valori.
6. Immettere l'indirizzo IP `192.168.6.1` o un indirizzo IP simile valido (ad esempio*192.168.6.x* laddove *x* è un numero tra 1 e 254 tranne 6).
7. Cambiare il valore della **lunghezza del prefisso di sottorete** a `255.255.255.0`.

   Il gateway predefinito non deve essere modificato.
8. Fare clic su **OK** e **Chiudere** fino alla chiusura di tutte le finestre aperte.
9. Prima di avviare l'ITC, se la stazione di lavoro client dispone di un firewall, disattivarlo.
10. Passare a Utilizzazione dell' ICT per configurare gli IPSDC a pagina 112.

## Utilizzazione dello strumento di configurazione integrato (ITC)

Questa sezione descrive come utilizzare lo strumento di configurazione per configurare un IPSDC per riconoscere l'indirizzo IP del controller del sistema e consentire il rilevamento IPSDC tramite il pulsante [Scansione modifiche hardware] nella pagina ***Amministrazione del sistema > Dispositivi.***

### Prima di iniziare

Prima di utilizzare l'"ITC notare i seguenti dettagli:

- La stazione di lavoro client locale utilizzata per l'accesso a ICT deve essere configurata correttamente. Consultare Preparazione delle stazioni di lavoro client per l'utilizzazione dello Strumento di configurazione integrato (ITC) a pagina 110.
- Prima di avviare l'ITC, se la stazione di lavoro locale dispone di un firewall, disattivarlo.

- Se l'installazione richiede un IPSDC e l'host corrispondente comunica attraverso un firewall, utilizzare l'l'CT per configurare il firewall IPSDC per consentire i collegamenti tramite la porta 3001.
- Disattivare o raggirare le reti proxy durante l'utilizzazione dell'ITC.
- Al termine della configurazione, l'ITC può essere disattivato per prevenire l'accesso non autorizzato. Consultare Attivare e disattivare l' ICT a pagina 114.
- Quando si modificano le opzioni su un modulo ITC, fare clic su **Salvare** nella parte inferiore del modulo, per salvare le modifiche prima di passare al successivo. Le ultime modifiche saranno salvate in un file di configurazione temporaneo.
- Una volta compilati tutti i moduli, fare clic su **Applicare modifiche** e poi su **Riavviare applicazione** per applicare le modifiche. Le modifiche saranno salvate nella configurazione del database sul IPSDC.

La tabella che segue descrive i pulsanti disponibili nell'interfaccia ICT:

| Pulsante | Utilizzazione | Risultato |
|---|---|---|
| Salvare | Dopo aver modificato i valori su un modulo | Salva le modifiche in un file di configurazione temporaneo |
| Applicare modifiche | Dopo aver terminato le modifiche | Salva le modifiche dal file di configurazione temporaneo al file di configurazione del database. |
| Riavviare l'applicazione | Dopo aver selezionato **Applicare modifiche** | The ICT recupera le ultime modifiche dalla configurazione del database e viene riavviato. |
| Riavviare il controller | Dopo aver selezionato **Applicare modifiche** | IPSDC applica le ultime modifiche dalla configurazione del database e viene riavviato. |
| Impostazioni di fabbrica[a] | Per ripristinare le impostazioni predefinite IPSDC | Le impostazioni IPSDC sono ripristinate ai predefiniti di fabbrica. Le impostazioni dell'indirizzo IP sono conservate. |
| Modificare utente/ password | Per impostare l'ID utente e/o la password per il collegamento nell'ITC. | Modifica l'ID utente e/o la password per ITC. I valori predefiniti sono `install, install`. Per migliorare la sicurezza, cambiare i valori predefiniti. |

a. In caso di ripristino dei parametri di rete predefiniti tramite il pulsante SW7, tutti i parametri (incluso l'indirizzo IP del IPSDC) saranno modificati.

## Utilizzazione dell' ICT per configurare gli IPSDC

Seguire i passaggi seguenti per configurare un IPSDC per la rilevazione dell'indirizzo IP del controller del sistema. Gli stessi passaggi possono essere configurati per riconfigurare un IPSDC se l'indirizzo IP del controller del sistema cambia.

1. Utilizzare uno dei seguenti browser Internet per aprire una finestra nella stazione di lavoro client:
   - Microsoft Internet Explorer 7.0 o successivo
   - Netscape 7.0 o successivo
   - Mozilla Firefox 12.0 o successivo

2. Nel campo **Indirizzo** del browser, immettere l'indirizzo IP del PSDC.

   L'indirizzo IP predefinito di un IPSDC è `192.168.6.6`. Se non si conosce l'indirizzo IP di un IPSDC, premere e mantenere premuto il pulsante Ripristinare predefiniti (SW7) sull'IPSDC per almeno 5 secondi per ripristinare le impostazioni ai valori predefiniti di fabbrica
3. All'avvio dell'ICT, immettere **l'ID utente** e la **Password** per l'IPSDC.

   I valori predefiniti sono `install` e `install`.
4. Fare clic su [Login].

   La pagina Informazioni sul controller visualizza il modulo Parametri.
5. (Consigliato) Modificare la password predefinita per migliorare la sicurezza:
   a. Fare clic su [Modificare utente/password] per aprire il modulo Modificare utente/password.
   b. Immettere l' **ID utente**.
   c. Immettere la **Nuova password**.
   d. Immettere nuovamente la password nel campo **Conferma password**.
   e. Fare clic su [Modificare credenziali].
6. Fare clic sul menu Parametri del controller per aprire il modulo Rete principale.
7. Per utilizzare un collegamento dinamico per IPSDC, selezionare **Utilizzare DHCP**. (Utilizzare questa opzione se la rete contiene un server DHCP e IPSDC può essere raggiunto tramite la porta della console.)

   Per utilizzare un collegamento statico (ad esempio in indirizzo IP impostato):
   a. Immettere l' **IP del controller**.
   b. Immettere l' **IP del Gateway**.
   c. Immettere la **maschera di sottorete**.
8. Immettere il nome dell'IPSDC nel campo **Nome controller.**
9. (Raccomandato) Annotare questa informazione nello schema di installazione. Consultare Documentazione della posizione fisica di ciascun dispositivo a pagina 5.
10. Fare clic su **Salvare**.
11. Passare alla scheda Configurazione pannello ed immettere l'indirizzo IP del controller del sistema nel campo **Indirizzo IP pannello** .
12. Fare clic su **Salvare**.
13. Se la configurazione dell'IPSDC tramite ICT è terminata, fare clic su **Applicare modifiche**, qundi **Riavviare applicazione**.
14. Se la stazione di lavoro client locale utilizzata per accedere l'ICT aveva in origine un indirizzo IP statico, ripristinare la stazione di lavoro per l'utilizzazione dell'indirizzo originale. Consultare Preparazione delle stazioni di lavoro client per l'utilizzazione dello Strumento di configurazione integrato (ITC) a pagina 110.
15. Dopo aver configurato IPSDC per riconoscere l'indirizzo IP del controller del sistema, può essere aggiunto al sistema in due modi:
    - Utilizzare il pulsante [Scansione per le modifiche hardware] per rilevare i dispositivi. Consultare Scansione per le modifiche hardware a pagina 23, oppure
    - Aggiungere IPSDC manualmente selezionando il controller del sistema nella pagina ***Amministrazione del sistema > Dispositivi***, facendo clic su [Aggiungere] e selezionando *IP 1 Porta 2 Lettore Controller*. Una volta terminato, fare clic su [Accettare modifiche].
16. Per completare la configurazione di un IPSDC nell'interfaccia utente:
    - Configurare le opzioni IPSDC per tutto il sistema nella scheda Sicurezza della pagina ***Amministrazione del sistema > Impostazioni del sistema***. Consultare Configurazione della sicurezza a pagina 18 e

- Configurare le opzioni specifiche per il controller nella pagina ***Amministrazione del sistema > Dispositivi*** . Consultare Configurare un controller della porta a pagina 25.

### Attivare e disattivare l' ICT

Controllare l'accesso all'ITC selezionando una delle due opzioni:

- **Temporaneo**: Consente l'accesso all'ITC fino alla reimpostazione dell'IPSDC.
- **Permanente**: Consente l'accesso fino alla nuova disattivazione manuale ITC.

**IMPORTANTE:** Prima di iniziare si **deve** disporre dell'accesso fisico al controller.

Per attivare l'ITC temporaneamente:

1. Premere e mantenere premuto SW4 finché D19 (ad es. Watchdog LED) è ON. L'attivazione di DN19 richiede circa cinque (5) secondi. (Per ulteriori informazioni sulle posizioni degli interruttori consultare *Guida rapida ai controller porta singola basati su IP.*)
2. Dopo l'accensione di D19, lasciare SW4.
3. D19 è disattivato quando ITC è attivato manualmente.

   L'ITC è attivato fino al riavvio del controller.

Per attivare l'ITC permanentemente:

1. Completare i passaggi per attivare l'ITC temporaneamente, come indicato sopra.
2. Collegarsi all'ITC.
3. Dal menu **Parametri del controller**, selezionare **Altri parametri**.
4. Deselezionare **Disattivare lo strumento di configurazione integrato**, quindi fare clic su **OK**.
5. Per rendere la selezione permanente, fare clic su **Salvare**, **Applicare modifiche**, quindi **Riavviare il controller**.

   IPSDC riavvierà automaticamente il sistema e ICT sarà attivato permanentemente.

Per disattivare ITC.

1. Collegarsi all'ITC.
2. Dal menu **Parametri del controller**, selezionare **Altri parametri.**
3. Selezionare **Disattivare lo strumento di configurazione integrato**, quindi fare clic su **OK**.
4. Per rendere la selezione permanente, fare clic su **Salvare**, **Applicare modifiche**, quindi **Riavviare il controller**. IPSDC riavvierà automaticamente il sistema e ICT sarà disattivato permanentemente.

## Autorizzazioni ruolo operatore predefiniti

Come discusso in Configurazione dei ruoli operatore a pagina 45, il ruolo operatore è un gruppo di policy di autorizzazione utilizzate per espandere o limitare le pagine dell'interfaccia utente che gli utenti possono visualizzare e le azioni che gli utenti possono intraprendere nel sistema.

I vari livelli di autorizzazione includono:

- **Nessuno**: L'operatore non può accedere o visualizzare la pagina.
- **Visualizzazione**: L'operatore è in grado di visualizzare la pagina o i dati, ma non può effettuare modifiche o eseguire comandi.

- **Modifica**: L'operatore può modificare le impostazioni.
- **Esecuzione**: L'operatore può eseguire comandi.

La tabella che segue fornisce i livelli d autorizzazione predefiniti per il sistema.

| Caratteristica | Livelli di autorizzazione | Amministratore | Operatore | Protezione | Solo visualizzazione | Distributore |
|---|---|---|---|---|---|---|
| Livelli di Accesso | Nessuno, visualizzazione, modifica | Modifica | Modifica | Visualizzazione | Visualizzazione | Modifica |
| Trigger azione: Gestione | Nessuno, visualizzazione, modifica | Modifica | Visualizzazione | Visualizzazione | Visualizzazione | Modifica |
| Trigger azione: Controllo | Nessuno, visualizzazione, esecuzione | Esecuzione | Esecuzione | Esecuzione | Visualizzazione | Esecuzione |
| Reimpostare l'anti-passback | Nessuno, visualizzazione, esecuzione | Esecuzione | Esecuzione | Esecuzione | Visualizzazione | Esecuzione |
| Aree | Nessuno, visualizzazione, modifica | Modifica | Visualizzazione | Visualizzazione | Visualizzazione | Modifica |
| Effettuare backup del database | Nessuno, esecuzione | Esecuzione | Esecuzione | Nessuno | Nessuno | Esecuzione |
| Controllo telecamera PTZ | Nessuno, esecuzione | Esecuzione | Esecuzione | Esecuzione | Nessuno | Nessuno |
| Formati tessera | Nessuno, visualizzazione, modifica | Modifica | Visualizzazione | Nessuno | Nessuno | Modifica |
| Credenziali | Nessuno, visualizzazione, modifica | Modifica | Modifica | Visualizzazione | Nessuno | Modifica |
| Data e ora | Nessuno, visualizzazione, modifica | Modifica | Modifica | Visualizzazione | Visualizzazione | Modifica |
| Dispositivi | Nessuno, visualizzazione, modifica | Modifica | Visualizzazione | Visualizzazione | Visualizzazione | Modifica |
| Diagnostica | Nessuno, visualizzazione | Visualizzazione | Visualizzazione | Visualizzazione | Visualizzazione | Visualizzazione |
| Porte (incluso IPSDC) | Nessuno, visualizzazione, esecuzione | Esecuzione | Esecuzione | Esecuzione | Visualizzazione | Esecuzione |
| Configurazione email | Nessuno, visualizzazione, modifica | Modifica | Visualizzazione | Nessuno | Visualizzazione | Modifica |

| Caratteristica | Livelli di autorizzazione | Amministratore | Operatore | Protezione | Solo visualizzazione | Distributore |
|---|---|---|---|---|---|---|
| Eventi | Nessuno, visualizzazione | Visualizzazione | Visualizzazione | Visualizzazione | Visualizzazione | Visualizzazione |
| Aggiornamenti del firmware | Nessuno, esecuzione | Esecuzione | Nessuno | Nessuno | Nessuno | Esecuzione |
| Vacanze | Nessuno, visualizzazione, modifica | Modifica | Modifica | Visualizzazione | Visualizzazione | Modifica |
| Ingresso/ Uscita | Nessuno, visualizzazione, esecuzione | Esecuzione | Esecuzione | Esecuzione | Visualizzazione | Esecuzione |
| Pacchetti lingue | Nessuno, visualizzazione, modifica | Modifica | Nessuno | Nessuno | Nessuno | Modifica |
| Configurazione di rete | Nessuno, visualizzazione, modifica | Modifica | Visualizzazione | Visualizzazione | Visualizzazione | Modifica |
| Condivisione di rete | Nessuno, visualizzazione, modifica | Modifica | Visualizzazione | Visualizzazione | Visualizzazione | Modifica |
| Ruoli operatore | Nessuno, visualizzazione, modifica | Modifica | Visualizzazione | Visualizzazione | Visualizzazione | Visualizzazione |
| Persone | Nessuno, visualizzazione, modifica | Modifica | Modifica | Visualizzazione | Visualizzazione | Modifica |
| Campi utente protetti | Nessuno, visualizzazione, modifica | Modifica | Nessuno | Nessuno | Nessuno | Nessuno |
| Gruppi lettori | Nessuno, visualizzazione, modifica | Modifica | Modifica | Visualizzazione | Visualizzazione | Modifica |
| Report | Nessuno, esecuzione | Esecuzione | Esecuzione | Esecuzione | Esecuzione | Esecuzione |
| Ripristinare database | Nessuno, esecuzione | Esecuzione | Nessuno | Nessuno | Nessuno | Esecuzione |
| Salvare/ Ripristinare le impostazioni | Nessuno, esecuzione | Esecuzione | Nessuno | Nessuno | Nessuno | Esecuzione |
| Backup programmati | Nessuno, visualizzazione, modifica | Modifica | Visualizzazione | Nessuno | Nessuno | Modifica |
| Pianificazioni | Nessuno, visualizzazione, modifica | Modifica | Modifica | Visualizzazione | Visualizzazione | Modifica |

| Caratteristica | Livelli di autorizzazione | Amministratore | Operatore | Protezione | Solo visualizzazione | Distributore |
|---|---|---|---|---|---|---|
| Sicurezza | Nessuno, visualizzazione, modifica | Modifica | Visualizzazione | Visualizzazione | Visualizzazione | Modifica |
| Opzioni del sistema | Nessuno, visualizzazione, modifica | Modifica | Visualizzazione | Visualizzazione | Visualizzazione | Modifica |
| Account utente | Nessuno, visualizzazione, modifica | Modifica | Visualizzazione | Nessuno | Nessuno | Modifica |
| Campi definiti dall'utente | Nessuno, visualizzazione, modifica | Modifica | Modifica | Visualizzazione | Visualizzazione | Modifica |
| Video | Nessuno, visualizzazione | Visualizzazione | Visualizzazione | Visualizzazione | Visualizzazione | Nessuno |
| Layout video | Nessuno, visualizzazione, modifica | Modifica | Modifica | Visualizzazione | Visualizzazione | Modifica |

## Utilizzazione della porta

I dispositivi hardware utilizzano le porte per consentire alle applicazioni di condividere funzioni hardware senza interferire gli uno con gli altri.

La tabella seguente fornisce le informazioni relative alle porte per diversi dispositivi nel sistema:

| Dispositivo | Porta | Utilizzazione |
|---|---|---|
| Controller del sistema | TCP/22 | Collegamento Secure Shell (SSH) |
| Controller del sistema | TCP/80 | TruPortalInterfaccia utente e utilità |
| Controller del sistema | TCP/443 | TruPortalInterfaccia utente e utilità |
| Controller del sistema | TCP/3001 | Aggiornamenti del firmware di basso livello |
| Controller del sistema | UDP/5353 | Scansione per la rilevazione delle modifiche hardware |
| TruVision TVN 20 | TCP/8000 | Porta predefinita per stream video |
| TruVision TVN 21 | TCP/8000 | Porta predefinita per stream video |
| TruVision TVN 50 | TCP/8000 | Porta predefinita per stream video |
| TruVision TVR 10 | TCP/8000 | Porta predefinita per stream video |
| TruVision TVR 11 | TCP/8000 | Porta predefinita per stream video |
| TruVision TVR 30 | TCP/80 | Porta predefinita per stream video |

| Dispositivo | Porta | Utilizzazione |
|---|---|---|
| TruVision TVR 31 | TCP/80 | Porta predefinita per stream video |
| TruVision TVR 41 | TCP/8000 | Porta predefinita per stream video |
| TruVision TVR 60 | TCP/8000 | Porta predefinita per stream video |

## Precisione della durata della pulsazione

Per la configurazione dei trigger azione che attivano o disattivano una pulsazione, notare che la precisione della pulsazione varia in base alla lunghezza della stessa, come illustrato nella tabella seguente:

| Durata | Precisione della portata |
|---|---|
| 1 secondo | 1 |
| 2 secondi | 2 |
| 3 secondi | 3 |
| 5 secondi | 5 |
| 10 secondi | 10 |
| 15 secondi | 15 |
| 20 secondi | 00:19 – 00:20 |
| 30 secondi | 00:29 – 00:30 |
| 45 secondi | 00:45 – 00:46 |
| 60 secondi | 00:59 – 01:00 |
| 90 secondi | 01:23 – 01:32 |
| 2 minuti | 01:53 – 02:02 |
| 3 minuti | 02:53 – 03:02 |
| 5 minuti | 04:43 – 05:12 |
| 10 minuti | 09:43 – 10:12 |
| 15 minuti | 14:43 – 15:12 |
| 20 minuti | 19:43 – 20:12 |
| 30 minuti | 29:43 – 30:12 |
| 45 minuti | 44:43 – 45:12 |
| 60 minuti | 00:59:43 – 01:00:12 |
| 90 minuti | 01:20:43 – 01:40:42 |
| 2 ore | 01:40:43 – 02:00:42 |

| | |
|---|---|
| 4 ore | 03:40:32 – 04:00:42 |
| 6 ore | 06:00:43 – 06:20:42 |
| 8 ore | 08:00:43 – 08:20:42 |
| 10 ore | 10:00:43 – 10:20:42 |
| 12 ore | 12:00:43 – 12:20:42 |
| 16 ore | 16:00:43 – 16:20:42 |
| 20 ore | 20:00:43 – 20:20:42 |
| 1 giorno | 0d:23:40:43 – 1d:00:00:42 |
| 7 giorni | 7d:00:20:43 – 7d:16:20:42 |

# *Glossario*

**ANSI**
Acronimo per American National Standards Institute, è un'organizzazione privata senza scopo di lucro che produce standard per l'industria informatica.

**Anti-passback**
L'anti-passback può essere utilizzato per stabilire una sequenza specifica di credenziali per accedere ad un'area.

**APB**
Acronimo per anti-passback. La prevenzione dell'utilizzazione del badge per accedere ad un sistema di controllo dell'accesso se lo stesso badge è stato utilizzato per accedere recentemente allo stesso lettore o area (APB temporizzato) oppure se non si trova nell'area appropriata per accedere in un'altra zona (APB area). In parole semplici, si tratta di controllare l'ingresso e l'uscita del titolare del badge per assicurarsi che la persona non passi la tessera ad un altro individuo.

**Area APB**
Le aree sono definite dal lettore di ingresso e di uscita. L'area nella quale si trova il badge è registrata. Se un badge tenta di accedere ad un'area attraverso un determinato lettore, l'accesso sarà negato se la posizione del badge non è registrata nell'area dalla quale si tenta di uscire.

**Codice edificio**
Un campo opzionale del badge che consente l'identificazione univoca di un luogo. I fornitori di tessere Wiegand in genere forniscono il codice edificio memorizzato nelle tessere. Per gli altri tipi di tessere, il codice edificio è definito dall'utente. Un lettore può essere impostato in modalità solo codice edificio e richiede la presentazione del codice prima di consentire l'accesso.

**Condivisione di rete**
Risorsa di rete condivisa quale un sito FTP o una cartella di rete.

**Contatto porta**
Un dispositivo costituito da due componenti ed utilizzato da un sistema di accesso tramite tessera per indicare se la porta è aperta o chiusa. In genere un componente è alloggiato nella porta e l'altro in una posizione simile sul telaio della porta.

**Controllata**
Una porta o perimetro provvisto di un circuito per la rilevazione del sabotaggio.

**Credenziale**
Un badge di identificazione con un numero cifrato, che può essere aggiunto al sistema ed utilizzato per consentire o meno l'accesso.

**DHCP**

Acronimo per Dynamic Host Configuration Protocol. Un protocollo di comunicazione che consente agli amministratori della rete di gestire ed automatizzare l'assegnazione degli indirizzi IP nella rete aziendale.

**Elettroserratura**

Dispositivo elettrico e/o magnetico utilizzato per mantenere bloccata una porta. L'apertura di una elettroserratura richiede una carica elettrica attivata da un dispositivo quale un lettore.

**Ethernet**

Si tratta di una tecnologia per le reti LAN che utilizza tipicamente un cavo coassiale o doppini costituiti da una coppia di conduttori ritorti. IEEE 802.3 è lo standard Ethernet. Esistono i seguenti tipi di Ethernet: 10 Mbps (Mega (million) bit al secondo); 100 Mbps; 1 Gbps (Giga (billion) bit al secondo)

**Evento**

La registrazione di un evento effettuata dal sistema, ad esempio per accessi consentiti o rifiutati, violazioni anti-passback e l'attivazione dell'allarme.

**Fermaporta**

Un dispositivo che mantiene la porta in posizione aperta finché non riceve istruzioni dal sistema per cambiare stato.

**HTTP**

Acronimo per Hyper Text Transfer Protocol. HTTP definisce le modalità di formattazione e trasmissione dei messaggi e controlla il funzionamento dei web server e browser in risposta a diversi comandi.

**IP**

Acronimo per Internet Protocol, specifica il formato dei pacchetti e il formato dell'indirizzo su una rete.

**IPSDC**

Acronimo per controller porta singola basato su IP.

**Indirizzo IP**

Si tratta di un codice identificativo che consente il riconoscimento di un computer su una rete TCP/IP. L'indirizzo IP è composto da una sequenza di 32 cifre binarie in sequenza di quattro numeri separati da punto. Ogni numero va da 0 a 255. Ad esempio, 1.120.4.72 può essere un indirizzo IP.

**LAN**

Acronimo per Local Area Network. Il LAN collega le stazioni di lavoro in un'area limitata tramite cavi per la condivisione di dati, periferiche e l'utilizzazione di un dispositivo di memorizzazione detto file server.

**LDAP**

Acronimo per Lightweight Directory Access Protocol. LDAP è un protocollo software utilizzato per collegare server che memorizzano le informazioni relative agli utenti, inclusi i certificati digitali. Consente agli utenti di trovare aziende, individui ed altre risorse quali file e dispositivi in rete, sia nell'Internet pubblico che nell'Intranet aziendale. Il collegamento ad un server LDAP può essere non crittografato o crittografato tramite SSL.

**Livello di accesso**
Una o più combinazioni lettore/programmazione utilizzata per il controllo hardware dell'accesso da parte di uno o più titolari di tessera. I livelli di accesso assegnati ai badge attivi determinano i lettori ai quali i badge hanno accesso ed a che ora.

**National Television Standards Committee**
Detto anche NTSC, è il segnale video televisivo utilizzato negli Stati Uniti ed in Giappone.

**Ora UTC**
Acronimo per Coordinated Universal Time, un punto di riferimento universale che coincide con il Tempo medio di Greenwich (GMT) basato sulla rotazione inconsistente della Terra, con ora atomica precisa. Quando la differenza tra l'ora atomica e l'ora terrestre sta per arrivare ad 1 secondo, si aggiunge un secondo, detto secondo intercalare, all'ora UTC.

**PAL**
Standard video utilizzato in Europa, Australia e Nuova Zelanda. Il video PAL trasmette 625 linee ogni 1/25 di secondo.

**PIN**
Acronimo per numero di identificazione personale, si tratta di un numero spesso associato ad un individuo ed utilizzato per il controllo dell'accesso.

**PTZ**
Acronimo per Pan-Tilt-Zoom. Una funzione della telecamera per le funzioni panoramica, inclinazione e zoom controllate tramite computer. PTZ consente un'area di visualizzazione maggiore grazie alla capacità di rotazione in diverse direzioni.

**Porta TCP/IP**
Un processo che vuole comunicare con un altro processo si identifica presso TCP/IP attraverso una o più porte. La porta è un numero a 16 bit utilizzato dal protocollo host-to-host per identificare il protocollo o l'applicazione (processo) al quale deve inviare i messaggi in arrivo.

**Procedura guidata**
Utilità utilizzata come guida per i diversi passaggi di un processo.

**Richiesta di uscita**
I dispositivi richiesta di uscita (RTE) sono utilizzati per consentire il transito attraverso porte bloccate dal lato protetto di un punto d'ingresso. Un contatto RTE è in genere un pulsante situato accanto alla porta associata. Quando un titolare di tessera preme il pulsante, viene inviata una RTE al pannello.

**Router**
Si tratta di un dispositivo centrale che collega diverse sottoreti per la condivisione di risorse e dati.

**Senza supervisione**
Una porta o perimetro non provvisto di circuito per la rilevazione del sabotaggio.

**SMTP**
Acronimo per Simple Network Management Protocol. Uno standard per la trasmissione di email attraverso reti IP.

**SNMP**
Acronimo per Simple Mail Transfer Protocol. Metodo per la gestione di diversi componenti hardware, ad esempio una stampante collegate alla rete.

**Sottorete**
Gruppo di computer che condividono le stesse proprietà di rete e le stesse risorse di rete.

**SSL**
Acronimo per Secure Sockets Layer, un protocollo comune per la verifica e la cifratura della comunicazione tramite Internet. SSL è utilizzato per la comunicazione con i server web (HTTPS) e i server LDAP.

**Telecamera IP**

Una telecamera digitale collegata direttamente alla rete con il proprio indirizzo IP ed in grado di trasmettere immagini tramite protocolli di comunicazione standard quali TCP/IP. Una telecamera IP non necessita il collegamento ad un PC o ad una scheda acquisizione video.

**Tipo di tessera**

Classifica la tecnologia di cifratura della tessera, quale magnetica, Wiegand, Smart Card, primo accesso, ecc.

**TCP/IP**

Acronimo per Transmission Control Protocol/Internet Protocol. Una gamma di protocolli di comunicazione che collegano gli host all'Internet.

**URL**

Acronimo per Uniform Resource Locator. L'URL è l'indirizzo di una risorsa o di un file disponibile su una rete TCP/IP quale l'Internet.

**Wiegand**

Tecnologia di controllo dell'accesso che utilizza tessere contenenti cavi magnetici in tungsteno tagliati in fasce e montate verticalmente in colonne.

# *Elenco*

## D



## E

## F



## G



## H



## I



## L



## M

## N



## O



## P



## R

## S



## T



## U



## V



## W