# Manuale d'uso

## Serie Atlas

Versione: 1.0
Data: Luglio 2019

# Indice dei contenuti

# 1 Introduzione

La serie Atlas di ZKTeco è un sistema di controllo elettronico degli accessi potente ma intuitivo, che supporta le più recenti innovazioni in materia di sicurezza fisica e accesso biometrico. La serie Atlas offre:

- Accesso sicuro e comodo con le impronte digitali grazie alla tecnologia biometrica leader del settore di ZKTeco (solo per i modelli della serie Biometric Atlas)
- Supporto per lettori di schede Wiegand e OSDP standard del settore, con definizioni flessibili del formato delle schede.
- Applicazione di gestione web potente e intuitiva integrata nel controllore: tutto ciò che serve è un browser web; nessun software per PC da installare o gestire.
- Scalabilità fino a 84 porte con l'aggiunta di controller secondari, in modo rapido e semplice grazie al rilevamento basato sulla rete.
- Funzioni critiche di emergenza 20: blocco globale 111, sblocco globale di emergenza 113, allarme gestione 24, PIN di emergenza 114, codici di emergenza 48 e rapporti di adunata 30
- Applicazione mobile per iOS e Android

## Utilizzo di questa guida

Gli argomenti di questa Introduzione spiegano come utilizzare l'applicazione di gestione Web in generale.

Le quattro sezioni principali corrispondono ai quattro menu di navigazione principali: Monitoraggio 21, Controllo accesso 37, Configurazione 54 e Amministrazione 92. Questi argomenti forniscono una guida generale e hanno un sotto-argomento per ogni voce di menu.

Funzioni e compiti 111 descrive le funzioni speciali non centralizzate e spiega le attività comuni a più schermate.

Riferimento 28 comprende il Glossario 128 e altro materiale di riferimento.

## Come iniziare

Il controllore primario dovrebbe essere già installato e configurato. (Se al momento dell'accesso viene visualizzata l'Installazione guidata, la configurazione non è completa. Completare la configurazione prima di continuare).

Per iniziare:

1. Aprire un browser web e accedere all'applicazione di gestione web.
2. Registrare il prodotto e aggiungere eventuali licenze aggiuntive acquistate. La registrazione è necessaria per reimpostare la password del sistema e consente a ZKTeco di contattare l'utente per aggiornamenti del software e altre informazioni. Le licenze aggiuntive ampliano la capacità del sistema.
3. Esaminare la schermata iniziale e i menu.
4. Comprendere le viste elenco e le viste delle proprietà. La maggior parte delle schermate utilizza una di queste viste.
5. Esaminare la configurazione delle porte, in particolare la **modalità predefinita** e la **programmazione** della **modalità porta.**
6. Scoprite i diversi modi in cui è possibile assegnare l'accesso alle porte agli utenti. agli utenti.
7. Considerare l'impostazione dell'accesso per i dispositivi mobili.

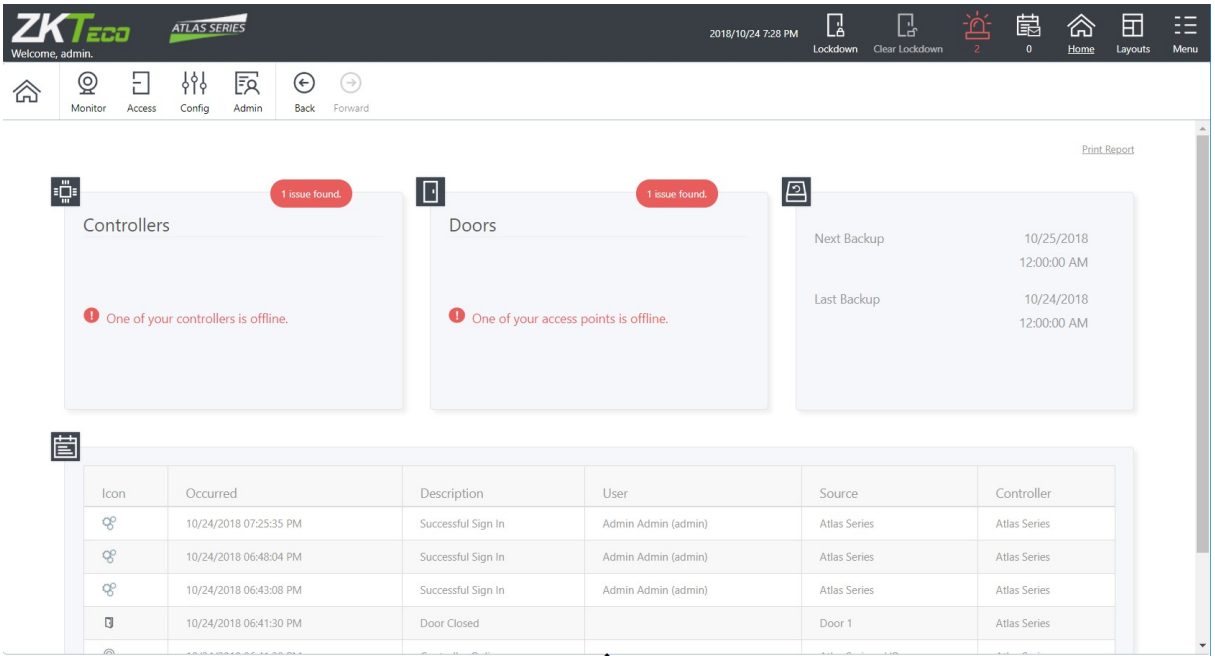
Ora avete un sistema di controllo degli accessi completamente funzionante. Leggete le informazioni sul monitoraggio e notifiche in modo da poter vedere cosa succede nel vostro sistema.

**Importante:** dopo aver iniziato, imparare a usare le funzioni di emergenza della serie Atlas. Alcune di esse richiedono un'impostazione significativa prima di poter essere utilizzate per proteggere gli utenti.

## 1.1 Schermata iniziale e menu

La schermata principale visualizza un riepilogo in stile dashboard del sistema, comprese le attività recenti degli eventi. La barra dei menu è disponibile in questa schermata, come in tutte le schermate dell'applicazione.

# Schermata iniziale Cruscotto




**clicca per ingrandire**

I potenziali problemi di sicurezza sono evidenziati in rosso, compreso il blocco e lo sblocco di emergenza. e lo sblocco di emergenza conta. È possibile fare clic sui collegamenti per ottenere ulteriori informazioni. È sempre possibile tornare a questa schermata utilizzando il pulsante **Home** in alto a destra nel menu principale.

I riquadri di riepilogo del cruscotto includono:

- Riepilogo dello stato dei controllori - il collegamento porta a Hardware
- Riepilogo dello stato delle porte - il link porta allo Stato della porta
- Stato del backup (prossimo backup pianificato, backup più recente) - il link porta a Backup e Ripristino
- Il numero di client connessi a Web/Mobile e se la password dell'amministratore è stata protetta (andare al modulo Utenti e modificare la password dell'amministratore per proteggerla). e modificare la password dell'amministratore per renderla sicura).
- Eventi recenti - il link **+ Vedi di più** vi porta agli eventi

Gli esatti riquadri di riepilogo visibili dipendono dal proprio Ruolo utente. Si noti inoltre che quando si accede a un Controllore secondario, i riquadri di riepilogo sono estremamente limitati, poiché il Controllore secondario riceve i dati dal Controllore

primario.

## Menu principale

La barra del menu principale si trova in alto a destra su tutte le schermate.

| | |
|---|---|
| Blocco e Blocco libero  | Fare clic su **Blocco** per bloccare rapidamente tutte le porte in una situazione di emergenza. Quando è attivo un blocco globale, un messaggio viene visualizzato in modo evidente nella barra dei menu. Si noti che l'avvio di un blocco creerà un'emergenza. Allarme 24 per impostazione predefinita.<br><br>Fare clic su **Cancella blocco** per abilitare nuovamente l'accesso e riportare le porte alla modalità predefinita o programmata.<br><br>Vedere Blocco 111 per ulteriori informazioni. |
| Allarmi  | Quando ci sono allarmi attivi, questa icona sarà rossa o gialla e mostrerà il numero di allarmi correnti. Fare clic per accedere alla schermata Allarmi 24 Allarmi. |
| Notifiche  | Fare clic per visualizzare le notifiche 17 a cui ci si è iscritti. Il numero di notifiche in attesa è visualizzato sotto l'icona. |

| | | |
|---|---|---|
| Casa |  | Torna alla schermata iniziale. |

| | | |
|---|---|---|
| Layout |  | I layout consentono di visualizzare più funzioni o schermate alla volta. Ad esempio, selezionare una Layout a 3 pannelli per lavorare su Livelli di accesso 49 e sulle pianificazioni mentre si visualizza eventi dal vivo 22. Ogni pannello ha il proprio menu di navigazione.<br><br>Selezionare il layout a riquadro singolo per tornare alla visualizzazione standard. |
| Menu |  | Apre un menu che mostra diversi opzioni varie. Vedere sotto. 7 |

Le esatte voci del menu principale disponibili dipendono dal ruolo dell'utente 92. Si noti inoltre che
quando si accede a un Controllore secondario, le voci di menu sono estremamente limitate, perché la maggior parte è gestita dal Controllore primario.

## Menu di navigazione

Il Menu di navigazione contiene le voci per tutte le schermate principali dell'applicazione, organizzate in quattro pulsanti tematici. Il Menu di navigazione è ripetuto in ogni pannello dei layout a più pannelli. Questo manuale di aiuto è organizzato come il menu: quattro sezioni principali contenenti un sottoargomento per ogni voce di menu.

Gli argomenti sono: monitoraggio 21, controllo degli accessi 37, configurazione 54 e Amministrazion 92.
e

Utilizzare i pulsanti **Indietro** e **Avanti** per navigare nella propria cronologia di accesso alle schermate. (I pulsanti di navigazione del browser non funzionano all'interno dell'applicazione di gestione Web).


Le esatte voci del menu di navigazione disponibili dipendono dal ruolo dell'utente 92 . Si noti inoltre che
quando si accede a un Controllore secondario, le voci di menu sono estremamente limitate, perché la maggior parte è gestita dal Controllore primario.

## Voci dei pulsanti di menu

| | |
|---|---|
| Lingua | Imposta la lingua dell'utente corrente. Viene salvata come predefinita per questo utente.<br><br>Le lingue disponibili dipendono dalla licenza del software 15 . Contattare il rappresentante autorizzato ZKTeco per l'aggiornamento della licenza. |
| Preferenze | Imposta le preferenze dell'utente corrente. Vengono salvate come predefinite per questo utente. Le preferenze sono<br><br>▪ "Voci per pagina", il numero di voci visualizzate in una pagina di una elenco 12 , e<br><br>▪ "Punto di registrazione della carta 117 ." |
| Salva registri... | Crea un file contenente i registri del programma e altre informazioni per indagare sui problemi. Utilizzarlo quando viene richiesto dall'assistenza tecnica. Se possibile, salvare i registri subito dopo aver riscontrato un problema e tenerli a disposizione quando si contatta l'assistenza tecnica. |
| Aiuto | Apre la Guida in linea. |

Informazioni Apre una finestra che mostra le informazioni sul prodotto, compresa la versione corrente e le licenze. Registrare o aggiungere licenze in questa schermata.

EsciEsci dall'applicazione di gestione Web e torna alla schermata di accesso.

## 1.2 Utilizzo delle viste elenco

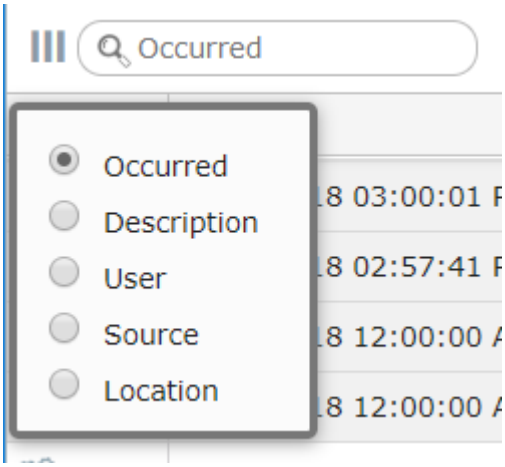
Le viste elenco mostrano un elenco di elementi in colonne. In molti casi, le colonne possono essere modificate, spostate e ricercate.

Si noti che le viste delle proprietà visualizzano anche un elenco a sinistra, che presenta gli stessi controlli.

### Ricerca

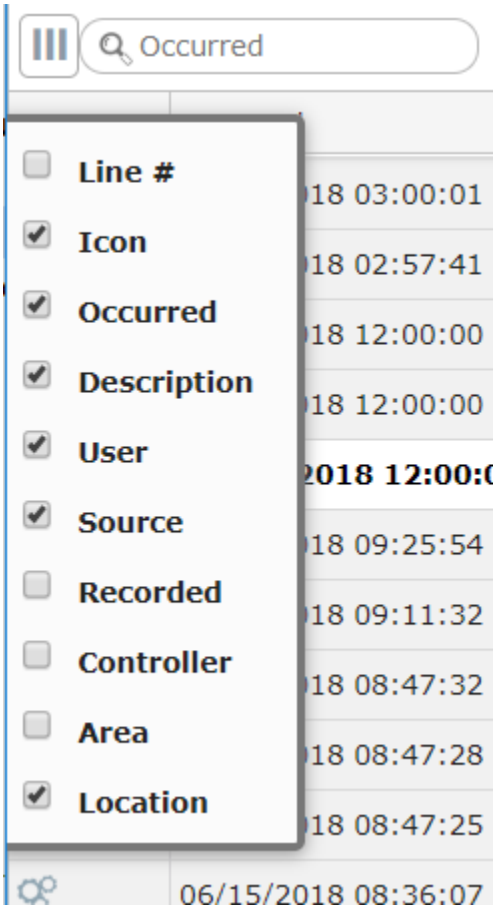
Per cercare in una colonna, inserire il testo nella casella in cima all'elenco.

Il testo grigio predefinito è la colonna che verrà cercata. Fare clic sulla lente di ingrandimento per modificare la colonna.



# Selezione della colonna

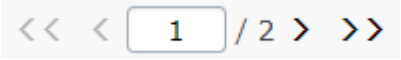
È possibile spostare le colonne visualizzate facendo clic e trascinando il titolo della colonna. Fare clic sull'icona della tripla barra per selezionare le colonne da visualizzare.




## Paging

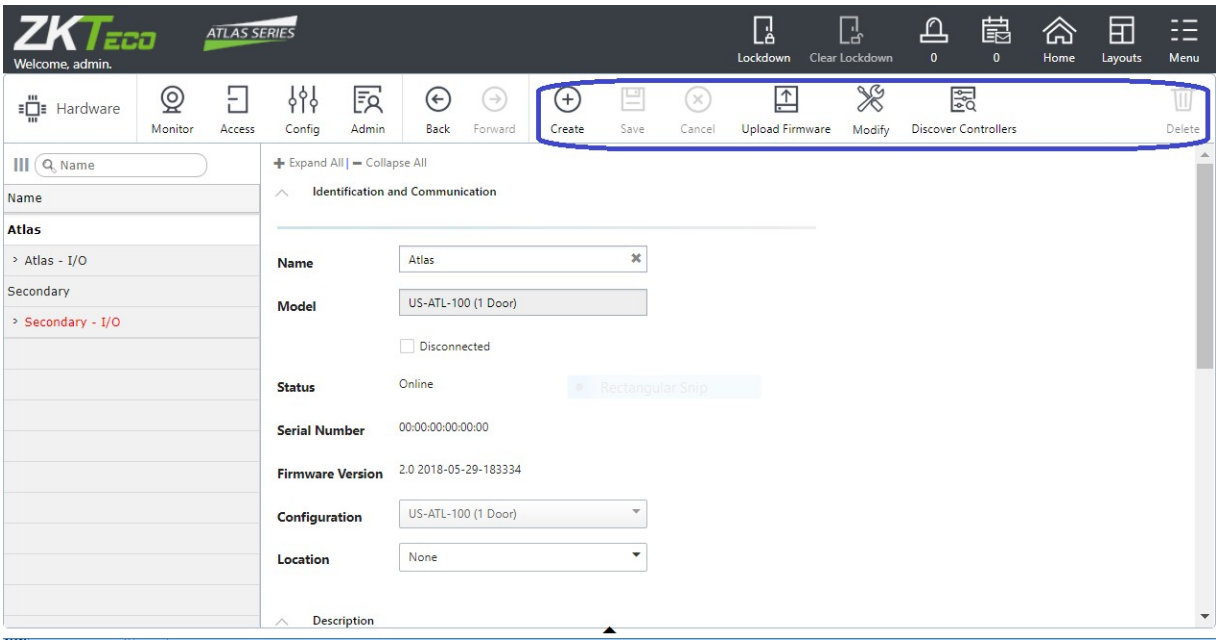
Gli elenchi si riempiono di pagine extra quando il numero di elementi supera il numero di **elementi per pagina** impostato.
impostato in Menu: Preferenze .

Questa casella appare in fondo all'elenco quando ci sono delle pagine. È possibile andare avanti o indietro di una pagina, andare alla fine o all'inizio o inserire un numero di pagina.



## 1.3 Utilizzo delle viste delle proprietà

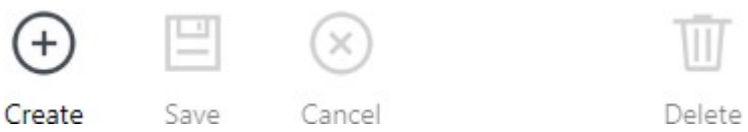
La maggior parte della configurazione viene visualizzata o modificata nelle viste delle proprietà. Queste schermate visualizzano un elenco di elementi creati a sinistra e le relative proprietà a destra.




**clicca per ingrandire**

L'elenco può essere ricercato utilizzando gli stessi strumenti di Viste elenco 12 .

Utilizzare i pulsanti sopra le proprietà per creare nuovi elementi, salvare le modifiche o eliminare gli elementi.




Molte viste delle proprietà aggiungono ulteriori pulsanti di azione alla barra dei menu. Questi sono generalmente specifici per il tipo di schermata in cui sono visualizzati e le loro funzioni

sono descritte in

la documentazione relativa alle schermate specifiche. Queste sono visualizzate in grigio se non si applicano alla voce attualmente selezionata.


## 1.4 Accesso e password

Per accedere all'applicazione di gestione web, aprire un browser web e inserire l'indirizzo IP del controllore primario fornito dall'amministratore della serie Atlas. (In alcuni browser, è necessario digitare "https://" prima dell'indirizzo). È necessario inserire questo link tra i preferiti.

Il browser potrebbe visualizzare un avviso di sito non sicuro. I mezzi per bypassare questo avviso variano a seconda delle applicazioni del browser, ma dovrebbero essere mostrati nella pagina di errore come un link etichettato "Avanzate", "Dettagli", "Ulteriori informazioni" o qualcosa di simile. È possibile evitare questo avviso per tutti gli utenti installando un certificato HTTPS firmato 108.

Inserire il nome utente e la password forniti dall'amministratore. Se si è persa la password dell'utente "admin", vedere Reimpostazione della password 120.

Non è possibile modificare la propria password a meno che non si disponga dei privilegi di accesso per modificare gli utenti dell'amministratore per la modifica della password. 38. Chiedere

## 1.5 Registrazione del prodotto e licenze

La registrazione è necessaria per reimpostare la password del sistema e consente a ZKTeco di contattare l'utente per aggiornamenti del software e altre informazioni.

Le licenze aggiuntive consentono di aumentare la capacità del sistema Atlas Series. È possibile

- aumentare il numero di Porte o Controllori secondari consentiti,
- aumentare il numero di connessioni dei dispositivi mobili e
- aggiungere alle lingue supportate dal sistema.

(Si noti che le porte "fuori" non vengono conteggiate nel numero massimo di porte autorizzate).

Per l'aggiornamento della licenza, contattare il rappresentante autorizzato ZKTeco. Le informazioni attuali sulla licenza possono essere visualizzate nella schermata della schermata Informazioni su.

## Come registrarsi

Seguite questi passaggi per registrarvi per la prima volta o per aggiornare le vostre informazioni di registrazione.

1. La registrazione può essere avviata in due modi:
    a. Quando si accede per la prima volta, fare clic su **Registra ora** nella finestra pop-up Registra il tuo prodotto oppure
    b. Selezionare **Menu: Informazioni** e fare clic sul pulsante **Registra.** (Se la registrazione è stata effettuata in precedenza, il link è **Aggiorna registrazione**).
2. Fare clic sul pulsante **Nuova registrazione** nella finestra successiva. (Se la registrazione è stata effettuata in precedenza, il pulsante è **Visualizza/Aggiorna registrazione**).
3. Compilare le informazioni di registrazione. Gli asterischi indicano le informazioni obbligatorie. L'*indirizzo e-mail inserito deve essere in grado di ricevere le informazioni di registrazione.*
4. Inviate la vostra registrazione automaticamente o via e-mail.
    a. Per la registrazione automatica, fare clic sul pulsante **Invia online**. Verrà visualizzata una finestra di avanzamento seguita da un messaggio di successo.
    b. Per la registrazione via e-mail:
        i. Fare clic sul pulsante **Registrazione offline**. Leggete le istruzioni nella finestra seguente.
        ii. Fare clic sul link **Scarica il file di registrazione** e salvare il file dei dati di registrazione sul computer.
        iii. Creare e inviare un messaggio e-mail facendo clic sul link o inserendolo nel programma di posta elettronica. L'e-mail deve contenere il file dei dati di registrazione come allegato, con il nome originale. L'oggetto e il testo dell'e-mail non sono importanti.

Riceverete un file di conferma della registrazione tramite un'e-mail di risposta. Quando lo fate,

1. Aprire l'e-mail e salvare l'allegato sul computer.

2. Fare clic sul pulsante **Carica conferma**. (Se si è già usciti dalla registrazione, tornare a questa opzione selezionando **Menu: Informazioni** e facendo clic sul pulsante **Registra**).
3. Trovare e aprire il file di conferma della registrazione

salvato. Dovrebbe apparire una finestra di messaggio

"Registrazione riuscita".

## Come aggiungere le licenze

Quando si acquista una licenza aggiuntiva, si riceve un file di licenza da ZKTeco. Salvare questo file sul proprio computer, quindi:

1. Selezionare **Menu: Informazioni.**
2. Fare clic sul pulsante **Carica licenze aggiuntive**.
3. Fare clic sul pulsante **Sfoglia** e **aprire** il file di licenza ricevuto.
4. Fare clic su **OK.** Le nuove funzionalità dovrebbero essere elencate nella schermata Informazioni.

## Argomenti correlati

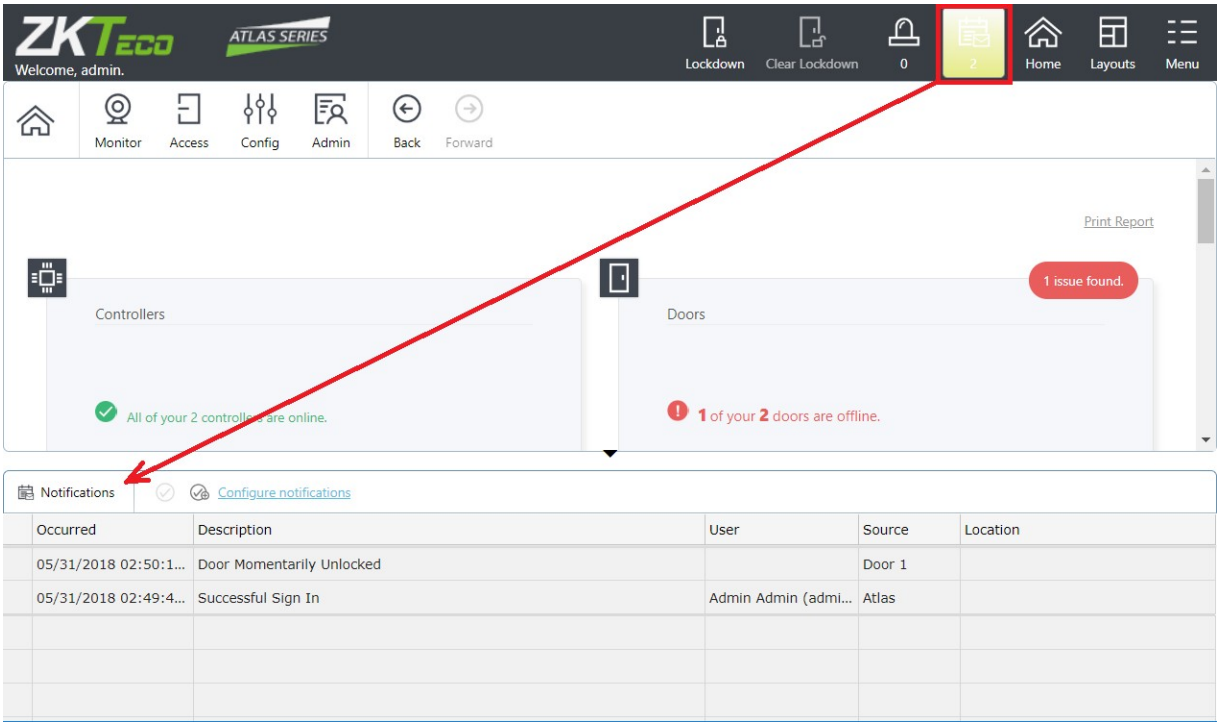
- Schermata iniziale e menu 7
- Ripristino della password 120

# 1.6 Notifiche

Le notifiche consentono a ogni utente di selezionare determinati eventi 72 che desidera siano portati alla sua attenzione. Quando si verifica uno di questi eventi, esso appare nella finestra di notifica di quell'utente e vi rimane fino a quando non viene confermato.

Le notifiche possono essere inviate via e-mail.

Fare clic sull'icona **Notifiche** nella barra dei menu per aprire e chiudere la finestra Notifiche nella parte inferiore dello schermo.




**clicca per ingrandire**

## Configurazione delle notifiche

Configurare le notifiche per selezionare gli eventi che generano notifiche per l'utente corrente. Non vengono create notifiche se non vengono selezionate.

1. Fare clic su **Notifiche** nella barra dei menu.
2. Fare clic sul link **Configura notifiche** nella finestra Notifiche.
3. Se si desidera, selezionare **Invia una copia delle notifiche via e-mail**.
   - ? Altrimenti, le notifiche vengono visualizzate solo nell'applicazione di gestione Web.
   - ? È necessario disporre di un indirizzo di posta elettronica configurato in Utenti e un server e-mail configurato in Impostazioni e-mail 106.
4. Selezionate le categorie e i tipi di eventi per i quali desiderate ricevere le notifiche.

? Selezionare una categoria per ricevere le notifiche per tutti i tipi di evento di quella categoria, oppure

- ? Espandere la categoria e selezionare Tipi di evento specifici.

5. Fare clic su **Salva**.

## Cancellazione delle notifiche

Per cancellare le notifiche nell'elenco, fare clic su uno dei pulsanti accanto a **Configura notifiche**.  - Selezionare una o più notifiche e fare clic su questo pulsante per cancellarle.

 - Fare clic per cancellare tutte le notifiche.

Dato che le notifiche sono basate su un criterio per utente, se un utente cancella una notifica, le notifiche degli altri utenti non ne risentono.

## Invio di notifiche via e-mail

Per ricevere copie di tutte le notifiche via e-mail, è necessario configurare l'e-mail per il sistema e per se stessi.

1. Configurazione delle impostazioni e-mail dell'applicazione di gestione web 106.
2. Inserire un **indirizzo e-mail** nella pagina Utente 38 pagina.
3. Selezionare **Invia una copia delle notifiche via e-mail** in **Configura notifiche, in** alto.

## Numero massimo di notifiche

Per definire il numero massimo di notifiche per utente:

1. Andare alle Impostazioni di sistema 100.
2. Immettere il numero **massimo di notifiche per utente**.
3. Fare clic su **Salva**.

Le notifiche più vecchie vengono eliminate quando si raggiunge il numero massimo.

## Argomenti correlati

- Impostazioni e-mail

- Impostazioni di sistema 100

## 1.7 Caratteristiche di emergenza

Il sistema della serie Atlas è stato progettato con una serie di importanti funzioni utilizzate per aiutare in diverse situazioni di emergenza.

- Blocco 111 può essere configurato e utilizzato per proteggere le strutture da un intruso o da una minaccia attiva.
- Sblocco di emergenza 72 può essere configurato e utilizzato per favorire l'accesso del personale di emergenza in caso di condizione di emergenza attiva segnalata da un altro sistema.
- PIN di emergenza 44 possono essere utilizzati per consentire agli utenti di segnalare una condizione di costrizione durante il loro altrimenti normale accesso.
- Codici di emergenza 28 possono essere configurati e utilizzati per consentire l'accesso al personale di emergenza o di sicurezza utilizzando esclusivamente un codice PIN, indipendentemente dalla modalità porta (compreso il blocco) o dalle regole di accesso multiutente.
- Muster 30 può essere utilizzato per aiutare a rintracciare gli utenti durante un'evacuazione o un'esercitazione di evacuazione.
- Allarmi 24 e notifiche 17 possono essere configurati e utilizzati per assicurarsi che il personale corretto sia a conoscenza di potenziali situazioni di emergenza.

**Importante:** tutte le funzioni di emergenza che si intendono utilizzare nel sistema devono essere testate in anticipo, per assicurarsi che tutto sia configurato e funzioni correttamente.

**Importante:** queste funzioni di emergenza sono state progettate per integrare, ma non per sostituire, l'infrastruttura di sicurezza per la vita della struttura. Le funzioni di sicurezza della vita sono regolate dalle norme antincendio specifiche di ogni paese e regione. Per garantire la conformità del sistema, è necessario fare riferimento a queste ultime durante la progettazione e la configurazione.

# 2 Monitoraggio

Il monitoraggio offre una visione in tempo reale di ciò che accade nel sistema e rapporti stampabili sulla configurazione e sulla cronologia.

## Monitoraggio in tempo reale

Eventi 22 è una visione in tempo reale di tutto ciò che accade nel sistema.

Allarmi 24 mostra gli eventi che l'utente ha deciso di esaminare immediatamente e di intervenire. Ogni allarme deve essere riconosciuto e cancellato da qualcuno che ha risolto il problema. Si noti che gli eventi non diventano allarmi finché non si impostano i trigger di allarme 87 .

Stato della porta 26 mostra lo stato attuale di ogni porta, che sia in linea, bloccata, allarmata e così via.

Mappe 28 mostrano uno stato simile a quello della porta, con indicatori visivi visualizzati su una mappa della struttura. Le mappe devono essere prima create in Mappe (Configurazione). 182 .

## Rapporti

Muster 30 è un rapporto speciale che mostra la posizione degli utenti in caso di emergenza o di esercitazione di evacuazione. Per utilizzare il rapporto Muster, occorre innanzitutto designare le Aree Muster. Gli utenti devono registrarsi nelle aree di raccolta per indicare che sono usciti dalla struttura in condizioni di sicurezza.

Le altre voci di menu sono semplici rapporti.

Audit 31 mostra le modifiche alla configurazione e le azioni eseguite dagli utenti connessi all'applicazione di gestione web.

Cronologia eventi 33 è una visualizzazione di report degli eventi, con la possibilità di visualizzare un numero maggiore di eventi e di esportare in CSV e PDF.

Cronologia allarmi 34 mostra tutti gli allarmi, compresi quelli che sono stati risolti (gli allarmi risolti non sono visualizzati nella schermata degli allarmi attivi).

Rapporto sul livello di accesso degli utenti 36 mostra quali utenti hanno un determinato

livello di accesso [48] .

Rapporto porta utente 38 mostra quali utenti hanno accesso a una specifica porta. Questo rapporto include le porte assegnate direttamente agli utenti e quelle assegnate tramite un livello di accesso.

## Argomenti correlati

- Rapporti e stampa 115

## 2.1 Eventi

Eventi visualizza un elenco in tempo reale degli eventi che si verificano nel sistema. Gli eventi che attivano gli allarmi 34 sono visualizzati in un colore configurabile.

Per ricevere un'e-mail quando si verificano eventi importanti, vedere Notifiche 17 .

È possibile visualizzare fino a 1000 eventi. Per visualizzare un numero maggiore di eventi, utilizzare la Cronologia eventi 33 .

## Pulsanti di menu

Filtro Apre un pannello in cui è possibile limitare gli eventi che si desidera visualizzare nell'elenco. I filtri rimangono attivi a ogni accesso.

Le impostazioni diventano effettive quando si fa clic sul pulsante **Cerca**, nella parte inferiore del pannello. Il pulsante **Ripristina** **cancella** tutti i filtri.

**Filtri per utenti e dispositivi**

La visualizzazione mostra solo gli eventi che corrispondono a *tutti i* filtri specificati. Si noti che i filtri **Nome** non fanno distinzione tra maiuscole e minuscole e troveranno corrispondenze parziali. Ad esempio, se si immette "john", la visualizzazione mostrerà anche gli eventi per "John" o "Johnny".

**Filtro del tipo di evento**

Il display mostra gli eventi che corrispondono a *uno qualsiasi* dei tipi di evento selezionati. Se non è stato selezionato nulla, vengono visualizzati tutti gli eventi.

Cancella Cancella l'elenco corrente di eventi dal display, in modo da far apparire solo i nuovi eventi. Gli eventi vengono nascosti, ma non cancellati.

## Colonne Eventi

Alcune colonne saranno vuote per alcuni tipi di eventi.

Icona Categoria dell'evento

Avvenuto Quando l'evento si è effettivamente verificato (determinato dal Controllore su cui si è verificato)

Descrizione dell'evento Testo dell'evento

L'utente L'utente 38 associato all'evento. Può trattarsi anche di un Codice di accesso condiviso 46 , di un Codice di emergenza 48 , o di una credenziale (tessera, PIN) non assegnata a un singolo Utente.

Fonte Il dispositivo che ha registrato l'evento. Per gli eventi di accesso alla porta, si tratta di una porta. Per altri eventi, può essere un controllore, un ingresso, un'uscita o un altro dispositivo.

Registrato (nascosto per impostazione predefinita) L'ora in cui l'evento è stato ricevuto e registrato dal controllore primario. È diverso da Avvenuto solo se il Controllore secondario in cui si è verificato l'evento era offline con il Controllore primario al momento dell'evento.

Controllore (nascosto per impostazione predefinita) Controllore in cui si è verificato l'evento

Area Se l'evento è associato a un'area (ad esempio una porta che entra in un'area), l'area viene indicata qui. (ad

esempio una porta che entra in un'area), l'area viene indicata qui.

| | |
|---|---|
| Località | (nascosto per impostazione predefinita) Se la sorgente è associata a una località 79 , questa viene indicata qui. |

## Archiviazione degli eventi

Gli eventi più vecchi vengono archiviati automaticamente in file CSV sul controllore primario quando si raggiunge il numero massimo. Per scaricare i dati archiviati, vedere Download archivi 107 .

Per modificare il numero massimo di eventi nel sistema, andare in Impostazioni di sistema e impostare il numero massimo di eventi nel database. e impostare il numero **massimo di eventi nel database**.

## Argomenti correlati

- Utilizzo delle viste elenco
- Impostazioni di sistema
- Storia dell'evento

## 2.2 Allarmi

Gli allarmi sono problemi che possono indicare una potenziale minaccia alla sicurezza o un altro problema. Essi causano la visualizzazione di un avviso sulla barra del menu principale e rimangono attivi finché non vengono risolti da un utente.

Gli allarmi sono attivati dagli eventi 22 . Alcuni tipi di evento sono impostati per attivare gli allarmi in modo predefinito. È possibile far scattare gli allarmi ad altri eventi o modificare le impostazioni predefinite in Trigger di allarme 87 .

Per ricevere un'e-mail quando un evento causa un allarme, vedere Notifiche 17 . Il colore di un allarme è determinato dal suo stato, che può essere:

- Nuovo (rosso) - significa che l'allarme è attivo.

- Riconosciuto (giallo): significa che un utente ha riconosciuto l'allarme.
Gli allarmi risolti vengono rimossi dall'elenco. Possono essere visualizzati nella Cronologia allarmi 34 .

Gli allarmi ripetuti vengono uniti in un unico allarme. La colonna **Conteggio** indica il numero di volte in cui si è verificato, mentre **Ultima registrazione** indica l'ora più recente in cui si è verificato. Gli allarmi vengono uniti quando sono identici in tutto, tranne che per la data e l'ora. Una volta risolti, ogni nuova occorrenza darà origine a un nuovo allarme.

## Pulsanti di menu

| | |
|---|---|
| Riconoscimento | Indica che l'utente è consapevole che l'allarme si è verificato, cambiando il suo stato in "Riconosciuto". L'utente indica di aver accettato un livello di responsabilità concordato per la risoluzione del problema. |
| Risolvi | Indica che il problema è stato risolto, cambiando lo stato in "Risolto". L'allarme viene rimosso da questa schermata, ma può essere visualizzato nella Cronologia allarmi 34 . Gli allarmi devono essere riconosciuti prima di essere risolti. |
| Riconoscere Tutti | Riconosce tutti gli allarmi che si trovano nello stato "Nuovo". |
| Risolvi tutto | Risolve tutti gli allarmi che si trovano nello stato "Riconosciuto". |

## Colonne Allarmi

| | |
|---|---|
| Descrizione | Descrizione dell'evento scatenante |
| Fonte | Il dispositivo che ha registrato l'evento. Per gli eventi di accesso alla porta, si tratta di una porta. Per altri eventi, può trattarsi di un controllore o di un altro dispositivo. |

| | |
|---|---|
| Priorità | La priorità di questo allarme (come configurato in Trigger di allarme 87 ) |
| Conteggio | Il numero di volte in cui l'evento scatenante si è verificato ed è confluito in un allarme. |
| Prima registrazione | Ora del primo evento scatenante |
| Ultima registrazione | Ora dell'evento di attivazione del duplicato più recente |
| Stato | "Nuovo" o "Riconosciuto". Lo stato "Risolto" è visibile solo nella Cronologia allarmi 34 . Lo stato determina il colore (vedere sopra). |
| Posizione | Posizione 79 dove si è verificato l'evento scatenante |
| Area | (nascosta per impostazione predefinita) Area 80 dove si è verificato l'evento scatenante |

## Argomenti correlati

- Utilizzo delle viste elenco 22
- Trigger di allarme 87
- Storia dell'allarme 34
- Caratteristiche di emergenza 20

## 2.3 Stato della porta

Stato porta visualizza un elenco in tempo reale di tutte le porte e del loro stato. È inoltre possibile utilizzare i comandi manuali 72 per sbloccare temporaneamente una porta o cambiare la modalità della porta.

# Pulsanti di menu

| | |
|---|---|
| Coman di manuali | Inviare un comando manuale 115 alla porta selezionata, ad esempio per sbloccarla temporaneamente o per cambiare la modalità della porta. |

## Colonne di stato della porta

| | |
|---|---|
| La porta | Il nome della porta |
| Comunicazioni | "Online" o "Offline" |
| Modalità porta | La modalità porta 142, ad esempio "Solo carta" o "Carta e PIN". |
| Stato | Se la porta è "bloccata" o "sbloccata" e "aperta" o "chiusa". |
| Errori | Mostra gli errori "Porta forzata" o "Porta bloccata", "Lettore offline" e "Manomissione". |
| Allarme | Indica se esiste un allarme attivo 24 attivo per la porta |
| Tipo | Il tipo di porta<br>▪ In<br>▪ Fuori<br>▪ Punto di raccolta<br>▪ Punto di registrazione della carta |
| La posizione | Posizione 79 della porta |

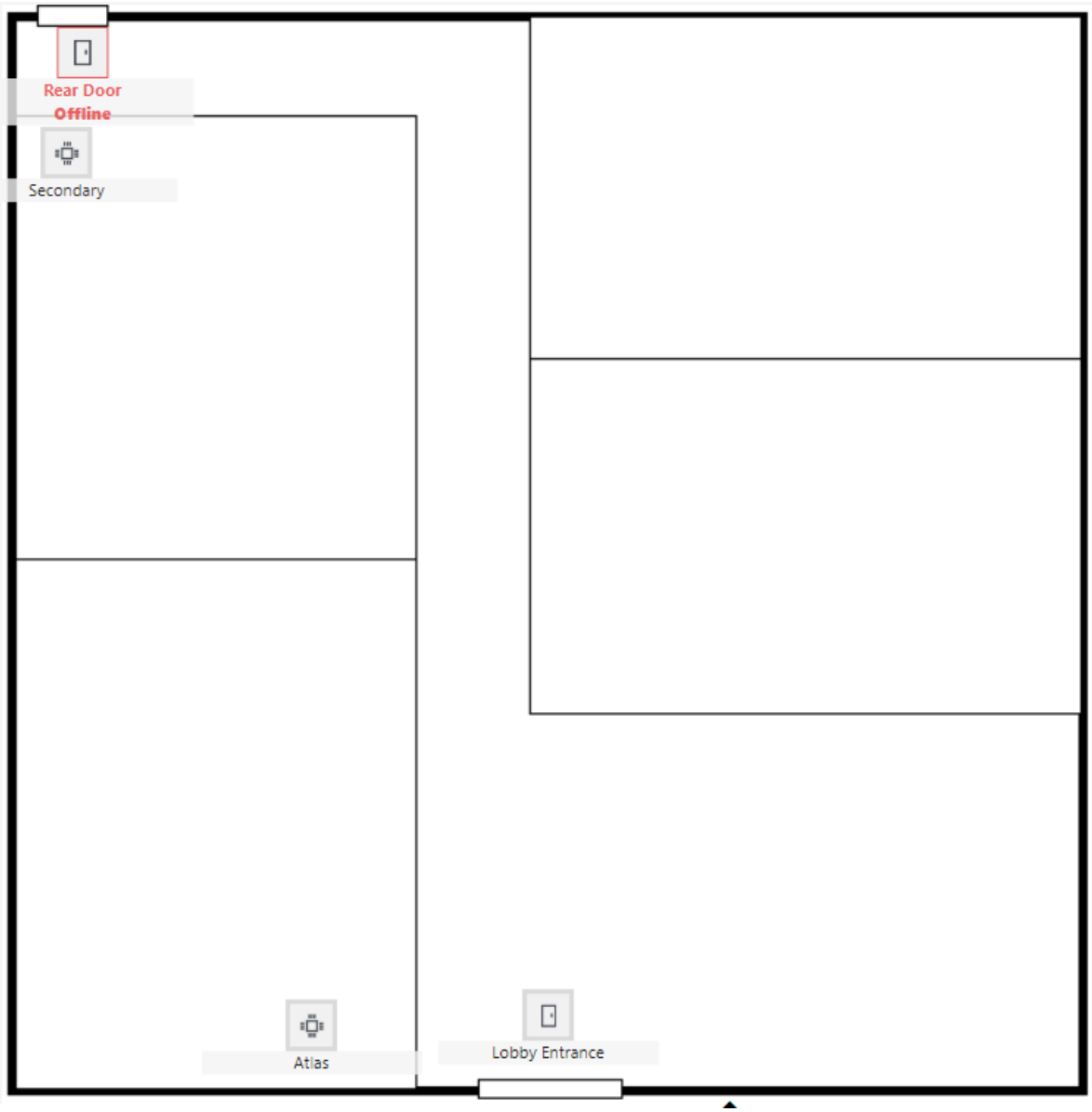
## Argomenti correlati

- Utilizzo delle viste elenco
- Comandi manuali 115

## 2.4 Mappe

La vista Mappe viene utilizzata per mostrare lo stato delle porte e dei controller su sfondi grafici, ad esempio sulle mappe dell'edificio o del campus. Evidenzia tutti i problemi in rosso e consente di inviare comandi alle porte. Le mappe possono anche contenere collegamenti ad altre mappe per facilitare la navigazione.

In questo esempio ci sono due porte e due controller. La "Porta posteriore" è offline e deve essere controllata. Le icone grigie rappresentano il funzionamento normale.




**Fare clic per ingrandire.**

Prima di poterle visualizzare, le mappe devono essere create e configurate nella schermata Mappe (Configurazione). 82 nella schermata Mappe (Configurazione).

## Pulsanti di menu

| | |
|---|---|
| Comandi manuali | Fare clic su una porta per attivare il pulsante Comandi manuali, che consente di impartire comandi quali lo sblocco temporaneo o la modifica della modalità. Vedere Comandi manuali 115. |

| | |
|---|---|
| Zoom In / Zoom Fuori | Ingrandire o rimpicciolire la mappa. Quando si esegue lo zoom, è possibile fare clic e trascinare sulla mappa per visualizzare le diverse aree. |

## Argomenti correlati

- Utilizzo delle viste elenco 42
- Mappe (configurazione) 82
- Comandi manuali 115

## 2.5 Armamento

Il rapporto Muster mostra l'ultima posizione nota degli utenti che *non sono* registrati in un'area sicura. Utilizzare questo rapporto durante l'evacuazione di uno o più edifici o durante un'esercitazione di evacuazione. In questo modo il personale di sicurezza può sapere chi si trova ancora all'interno dell'edificio o degli edifici.

Gli utenti considerati "sicuri" sono

- Gli utenti che sono usciti in Global Out o che si sono presentati ad un Muster Point e
- Utenti che non hanno utilizzato alcuna Porta nelle 24 ore.

I rapporti di raccolta possono includere o meno gli utenti che hanno utilizzato un codice di accesso condiviso o un codice di emergenza.

## Creazione di un punto d'incontro

I punti di raccolta possono essere creati quando si crea un modello di controllore a 1 porta 70 .

1. Vai a Hardware 56 .
2. Selezionare un modello a 1 porta.
3. Per la Configurazione, selezionare un'opzione di fusione, ad esempio **Solo dentro + Punto di fusione**.

È inoltre possibile modificare i controllori a 1 o 2 porte o i punti di iscrizione in punti di raccolta. Ad esempio:

1. Vai a Hardware 56

2. Selezionare un controller a 1 o 2 porte.
3. Trasformare i lettori di riserva in punti di raccolta.

## Generazione di un rapporto di chiamata alle armi

1. Andare a **Muster**. In basso viene visualizzato un elenco dei punti di raccolta esistenti.
2. Selezionare **Elenco per** - **Cognome** o **Area**.
3. Selezionare l'**orientamento** - **Paesaggio** o **Ritratto**.
4. Fare clic su **Genera**.

## Argomenti correlati

- Rapporti e stampa 115
- Hardware 56
- Caratteristiche di emergenza 20

# 2.6 Audit

I rapporti di audit elencano le modifiche alla configurazione e le azioni eseguite dagli utenti dell'applicazione di gestione Web. Questi rapporti consentono di vedere chi ha sbloccato una porta, chi ha dato accesso a un utente, chi ha configurato i livelli di accesso e altre operazioni di sistema.

Quando si genera il rapporto, vengono richieste le seguenti opzioni. Le opzioni variano in base al tipo di audit selezionato. Fare clic su **Genera** per creare il rapporto.

## Opzioni del rapporto

Orientamento Visualizza il rapporto in vista "verticale" o "orizzontale".

Tipo di
- **auditModifica** del database : mostra le modifiche agli elementi del database (utenti, porte, livelli di accesso, ecc.) e consente di filtrare ulteriormente.

opzioni.

- **Comando manuale** - mostra i comandi manuali 115 eseguiti sulle Porte e consente ulteriori opzioni di filtraggio.

**- Qualsiasi/Tutti** - entrambi i precedenti

| | |
|---|---|
| Utente | Se selezionato, il rapporto mostrerà solo le azioni intraprese da un utente specifico. |
| Da / A | Limita il rapporto a un intervallo di date |
| Tipo di modifica | Per la **Modifica del database,** quali tipi di modifiche includere:<br>▪ **Inserito**<br>▪ **Aggiornato**<br>▪ **Soppresso**<br>▪ **Qualsiasi/Tutti** |
| Tipo di oggetto | Per la **modifica del database,** quali tipi di oggetti includere (utente, porta, ecc.). |
| Comando manuale | Per **Comando manuale,** limita il rapporto a un solo tipo di comando. |
| Dispositivo | Per il **comando manuale,** limita il rapporto a una singola porta. |

## Argomenti correlati

- Rapporti e stampa 115
- Utenti 38

- Comandi manuali 115

## 2.7 Storia dell'evento

La Cronologia eventi visualizza un elenco di eventi in base a un filtro e consente l'esportazione in CSV e PDF. Il numero massimo di eventi in questa schermata è limitato solo dal numero di eventi presenti nel database. Per una visualizzazione in tempo reale, vedere Eventi 22 .

### Pulsanti di menu

**Esportazione CSV** Esporta gli eventi visualizzati in un file di dati adatto all'importazione in programmi come Excel. ("CSV" indica il formato di file "valori separati da virgola").

**Esportazione PDF** Salva gli eventi visualizzati come report stampabile in formato PDF.

### Riquadro filtro

Le impostazioni diventano effettive quando si fa clic sul pulsante **Cerca**, nella parte inferiore del pannello. Il
Il pulsante **Reset** cancella tutti i filtri.

**Filtro data e ora**

Mostra solo gli eventi del periodo di tempo specificato.

**Filtri per utenti e dispositivi**

La visualizzazione mostra solo gli eventi che corrispondono a *tutti i* filtri specificati. Si noti che i filtri **Nome** non fanno distinzione tra maiuscole e minuscole e troveranno corrispondenze parziali. Ad esempio, se si immette "john", la visualizzazione mostrerà anche gli eventi per "John" o "Johnny".

**Filtro del tipo di evento**

Il display mostra gli eventi che corrispondono a *uno qualsiasi* dei tipi di evento selezionati. Se non è stato selezionato nulla, vengono visualizzati tutti gli eventi.

# Colonne Eventi

Vedi Eventi 22.

## Archiviazione degli eventi

Gli eventi più vecchi vengono archiviati automaticamente in file CSV sul controllore primario quando si raggiunge il numero massimo. Per scaricare i dati archiviati, vedere Download archivi 107.

Per definire il numero massimo di eventi nel sistema, andare in Impostazioni di sistema e impostare il numero massimo di eventi nel database. e impostare il numero massimo di **eventi nel database**.

## Argomenti correlati

- Utilizzo delle viste elenco
- Rapporti e stampa 115
- Impostazioni di sistema
- Eventi 22

## 2.8 Storia dell'allarme

La Cronologia allarmi visualizza tutti gli allarmi, compresi quelli risolti. Gli allarmi risolti sono nascosti nella schermata Allarmi. Allarmi. Questa visualizzazione non si aggiorna in tempo reale e non consente di riconoscere o risolvere gli allarmi.

## Pulsanti di menu

| | |
|---|---|
| Filtro | Apre un pannello in cui è possibile definire il tipo di allarmi che si desidera visualizzare. |

Le impostazioni diventano effettive quando si fa clic sul pulsante **Cerca**, nella parte inferiore del pannello. Il pulsante **Ripristina cancella** tutti i filtri.

**Filtro data e ora**

Visualizzare gli allarmi da una serie di date e orari.

**Filtri per utenti e dispositivi**

La visualizzazione mostra solo gli eventi che corrispondono a *tutti i* filtri specificati. Si noti che i filtri **Nome** sono sensibili alle maiuscole e alle minuscole. Ad esempio, se si immette "john", la visualizzazione non mostrerà gli eventi relativi a "John".

**Filtro del tipo di evento**

Il display mostra gli allarmi che corrispondono a *uno qualsiasi* dei tipi di evento selezionati. Se non è stato selezionato nulla, vengono visualizzati tutti gli allarmi.

| | |
|---|---|
| Esportazione PDF | Salva gli allarmi visualizzati come rapporto stampabile in formato PDF. |

## Colonne Allarmi

Vedere Allarmi 24 .

## Argomenti correlati

- Utilizzo delle viste elenco 42
- Rapporti e stampa 115
- Allarmi 24
- Trigger di allarme 87
- Caratteristiche di emergenza 20

## 2.9 Rapporto sul livello di accesso degli utenti

Il rapporto sul livello di accesso degli utenti crea un rapporto di tutti gli utenti che hanno un livello di accesso selezionato 48 .

Questo rapporto non comprende i codici di accesso condivisi o codici di emergenza. o i codici di emergenza 48 .

### Argomenti correlati

- Rapporti e stampa 115
- Utenti 38
- Livelli di accesso 48

## 2.10 Rapporto sulla porta utente

Il rapporto sulle porte utente crea un rapporto che mostra quali utenti hanno accesso a una specifica porta. Questo rapporto include le porte assegnate direttamente agli utenti e quelle assegnate tramite un livello di accesso.

Questo rapporto non include i codici di accesso condivisi o i codici di emergenza 48 .

Questo report esclude anche gli utenti senza credenziali (senza carte, PIN o biometria).

### Argomenti correlati

- Rapporti e stampa 115
- Utenti 38

- Livelli di accesso 48

# 3 Controllo degli accessi

Il menu Controllo accesso serve principalmente a determinare chi può aprire le porte, quando e come (schede, PIN e biometria).

È inoltre possibile eseguire attività correlate, come la creazione di utenti per l'applicazione di gestione web e la creazione di pianificazioni della modalità porta 50 .

## Accesso alle porte

Creare utenti 39 per fornire l'accesso alla porta a singoli utenti che utilizzano una credenziale come una tessera, un PIN o un'impronta digitale biometrica. Questo è il metodo di accesso alle porte più comune e consente di tenere traccia di chi va e viene. È possibile dare a ciascun utente un accesso illimitato alle porte, 24 ore su 24, 7 giorni su 7, oppure limitare ulteriormente l'accesso utilizzando le seguenti funzioni.

Impostare gli orari 49 per consentire l'accesso solo in determinati orari, ad esempio durante le ore di lavoro.

Creare livelli di accesso 48 per predefinire una serie di porte e orari che possono essere assegnati rapidamente a più utenti.

Specificare Giorni speciali 51 per limitare l'accesso più del solito in caso di festività, eventi aziendali o altri giorni in cui le regole di accesso dovrebbero essere diverse. I giorni speciali sono utilizzati nelle Pianificazioni.

Creazione di codici di accesso condivisi 46 , che crea codici PIN che chiunque può utilizzare per sbloccare le porte designate.

## Caratteristiche speciali

Le seguenti funzioni sono utilizzate in situazioni speciali:

Codici di emergenza 48 sono codici PIN che sbloccano le porte in caso di emergenza.

Accesso multiutente 52 richiede che più di un utente presenti le credenziali per sbloccare le aree sensibili. Ad esempio, è possibile creare una regola che preveda che tre utenti debbano presentare la propria tessera per aprire una porta.

Orari in modalità porta 50 funzionano come le normali pianificazioni 49 ma vengono utilizzate nella configurazione delle porte 73 per programmare le modifiche della modalità

porta.

## Accesso all'applicazione di gestione web

Gli utenti dell'applicazione di gestione Web vengono aggiunti nella stessa schermata di configurazione degli utenti. nella stessa schermata di configurazione degli utenti. Un utente può avere sia l'accesso alla porta che all'applicazione web.

## 3.1 Utenti

Gli utenti possono essere creati per i seguenti scopi:

- Titolari di carta che possono accedere a Doors.
- Utenti che possono accedere all'applicazione di gestione web.

Un singolo utente può avere accesso sia alla porta che all'applicazione.

### Pulsanti di menu

| | |
|---|---|
| Filtro | Visualizza un pannello sopra l'elenco in cui è possibile cercare un utente in base a diverse proprietà. Gli utenti vengono visualizzati se corrispondono a *tutti i* filtri.<br><br>Le impostazioni diventano effettive quando si fa clic sul pulsante **Cerca**, nella parte inferiore del pannello. Il pulsante **Ripristina cancella** tutti i filtri. |
| Importazione | Vedere Importazione di utenti da un file CSV 45 . |
| Perdono | Azzera lo stato di anti-passback dell'utente selezionato. Si usa quando le regole anti-passback impediscono l'accesso di un utente e occorre annullarle. |

### Proprietà chiave

Per l'elenco completo e maggiori dettagli, vedere Proprietà dell'utente. 40

Nome e Cognome

Nome e cognome dell'utente. Entrambi richiesti, massimo 32 caratteri ciascuno.

Foto su una scheda 45

Una foto dell'utente. Questa viene mostrata qui e può essere stampata . Per aggiungere o modificare la foto, fare clic sull'immagine della foto e selezionare un'immagine dal computer. I formati immagine supportati sono PNG, JPEG e GIF.

Ruolo

**Titolare della carta Solo** per il titolare della carta. Gli altri ruoli consentono di accedere all'applicazione di gestione Web. Ogni ruolo fornisce un diverso livello di accesso; vedere Ruoli utente 92 . Gli utenti che hanno la possibilità di accedere possono avere anche l'accesso alla Porta.

Nome utente e Password

Se il **ruolo** non è **Solo titolare di carta**, si tratta del nome utente/password utilizzato per accedere all'applicazione web.

Carte

Aggiungere un numero qualsiasi di tessere da utilizzare per l'accesso. È possibile utilizzare un punto di registrazione della carta per aggiungere un numero di tessera.

L'aggiunta di una scheda non fornisce l'accesso; all'utente dovranno essere assegnati anche i Livelli di accesso o le Porte, come indicato di seguito.

Impronte digitali

Mostra se l'utente ha delle impronte digitali registrate e ne consente la registrazione. (Le impronte digitali sono disponibili solo se il controller primario supporta la biometria).

PIN

PIN (Personal Identification Number) dell'utente, solo numerico. Fare clic su **Crea nuovo** per generare un PIN casuale e unico. La lunghezza deve corrispondere a quella del PIN definito in Impostazioni di sistema 100. (Il valore predefinito è di 4 caratteri).

Livelli di accesso, accesso alla porta

48

- Aggiungere i livelli di accesso che sono stati definiti, e/o
- Aggiungere voci di **accesso alla porta** per personalizzare l'accesso di questo utente.

Design della carta Utilizzare per stampare i biglietti 45 .

## Argomenti correlati

- Utilizzo delle viste delle proprietà 44
- Proprietà dell'utente 40
- Ruoli utente 92
- Costrizione 144
- Livelli di accesso 98
- Anti-Passback 118
- Stampa di carte 45

### 3.1.1 Proprietà dell'utente

Le proprietà disponibili nella schermata Utenti 38 sono le seguenti :

## Identità

| | |
|---|---|
| Stato | Visualizza se lo stato dell'utente corrente è **Valido** o **Invalido**. Lo stato sarà **Invalido** se la data corrente non rientra nell'intervallo e **Valido a, o se** è selezionata l'opzione **Disattiva utente**. |
| Nome e Cognome | Nome e cognome dell'utente. Entrambi richiesti, massimo 32 caratteri ciascuno. |
| Foto | Una foto dell'utente. Questa è mostrata qui e può essere stampata su un cartoncino 45 . Per aggiungere o modificare la foto, fare clic sull'immagine della foto e selezionare un'immagine dal computer. I formati immagine supportati sono PNG, JPEG e GIF. |

Identificatore univoco IDA del personale , ad esempio l'ID del dipendente. Massimo 32 caratteri

Ruolo **Titolare della carta Solo** per il titolare della carta. Per gli utenti che hanno la possibilità di accedere, selezionare un altro ruolo. Vedere Ruoli utente 92 . Gli utenti che hanno la possibilità di accedere possono anche avere delle carte.

Gruppo di utenti 87 Selezionare un gruppo di utenti che verrà utilizzato quando si applica la funzione Multi-Utente. Regole di accesso 52 . Viene utilizzato se più utenti devono presentare le proprie credenziali per aprire una Porta.

Nome utente Se il **ruolo** non è **Solo titolare di carta**, questo è il nome utente utilizzato per accedere all'applicazione web.

Password Se il **ruolo** non è **Solo titolare di carta**, questa è la password utilizzata per accedere all'applicazione web.

Lingua La lingua preferita dall'utente, che sarà

- visualizzati sui lettori di schede che supportano più lingue (come alcuni lettori OSDP), e
- la lingua predefinita dell'utente nell'applicazione di gestione web. Le lingue disponibili dipendono dalla licenza del software 15 . Contattare il rappresentante autorizzato ZKTeco per l'aggiornamento della licenza.

Valido da La data di inizio dell'accesso. L'impostazione predefinita è la data corrente. Questo vale sia per l'accesso alla porta che per l'accesso all'applicazione di gestione web.

Fino a nuovo avviso, valido A

Se l'opzione **Fino a nuovo avviso** è selezionata, l'accesso dell'utente non scade mai. Se è deselezionata, è necessario fornire la data di **validità**, che determina la scadenza dell'accesso dell'utente. Questo vale sia per l'accesso alla porta che per l'accesso all'applicazione di gestione web.

| | |
|---|---|
| Disabilita utente | Se selezionata, l'accesso dell'utente è disabilitato. Questo vale sia per l'accesso alla porta che per l'accesso all'applicazione di gestione web. |
| Vacanza da, vacanza a | Se viene inserito questo intervallo di date, si tratta di un intervallo di date di ferie durante il quale l'accesso alla porta dell'utente è sospeso. L'accesso all'applicazione di gestione web non è influenzato dalle date di ferie. |

## Informazioni aggiuntive

| | |
|---|---|
| Indirizzo di posta elettronica | L'indirizzo e-mail dell'utente. È necessario affinché l'utente possa ricevere le e-mail del sistema, come le notifiche. |
| Telefono cellulare | Il numero di cellulare dell'utente. |
| Personalizzati | 1-4Campi personalizzati corrispondenti a quelli configurati in Impostazioni di sistema 100. |

## Accesso

| | |
|---|---|
| Schede | Fare clic su **Aggiungi** per aggiungere i numeri di scheda per l'accesso alla porta. Fare clic su **Abilitato** per abilitare o disabilitare una tessera. Per inserire un numero di tessera strisciando la tessera, vedere Punti di registrazione della tessera 117. |
| Impronte digitali | Mostra se l'utente ha delle impronte digitali registrate e consente di registrarle.<br><br>La registrazione delle impronte digitali richiede un lettore di |

impronte USB ZKTeco e il relativo software Fingerprint Driver (disponibile alla pagina Download di ZKTecoUSA.com).

PIN Il PIN (Personal Identification Number) utilizzato per l'accesso alla porta. Solo numerico. La lunghezza deve corrispondere a quella del PIN definito nelle Impostazioni di sistema (l'impostazione predefinita è di 4 caratteri).

- I numeri PIN devono essere univoci, compresi i codici **PIN di emergenza**, condivisi e non modificati. Codici di accesso 46 , e Codici di accesso di emergenza 48 .
- Fare clic su **Crea nuovo** per generare un numero PIN univoco e casuale.
- Fare clic su **Cancella** per cancellare il PIN.

PIN di emergenza Il PIN di emergenza genera un evento di accesso di emergenza quando viene utilizzato al posto del PIN normale. L'accesso è comunque consentito se sono soddisfatte tutte le altre condizioni di accesso normali. Per maggiori dettagli, vedere per maggiori dettagli. Per il **tipo di PIN Duress**:

- Selezionare **Nessuno** se il PIN Duress non viene utilizzato.
- Selezionare **Aggiungi 1 all'ultima cifra** per aggiungere una cifra solo all'ultima cifra del PIN normale. Ad esempio, un PIN normale di 1111 avrà un PIN di coercizione di 1112 e un PIN normale di 9999 avrà un PIN di coercizione di 9990.
- Selezionare **Esplicito** per inserire un PIN di costrizione specifico per questo utente. Solo numerico. La lunghezza deve corrispondere alla lunghezza del PIN definita in Impostazioni di sistema. (l'impostazione predefinita è di 4 caratteri).

Utilizzare orari di apertura prolungati Se l'opzione è selezionata, i tempi di sblocco e di mantenimento della porta vengono utilizzati quando l'utente è autorizzato ad accedere. Questo serve agli utenti che necessitano di un tempo supplementare per attraversare una porta, ad esempio le persone disabili. La quantità di tempo supplementare è impostata su ciascuna porta 75 .

| | |
|---|---|
| Anti-passback Esente | Se l'opzione è selezionata, l'utente non è soggetto alle regole anti-passback. regole anti-passback. |

| | |
|---|---|
| Porte di accesso in Nessun accesso Modalità | Se questa opzione è selezionata, l'utente può accedere alle porte in modalità di non accesso. Questa modalità è tipicamente riservata agli amministratori e al personale di sicurezza. |
| Porte di accesso in Blocco Modalità | Se questa opzione è selezionata, l'utente può accedere alle porte in modalità di blocco. in modalità di blocco. In genere, questa opzione è riservata agli amministratori e al personale di sicurezza. |
| Livelli di accesso | Livelli di accesso 48 assegnati all'utente per l'accesso alla porta. |
| Accesso alla portaAutorizza | l'utente ad accedere a singole porte durante la programmazione selezionata. Questo si aggiunge ai **livelli di accesso** assegnati. |

## Design della carta

| | |
|---|---|
| Design della carta | Selezionare un disegno del biglietto 83 . Se selezionato, viene visualizzata un'anteprima.<br>Fare clic su Stampa scheda 145 per stampare. Quando si stampa, se il numero della tessera fa parte del disegno, è necessario selezionare il numero della tessera.<br>Fare clic su **Stampa ricevuta** se la carta viene stampata in un luogo remoto e il destinatario deve andare a ritirarla. |

## Argomenti correlati

- Ruoli utente 92
- Gruppi di utenti 87
- Punti di iscrizione alla carta 141

- Livelli di accesso 48

- Stampa di carte 45

### 3.1.2 Stampa di carte

È possibile stampare su una stampante specializzata che scrive carte d'identità. È inoltre possibile stampare una ricevuta cartacea da utilizzare come registrazione o per autorizzare il ritiro presso una stampante remota.

Per fare una delle due cose, è necessario creare

prima dei progetti di schede 83 . Per stampare,

selezionare un utente e:

1. Selezionare il design di un biglietto. (La scelta verrà salvata per questo utente).
2. Fare clic su **Stampa tessera** o **Stampa ricevuta.**
3. Selezionare un numero di carta dall'elenco.
4. Fare clic su **Stampa** e seguire le istruzioni.

Per completare le richieste, vedere Rapporti e stampa 115.

## Argomenti correlati

- Utenti 38
- Disegni di carte 83
- Rapporti e stampa 115

### 3.1.3 Importare gli utenti da un file CSV

Un file CSV (comma-separated value) può essere aggiunto da un numero qualsiasi di Utenti utilizzando i dati di un altro programma. L'altro programma deve essere in grado di esportare in CSV o in un formato convertibile in CSV. Il CSV stesso deve essere modificato in modo da corrispondere esattamente al formato di importazione di Atlas Series utilizzando un software come un editor di fogli di calcolo.

Nella schermata Utenti è possibile visualizzare la schermata

1. Fare clic su **Importa.**
2. Fare clic sul link per scaricare un file modello che include un esempio del formato dei dati richiesto.

Nel proprio software:

3. Aprite il file e leggete le istruzioni incluse.
4. Creare una copia del file.
5. Modificare il file con i dati degli utenti che si desidera creare.
6. Salvare il file in formato CSV.
   a. Assicurarsi che il file sia in testo normale e non includa caratteri aggiuntivi o codifiche.
   b. Ad esempio, se si utilizzano caratteri non ASCII, il file deve essere codificato come

UTF-8. Nella schermata Utenti è possibile accedere alla schermata Utenti:

7. Fare clic su **Importa.**
8. Nella finestra di dialogo, fare clic su **Importa**.
9. Selezionare il file dal computer. Il file deve avere l'estensione ".csv".
10. Fare clic su **Sì** per verificare e importare il file.
11. Viene visualizzato il numero di utenti importati. Fare clic su **OK** per visualizzare gli utenti appena importati.

## Argomenti correlati

- Utenti 38
- Proprietà dell'utente 40

## 3.2 Codici di accesso condivisi

Un codice di accesso condiviso è un PIN che più persone possono utilizzare per accedere a determinate porte.

Questi codici funzionano solo se la modalità porta corrente consente a un PIN di aprire la porta. Ad esempio, solo PIN o qualsiasi modalità che indichi "o PIN", come "Carta o PIN".

I codici di accesso condivisi non funzionano con:

- Porte in modalità solo carta, carta e PIN, ecc.
- Porte con regole di accesso per più utenti (perché un gruppo di utenti non può essere assegnato a un codice di accesso condiviso).

I codici di accesso condivisi sono sempre esenti dall'anti-passback.

L'uso dei codici di accesso condivisi influisce sull'accuratezza di un rapporto rapporto Muster.

## Proprietà del codice di accesso condiviso

| | |
|---|---|
| Nome | Richiesto. Massimo 32 caratteri. |
| PIN | Il codice di accesso condiviso stesso. Solo numerico. Fare clic su **Crea nuovo** per generare un codice unico e casuale. |
| Abilitato | Selezionato per attivare, deselezionato per disattivare |
| Descrizione | Descrizione o commenti |
| Diritti di accesso | - Aggiungere livelli di accesso, e/o aggiungere voci di accesso alla porta per assegnare direttamente le coppie porta/schedario per l'accesso. |

## Argomenti correlati

- Utilizzo delle viste delle proprietà
- Codici di emergenza
- Livelli di accesso

## 3.3 Codici di emergenza

Un codice di emergenza è un PIN che consente l'accesso alle porte indipendentemente da altre impostazioni, compresa la modalità porta. (Confronta con i Codici di accesso condivisi 46 ). È destinato a essere utilizzato dal personale di emergenza e di sicurezza per ottenere l'accesso in situazioni di emergenza.

Ciò significa che un codice di emergenza può accedere a una porta in stato di blocco 111 .

L'uso corretto di un codice di emergenza genera un evento di presentazione del codice di emergenza.

L'evento Codice di emergenza presentato è configurato come un trigger di allarme 87 per impostazione predefinita, generando un allarme 24 . L'evento Codice di emergenza presentato può essere utilizzato anche come collegamento per attivare un'uscita ausiliaria nella schermata Hardware. 61 sullo schermo.

I codici di emergenza sono esenti dal sistema anti-passback e dall'accesso multiutente. 85 e dall'accesso multiutente 52 .(Confronta ai codici di accesso condivisi 46 .)

I codici di emergenza hanno le stesse proprietà dei codici di accesso condivisi. 46 .

L'uso dei codici di emergenza influisce sull'accuratezza di un rapporto 90 per il personale di emergenza che li utilizza.

### Argomenti correlati

- Utilizzo delle viste 14
- delle proprietà
- Codici di accesso 46
- condivisi
- Livelli di accesso 48
- Caratteristiche di 20
- emergenza

## 3.4 Livelli di accesso

Un livello di accesso è un elenco predefinito di porte abbinato agli orari in cui è consentito l'accesso per ciascuna porta. Quando si modifica un livello di accesso, la nuova definizione si applica immediatamente a ogni utente o codice assegnato a quel livello di accesso.

I livelli di accesso possono essere applicati agli utenti 38, Codici di accesso condivisi 46, e Emergenza Codici 48. In ognuna di queste schermate è possibile applicare uno o più Livelli di accesso, e si può fornire un accesso personalizzato alle singole coppie porta/schedario.

## Utilizzo dello schermo

Fare clic sui pulsanti **Aggiungi** e **Rimuovi** per aggiungere e rimuovere porte dall'elenco. Utilizzare i **pulsanti ellissi** (...) per modificare le porte e gli orari selezionati.

È possibile includere la stessa porta più volte con orari diversi. L'accesso a una determinata porta sarà consentito durante tutte le pianificazioni ad essa associate.

## Argomenti correlati

- Utilizzo delle viste delle proprietà 44
- Orari 49
- Utenti 38
- Codici di accesso condivisi 46
- Codici di emergenza 48

# 3.5 Orari

Le pianificazioni vengono utilizzate per limitare l'accesso a determinati giorni e orari. Possono essere utilizzati nei Livelli di accesso e ovunque sia assegnato l'accesso alla porta.

Per impostazione predefinita, l'accesso *non è* consentito nei giorni speciali 51 .

La programmazione integrata "24/7" consente l'accesso in qualsiasi momento, *compresi i* giorni speciali.

## Utilizzo dello schermo

L'accesso sarà consentito per tutti i periodi di tempo creati. Fare clic sul pulsante **Aggiungi** e **rimuovi**
per aggiungere e rimuovere periodi di tempo dall'elenco.

| | |
|---|---|
| Tempi (inizio - Stop) | La barra di sinistra mostra in verde il periodo di tempo in cui è consentito l'accesso. È possibile trascinare le estremità della barra verde per modificare l'intervallo di tempo. È inoltre possibile inserire gli orari esatti desiderati nelle caselle |

sotto la barra. Ogni barra può avere un solo intervallo di tempo; per avere due intervalli di tempo negli stessi giorni, aggiungere un'altra voce. Il pulsante **Tutto il giorno** è utile per azzerare la barra.

Giorni — La barra centrale mostra in verde i giorni in cui è consentito l'accesso. È possibile fare clic su ciascun giorno per cambiare l'accesso, oppure utilizzare i pulsanti di scelta rapida per modificare la selezione corrente. I pulsanti di scelta sono **Giorni feriali**, **Tutti i giorni** e **Fine settimana**.

Giorni speciali — La barra di destra appare verde se sono stati inclusi dei giorni speciali per quel periodo. Fare clic sulla barra per selezionare i giorni speciali da includere. Nella schermata di selezione dei giorni speciali, è possibile selezionare uno o più tipi di giorni speciali.

L'accesso è normalmente negato nei giorni speciali. L'accesso sarà consentito se si includono i giorni speciali nella pianificazione. Per maggiori informazioni informazioni, vedere Giorni speciali 51.

## Argomenti correlati

- Utilizzo delle viste delle proprietà 44
- Giorni speciali 51

## 3.6 Orari della modalità porta

Le pianificazioni della modalità porta vengono utilizzate per cambiare la modalità delle porte in momenti diversi. Ad esempio, sono comunemente utilizzati per sbloccare

automaticamente le porte pubbliche durante l'orario di lavoro.

Vedere Modalità porta per un elenco delle possibili modalità della porta.

Le pianificazioni della modalità porta sono assegnate alle porte nella schermata Porte.
nella schermata Porte.

Una programmazione della modalità porta può avere più intervalli di tempo con diverse modalità associate. Si noti che le modalità porta di emergenza non possono essere programmate.

## Utilizzo dello schermo

Fare clic sui pulsanti **Aggiungi** e **Rimuovi** per aggiungere e rimuovere periodi di tempo dall'elenco.

Nella colonna di sinistra, selezionare una singola modalità della porta. Una porta passerà automaticamente a questa modalità durante il periodo di tempo definito.

I periodi di tempo sono definiti come per le Pianificazioni. Vedere Orari 49 .

## Argomenti correlati

- Utilizzo delle viste delle proprietà
- Modalità della porta
- Giorni speciali
- Orari

# 3.7 Giorni speciali

I Giorni speciali sono singoli giorni di calendario (come il 5 maggio) in cui l'accesso è negato per impostazione predefinita, anche se normalmente sarebbe consentito da una Pianificazione 49 . Possono essere aggiunti alle Pianificazioni in modo che alcuni utenti abbiano accesso in quei giorni.

I giorni speciali sono utilizzati per le vacanze, gli eventi aziendali e altri casi in cui non si desidera che venga concesso l'accesso abituale. Ad esempio, si possono utilizzare le pianificazioni della modalità porta per sbloccare automaticamente le porte durante l'orario di lavoro dal lunedì al venerdì, ma non si desidera farlo nei giorni festivi.

Si noti che l'orario speciale "24/7" consente l'accesso in qualsiasi momento e non è influenzato dai giorni speciali.

# Tipi di giornate speciali

I giorni speciali sono raggruppati in una serie di tipi di giorni speciali. Un tipo è essenzialmente un calendario. Ad esempio, un tipo potrebbe includere tutte le festività governative, mentre un altro potrebbe riguardare i giorni lavorativi degli insegnanti. È possibile impostare regole di accesso diverse per i vari calendari.

Solo i tipi di giorni speciali possono essere aggiunti a una pianificazione. Pertanto, è possibile aggiungere l'accesso a tutti i giorni festivi, ma non a uno solo di essi, a meno che non si crei un tipo con un solo giorno.

## Utilizzo dello schermo

Nella prima sezione, **Tipi di giorni speciali**, è possibile cambiare il nome dei tipi in qualcosa di utile, come "Giorni festivi" o "Giorni lavorativi degli insegnanti". È inoltre possibile modificare il colore assegnato a ciascun tipo. Il colore non ha effetto se non in questa schermata.

La seconda sezione, **Giorni speciali**, mostra un calendario che evidenzia tutti i giorni speciali di ogni tipo nel loro colore. Per aggiungere o rimuovere un giorno, fare clic su di esso.

Le due opzioni sopra il calendario modificano ciò che accade quando si fa clic su un giorno. Non possono modificare le proprietà dei giorni speciali correnti.

- **Selezionare Tipo di giorno speciale: i** giorni aggiunti al calendario saranno di questo tipo. Non è possibile aggiungere giorni se non è selezionato alcun tipo.
- **Imposta come ripetitivo:** se si seleziona, i giorni aggiunti al calendario saranno ripetitivi. Ciò significa che si verificheranno ogni anno alla stessa data del calendario. Vengono visualizzati con una piccola "R" e sono visibili in ogni anno.

Si noti che un singolo giorno può essere un solo tipo di giorno speciale.

## Argomenti correlati

- Orari 49
- Orari della modalità porta 50

# 3.8 Accesso multiutente

L'accesso multiutente viene utilizzato per richiedere a più utenti di presentare le proprie

credenziali per aprire una porta. Questo è spesso utilizzato per le aree ad alta sicurezza. Ad esempio, un'area potrebbe richiedere due

dirigenti e una guardia giurata per presentare le proprie credenziali. Le credenziali che possono presentare sono quelle richieste dall'attuale modalità della porta.

Codici di accesso condivisi 146 non possono accedere a porte con regole di accesso multiutente 148 in vigore. I codici di emergenza sono esenti dalle regole di accesso multiutente.

## Utilizzo dello schermo

È necessario creare prima uno o più gruppi di utenti 87 i cui membri possono collaborare per accedere a una porta specifica.

Fare clic sui pulsanti **Aggiungi** e **Rimuovi** per aggiungere e rimuovere i **gruppi di utenti** dall'elenco delle **regole**. Se vengono create più regole, tutte devono essere soddisfatte affinché l'accesso sia concesso. Se non ci sono **regole** in una specifica definizione di Accesso multiutente, le porte associate si comporteranno come se non avessero restrizioni di Accesso multiutente.

Applicare la regola Accesso multiutente nella schermata Porte 73 .

## Argomenti correlati

- Utilizzo delle viste delle proprietà 94
- Gruppi di utenti 87
- Porte 73

# 4 Configurazione

Utilizzare il menu Configurazione per:

- Collegare e configurare hardware e porte.
- Organizzate il vostro hardware in posizioni e aree e tracciatelo su Maps.
- Configurare le impostazioni generali per il Monitor 21 e Controllo accesso 37 92 e il controllo degli accessi.

Gli utenti con il ruolo di amministrazione del sistema possono aggiungere e configurare controller e porte. Gli utenti della gestione del controllo accessi possono configurare solo le porte. Gli altri ruoli utente integrati non possono fare nessuna delle due cose.

Vedere Amministrazione 92 per configurare le impostazioni del sistema, come l'ora o la connessione di rete.

## Configurazione di hardware e porte

Prima di eseguire qualsiasi configurazione, è importante leggere il breve argomento "Comprensione del sistema". Controllori e porte 55 . È particolarmente utile per qualsiasi applicazione di gestione web L'utente deve comprendere la definizione di "porta" nel software della serie Atlas.

L'hardware 56 È il luogo in cui vengono aggiunte e configurate le apparecchiature fisiche (controllori e relativi lettori, ingressi e uscite). La configurazione dell'hardware viene solitamente eseguita da un esperto che installa il sistema.

La configurazione della porta 178 è il punto di partenza di tutto il controllo degli accessi. Soprattutto, è il punto in cui si specifica se e quando le porte sono bloccate e come possono essere aperte. Tutte le impostazioni del Controllo accessi 37 sono influenzate dalla configurazione della porta.

Modelli di ferramenta 90 e modelli di porta 88 possono essere utilizzati per configurare rapidamente più subcontroller (I/O) o porte con le stesse impostazioni.

## Organizzare l'hardware

Le posizioni 79 sono etichette che possono essere applicate a porte, controllori, mappe e altri

elementi.

Le posizioni vengono visualizzate in Eventi 24 e Allarmi 22.

Aree 80 sono utilizzate con anti-passback 81 e le camere di compensazione. Definiscono le regioni fisiche in cui è possibile limitare l'accesso 79 utilizzando tali funzioni. Anche il rapporto Muster si basa anche sulle aree per determinare se ogni utente si trova in un'area sicura e conosciuta (Muster o Global Out).

È inoltre possibile creare mappe 82 degli edifici e del campus. Monitorate queste mappe per osservare lo stato in tempo reale di porte e controllori su una mappa reale della vostra struttura.

## Impostazioni generali

Disegni di biglietti 183 consente di creare i layout di stampa per la stampa dei biglietti 45 .

Formati delle carte 85 definire il tipo o la marca di schede da utilizzare. Il sistema Atlas Series include tutti i formati di tessera di cui probabilmente avrete bisogno. Utilizzare questa schermata per creare un formato per un tipo di tessera insolito o per inserire un "codice struttura" come indicato dal fornitore della tessera.

Creare gruppi di utenti 87 da utilizzare con l'accesso multiutente 52 .

Impostare i trigger di allarme 147 per definire quali eventi attivano gli allarmi 24 .

# 4.1 Comprendere i controllori e le porte

## Controllori

Ogni sistema comprende un controllore primario. È quello a cui si accede con il browser web per gestire o monitorare l'intero sistema. Mantiene tutti i dati e la configurazione e dirige tutti i controllori secondari.

I controller secondari vengono aggiunti per gestire altre porte. Ricevono la configurazione dal controller primario. Tuttavia, conservano una copia dei dati, per cui continuano a funzionare anche se il primario non è in linea. È possibile accedere direttamente a un Controllore secondario tramite un link nella sua pagina Hardware, ma solo per modificare alcuni valori locali, come le impostazioni di rete.

**Importante:** il controllore primario deve supportare la biometria se nel sistema viene utilizzato un controllore biometrico.

## Subcontrollori (I/O)

Ogni controllore ha un sottocontrollore incorporato (I/O). È visualizzato sotto il Controllore nell'Hardware con l'etichetta aggiuntiva "I/O", che significa "input/ouput". Il Sottocontrollore gestisce i dettagli avanzati dei lettori, degli ingressi e delle uscite dell'hardware.

## Porte

Ogni tessera, PIN e lettore biometrico del sistema è rappresentato come una porta, anche se per alcuni non si tratta affatto di porte! Una porta nell'applicazione di gestione Web può rappresentare una delle tante cose:

- Una porta reale, fisica, che può essere aperta
- Un secondo lettore che consente l'uscita attraverso una porta fisica. Si noti che ciò significa che una porta fisica In/Out 57 è rappresentata da due porte, una per "In" e una per "Out".
- Qualcosa che funziona come una porta fisica, come un tornello o un cancello di garage.
- Un lettore da solo, senza porta fisica, utilizzato come punto di raccolta 91 o punto di registrazione delle carte. 72 o punto di registrazione delle tessere

Le porte vengono create nella schermata Hardware 56 automaticamente quando viene creato il controllore, oppure personalizzando il controllore. 60 il Controllore.

## Argomenti correlati

- Hardware 56
- Porte 73

# 4.2 Hardware

L'hardware rappresenta i controllori del sistema e tutti i loro collegamenti fisici a lettori, serrature, contatti della porta e altri ingressi e uscite. Qui si configurano i collegamenti elettrici e le impostazioni dei controllori. Il comportamento delle porte, come la modalità o i tempi di apertura, sono configurati in Porte 73 .

# Argomenti hardware

## Argomenti correlati



### 4.2.1 Modelli e configurazioni

## Modelli della serie Atlas

| Modello | Tipo | Porte Wiegand | RS-485 Slot macchine | Numero di porte "in" | Max "Secondary" Porte | Tipo di lettore predefinito | Tipo predefinito per i lettori secondari |
|---|---|---|---|---|---|---|---|
| Atlante 100 | 1 Porta | 2 | 2 OSDP | 1 | 1 | Wiegand | Wiegand |
| Atlante 200 | 2 Porta | 4 | 4 OSDP | 2 | 2 | Wiegand | Wiegand |
| Atlante 400 | 4 Porte | 4 | 4 OSDP | 4 | 4 | Wiegand | OSDP |
| Atlante 160 | 1 porta biometrica | 2 | 2 OSDP **O** 2 ZKTeco | 1 | 1 | ZKTeco RS-485 | ZKTeco RS-485 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | RS-485 | | | | |
| Atlante 260 | Biometrico a 2 porte | 4 | 4 OSDP **O** | 2 | 2 | ZKTeco RS-485 | ZKTeco RS-485 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | 4<br>ZKTeco<br>RS-485 | | | | |
| Atlante 460 | Biometrico a 4 porte | 4 | 8 OSDP<br>**O**<br>8<br>ZKTeco<br>RS-485 | 4 | 4 | ZKTeco RS-485 | ZKTeco RS-485 |

**Importante:** il controllore primario deve supportare la biometria se nel sistema viene utilizzato un controllore biometrico.

Le porte "In" vengono create automaticamente e sono permanenti, anche se non devono essere utilizzate.

Le porte secondarie sono porte di uscita, punti di registrazione delle tessere e punti di raccolta. I lettori delle porte secondarie sono sempre abbinati ai lettori delle porte interne in un modo definito.

| Tipo di controllore | "Accoppiamenti tra lettori "interni" e "secondari |
|---|---|
| 1 porta | Da 1 a 2 |
| 2 porte | Da 1 a 3<br>Da 2 a 4 |
| 4 porte | Da 1 a 5<br>Da 2 a 6<br>Da 3 a 7<br>Da 4 a 8 |

Ad esempio, in un controller a 4 porte, la porta 2 utilizza sempre il lettore #2 ed è una porta di ingresso. Se ha una porta "Out", quella porta utilizzerà sempre il lettore #6.

Il numero del lettore non corrisponde necessariamente al suo indirizzo. Per il Wiegand, il numero del lettore *è lo* stesso delle etichette sull'hardware, ma qualsiasi lettore può

essere modificato per utilizzare qualsiasi indirizzo RS-485 disponibile.

Si noti che i controller a 4 porte hanno porte di lettura Wiegand sufficienti solo per le porte "In". Eventuali porte secondarie devono utilizzare l'RS-485.

## Proprietà di configurazione

La proprietà Configuration di un controllore determina lo scopo delle porte del controllore: autorizzare l'ingresso della porta, forse l'uscita della porta o come lettori per scopi speciali.

Le opzioni di configurazione disponibili dipendono dal modello di controllore. Ogni opzione comporta una o più delle seguenti possibilità. Ogni possibilità determina la funzione dei lettori di schede, PIN o biometrici collegati al Controllore.

| | |
|---|---|
| In | OnlyThis è la configurazione più comune, in cui si utilizza un lettore per entrare, ma non sono necessarie credenziali per uscire (anche se può essere configurato un pulsante di uscita per aprire la porta dall'interno). |
| Entrata/Uscita | La porta fisica avrà un lettore sia all'interno che all'esterno. L'autorizzazione è necessaria per passare in entrambe le direzioni. |
| + Punto d'incontroll | secondo lettore servirà come punto d'incontro 30 , dove gli utenti potranno registrare di aver raggiunto un luogo sicuro. |
| + Iscrizione alla carta Punto | Il secondo lettore verrà utilizzato per inserire facilmente i numeri di tessera quando si aggiungono gli utenti. Vedere Punti di registrazione della carta 117 . |

Le opzioni disponibili non coprono tutte le possibilità. Ad esempio, i controllori a 2 e 4 porte non offrono punti d'incontro o punti di registrazione come configurazioni standard. Per adattare la configurazione alle proprie esigenze, vedere Modifica della configurazione del controllore 60 . La modifica potrebbe essere più semplice se si inizia con "Solo ingresso" come base.

## Argomenti correlati

- Aggiunta di controllori

- Modifica della configurazione del controllore 60

### 4.2.2 Modifica della configurazione del controllore

Il pulsante "Modifica" sulla barra dei menu serve a personalizzare la proprietà 57 Configurazione di un controllore. Per personalizzare efficacemente una configurazione 57, è necessario conoscere i modelli e la configurazione.

Facendo clic su "Modifica" viene visualizzato un elenco di opzioni. Alcune opzioni saranno disabilitate se non possono essere applicate al Controllore così come è attualmente configurato il suo lettore.

Tutte le opzioni presentano una finestra di dialogo che consente di inserire le specifiche della modifica. Le opzioni sono:

| | |
|---|---|
| Passare a Entrata/uscita | Selezionare il numero della **porta** "In" a cui sarà abbinata una porta "Out". |
| Aggiungi Muster Punto | Inserire un **nome** per la nuova porta e selezionare il numero della **porta** "In" a cui abbinarla. |
| Aggiungere l'iscrizione alla carta Punto | Inserire un **nome** per la nuova porta e selezionare il numero della **porta** "In" a cui abbinarla. |
| Rimuovere le funzioni secondarie, di raduno o di Iscrizione alla carta Punto | |

Selezionare il numero della **porta** "In" che verrà rimossa dalla porta abbinata.

## Argomenti correlati

- Modelli e configurazione 57

### 4.2.3 Proprietà dell'hardware

Il corpo della schermata Hardware consente la configurazione del controllore e visualizza i dati relativi al controllore. Ogni controllore è rappresentato da due componenti: (1) il Controllore stesso per la configurazione generale e (2) un Sottocontrollore (I/O) per le impostazioni dettagliate di lettori, serrature, contatti della porta e altri ingressi e uscite.

I subcontrollori possono essere configurati in base a un gruppo di impostazioni salvate utilizzando i modelli di hardware 90 .

I comportamenti delle porte, come le modalità e gli orari di apertura, sono configurati in Porte 73 .

## Proprietà del controllore

| | |
|---|---|
| Nome | Il nome del controllore. Richiesto, massimo 32 caratteri. |
| Modello | Il modello del controllore. |
| Indirizzo IP | (solo controller secondari) Indirizzo IP o nome host del controller. |
| Porta | (solo controller secondari) Numero di porta del controller. |
| Disconnesso | Se questa opzione è selezionata, il Controllore secondario viene trattato come se non esistesse e la comunicazione non è consentita. Questa opzione non può essere selezionata sul controllore primario.<br><br>Può essere utile durante l'installazione dell'hardware. |
| Stato | Visualizza lo stato attuale del dispositivo, compreso Online/Offline. Se sono presenti problemi di manomissione, di alimentazione o di batteria, questi vengono visualizzati come |

indicato anche qui. Blocco 111 o Sblocco di emergenza 113 saranno indicati qui, quando attivi.

| | |
|---|---|
| Numero di serie | Il numero di serie del controller. Viene visualizzato solo se il dispositivo è online. |
| Versione del firmware | La versione del firmware del controller. Viene visualizzata solo se il dispositivo è online. |
| Configurazione | Vedere Modelli e configurazione 57. |
| La posizione | 79 La posizione del controllore. |
| Descrizione | Descrizione o commenti |
| Lingua | Imposta la lingua predefinita per<br>- l'applicazione di gestione web sul controllore primario,<br>- l'applicazione di gestione semplificata su un Controllore secondario, e<br>- lettori OSDP multilingue collegati a questo controllore, se dotati di display.<br>Le lingue disponibili dipendono dalla licenza del software 15. Contattare il rappresentante autorizzato ZKTeco per l'aggiornamento della licenza. |
| Fuso orario | (solo controllori secondari) Il fuso orario del controllore secondario. Il fuso orario del controllore primario è impostato in Data e ora 105. |

| | |
|---|---|
| Gestito Porte | Un elenco delle porte gestite dal controllore, con collegamenti alle relative schermate di configurazione 73 . |
| Controllori secondari gestiti | Un elenco dei subcontrollori gestiti da questo controllore, con collegamenti alla loro configurazione hardware. |
| Download del firmware | (solo per i controllori secondari) Selezionare un file di firmware caricato in precedenza e scaricarlo sul controllore. Il firmware del controllore primario viene aggiornato in Impostazioni firmware 107 . |
| "Aprire la pagina web dell'amministratore in una nuova finestra". | Fare clic sul link per accedere direttamente a un controllore secondario. Si accede a un'applicazione di gestione web semplificata che consente opzioni limitate di configurazione del controllore, come le impostazioni di rete. |
| Pulsante di riavvio | (solo per i controllori secondari) Riavvia il controllore. |
| Pulsante Resync | (solo controllori secondari) Aggiorna la configurazione di questo controllore secondario. di questo controllore secondario. |

## Proprietà del sottocontrollore (I/O)

| | |
|---|---|
| Nome | (Di sola lettura) Il nome del subcontrollore. |
| Disconnesso | (Solo lettura) È sempre deselezionato e non può essere modificato. |
| Stato | (sola lettura) Sempre in linea per i subcontrollori integrati della serie |

Atlas.

Modello (Solo lettura) Il modello del dispositivo.

| | |
|---|---|
| Descrizione | Descrizione o commenti |
| Modello di hardware | Selezionare un modello esistente e fare clic su **Applica modello**. Deselezionare **Applica modello** per modificare le impostazioni.<br>Fare clic su **Crea modello hardware** per creare un nuovo modello dalle impostazioni correnti. Il modello contiene la maggior parte della configurazione del subcontrollore. Vedere Modelli hardware 90 . |

## Proprietà del lettore

| | |
|---|---|
| Indirizzo | Se Wiegand, l'etichetta dell'indirizzo stampata sul controllore. Altrimenti, **L'indirizzo** è un'etichetta arbitraria. |
| Gestito da | La porta a cui è associato il dispositivo |
| Modello | Il modello del dispositivo:<br>▪ **Personalizzato** - per lettori Wiegand o OSDP<br>▪ **ZKTeco** - per lettori ZKTeco RS-485 |
| Tipo di lettore | **- Dati0/Dati1 (Wiegand)**<br>▪ **OSDP** - per il modello **Custom**<br>▬ **ZKTeco RS-485** - per il modello **ZKTeco**. È disponibile solo per i modelli di controller biometrico. |
| Tipo di tastierino | Solo per lettori **Data0/Data1 (Wiegand)**.<br>▬ Se Auto, le cifre del PIN vengono accettate tramite Wiegand, decodificando automaticamente il formato. |

- "Nessuno" viene visualizzato per non avere un PIN pad. (In genere è opportuno lasciare questa opzione su Auto, a meno che non si voglia disabilitare specificamente un PIN pad su un lettore Wiegand).
- I lettori OSDP e ZKTeco RS-485 inviano i loro dati PIN in modo diverso, pertanto questa impostazione non viene utilizzata per loro.

Tamper — Il tipo di rilevamento delle manomissioni. Sui lettori **OSDP** è supportato solo **OSDP**.

Tipo di LED — Il tipo di controllo del LED:

- Per Wiegand si tratta di:
  - **Nessuno** - selezionare questa opzione per disattivare completamente il controllo dei LED.
  - **A 1 filo (verde)** - un filo collegato al LED verde (il LED rosso è generalmente acceso quando il verde non lo è)
  - **A 2 fili (rosso e verde)** - Solo controllori biometrici Atlas
- Per i lettori di OSDP, questo è **OSDP**.

OSDP/RS-485 Indirizzo — L'"indirizzo di polling" del lettore OSDP o ZKTeco RS-485.

Per la maggior parte dei lettori OSDP l'indirizzo predefinito è 0. Per modificare l'indirizzo, vedere **Riconfigurazione,** di seguito, e le istruzioni di installazione del produttore del lettore.

I lettori ZKTeco RS-485 dispongono di un interruttore DIP per configurare l'indirizzo. Per l'impostazione dell'indirizzo, consultare le istruzioni di installazione del lettore ZKTeco RS-485.

Riconfigura — Modifica l'indirizzo OSDP che il lettore stesso è configurato per utilizzare. Questo *non è* l'**indirizzo OSDP/RS-485** che il subcontrollore è impostato per utilizzare, anche se alla fine devono avere lo stesso valore.

1. Impostare l'**indirizzo OSDP/RS-485** sull'impostazione attuale dell'indirizzo del lettore.

2. Fare clic su **Salva**.
3. Fare clic sul pulsante **Riconfigura.** Selezionare un nuovo numero di indirizzo per il lettore.
4. Modificare l'**indirizzo OSDP/RS-485** con il nuovo numero.
5. Fare clic su **Salva.**

Alcuni lettori OSDP potrebbero non supportare la **riconfigurazione.**

## Proprietà di ingresso

**Indirizzo** L'indirizzo stampato sulla scheda.

**Nome** Il nome dell'input. Richiesto, massimo 32 caratteri.

**Abilitato** Selezionare per abilitare, deselezionare per disabilitare.

**Normalmente apertoSe** l'ingresso è normalmente aperto (NO). Gli ingressi normalmente aperti sono attivi quando i fili sono normalmente non collegati (circuito aperto).
Questo vale generalmente per i pulsanti di uscita. La maggior parte degli altri ingressi, come i sensori di manomissione, alimentazione e batteria, sono normalmente chiusi (NC).

**Funzione** Funzione per cui viene utilizzato l'ingresso. Non tutte le opzioni sono disponibili per tutti gli ingressi e alcune non possono essere modificate. Le **funzioni** sono:

- **Pulsante di uscita**
- **Sensore porta**
- **Manomissione**
- **Monitoraggio della potenza**

## Monitoraggio della batteria

- **Collegamento**
- **Non utilizzato**

Gestito daPer i pulsanti di uscita e i sensori di porta, questa è la porta di cui fa parte l'ingresso. Per i tamper, i monitor di alimentazione e i monitor della batteria, si tratta del controllore di cui fanno parte. Per gli ingressi di collegamento, questo è il dispositivo interessato dal criterio. (Vedere **Tipo di criterio).**

Le porte "Out" non possono essere utilizzate nei collegamenti, né per gestire l'hardware.

Tipo di criterioPer gli ingressi di **collegamento**, si tratta del criterio da eseguire quando l'ingresso diventa attivo. Le opzioni dipendono dall'impostazione **Gestito da**

- **Allarme innescato dall'ingresso** (gestito da: vuoto) - Questo provoca la generazione di un allarme quando l'ingresso diventa attivo. quando l'ingresso diventa attivo. Non confondetelo con un relè che attiva un allarme acustico, che può essere configurato per un'uscita, più avanti.
- **Blocco attivato dall'ingresso** (gestito da: un controllore) - Quando l'ingresso è attivato, viene avviato un blocco globale. globale. Il blocco termina solo quando l'utente fa clic su **Annulla blocco** nel menu principale. (con alcune eccezioni*).
- **Sblocco di emergenza guidato dall'ingresso** (gestito da: un controllore) - Ogni volta che l'ingresso è attivo, si attiva una condizione di sblocco di emergenza globale. Lo sblocco di emergenza termina solo quando l'ingresso torna inattivo (con alcune eccezioni*).
- **Sblocco momentaneo innescato dall'ingresso** (gestito da: una porta) - Provoca lo sblocco momentaneo della porta quando l'ingresso diventa attivo.

***Importante:** come per tutte le funzioni di emergenza, è necessario

comprendere a fondo i relativi argomenti prima di affidarsi al blocco e allo sblocco di emergenza.

| | |
|---|---|
| Programma | (Solo collegamento) Se si seleziona una pianificazione, il **collegamento verrà** applicato solo durante questa pianificazione. |

## Proprietà di uscita

| | |
|---|---|
| Indirizzo | L'indirizzo stampato sulla scheda. |
| Nome | Il nome dell'uscita. Richiesto, massimo 32 caratteri. |
| Funzione | Funzione per cui viene utilizzata l'uscita: Non tutte le opzioni sono disponibili per tutte le uscite e non tutte possono essere modificate. Le opzioni sono:<br>▪ **Cicalino del lettore**<br>▪ **LED del lettore (verde)**<br>▪ **LED del lettore (rosso)**<br>▪ **Blocco**<br>▪ **Collegamento**<br>▪ **Non utilizzato** |
| Gestito daPer | ¡l **blocco, il segnalatore acustico del lettore** e i LED questa è la porta per cui sono utilizzati.<br>Per i **collegamenti, si tratta** del dispositivo i cui eventi possono attivare questa uscita. Le porte "Out" non possono essere utilizzate nei collegamenti, né per gestire l'hardware. |
| Evento / Condizione | (solo per il **collegamento**) Definisce l'evento o la condizione che attiva un'uscita.<br>Inneschi del controller: |

## Manomissione

Inneschi della porta:

- **Accesso negato**
- **Accesso consentito**
- **Porta aperta forzatamente**
- **Porta tenuta aperta**
- **Costrizione**
- **Codice di emergenza presentato**

Inneschi in ingresso:

- **Ingresso attivo**

Toggle / Pulse (solo **Linkage**) Se **Pulse,** l'evento attiva brevemente questa uscita. Se **Toggle,** questa uscita è attiva finché l'evento non viene "terminato" dall'evento inverso. Ad esempio, "Porta aperta" è invertito da "Porta aperta ripristinata". L'opzione **Toggle** non è disponibile quando l'evento non ha un evento inverso.

Tempo di impulso (solo per il **collegamento**) Il tempo di impulso in secondi.

Programma (Solo **collegamento**) Se si seleziona una pianificazione, il **collegamento verrà** applicato solo durante questa pianificazione.

## Argomenti correlati

- Utilizzo delle viste delle proprietà 44
- Comprendere i controllori e le porte 55
- Modelli di hardware 90
- Modelli e configurazione 57

- Luoghi 79
- Porte 73

### 4.2.4 Aggiunta di controllori

I controllori secondari possono essere trovati e aggiunti automaticamente dall'applicazione di gestione Web. Questa operazione è chiamata "Discovery". Quando non è possibile utilizzare Discovery, è possibile aggiungere i controller manualmente. È inoltre possibile utilizzare l'installazione manuale per aggiungere i controllori che non sono ancora stati installati.

Una volta aggiunto un Secondario, non può essere riassegnato a un nuovo Primario o a una fabbrica.
reset primario, fino a quando non viene eseguito un 121.
reset di fabbrica.

Il numero di controller secondari che è possibile aggiungere e il numero di porte che è possibile creare sono limitati dalla licenza. Contattare il rappresentante autorizzato ZKTeco per
aggiornamenti della licenza 15.

## Scoprire i controllori secondari

Ci sono due importanti qualifiche riguardo a Discovery.

- Quando si utilizza Discovery, è necessario collegare e scoprire i controller uno alla volta. Solo in questo modo è possibile sapere quale sia.
- Il rilevamento funziona solo se tutti i controller sono collegati alla stessa subnet. Se si dispone di una rete semplice, questo sarà quasi sempre vero. In un ambiente aziendale più grande, potrebbe essere necessario aggiungere manualmente i controller secondari.

Per scoprire i controllori:

1. Fare clic su **Scoprire i controllori** nella barra dei menu.
2. In pochi istanti, un modulo visualizzerà tutti i controllori scoperti.

3. Fare clic sul link per aggiungere un controllore. Viene visualizzata la schermata di creazione del controllore.

   a. Selezionare una configurazione  .

b. Immettere un **nome** e selezionare **Nomi porta personalizzati** per poter assegnare un nome alle porte nel riquadro sottostante.

c. Lasciare invariate tutte le altre impostazioni. Queste sono le impostazioni rilevate.

4. Fare clic su **Salva** nella barra dei menu.

## Aggiunta manuale di controllori secondari

Per aggiungere un controllore manualmente:

1. Fare clic su **Crea** nella barra dei menu. Viene visualizzata la schermata di creazione del controllore.
2. Selezionare un modello 57 .
3. Selezionare una configurazione 57 .
4. Immettere un **nome** e selezionare **Nomi porta personalizzati** per poter assegnare un nome alle porte nel riquadro sottostante.
5. Inserire l'**indirizzo IP** del controllore.
6. Immettere il numero di **porta** predefinito, 443.
1. Fare clic su **Salva** nella barra dei menu.

## Argomenti correlati

- Modelli e configurazione 57
- Modifica della configurazione del controllore 60

### 4.2.5 Aggiornamenti del firmware

Per "firmware" si intende tutto il software in esecuzione su un controller, compresi l'applicazione di gestione web e il software che gestisce le porte. L'aggiornamento del firmware installa gli aggiornamenti ricevuti da ZKTeco.

È possibile aggiornare il firmware in due modi: (1) accedendo a qualsiasi controllore e aggiornandolo direttamente, oppure (2) utilizzando l'applicazione di gestione Web per aggiornare qualsiasi controllore secondario da remoto. Si noti che solo il metodo 1 è utilizzato per il controllore primario.

In entrambi i casi, è necessario disporre di un file di aggiornamento sul proprio

computer. Entrambi i metodi comportano il riavvio del controller aggiornato.

## Aggiornamento del firmware del controllore a cui si è connessi

1. Andare alle impostazioni del firmware 107 .
2. Fare clic su **Aggiorna firmware**.
3. Fare clic su **Sfoglia** e selezionare il file del firmware dal computer.
4. Attendere che il file venga trasferito al controller.
5. Al termine, fare clic su **Ok. L'**installazione dell'aggiornamento subirà un ritardo, quindi il controller andrà offline mentre si riavvia.

## Aggiornamento del firmware di un controller secondario da quello primario

Questo metodo prevede due fasi: (1) inviare il file di aggiornamento all'applicazione di gestione Web, quindi (2) scaricare il file sui controllori secondari.

1. Vai a Hardware 56 .
2. Fare clic su **Carica firmware** nella barra dei menu.
3. Fare clic su **Sfoglia** e selezionare il file del firmware dal computer.
4. Seguire le istruzioni e l'immagine del firmware verrà caricata, ma *non applicata a nessun controller.*
5. Selezionare un controllore secondario.
6. Scorrere fino a **Download del firmware** e selezionare il file di aggiornamento.
7. Fare clic su **Download.**
8. Seguire le indicazioni sullo schermo per aggiornare il firmware del controller

secondario selezionato.

## Argomenti correlati

- Impostazioni del firmware 107

### 4.2.6 Risincronizzazione dei controllori secondari

Il pulsante **Risincronizza controllori secondari** sulla barra dei menu provoca un reset importante di tutti i controllori secondari. Tutta la configurazione dell'applicazione di gestione Web (sul controllore primario) viene aggiornata su tutti i secondari. Questo include tutta la configurazione dell'hardware, delle porte e degli accessi, compresi i dati degli utenti. Non sono incluse le impostazioni di rete o del firmware.

I singoli controllori secondari possono essere risincronizzati alla voce **Manutenzione** delle rispettive pagine hardware. nelle pagine dedicate all'hardware.

## 4.3 Porte

Ogni scheda, PIN e lettore biometrico del sistema è rappresentato come una porta (vedere Comprensione dei controllori e delle porte 55 ).

Le porte vengono create automaticamente per corrispondere alla proprietà **Configuration** dei controllori in Hardware 56 . Il numero di Porte che è possibile creare è limitato dalla licenza. Contatto il vostro rappresentante autorizzato ZKTeco per l'aggiornamento della licenza 15 .

## Pulsanti di menu

| | |
|---|---|
| Coman di manuali | Consente il controllo diretto della porta selezionata utilizzando i comandi manuali 115 per cambiare la modalità della porta o sbloccarla. |

## Proprietà chiave

Per l'elenco completo e i dettagli, vedere Proprietà della porta 75 .

| | |
|---|---|
| Il nome | Il nome della porta. Richiesto, massimo 32 caratteri. |
| Tipo | Indica la funzione della porta: "Ingresso", "Uscita", "Punto di registrazione della tessera" o "Punto di raccolta". Questo viene determinato in Hardware 56 . |
| Modello di porta | Utilizzato per configurare questa porta con un modello 88 , che sovrascrive e disabilita alcune proprietà di questa schermata. |
| Modalità predefinita | La 142 modalità della porta per questa porta ogni volta che non viene modificata da una programmazione, da un comando manuale o da un evento. La modalità della porta determina se una porta è bloccata e quali tipi di accesso possono sbloccarla. 50 |
| Programmazione della modalità porta | Scegliere una programmazione della modalità porta per modificare la modalità porta in base al giorno e all'ora. |
| Multiutente Accesso | Vedere Accesso multiutente 52 . |
| Aree e Anti-passback | Vedere le 80 aree |

## Argomenti correlati

- Utilizzo delle viste delle 44 proprietà
- Proprietà della porta 75
- Modalità della porta 142

- Modelli di porte 88
- Comandi manuali 115
- Stato della porta 26

### 4.3.1 Proprietà della porta

Le proprietà della porta variano a seconda del tipo di porta. Ad esempio, i punti di accesso e i punti di registrazione delle tessere hanno un numero molto inferiore di proprietà, poiché non controllano un apriporta o altri elementi hardware della porta.

| | |
|---|---|
| Il nome | Il nome della porta. Richiesto, massimo 32 caratteri. |
| Stato | Lo stato attuale della porta, compreso online/offline, modalità porta 142, bloccata/sbloccata, aperta/chiusa, o errori come forzatura, trattenuta, manomissione, lettore offline. Blocco 111 o lo Sblocco di emergenza 113 saranno indicati qui, quando attivi. |
| Allarme | Se un allarme 24 è in corso sul portone, viene visualizzato qui. |
| Tipo | Come viene utilizzata la porta:<br>▪ **In** - una porta di ingresso. Una porta di solo ingresso o una porta di ingresso come parte di una coppia di porte di ingresso/uscita (in/out).<br>▪ **Fuori** - una porta di uscita.<br>▪ **Punto di raccolta** - utilizzato per il check-in durante un'emergenza per il rapporto di raccolta 30.<br>▪ **Punto di registrazione della carta** - utilizzato solo per registrare le carte 117. |
| Controllore | Il controllore da cui è gestita questa porta. |
| Sottocomando | Il subcontrollore (I/O) che gestisce l'hardware di questa porta. |
| Modello di portaUn | 88 modello di porta definisce i parametri |

comuni. Una volta che una porta è collegata al modello, i campi sono di sola lettura nella porta.

schermo.

Se il modello di porta viene modificato, vengono aggiornate anche le porte associate.

| | |
|---|---|
| Posizione | Posizione 79 della porta. |
| Descrizione | Descrizione o commenti |
| Modalità predefinita | La 142 modalità della porta per questa porta ogni volta che non viene modificata da una programmazione, da un comando manuale o da un evento. La modalità della porta determina se una porta è bloccata e quali tipi di accesso possono sbloccarla. 50 |
| Programmazione della modalità porta | Scegliere una programmazione della modalità porta per modificare la modalità porta in base al giorno e all'ora. 52 |
| Multiutente Accesso | L'accesso multiutente se per aprire una porta sono necessari più utenti. |
| Tempo di sblocco (s) | Il tempo di attivazione della serratura per un accesso (accesso consentito, uscita richiesta, ecc.). |
| Tempo di allarme di tenuta aperta (s) | La quantità di tempo in cui una porta può essere tenuta aperta prima che venga generato un evento di apertura. Questo evento può essere configurato nella configurazione del subcontrollore per pilotare un'uscita ausiliaria, ad esempio per emettere un segnale acustico. 61 |

| | |
|---|---|
| Tempo minimo di sblocco (s) | Se l'opzione **Re-lock On** consente di ribloccare la porta prima dello scadere del tempo di azionamento, questo è il tempo minimo in cui la porta rimarrà sbloccata. In questo modo si evita un impulso di sblocco troppo breve, che può essere un problema per alcune ferramenta. |

| | |
|---|---|
| Tempo di sblocco prolungato (s) | Se per un utente è selezionata l'opzione **Usa orari porta estesi**, questo orario viene utilizzato al posto dell'**orario di sblocco**. |
| Detenzione prolungata Tempo (s) | Se un utente ha selezionato l'opzione **Usa tempi estesi della porta**, questo tempo viene utilizzato al posto del **tempo di allarme di apertura**. |
| Avvertimento di preallarme in posizione aperta Tempo (s) | L'intervallo di tempo che precede il raggiungimento del **tempo di allarme di tenuta aperta**, quando viene generato un evento di avviso di preallarme di tenuta aperta.<br>Questo evento può essere configurato nella configurazione del subcontrollore per pilotare un'uscita ausiliaria, ad esempio per emettere un segnale acustico. 61 |
| Sopprimere gli eventi del pulsante di uscita | Se si seleziona questa opzione, gli Eventi richiesti in uscita non vengono creati per questa Porta. Questa opzione può essere utilizzata se il numero di questi eventi è considerato troppo elevato e poco importante. |
| Sblocco all'uscita Pulsante | Se questa opzione è selezionata, la porta viene sbloccata quando si preme il pulsante di uscita. Questo potrebbe non essere necessario per i sistemi in cui il pulsante di uscita è cablato direttamente per interrompere l'alimentazione alla serratura della porta, ad esempio.<br>**Importante:** le funzioni dei pulsanti di uscita sono regolamentate dalle norme antincendio specifiche di ogni paese e regione. Per garantire la conformità del sistema, fare riferimento a queste norme durante la progettazione e la configurazione. |
| Riblocco su | Quando il lucchetto deve essere ribloccato dopo l'accesso:<br>▪ **Fine del tempo di sblocco**<br>▪ **Porta aperta** |

- **Chiusura della porta**
- **Chiusura della porta o fine del tempo di sblocco** (se precedente)

| | |
|---|---|
| Esente da Blocco globale | Se questa opzione è selezionata, la porta non sarà interessata da un blocco globale. |
| Esente da Emergenza globale Sbloccare | Se è selezionata, la porta non sarà interessata da uno sblocco di emergenza globale. |
| Area di ingresso | L'area in cui la porta conduce per le configurazioni anti-passback (e airlock). (e delle camere di compensazione). |
| Area di uscita | L'area da cui esce la porta per le configurazioni anti-passback (e airlock). (e delle camere di compensazione). |
| Anti-passback Metodo | - **Nessuno** - nessun anti-passback applicato<br>- **Door-Based** - non è possibile utilizzare la stessa credenziale entro un certo periodo di tempo presso la stessa porta.<br>- **Basato sull'area** - controlla che sia noto che si trovano nell'area corretta prima di utilizzare una porta che conduce da quell'area a un'altra area.<br>Vedere Anti-Passback. |
| Anti-passback Modalità | Disponibile se il **metodo di anti-passback** è **basato sull'area**: se negare o concedere l'accesso in caso di violazione dell'anti-passback:<br>- **Difficile (negare l'accesso)** |

- **Soft (concedere l'accesso)**

| | |
|---|---|
| Verbale negato | Disponibile se il **metodo anti-passback** è **basato sulla porta**. Il numero di minuti prima che la stessa credenziale possa essere usata alla porta. |

## Argomenti correlati

- Porte 73
- Modelli di porte 88
- Stato della porta 26
- Modalità della porta 42
- Anti-Passback 118
- Comandi manuali 115
- Proprietà dell'hardware 64
- Luoghi 79
- Aree 80

## 4.4 Luoghi

Le posizioni sono etichette che si possono applicare per organizzare le porte e la ferramenta negli elenchi e nei rapporti, in particolare negli Eventi e negli Allarmi. 22 e Allarmi 24 . Le posizioni possono essere assegnate a Porte 73 , Controllori 56 , Aree 80 e Mappe 82 .

## Proprietà della posizione

| | |
|---|---|
| Nome | Il nome della posizione. Richiesto, massimo 32 caratteri. |
| Tipo | Categoria per dimensione della sede. Da grandi a piccoli, sono: |

**Regione > Campus > Edificio > Piano > Stanza**

Posizione del genitore

Designa questa sede come inclusa in una sede *più grande*. Il genitore **di** un **edificio** può essere un **campus** o una **regione,** ma non un **piano** o una **stanza.**

Quando si filtrano gli eventi per una località, vengono visualizzate anche tutte le località più piccole che ne fanno parte.

## Argomenti correlati

- Utilizzo delle viste delle proprietà 44
- Eventi 22
- Allarmi 24

## 4.5 Aree

Le aree sono regioni fisiche definite dall'utente e sono utilizzate per l'Anti-Passback 118, l'Arresto 30 e le camere di compensazione. Una colonna che mostra l'area può essere aggiunta a Eventi e Allarmi 24 . e Allarmi 24 .

Le aree non sono altro che un'etichetta. Non hanno alcuna funzione finché non si definiscono le porte che entrano e escono dall'area. A tale scopo, è necessario impostare l'**Area di entrata** e l'**Area di uscita** di ciascuna porta interessata.

## Aree predefinite

Esistono due aree predefinite dal sistema che non possono essere modificate o eliminate:

- **Global Out** - Le porte che entrano o escono dal "mondo esterno" devono utilizzare questa come **area di uscita** o di **entrata,** rispettivamente.
- **Muster** - Un'area in cui tutti i punti Muster 30 "entrano in gioco. Chiunque utilizzi un Punto d'incontro avrà la sua ultima Area conosciuta impostata sull'Area d'incontro e sarà escluso dal rapporto d'incontro.

## Utilizzo dello schermo

**Nome** Il nome dell'area. Richiesto, massimo 32 caratteri.

**La posizione** Una posizione da associare all'Area

**Tipo**
- **Locale** - Utilizzato solo su un singolo controller. Può essere utilizzato per la camera di compensazione.
- **Globale** - Può essere usato su più controllori, per l'applicazione globale dell'anti-passback. applicazione.

**Genitore** (Solo aree locali) Il singolo controllore per quest'area.

**Modalità camera di compensazione** (solo aree locali)

- **Nessuna uscita durante l'ingresso** - Una porta che esce dall'area non può essere utilizzata mentre una porta che entra nell'area è aperta.
- **Porta singola rigorosa** - Non è possibile sbloccare/aprire contemporaneamente due porte nell'area.

**Descrizione** Descrizione o commenti

## Argomenti correlati

- Utilizzo delle viste delle proprietà
- Anti-Passback
- Armamento

## 4.6 Mappe

La configurazione delle mappe viene utilizzata per creare le schermate della vista Mappe 28 .

La vista Mappe viene utilizzata per mostrare lo stato delle porte e dei controller su sfondi grafici, ad esempio su mappe dell'edificio o del campus. Evidenzia tutti i problemi in rosso e consente di inviare comandi alle porte. Le mappe possono anche contenere collegamenti ad altre mappe per facilitare la navigazione.

### Proprietà e controlli della mappa

| | |
|---|---|
| Nome | Nome della mappa (obbligatorio, massimo 32 caratteri) |
| Posizione | Posizione opzionale 79 della mappa. |
| Sfondo | Fare clic su **Carica** per caricare un'immagine dal computer. Questa sarà la tela su cui posizionare i dispositivi. Le immagini di grandi dimensioni si ridurranno per adattarsi allo spazio disponibile. |
| Elementi | Gli elementi, contenuti in tre caselle di riepilogo, possono essere cliccati e trascinati sulla Mappa. Quando si trovano sulla Mappa, l'icona della chiave inglese blu offre le opzioni per<br>▪ eliminare l'elemento, oppure<br>▪ impostare la destinazione di un elemento "Collegamento" da un elenco di altre Mappe.<br>Il testo inserito nella **ricerca** filtra tutti e tre gli elenchi di elementi. |

### Argomenti correlati

- Utilizzo delle viste delle proprietà 94
- Mappe (monitoraggio) 28

## 4.7 Disegni di carte

Un progetto di tessera è un layout di stampa creato per essere utilizzato nella stampa delle tessere 45 . Può includere informazioni sull'utente, come il nome e la data di scadenza, e immagini, come la foto dell'utente e i loghi.

### Proprietà

| | |
|---|---|
| Il nome | Il nome del progetto della scheda. Richiesto, massimo 32 caratteri. |
| Descrizione | Descrizione o commenti. |

### L'area di progettazione

#### Colonna centrale

L'area centrale è la tela su cui "disegnare" la carta. Mostra un biglietto d'accesso di dimensioni standard, con i lati anteriore e posteriore.

**Importante:** Consultare il manuale della stampante per schede per capire le sue limitazioni, ad esempio se può stampare sia sul fronte che sul retro e se è possibile stampare fino al bordo della scheda.

#### Colonna sinistra

Fare clic e trascinare gli elementi dei pannelli di sinistra nell'area della scheda.

Fare clic sugli elementi nell'area della scheda per selezionarli. Fare clic con il tasto

Maiuscolo per selezionare più elementi. Trascinare gli elementi selezionati per spostarli.

Le immagini (solo) possono essere dimensionate trascinando gli angoli.

#### Colonna destra

La prima fila di tre icone esegue le azioni standard di cancellazione, annullamento e ripetizione.

La seconda riga contiene sei opzioni per l'allineamento degli elementi, seguite da quattro opzioni che controllano quali elementi si trovano sopra gli altri. Passare il mouse su ogni icona per vedere la sua funzione esatta. È necessario selezionare più di un elemento per attivare le opzioni di allineamento.

Il resto del pannello mostra le proprietà dell'elemento attualmente

selezionato. Per le **immagini**, fare clic su **Seleziona immagine** per caricare

un file immagine dal computer.

Per i **campi Testo** e **Utente,** inserire il **testo**. Il testo tra "{{" e "}}" verrà sostituito con la proprietà denominata dell'utente. È possibile aggiungere altro testo al di fuori delle parentesi, ma il testo all'interno deve essere un nome di campo valido.

Le altre opzioni per il testo impostano il carattere e il colore.

**L'origine X** e l'**origine Y** sono proprietà sia delle immagini che del testo. Determinano la direzione in cui l'elemento crescerà per adattarsi al contenuto, *scegliendo quale angolo non si sposterà mai. L'*impostazione predefinita è in alto a sinistra e il riquadro si espanderà verso destra e verso il basso quando, ad esempio, il campo del nome è lungo o la dimensione del carattere aumenta. Se si cambia l'origine in basso a destra, il riquadro si espanderà verso l'alto e verso sinistra, consentendo di posizionare il riquadro sul bordo destro o inferiore della scheda.

### Note

I formati immagine supportati sono PNG, JPEG e GIF.

Il testo viene stampato sopra le immagini (se in alto) e la trasparenza delle immagini è supportata.

## Argomenti correlati

- Utilizzo delle viste delle proprietà 34
- Utenti 38
- Stampa di carte 45

## 4.8 Formati delle schede

I formati delle carte definiscono i tipi o le marche di carte da utilizzare. Il sistema Atlas Series include tutti i formati di carta necessari, anche se è possibile inserire un "codice struttura" specificato dal fornitore della carta.

Se si utilizza un tipo di carta non comune, è necessario creare un formato di carta personalizzato. Si tratta di un'operazione piuttosto tecnica, che richiede specifiche precise da parte del fornitore della carta.

### Note

È possibile utilizzare più di un formato di scheda nel sistema.

I formati delle carte non sono associati a specifiche Porte o a specifici Utenti: sono tutti utilizzati per tutti.

Due formati di carta con lo stesso numero di bit non possono essere abilitati contemporaneamente, a meno che non siano entrambi dotati di codici di facilitazione e questi codici siano diversi.

### Immissione del codice della struttura

È necessario sapere quale dei formati di tessera esistenti corrisponde alle proprie tessere. È sufficiente selezionare tale formato, inserire il numero di **codice della struttura** e salvare.

### Proprietà del formato della scheda

**Nota:** i campi di inizio e di posizione sono il numero del bit, dove il primo bit della scheda è il numero 0.

| | |
|---|---|
| Nome | Nome del formato. Richiesto, massimo 32 caratteri. |
| Bit | Il numero totale di bit sulla scheda, compresi i bit di parità, ecc. |
| Abilitato | Utilizzare o non utilizzare il formato. |

| | |
|---|---|
| Codice struttura | (facoltativo) Se è presente un campo codice struttura (inizio/lunghezza specificati), questo è il valore a cui il codice struttura deve essere uguale affinché il formato venga abbinato. |

| | |
|---|---|
| Codice struttura Inizio | Inizio del codice della struttura (numero di bit). |
| Codice struttura Lunghezza | Lunghezza del codice di struttura (in bit). |
| Numero di carta Avvio | Inizio del numero della carta (numero di bit). |
| Numero di carta Lunghezza | Lunghezza del numero di carta (in bit). |
| Parità (1-4) | ▪ **Nessuno/Even/Odd** - **Nessuno** per non utilizzare affatto questo campo di parità, **Even** o **Dispari** per il metodo di calcolo della parità.<br>▪ **Start** - Il bit iniziale della sorgente di parità (l'intervallo di bit da controllare per la parità). NON include la posizione del bit di parità. stesso.<br>▪ **Lunghezza** - La lunghezza in bit della sorgente di parità.<br>▪ **Posizione** - Il numero di bit del bit di parità.<br>▪ **Maschera** - Normalmente viene utilizzata l'intera sorgente. Se nella sorgente devono essere utilizzati solo alcuni bit di un modello, questo viene inserito qui come maschera come una stringa di 0 e 1. |

## Argomenti correlati

- Utilizzo delle viste delle proprietà

## 4.9 Gruppi di utenti

I gruppi di utenti sono utilizzati nell'accesso multiutente 52 . Un gruppo di utenti è semplicemente un nome e un descrizione. I membri del gruppo vengono aggiunti in Utenti 38 .

### Argomenti correlati

- Utilizzo delle viste delle proprietà 14
- Utenti 38
- Accesso multiutente 52

## 4.10 Trigger di allarme

Gli allarmi 24 sono attivati dagli eventi, il che significa che ogni volta che si verifica un evento di un tipo 134 specifico, viene generato anche un allarme. La schermata Trigger allarme consente di aggiungere agli eventi che attivano gli allarmi e di modificare o rimuovere i trigger predefiniti.

### Proprietà di attivazione dell'allarme

**Attivazione Evento** — Il tipo di evento che farà scattare l'allarme.

**La priorità** — L'importanza dell'allarme creato. La **priorità** può essere utilizzata per ordinare la schermata Allarmi.

**Attivazione del colore Evento** — L'evento scatenante sarà di questo colore nella schermata Eventi. 22 nella schermata Eventi. Questo non influisce sul colore dell'allarme (anche alcuni tipi di evento hanno un colore, indipendentemente dal fatto che si tratti o meno di allarmi).

### Argomenti correlati

- Utilizzo delle viste delle proprietà 44
- Allarmi 24
- Eventi 22
- Categorie e tipi di eventi 134
- Caratteristiche di emergenza 20

## 4.11 Modelli di porte

I modelli di porta possono essere creati a partire da configurazioni di porte esistenti e quindi applicati ad altre porte che richiedono le stesse impostazioni. Le modifiche successive al modello vengono applicate a tutte le porte che lo utilizzano. Solo alcune proprietà della porta sono controllate dal modello (vedere sotto).

Quando un modello di porta viene applicato a una porta, le proprietà che derivano dal modello non sono più modificabili nella schermata Porte. Per modificarle, è necessario modificare il modello o rimuovere il modello dalla porta.

Un modello di porta non può essere applicato a una porta che ha un **tipo** diverso nelle sue proprietà 73 .

### Creazione di un modello di porta da una porta esistente

1. Andare alla schermata Porte 73 schermo.
2. Selezionare una porta.
3. Fare clic sul pulsante **Crea modello di porta** nelle proprietà della porta.
4. Inserire un nome (obbligatorio, massimo 32 caratteri) e, facoltativamente, una descrizione.
5. Fare clic su **Salva.**

### Applicazione di un modello di porta a una porta

1. Andare alla schermata Porte 73 schermo.

2. Selezionare una porta.
3. Selezionare un **modello di porta** nelle proprietà della porta.
4. Selezionare **Applica modello**. La porta utilizzerà le impostazioni del modello solo se questa opzione è selezionata. Se si toglie la spunta, la porta manterrà le impostazioni del modello, a meno che non vengano modificate.
5. Fare clic su **Salva**.

## Proprietà del modello di porta

Un modello di porta sovrascrive queste proprietà della porta 75 . Alcuni tipi di porta non utilizzano tutte queste proprietà.

- **Comandi manuali abilitati**
- **Sbloccare il tempo**
- **Tempo di allarme di apertura in attesa**
- **Tempo minimo di sblocco**
- **Tempo di sblocco prolungato**
- **Tempo di permanenza prolungato**
- **Tempo di avviso preallarme tenuto aperto**
- **Sopprimere gli eventi del pulsante di uscita**
- **Sblocco su pulsante di uscita**
- **Riattivare il blocco su**

## Argomenti correlati

- Utilizzo delle viste delle proprietà 44
- Porte 73
- Modelli di hardware 90

## 4.12 Modelli di hardware

I modelli di hardware possono essere creati a partire dalle proprietà di un subcontrollore (I/O) esistente, quindi applicati ad altri subcontrollori che richiedono le stesse impostazioni. Le modifiche successive al modello vengono applicate a ogni subcontrollore che lo utilizza. Solo alcune proprietà del subcontrollore sono controllate dal modello.

Quando un modello di hardware viene "applicato" a un sottocontrollore, le proprietà che derivano dal modello non sono più modificabili nella schermata del sottocontrollore. Per modificarle, è necessario modificare il modello o rimuovere il modello dal subcontrollore.

### Creazione di un modello hardware da un sottocontrollore esistente

1. Andare alla schermata Hardware schermata.
2. Selezionare un sottoregolatore.
3. Fare clic sul pulsante **Crea modello hardware** nelle proprietà del subcontrollore.
4. Inserire un nome (obbligatorio, massimo 32 caratteri) e, facoltativamente, una descrizione.
5. Fare clic su **Salva**.

### Applicazione di un modello hardware a un sottocontrollore

1. Andare alla schermata Hardware schermata.
2. Selezionare un sottoregolatore.
3. Selezionare un **modello hardware** nelle proprietà del subcontrollore.
4. Selezionare **Applica modello**. Il Subcontroller utilizzerà le impostazioni del modello solo se questa opzione è selezionata. Se si toglie la spunta, il Subcontroller manterrà le impostazioni del modello, a meno che non vengano modificate.
5. Fare clic su **Salva**.

### Argomenti correlati

- Utilizzo delle viste delle proprietà 44
- Hardware 56
- Modelli di porte 88

# 5 Amministrazione

Il menu Amministrazione comprende una serie di impostazioni per l'intero sistema.

Ruoli utente 92 consente di vedere la definizione dei ruoli utente integrati per gli utenti che accedono all'applicazione web e di definire nuovi ruoli personalizzati.

Backup e ripristino 99 consente di eseguire il backup e il ripristino del database di sistema e di gestire i backup pianificati.

Impostazioni di sistema 101 consente di controllare le impostazioni di archiviazione e le etichette dei campi personalizzati.

Rete 103 consente di configurare le impostazioni di rete.

Data e ora 105 consente di configurare il fuso orario e le impostazioni dell'ora di rete.

Impostazioni e-mail 106 consente di configurare un server di posta SMTP per l'invio di notifiche 17 via e-mail.

Download di archivi 107 consente di scaricare i file di archivio generati in base alle Impostazioni di sistema.

Impostazioni del firmware 97 consente l'aggiornamento del firmware, il reset di fabbrica e la conversione tra le funzionalità del controllore primario e secondario.

Impostazioni del server Web 108 consente di caricare un certificato HTTPS.

Dispositivi mobili autorizzati 108 consente di fornire l'accesso ai dispositivi mobili che hanno installato l'applicazione mobile.

## 5.1 Ruoli utente

I ruoli utente definiscono le operazioni che i diversi utenti possono svolgere all'interno dell'applicazione di gestione web. Il sistema è dotato di una serie di ruoli utente integrati che non possono essere modificati o eliminati. È possibile creare ruoli utente personalizzati.

Ecco un riepilogo dei ruoli utente integrati.

| | |
|---|---|
| Sistema | Illimitato; in grado di accedere a tutte le schermate e le funzioni. |

Amministrazione

| | |
|---|---|
| Gestione del controllo degli accessi | Fornisce l'accesso agli utenti e definisce le porte, gli orari e altre regole di controllo degli accessi che consentono o negano l'accesso. È in grado di configurare le porte, ma non l'hardware. In grado di eseguire tutti i comandi manuali. |
| Monitoraggio di base | La maggior parte delle funzioni di monitoraggio. È in grado di visualizzare gli allarmi, ma non di riconoscerli o risolverli. Possibilità di visualizzare gli utenti, ma non di crearli o modificarli. |
| Gestione degli utenti e delle credenziali | Aggiungere e gestire gli utenti e le loro credenziali associate. È anche in grado di eseguire alcune attività di monitoraggio limitate. Nessuna gestione degli allarmi e nessuna configurazione di hardware o porte. |
| Monitoraggio degli allarmi | Simile al Monitoraggio di base, ma anche in grado di riconoscere e risolvere gli allarmi. |

## Opzioni del ruolo utente - Voci di menu

| Opzione | Sistema | Accesso | Base | Utente e | Allarme |
|---|---|---|---|---|---|
| | Amministrazione | controllo | Monitoraggio | Credenziale | Monitoraggio |
| | | Gestione | | Gestione | |
| Controllo degli accessi: Livelli di accesso | Sì | Sì | | | |
| | Sì | Sì | | | |
| | Sì | Sì | | | |

Controllo degli accessi: Pianificazione della modalità della porta

Controllo degli accessi: Codici di emergenza

| Opzione | Sistema<br>Amministrazione | Accesso<br>controllo | Base<br>Monitoraggio | Utente e<br>Credenziale | Allarme<br>Monitoraggio |
|---|---|---|---|---|---|
| | | Gestione | | Gestione | |
| Controllo degli accessi: Accesso multiutente | Sì, sì, sì | Sì | | Sì | |
| Controllo degli accessi: Orari | Sì, sì, sì | Sì | | | |
| Controllo degli accessi: Codici di accesso condivisi | Sì, sì, sì | Sì | | Sì | |
| Controllo degli accessi: Giorni speciali | Sì, sì, sì | Sì | | Sì | |
| Controllo degli accessi | Sì, sì, sì | Si | Sì | Sì | Si |
| Controllo dell'accesso: Utenti (sola lettura) | Sì | | | | |
| Amministrazione: Archivio Download | Sì | | | | |
| Amministrazione: Backup e ripristino | Sì | | | | |
| Amministrazione: Data e ora | Sì | | | | |
| Amministrazione: Impostazioni e-mail | Sì | | | | |
| Amministrazione: Impostazioni del | Sì | | | | |

firmware

Amministrazione:
Rete

Amministrazione:
Impostazioni di
sistema

| Opzione | Sistema<br>Amministrazione | Accesso<br>controllo<br>Gestione | Base<br>Monitoraggio | Utente e<br>Credenziale<br>Gestione | Allarme<br>Monitoraggio |
|---|---|---|---|---|---|
| Amministrazione: Ruoli utente | Sì | | | | |
| Amministrazione: Impostazioni del server web | Sì | | | | |
| Configurazione: Trigger di allarme | Sì | | | | |
| Configurazione: Aree | Sì, sì, sì | Sì | | | |
| Configurazione: Disegni di schede | Sì, sì, sì | Sì | | | |
| Configurazione: Formati delle schede | Sì | | | | |
| Configurazione: Modelli di porte | Sì, sì, sì | Sì | | | |
| Configurazione: Porte | Sì, sì, sì | Sì | | | |
| Configurazione: Hardware | Sì | | | | |
| Configurazione: Modelli hardware | Sì | | | | |
| Configurazione: Posizioni | Sì | | | | |
| Configurazione: Mappe | Sì | | | | |
| Configurazione: Gruppi di utenti | Sì | | Sì | | |

Monitoraggio:
Cronologia degli
allarmi

| Opzione | Sistema<br>Amministrazione | Accesso<br>controllo<br>Gestione | Base<br>Monitoraggio | Utente e<br>Credenziale<br>Gestione | Allarme<br>Monitoraggio |
|---|---|---|---|---|---|
| Monitoraggio: Allarmi | Sì | | | | Sì |
| Monitoraggio: Allarmi (di sola lettura) | Sì | Sì | Sì | | Sì |
| Monitoraggio: Audit | Sì | Sì | | | Sì |
| Monitoraggio: Stato della porta | Sì | Sì | Sì | Sì | Sì |
| Monitoraggio: Eventi | Sì | Sì | Sì | Sì | Sì |
| Monitoraggio: Cronologia eventi | Sì | Sì | Sì | Sì | Sì |
| Monitoraggio: Mappe | Sì | Sì | Sì | Sì | Sì |
| Monitoraggio: Muster | Sì | Sì | Sì | Sì | Sì |
| Monitoraggio: Rapporto sul livello di accesso degli utenti | Sì | Sì | Sì | Sì | Sì |
| Monitoraggio: Rapporto sulla porta utente | Sì | Sì | Sì | Sì | Sì |

## Opzioni del ruolo utente - Comandi manuali

| Opzione | Sistema Amministrazione | Accesso Gestione del controllo | Base Monitoraggio | Utente e Gestione delle credenziali | Allarme Monitoraggio |
|---|---|---|---|---|---|
| Porta: Accesso momentaneo | Sì | Sì | Sì | Sì | Sì |
| Porta: Imposta modalità porta | Sì | Sì | | | Sì |

| Opzione | Sistema Amministrazione | Accesso Gestione del controllo | Base Monitoraggio | Utente e Gestione delle credenziali | Allarme Monitoraggio |
|---|---|---|---|---|---|
| Controllore: Risincronizzazione | Sì | | | | |
| Utente: Perdono | Sì | Sì | Sì | Sì | Sì |
| Controllore: Riavvio | Sì | | | | |
| Controllore: Download del firmware | Sì | | | | |

## Opzioni del ruolo utente - Modalità porta

| Opzione | Sistema Amministrazione | Accesso Gestione del controllo | Base Monitoraggio | Utente e Gestione delle credenziali | Allarme Monitoraggio |
|---|---|---|---|---|---|
| Annullamento/Cancellazione | Sì | Sì | | | Sì |
| Sbloccato | Sì | Sì | | | Sì |
| Nessun accesso | Sì | Sì | | | Sì |
| Solo carta | Sì | Sì | | | |
| Carta e PIN | Sì | Sì | | | |
| Solo PIN | Sì | Sì | | | |
| Carta o PIN | Sì | Sì | | | |
| Sbloccato (emergenza) | Sì | Sì | | | Sì |
| Blocco | Sì | Sì | | | Sì |

| | | |
|---|---|---|
| Solo carta (primo sblocco) | Sì | Sì |

| Opzione | Sistema<br>Amministrazione | Accesso<br>controllo<br>Gestione | Base<br>Monitoraggio | Utente e<br>Credenziale<br>Gestione | Allarme<br>Monitoraggio |
|---|---|---|---|---|---|
| Carta e biometria | Sì | Sì | | | |
| Carta, biometria e PIN | Sì | Sì | | | |
| Solo biometrico | Sì | Sì | | | |
| Biometrico e PIN | Sì | Sì | | | |
| Biometrico o PIN | Sì | Sì | | | |
| Carta o biometrico | Sì | Sì | | | |
| Biometrico, carta o PIN | Sì | Sì | | | |
| Nessun accesso, nessun pulsante di uscita | Sì | Sì | | | Sì |
| Carta e PIN (primo sblocco) | Sì | Sì | | | |
| Solo PIN (primo sblocco) | Sì | Sì | | | |
| Carta o PIN (primo sblocco) | Sì | Sì | | | |
| Carta e biometrica (primo sblocco) | Sì | Sì | | | |
| Scheda, biometrica e PIN (primo sblocco) | Sì | Sì | | | |
| Solo biometrico (primo sblocco) | Sì | Sì | | | |

| Opzione | Sistema<br>Amministrazione | Accesso<br>controllo<br>Gestione | Base<br>Monitoraggio | Utente e<br>Credenziale<br>Gestione | Allarme<br>Monitoraggio |
|---|---|---|---|---|---|
| Biometrico e PIN (primo sblocco) | Sì | Sì | | | |
| Biometrico o PIN (primo sblocco) | Sì | Sì | | | |
| Scheda o biometrica (primo sblocco) | Sì | Sì | | | |
| Biometrico, carta o PIN (primo sblocco) | Sì | Sì | | | |

## Argomenti correlati

- Utilizzo delle viste delle proprietà 64
- Utenti 38

## 5.2 Backup e ripristino

Backup e ripristino consente di configurare le impostazioni di backup pianificato e di eseguire il backup o il ripristino manuale del database.

I file di backup vengono salvati nel formato `.dbbackup`. È possibile salvare fino a tre backup sul controller. I backup più vecchi vengono eliminati automaticamente. È anche possibile scaricare i file di backup sul computer.

Per impostazione predefinita, il backup del database viene eseguito automaticamente sul controller primario ogni notte a mezzanotte. È anche possibile programmare un backup su una pianificazione personalizzata. Se il backup pianificato non è abilitato, i backup automatici non vengono eseguiti.

# Modifica della pianificazione del backup

Per programmare un backup a un'ora o a una frequenza diversa:

1. In **Backup pianificato,** lasciare selezionata la casella **Abilitato (**consigliato).
2. Selezionare **Giornaliero**, **Settimanale** o **Mensile**. Si consiglia di selezionare **Giornaliero.**
3. Selezionare l'ora del giorno in cui eseguire i backup pianificati.
4. Fare clic su **Salva**.

### Backup manuale del database

Fare clic su **Backup ora** per eseguire il backup del database in un file sul controller e, facoltativamente, scaricare il backup appena creato sul computer.

Fare clic su **Download Now** per scaricare il file sul computer.

### Ripristino di un backup

I backup possono essere ripristinati da un file sul controller o da un file caricato.

**Attenzione: I** dati esistenti saranno cancellati se si sceglie di ripristinare.

1. In **Ripristino**, selezionare il backup o selezionare un file `.dbbackup` dal computer.
2. Fare clic su **Ripristina**, quindi fare nuovamente clic su **Ripristina** quando viene richiesto di confermare.
3. Attendere il completamento del processo di ripristino. L'utente verrà disconnesso automaticamente.
4. Accedere nuovamente all'applicazione di gestione Web.

## 5.3 Impostazioni di sistema

Le impostazioni di sistema definiscono una serie di impostazioni utilizzate dal sistema, come la manutenzione del database, i campi personalizzati e la lunghezza del PIN.

### Manutenzione del database

Queste impostazioni definiscono i requisiti di archiviazione per le 17, Eventi 22, Audit notifiche. 31
e allarmi 24. Le impostazioni predefinite sono in genere sufficienti e non devono essere modificate. Se necessario, modificare quanto segue. I file di archivio generati in base a queste impostazioni sono disponibili in Download archivi 107.

| | |
|---|---|
| Notifiche massime per Utente | Le notifiche più vecchie vengono eliminate automaticamente, anche se non sono state cancellate dall'Utente, per mantenere il totale per Utente a questo limite o al di sotto di esso. |
| Eventi massimi in Database | Gli eventi più vecchi vengono archiviati, per mantenere il numero totale di eventi nel database al di sotto di questo limite. |
| File di archivio eventi massimi | Gli eventi vengono archiviati in file CSV sul controller. Questo è il numero massimo di file di archivio degli eventi da conservare. |
| Dimensione massima del file dell'archivio eventi (Byte) | La dimensione massima di ogni singolo file di archivio eventi. |
| Audit massimi in Database | Gli audit più vecchi vengono archiviati, per mantenere il numero totale di audit nel database al di sotto di questo limite. |
| File di archivio di audit massimi | Gli audit vengono archiviati in file CSV sul controller. Questo è il numero massimo di file di archivio degli audit da conservare. |
| Dimensione massima del file | dell'archivio di audit (Byte) |

La dimensione massima di ogni singolo file di archivio di audit.

| | |
|---|---|
| Allarmi massimi in Database | Gli allarmi più vecchi vengono archiviati per mantenere il numero totale di allarmi nel database al di sotto di questo limite. |
| File di archivio degli allarmi massimi | Gli allarmi vengono archiviati in file CSV sul controller. Questo è il numero massimo di file di archivio degli allarmi da conservare. |
| Dimensione massima del file dell'archivio allarmi (Byte) | La dimensione massima di ogni singolo file di archivio Alarm. |

## Campi personalizzati

Questa sezione consente di modificare le etichette dei campi personalizzati che appaiono nella schermata Utenti. Massimo 32 caratteri.

## Accesso condiviso/Codici di emergenza/PIN

Questa sezione consente di modificare la lunghezza a livello di sistema di tutti i codici di accesso condivisi, Codici di emergenza, e codici PIN (schermata Utenti utenti). La stessa lunghezza viene utilizzata per tutti i codici questi.

La modifica della lunghezza altera tutti i PIN esistenti.

- Aumentando la lunghezza del PIN si anteporranno degli zeri ai codici di accesso condivisi, ai codici di emergenza e ai codici PIN utente esistenti.
- Diminuendo la lunghezza del PIN si rigenerano casualmente tutti i codici di accesso condivisi e i codici di emergenza e si cancellano tutti i codici PIN utente.

La lunghezza deve essere compresa tra 4 e 8 caratteri. La lunghezza predefinita è 4.

## Argomenti correlati

- Utenti

38

- Notifiche 17
- Eventi 22
- Audit 31
- Allarmi 24
- Codici di accesso condivisi 46
- Codici di emergenza 48

## 5.4 Rete

Utilizzare la schermata Rete per visualizzare o modificare le impostazioni di rete di un controllore. Le impostazioni si applicano solo al controllore a cui si accede. Per modificare il collegamento in rete di un Controllore secondario, è necessario accedere direttamente a quel Controllore utilizzando il link nella sua pagina Hardware 61.

Si consiglia di assegnare al controller primario un indirizzo IP statico. Nella maggior parte dei casi, i controller secondari dovrebbero utilizzare DHCP, a meno che non sia possibile utilizzare Discovery 70 .

Selezionare **Ethernet** per modificare la connessione cablata o **WiFi** per impostare la rete wireless (sui modelli supportati). Quando le impostazioni di rete vengono salvate, il controller si riavvia e potrebbe avere un indirizzo di rete diverso.

### Proprietà della rete

Queste proprietà si applicano sia alle connessioni cablate che a quelle wireless.

Configurazione

- **IPv4Manuale** - Il controller avrà un indirizzo IP statico e tutte le impostazioni devono essere inserite nelle restanti proprietà.
- **Utilizzo di DHCP** - Il controller riceve tutte le impostazioni dalla rete. Il suo indirizzo IP sarà essenzialmente casuale e potrà cambiare di giorno in giorno. Non è necessario inserire altre proprietà.

| | |
|---|---|
| Indirizzo IP | L'indirizzo IP statico da utilizzare per il controller a cui si accede. |
| Maschera di sottorete | La maschera della rete, di solito "255.255.255.0". |
| Gateway | Indirizzo IP del gateway Internet, di solito l'indirizzo del router di rete. |
| Server DNSL' | indirizzo IP del vostro server DNS, solitamente specificato dal vostro reparto IT o fornito dal vostro provider di servizi Internet. Se non lo sapete, potete usare un DNS pubblico. (Uno di questi è "Google Public DNS" a "8.8.8.8" e "8.8.4.4"). |
| Ricerca domini | Utilizzato solo su indicazione dell'amministratore di rete |

## Impostazione del WiFi

1. Selezionare **WiFi** nell'elenco.
2. Selezionare **Attivo** per attivare il WiFi.
3. Fare clic sul pulsante **Scansione reti.** Nella finestra dei risultati, selezionare una rete a cui unirsi.
4. Fare clic sul pulsante **Modifica** per inserire e confermare la password di rete.
5. Impostare le proprietà della rete.
6. Fare clic su **Salva.**

## Reset della rete

Se in qualsiasi momento si scopre che non è possibile connettersi al controller con l'indirizzo IP definito, si può provare a ripristinare la rete.

Il reset della rete cambia il controller in un indirizzo IP "link local", che consente di collegarsi direttamente al computer. Tramite questa connessione è possibile accedere all'applicazione di gestione Web per correggere le impostazioni di rete.

1. Individuare la piccola apertura sul controller con l'etichetta "Reset". Inserire una graffetta per premere il pulsante per 5-10 secondi. L'indirizzo cablato del controller tornerà al valore predefinito, 169.254.202.242, fino al riavvio, al reset o alla modifica della configurazione.
2. Collegare un cavo Ethernet direttamente dal computer al controller.
3. Se il computer è impostato per utilizzare un indirizzo IP statico, è necessario cambiarlo temporaneamente con uno compreso nell'intervallo 169.254.202.xxx o con uno DHCP. Se si utilizza già DHCP, saltare questo passaggio. Se non lo sapete, provate a supporre che usiate DHCP, il che è comune.
4. Aprire un browser Web e inserire l'indirizzo predefinito del controllore, **169.254.202.242**. Verrà visualizzata la schermata di accesso all'applicazione di gestione Web. La connessione potrebbe richiedere un minuto prima di essere disponibile.

## Argomenti correlati

- Utilizzo delle viste delle proprietà 14

## 5.5 Data e ora

Data e ora si usa per impostare il fuso orario del controllore primario e le impostazioni dell'ora di rete (NTP).

Per impostare il fuso orario del controllore primario, selezionare il fuso orario in cui è installato il controllore primario. Per impostazione predefinita, i controllori sono impostati sul fuso orario dell'**Est (USA e Canada)**.

La casella di controllo **Usa l'ora legale** determina l'applicazione dell'ora solare.

**Data e ora** mostra l'ora del controller. **Browser Time** è l'ora del computer.

L'opzione **Imposta l'ora del server sull'ora corrente del browser** può essere utilizzata se non si utilizza NTP, per sincronizzare una sola volta l'ora del controllore con l'ora del browser. Si noti che questa operazione non sincronizza il fuso orario del browser, ma solo l'ora assoluta sottostante.

La casella di controllo **Aggiorna automaticamente la data e l'ora dalla rete** determina se viene utilizzato l'NTP.

Per impostazione predefinita, i controllori primari sono configurati per utilizzare l'NTP per ottenere l'ora dalla rete e sono preconfigurati con un set predefinito di server NTP. Queste impostazioni predefinite presuppongono che il controller abbia accesso a Internet. In caso contrario, è possibile utilizzare i server NTP all'interno della rete o disattivare completamente l'NTP se non è disponibile.

## 5.6 Impostazioni e-mail

Le Impostazioni e-mail sono utilizzate per configurare un server SMTP per l'invio di copie delle notifiche via e-mail, se configurate da un Utente. Le e-mail vengono inviate all'indirizzo e-mail associato all'utente specifico nella schermata Utenti. nella schermata Utenti.

Queste impostazioni sono riportate di seguito. Di solito queste impostazioni provengono da un provider Internet, da un provider di servizi di posta elettronica o dal reparto IT dell'azienda. Assicuratevi di testare le impostazioni con il pulsante **Invia posta di prova**.

| | |
|---|---|
| Attivo | Attiva o disattiva le impostazioni della posta elettronica. |
| Inviare la posta Da | Inserire l'indirizzo e-mail "da" per le notifiche via e-mail. Le e-mail saranno "da" questo indirizzo e-mail. |
| Posta SMTP Server | Il nome host del server di posta SMTP attraverso cui inviare i messaggi di posta. |
| Porta | Porta del server di posta SMTP. |
| Nome utente | Nome utente per l'account del server di posta SMTP. |
| Password | password per l'account del server di posta SMTP. |

Usare SSL/TLSCheck per utilizzare una connessione sicura e crittografata quando si comunica con il server di posta.

In corrispondenza della voce **Posta di prova**, inserire un indirizzo e-mail a cui inviare e fare clic su **Invia posta di prova** per verificare le impostazioni.

## Argomenti correlati

- Utenti 38
- Notifiche 17

## 5.7 Archivio Download

Eventi 22, Audit 31 e allarmi 24 vengono archiviati dopo che il sistema ha funzionato abbastanza a lungo da superare i limiti definiti in Impostazioni di sistema 100. Questo elenco sarà vuoto fino al raggiungimento di tali limiti.

I file sono archiviati in formato CSV. È possibile selezionarne uno qualsiasi e scaricarlo.

## Argomenti correlati

- Impostazioni di sistema 100
- Eventi 22
- Audit 31
- Allarmi 24

## 5.8 Impostazioni del firmware

## Firmware

Questa sezione mostra la versione attuale del firmware e ne consente l'aggiornamento. Vedere Aggiornamento del firmware 71 .

### Reset di fabbrica

Questa sezione consente di eseguire un ripristino di fabbrica 141 e un pulsante per riavviare il dispositivo.

## 5.9 Impostazioni del server web

Impostazioni del server web serve a caricare un certificato HTTPS firmato, per connessioni più sicure.

**Nota:** se non viene caricato un certificato, verrà utilizzato un certificato autofirmato, con conseguente avviso del browser. Il reparto IT può fornire facoltativamente un certificato firmato per HTTPS, che non è necessario per la comunicazione HTTPS crittografata, ma offre una maggiore sicurezza ed evita gli avvisi del browser.

1. Procurarsi un file di certificato ".pem" o ".pfx" e copiarlo sul computer.
2. Fare clic su **Carica certificato**.
3. Completare le richieste online per selezionare e caricare il file del

certificato. La modifica del certificato comporta il riavvio del controller.

## 5.10 Dispositivi mobili autorizzati

Un dispositivo mobile deve essere autorizzato prima di potersi collegare al sistema Atlas Series.

Per autorizzare un dispositivo, creare un'autorizzazione qui. Quindi scattare una foto del dispositivo
**Codice di autorizzazione** (un codice QR) quando l'applicazione mobile lo richiede.

Ogni codice può autorizzare un solo dispositivo mobile. È possibile eliminare e aggiungere autorizzazioni se necessario per supportare più dispositivi. Il numero di dispositivi autorizzabili è limitato dalla licenza. Contattare il rappresentante autorizzato ZKTeco per l'aggiornamento della licenza 15 .

# Proprietà dei dispositivi mobili autorizzati

| | |
|---|---|
| Nome | Il nome dell'autorizzazione. Richiesto, massimo 32 caratteri. |
| Abilitato | Selezionare per abilitare. Deselezionare per disabilitare. |
| Valido daLa | data di inizio dell'autorizzazione. L'impostazione predefinita è la data corrente. |
| Fino a nuovo avviso, valido A | Se l'opzione **Fino a nuovo avviso** è selezionata, l'autorizzazione del dispositivo non scade mai. Se è deselezionata, è necessario fornire la data di **validità**, che determina la scadenza dell'autorizzazione. |
| Autorizzazione Codice | Il codice QR dell'autorizzazione viene visualizzato qui una volta salvata l'autorizzazione. È possibile fare clic con il tasto destro del mouse su questa immagine per salvarla e inviarla via e-mail a un utente. |

## Accesso da un dispositivo mobile

1. Installare ed eseguire l'applicazione mobile "Atlas", disponibile nell'"App Store" di Apple e in "Google Play".
2. Premere **Scansione codice QR**.
3. Potrebbe essere necessario confermare che Atlas può utilizzare la fotocamera.
4. Viene visualizzato il mirino fotografico. Puntare la casella di scansione quadrata su una qualsiasi copia del codice QR di autorizzazione. Quando un codice QR si trova all'interno del riquadro, viene scattata automaticamente una foto che mostra il messaggio "Codice di autorizzazione individuato con successo".
5. Viene visualizzata la schermata "Accedi". Inserire l'indirizzo del server del controllore Atlas Series primario. Inserire il "Nome utente" e la "Password" della serie Atlas. Premere **Accedi**.
6. Una volta effettuato l'accesso, viene visualizzato un elenco di tutte le operazioni

possibili, tra cui la visualizzazione degli allarmi o dello stato e l'avvio del blocco di emergenza.

**Importante:** il dispositivo mobile deve essere collegato via WiFi alla stessa rete locale dei controllori della serie Atlas. Per collegarsi a distanza, l'amministratore di rete deve

aprire in qualche modo l'accesso da Internet (ad esempio utilizzando un NAT) e fornire il necessario "indirizzo server".

## Argomenti correlati

- Utilizzo delle viste elenco

# 6 Caratteristiche e compiti

Questa sezione fornisce informazioni sulle funzioni che si estendono a più schermate e informazioni sulle attività comuni.

Blocco 111 , Sblocco d'emergenza 113 e Sollecitazione 114 sono utilizzati per gestire le emergenze situazioni 120 .

Rapporti e stampa 115 spiega come stampare dall'applicazione di gestione web

Gli operatori utilizzano i comandi manuali per sbloccare direttamente le porte o per modificare temporaneamente la loro modalità di porta.

Sblocco della prima credenziale consente al primo arrivato di sbloccare completamente una porta. Utilizzare i punti di registrazione delle carte per registrare le carte di un utente strisciando la carta.

Anti-passback scoraggia le persone dal prestare o condividere la propria carta d'accesso.

È possibile reimpostare la password se avete registrato il prodotto 15.

Reset di fabbrica Riporta il controller alle impostazioni di fabbrica e rimuove tutte le configurazioni e i dati.

L'installazione guidata deve essere completata una volta durante l'installazione e dopo un ripristino di fabbrica.

## 6.1 Blocco

Il blocco globale è una funzione da utilizzare in situazioni di emergenza per bloccare tutte le porte del sistema, in modo da non consentire l'accesso. Programmato 115 e comandate manualmente Le modifiche della modalità porta non hanno effetto durante il blocco.

Ci sono delle eccezioni:

- Le porte 73 Le porte con l'opzione **Esente da blocco globale** selezionata non sono interessate.
- Codici di emergenza 48 , e gli utenti 138 con l'opzione **Accesso alle porte in modalità di blocco** selezionata sono in grado di accedere alle porte in stato di blocco.
- I pulsanti di uscita continuano a funzionare durante l'isolamento.

- Blocco contro sblocco di emergenza[113]:

- Uno sblocco di emergenza annulla un blocco se lo sblocco di emergenza avviene dopo il blocco.
- Un blocco annulla uno sblocco di emergenza 113 se il blocco avviene dopo lo sblocco di emergenza.
- Una condizione di sblocco di emergenza si ripresenterà quando un blocco viene annullato, se la sua condizione di attivazione è ancora attiva.

Il blocco globale può essere avviato tramite l'applicazione web, con il pulsante nella barra degli strumenti superiore. Può essere avviato anche tramite l'applicazione mobile. È presente anche un pulsante per cancellare il blocco, accanto ad esso.

Nelle proprietà del subcontrollore (I/O) 61 un ingresso ausiliario può essere configurato con un collegamento per avviare un blocco se l'ingresso diventa attivo. Questo può essere utilizzato per creare un pulsante di blocco fisico. Si noti che se un blocco viene avviato da un ingresso, può essere annullato solo tramite l'applicazione web o mobile.

Quando viene avviato il blocco, viene generato un evento 92 viene generato un 87 evento. Esiste un trigger di allarme 24 predefinito che genera un allarme in base a questo evento.

Se attivo, lo stato di blocco del sistema è chiaramente indicato nella parte superiore dello schermo 17 (indipendentemente dalla visualizzazione): "**SISTEMA SOTTO BLOCCO!**", in rosso. Inoltre, il conteggio dei Controllori e delle Porte bloccati viene visualizzato nelle statistiche del cruscotto nella home. schermata 7 . Si noti che quando un controllore si trova in uno stato di blocco, significa che tutti gli elementi del controllore sono in stato di blocco.
le porte del controllore sono in stato di blocco (a parte le eccezioni di cui sopra). Tutte le schermate che mostrano lo stato della porta o del controllore mostreranno questo stato (Stato della porta 26 , Mappe 28 , ecc.).

In un sistema con controllori primari e secondari, quando il controllore primario avvia il blocco, lo avvia anche per tutti i controllori secondari, consentendo un blocco totale del sistema.

Le singole porte possono essere messe manualmente in modalità di blocco utilizzando i comandi manuali 115 . Si noti che una porta non può avere una modalità 60 di blocco predefinita o programmata. di blocco predefinita o programmata.

**Importante:** come per tutte le funzioni di emergenza, il blocco deve essere testato prima del

tempo, per assicurarsi che tutto sia configurato e funzioni correttamente.

**Importante:** le funzioni delle uscite di emergenza sono regolamentate dalle norme antincendio specifiche di ogni paese e regione. Per garantire la conformità del sistema, è necessario fare riferimento a queste norme durante la progettazione e la configurazione.

## Argomenti correlati

- Caratteristiche di emergenza
- Sblocco di emergenza

## 6.2 Sblocco di emergenza

Lo sblocco globale di emergenza è una funzione da utilizzare in situazioni di emergenza per sbloccare tutte le porte del sistema. Comando programmato e il comando manuale Le modifiche della modalità porta non hanno effetto durante lo sblocco di emergenza.

Ci sono delle eccezioni:

- Le porte Le porte con l'opzione **Esente dallo sblocco di emergenza globale** selezionata non sono interessate.
- Blocco e sblocco di emergenza
  - Uno sblocco di emergenza annulla un blocco se lo sblocco di emergenza avviene dopo il blocco.
  - Un blocco annulla uno sblocco di emergenza se il blocco avviene dopo lo sblocco di emergenza.
  - Una condizione di sblocco di emergenza si ripresenterà quando un blocco viene annullato, se la sua condizione di attivazione è ancora attiva.

Nella schermata Hardware è necessario configurare un ingresso ausiliario per attivare lo sblocco di emergenza di tutte le porte. Queste porte rimangono sbloccate finché l'ingresso è attivo.

Lo sblocco globale dell'emergenza può essere attivato solo da un ingresso ausiliario. Anche la cancellazione dell'emergenza è regolata dall'ingresso.

Quando viene avviato uno sblocco di emergenza globale, viene generato un Evento viene generato. Esiste un trigger di allarme predefinito che genera un allarme in base a questo evento.

I conteggi dei controllori e delle porte sbloccati in emergenza sono visualizzati nel cruscotto. statistiche nella schermata principale . Si noti che quando un Controllore si trova in una

situazione di emergenza, non è possibile sbloccarlo.
significa che tutte le porte del controller sono in stato di sblocco di emergenza (a parte le eccezioni di cui sopra). Tutte le schermate che mostrano la porta o il controllore mostrerà questo stato (Stato porta 26, Mappe 28, ecc.).

In un sistema con controllori primari e secondari, quando il controllore primario avvia lo sblocco di emergenza, avvia anche lo sblocco di emergenza per tutti i controllori secondari, consentendo lo sblocco totale del sistema.

Le singole porte possono essere messe manualmente in modalità di sblocco di emergenza utilizzando i comandi manuali 115. Si noti che una porta non può avere una modalità predefinita o programmata di di emergenza sbloccata.

**Importante:** come per tutte le funzioni di emergenza, lo sblocco di emergenza deve essere testato in anticipo, per assicurarsi che tutto sia configurato e funzioni correttamente.

**Importante:** le funzioni delle uscite di emergenza sono regolamentate dalle norme antincendio specifiche di ogni paese e regione. Per garantire la conformità del sistema, è necessario fare riferimento a queste ultime durante la progettazione e la configurazione. Lo sblocco di emergenza è inteso come un'integrazione, ma non come una sostituzione, delle porte correttamente cablate per l'uscita di emergenza in conformità alle norme antincendio.

## Argomenti correlati

- Caratteristiche di emergenza 20
- Blocco 111

## 6.3 Costrizione

Il PIN di costrizione è un PIN alternativo che l'utente può immettere al posto del PIN normale per indicare in modo discreto una situazione di costrizione durante l'accesso alla porta (ad esempio, se è minacciato da un intruso). Dal punto di vista dell'utente, l'accesso allo sportello funziona normalmente, senza alcuna indicazione che lo sportello sia diverso. All'utente viene concesso o negato l'accesso secondo le stesse regole abituali. Nel sistema, tuttavia, in queste condizioni viene registrato un evento aggiuntivo, la **costrizione**.

L'evento Duress 22 è configurato come trigger di allarme per impostazione predefinita, generando un allarme 24.

Inoltre, l'evento di costrizione 22 è una delle opzioni che possono essere utilizzate come collegamento per attivare l'uscita ausiliaria nella schermata Hardware. nella schermata Hardware.

Il **PIN di emergenza** è configurato nella schermata Utenti per ogni utente.

Il **PIN di emergenza** può essere derivato automaticamente dal PIN normale utilizzando il metodo **Aggiungi 1 all'ultima cifra: Ad esempio,** a un PIN normale di 1111 corrisponderà un PIN di sicurezza di 1112, mentre a un PIN normale di 9999 corrisponderà un PIN di sicurezza di 9990.

In alternativa, è possibile specificare esplicitamente il **PIN Duress.**

Si noti che il valore del **PIN Duress** deve essere unico, anche rispetto a tutti i codici PIN normali, ai codici di accesso condivisi 46 e ai codici di accesso di emergenza 48 .

## Argomenti correlati

- Caratteristiche di emergenza 20

## 6.4 Rapporti e stampa

La stampa dall'applicazione di gestione Web è disponibile in due situazioni.

- Pulsanti di menu "Esporta PDF": Alcune viste elenco includono questo pulsante nel menu. Ovunque appaia questa opzione, è possibile creare un report di tutto ciò che è presente nell'elenco attualmente visualizzato.
- Pulsanti della schermata con etichette quali "Genera" o "Stampa scheda". Questi pulsanti appaiono direttamente nelle schermate dedicate alla stampa di documenti speciali.

La stampa di rapporti e altri documenti viene eseguita tramite il browser web. In tutti i casi, l'applicazione crea un documento formattato chiamato file PDF. A seconda della marca di browser utilizzata, sono disponibili due opzioni o entrambe. Entrambe sono attivate dai comandi del browser, non dall'applicazione di gestione Web.

- Salvare il file sul computer. È quindi possibile visualizzare o stampare il rapporto utilizzando un programma di visualizzazione PDF.
- Aprire immediatamente il file, dove è possibile visualizzarlo e stamparlo con le funzionalità del browser.

## 6.5 Comandi manuali

Comandi manuali è un pulsante di menu che comanda direttamente le porte per sbloccare o cambiare la modalità della porta 142 . Il pulsante appare in qualsiasi schermata in cui sono

elencate le porte. Le opzioni di comando sono:

| | |
|---|---|
| Momentaneo Accesso | Sblocca momentaneamente la porta per un singolo accesso. |
| Imposta modalità porta | Modifica la modalità porta 142.<br>- Se si seleziona **Fino all'annullamento o alla prossima modifica programmata**, la modalità verrà applicata fino all'annullamento o alla prossima modifica programmata.<br>- Altrimenti, inserire una **Durata**, specificando la durata del cambio di modalità. |
| Annulla | Annulla una precedente modifica manuale della modalità porta effettuata in questa schermata. |

## Argomenti correlati

- Stato della porta 26
- Mappe (Monitoraggio) 23
- Porte 73
- Modalità della porta 142

## 6.6 Primo sblocco delle credenziali

Le modalità della porta con "Primo sblocco" rimangono bloccate solo fino al successivo accesso valido. La porta si sblocca e rimane sbloccata fino al successivo cambio di modalità programmato (o al cambio di modalità da un comando manuale).

Il primo sblocco delle credenziali è disponibile ovunque sia selezionata la modalità porta.

Una volta presentati una tessera e un PIN validi, la porta passerà in modalità **sbloccata.** Questo sarà visibile ovunque sia visualizzato lo stato della porta. La modalità può essere modificata in seguito utilizzando i comandi manuali 115.

## Argomenti correlati

- Porte 73
- Orari della modalità porta 90
- Comandi manuali 115
- Stato della porta 26

## 6.7 Punti di iscrizione alla carta

È possibile designare i lettori da utilizzare per aggiungere carte a un utente senza digitare il numero della carta. Potreste anche non conoscere il numero della tessera. Questi lettori sono chiamati punti di iscrizione delle carte e sono un tipo di porta. È anche possibile utilizzare qualsiasi lettore di schede per creare le schede per i nuovi utenti.

## Impostazione di un punto di registrazione della carta

È necessario un controllore con una configurazione che includa "+ Punto di registrazione della tessera". È possibile farlo quando si aggiunge un controllore 69 70, oppure si può modificare un controllore esistente. un Controllore esistente. In questo caso, una delle porte del controllore sarà un punto di registrazione della tessera.

Ogni utente può selezionare un punto di registrazione della carta da utilizzare. Selezionare la scelta in Menu: Preferenze .

## Utilizzo di un punto di registrazione della carta

Nella schermata Utenti 98 è possibile visualizzare la schermata

1. Fare clic su "Aggiungi" accanto alla casella "Carte".
2. Cliccare sul campo "Numero di carta".
3. Passare la carta al punto di registrazione della carta.

## Utilizzo di qualsiasi lettore per l'iscrizione

Qualsiasi lettore di schede del sistema può essere utilizzato per registrare un nuovo utente o per scoprire il numero di una scheda.

1. Passare la carta su qualsiasi lettore.
2. Andare alla schermata Eventi 22 schermo.
3. Individuare l'evento corrispondente **Accesso negato (numero di carta sconosciuto)**. Il numero della carta è indicato nella colonna Utente.
4. Fare clic sul numero della scheda per creare un nuovo utente con questa scheda.

Se la scheda è attualmente assegnata a un altro utente, si otterrà un evento diverso.

## Argomenti correlati

Hardware 56

Utenti 38

## 6.8 Anti-Passback

Usare l'anti-passback per impedire o rilevare gli utenti che attraversano la stessa porta due volte di seguito, senza uscire dall'area o attendere il periodo di tempo specificato. Ad esempio, gli utenti possono entrare da un'area con controllo di sicurezza, ma devono uscire da un'altra area.

L'anti-passback ha lo scopo di impedire a qualcuno di "ripassare" una credenziale affinché un'altra persona la utilizzi alla stessa porta o a un'altra porta che accede alla stessa area. Questo sistema è comunemente utilizzato con i tornelli e altri dispositivi di ingresso speciali. L'anti-passback basato sull'area può anche aiutare a prevenire la condivisione dei PIN. Tuttavia, con una porta normale non c'è modo di impedire che un utente la tenga aperta per un altro.

Se viene effettuato un tentativo di accesso che viola le regole anti-passback, verrà sempre creato un Evento 22 . All'utente può essere negato o meno l'accesso, a seconda della configurazione.

Esistono due metodi di applicazione dell'anti-passback.

- Basato sulle porte - Una porta può essere aperta dalla stessa credenziale solo una

volta durante un periodo di tempo prestabilito.

- Basato sull'area - L'anti-passback basato sull'area tiene traccia della posizione di un utente e genera una violazione se la sua credenziale viene utilizzata altrove. Ad esempio, se la porta 1 esce dall'area A ed entra nell'area B, e la porta 2 esce dall'area B ed entra nell'area C, la presentazione della stessa credenziale alla porta 1, poi alla porta 2, poi di nuovo alla porta 1 rappresenta una violazione dell'anti-passback, perché è noto che l'utente si trova nell'area C quando tenta di utilizzare una porta che esce dall'area A.

**Nota: L'**anti-passback non si applica agli utenti esenti da 46, Codici di emergenza 48 o codici di accesso condivisi (vedi sotto).

## Definizione delle aree anti-passback

Nella schermata 70 Aree è possibile definire le aree da utilizzare per l'anti-passback. È anche possibile utilizzare le aree predefinite, come Global Out.

## Configurazione delle porte anti-passback

Nella schermata 75 Porte è possibile definire le aree di entrata e di uscita e le impostazioni di antipassaggio.

1. Vai alle 73 porte.
2. Sotto aree e Anti-passback:
   a. Selezionare l'**area di inserimento**. Questa è l'80 area in cui la porta entra
   b. Selezionare l'**Area esistente**. Questa è l'80 area da cui esce la porta.
3. Selezionare il Metodo anti-passback:
   a. **Basato sull'area** - L'anti-passback viene applicato a questa porta utilizzando qualsiasi ingresso o uscita dall'area. Selezionare una modalità di anti-passback per concedere o negare l'accesso.
   b. **Basato sulla porta** - L'antipassback viene applicato esclusivamente in base all'accesso a questa porta. Immettere il numero di minuti in cui lo stato di anti-passback viene ripristinato dopo l'ingresso dell'utente nella porta.
4. Fare clic su **Salva**.

## Utenti esenti da passback

Per escludere gli utenti dalle regole di anti-passback, selezionate la casella **Anti-passback esente nella schermata** Utenti. nella schermata Utenti.

## Perdonare le violazioni dell'Anti-passback

Il pulsante **Perdono** nella schermata Utenti azzera lo stato di anti-passback dell'utente selezionato. Si usa quando le regole anti-passback impediscono l'accesso di un utente e si decide di perdonare la violazione.

## Argomenti correlati

- Utenti 38
- Aree 80
- Porte 73

# 6.9 Ripristino della password

Se si perdono le password di tutti gli utenti con il ruolo di amministratore, è possibile richiedere a ZKTeco un'autorizzazione per la reimpostazione della password via Internet. Questo è possibile solo se ci si è precedentemente registrati con ZKTeco, in modo da poter confermare il vostro indirizzo e-mail.

## Come reimpostare la password dell'amministratore

1. Nella schermata di accesso, fare clic su **Reimposta password**.
2. Fare clic sul pulsante **Richiedi la reimpostazione della password.**
3. In caso di successo, verrà visualizzato il messaggio "Un file di autorizzazione per la reimpostazione della password è stato inviato via e-mail a ".

Quando si riceve l'e-mail di risposta:

1. Aprite la mail e salvate l'allegato ("password.reset") sul vostro computer.

2. Tornare a **Reimpostare la password.**
3. Fare clic sul pulsante **Carica file di autorizzazione.**
4. Trovate e aprite il file salvato via e-mail.
5. Nella finestra seguente, inserire e **inviare** una nuova password per l'utente "admin".

## Argomenti correlati

- Registrazione del prodotto 15

## 6.10 Reset di fabbrica

Il reset di fabbrica serve a ripristinare la configurazione iniziale di un controllore.

**Avvertenze e informazioni**

- Questa operazione cancella il database. Tutti i dati e le configurazioni esistenti saranno cancell
- La password di amministrazione verrà ripristinata su
- Le informazioni relative alla registrazione del prodotto 15 andranno perse, anche se con ZKTeco.
- Le impostazioni di Rete 103 *non* vengono ripristinate. Se il controller dispone di un non cambierà. Se è impostato per il DHCP, probabilmente si riavvierà con lo stesso
  - Se è stato installato un certificato HTTPS 108, questo *non* verrà rimosso.
  - Le impostazioni di Data e Ora 105 *non* vengono ripristinate.

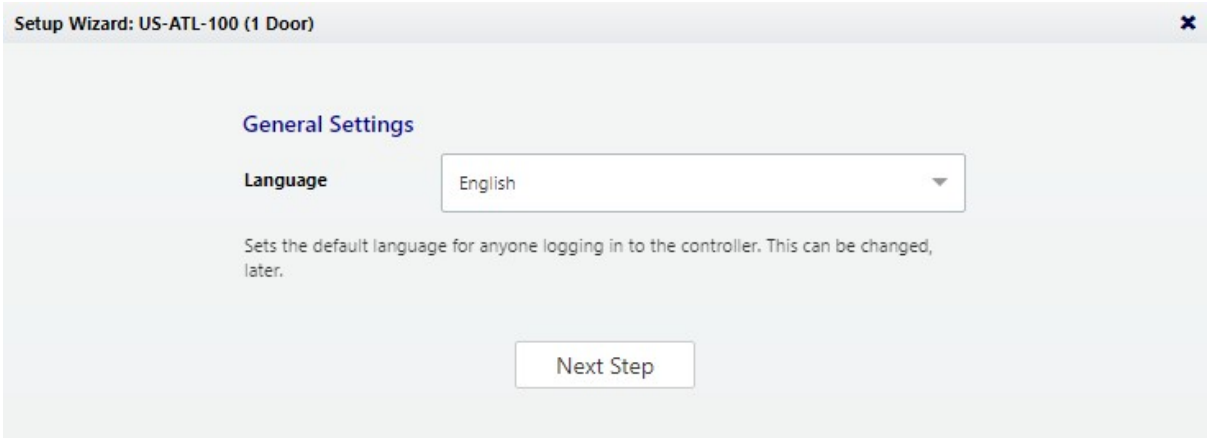
1. Andare su Impostazioni firmware 101 ed espandere la sezione **Ripristino dati di fabbrica.**

2. Fare clic su **Ripristino dati di fabbrica.**
3. Verrete disconnessi. Attendere il riavvio del controller e quindi effettuare il login.
4. Verrà visualizzata l'Installazione guidata 122, che deve essere completata.

## 6.11 Installazione guidata

La procedura guidata di configurazione viene visualizzata al primo accesso e dopo un ripristino di fabbrica 121. Deve essere completata. Tuttavia, è possibile uscire in qualsiasi momento e completarla successivamente.

### Pagina 1: Lingua



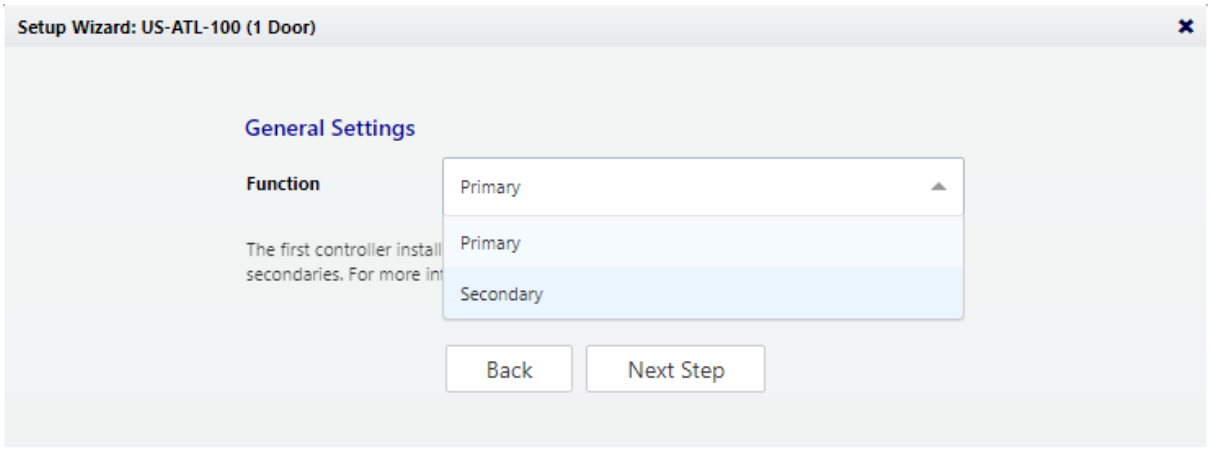

**clicca per ingrandire**

Scegliere una lingua. La scelta verrà utilizzata per questa procedura guidata. Se si tratta di un controllore primario, diventerà anche la lingua predefinita dell'applicazione di gestione web. Se si tratta di un Controllore secondario, diventerà la lingua predefinita dell'applicazione di gestione semplificata su questo Controllore.

Le lingue disponibili dipendono dal rappresentante della licenza software per gli aggiornamenti della licenza. 15. Contattare il proprio rivenditore autorizzato ZKTeco

Questa impostazione può essere modificata nelle proprietà hardware del controllore.

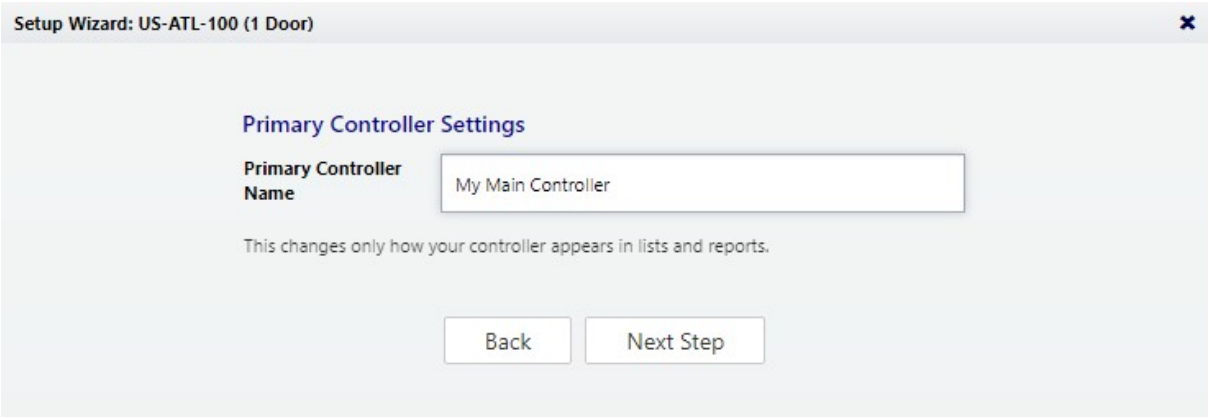
### Pagina 2: Funzione




clicca per ingrandire

Scegliere se questo controllore sarà primario o secondario, come discusso in Comprendere i controllori e le porte. 55

## Pagina 3: Nome del controllore primario (solo primari)

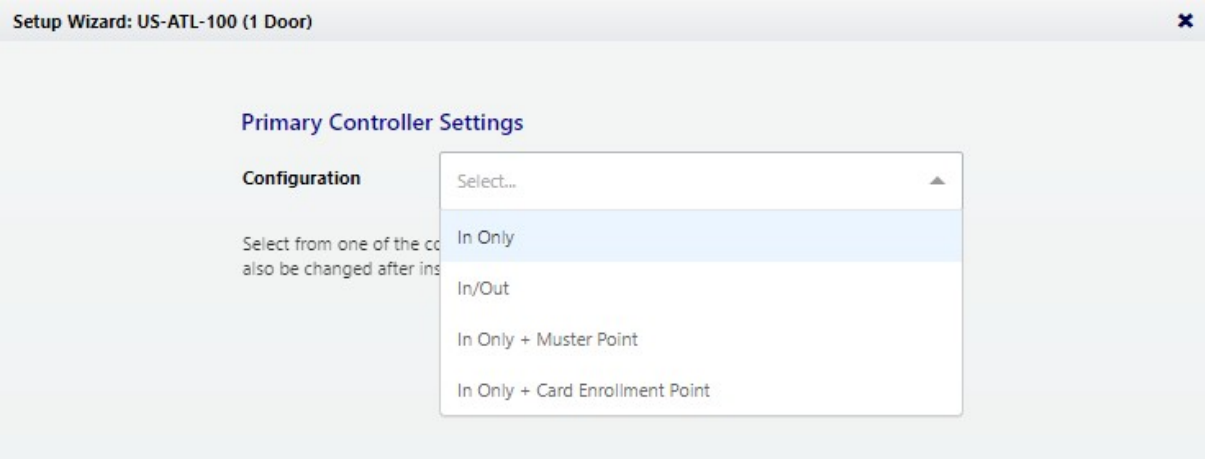



clicca per ingrandire

Il nome del controllore verrà utilizzato per la visualizzazione nell'applicazione di gestione web e nei report.

Nota: I controller secondari vengono nominati quando sono collegati al sistema nell'applicazione di gestione Web.

## Pagina 4: Configurazione (solo primari)

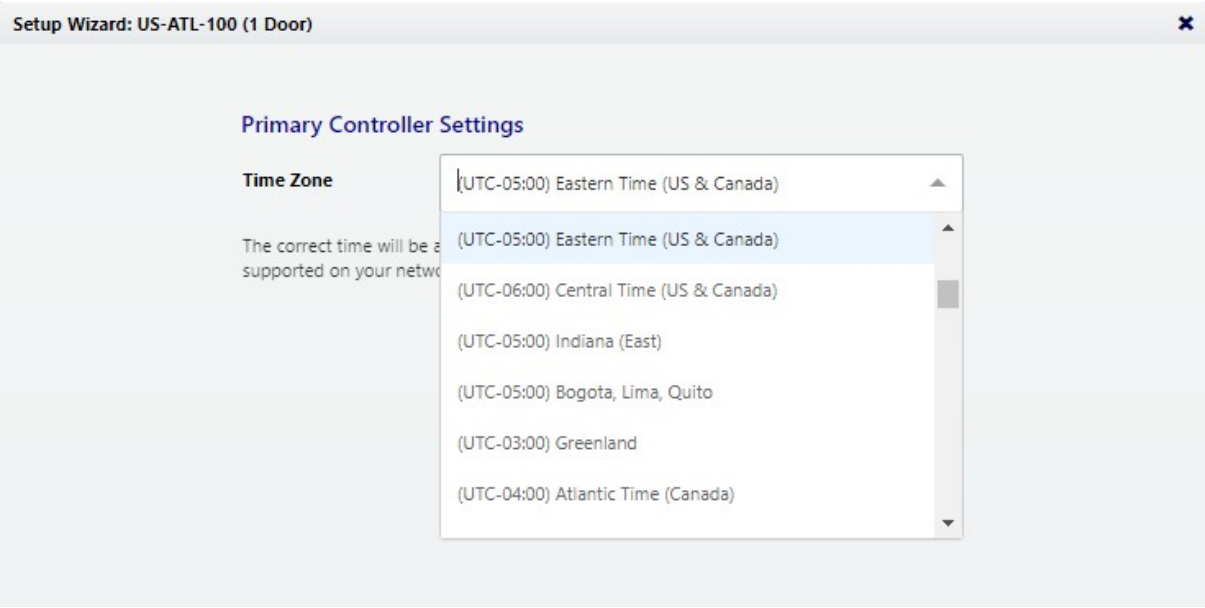



**clicca per ingrandire**

Vedere Proprietà di configurazione del controllore 57 .

Nota: I controllori secondari vengono configurati quando sono collegati al sistema.

## Pagina 5: Fuso orario (solo primarie)

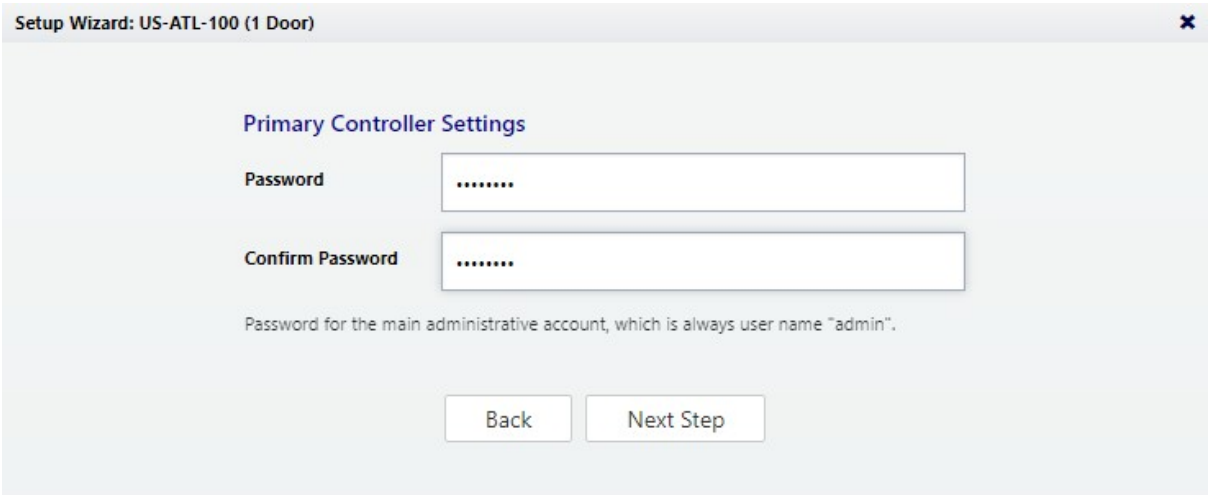



**clicca per ingrandire**

Selezionare il fuso orario. Nella maggior parte dei casi non sarà mai necessario impostare l'ora attuale; il controllore otterrà l'ora da Internet utilizzando una tecnologia chiamata NTP. In alcuni casi l'NTP non funziona a causa di firewall o criteri di rete. In questo caso, 105 vedere Data e ora
dopo aver completato la procedura guidata.

Nota: i controllori secondari ricevono l'ora e il fuso orario dal controllore primario.

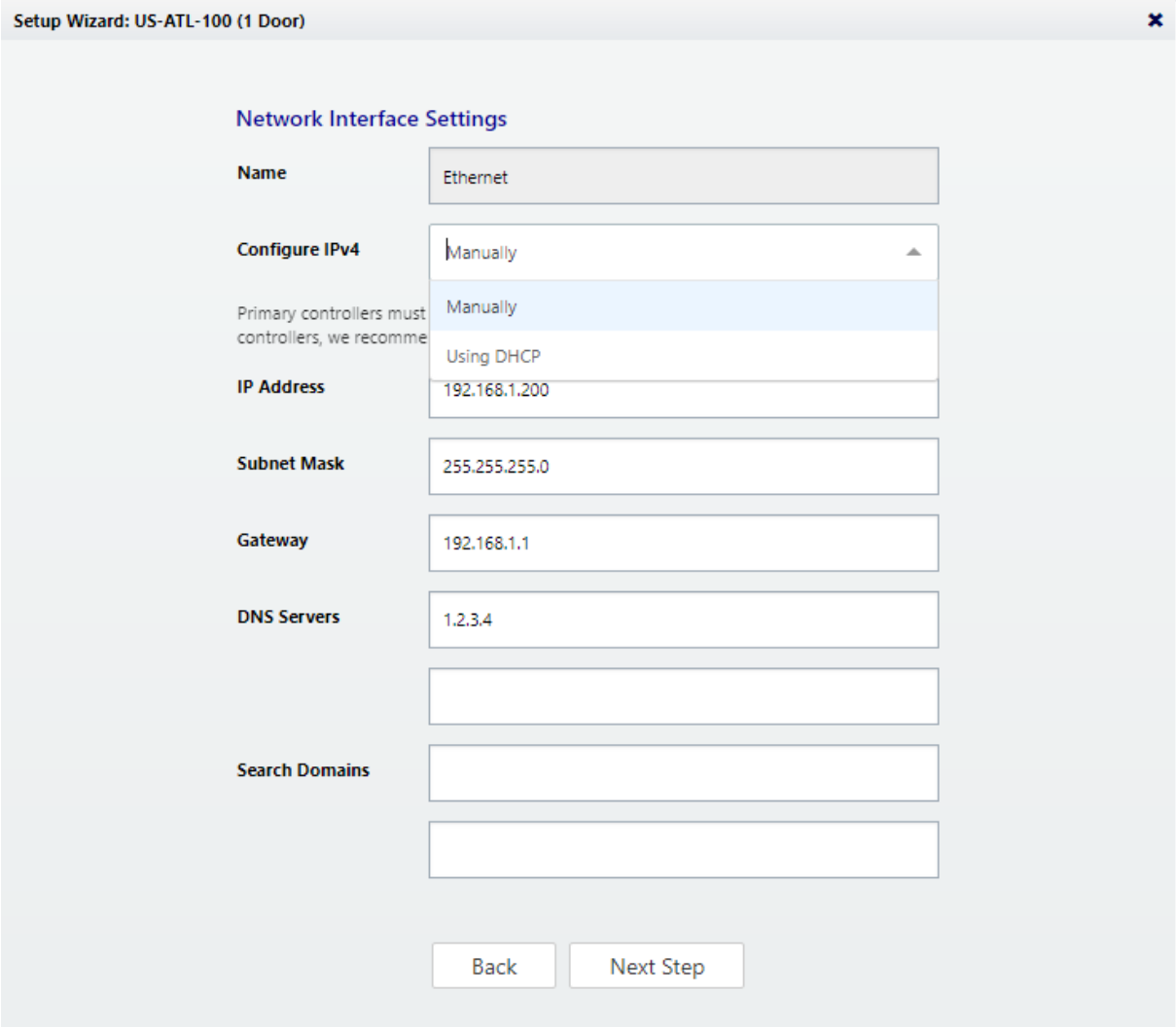
## Pagina 6: Password (solo per le primarie)




**clicca per ingrandire**

Inserire una password forte per l'account amministratore primario. Il nome utente di questo account è "admin" e non può essere modificato.

## Pagina 7: Impostazioni dell'interfaccia di rete




**clicca per ingrandire**

Se è stato appena eseguito un Ripristino delle impostazioni di fabbrica, queste impostazioni dovrebbero essere già impostate come prima del ripristino.

La scelta importante è "Configura IPv4".

Un controller primario deve avere un indirizzo IP statico. Questo perché i controller secondari devono sapere come trovare il primario sulla rete. Inoltre, gli utenti hanno bisogno di un indirizzo coerente per accedere all'applicazione di gestione Web.

Per assegnare un indirizzo IP statico, scegliere "Manualmente" e inserire l'indirizzo IP e la configurazione specificati dall'amministratore di rete.

"Usare DHCP" è probabilmente la scelta giusta per i controllori secondari, a meno che tutti i controllori non possano trovarsi su una sola subnet di rete o se il rilevamento è bloccato da restrizioni di rete. In questo caso:

? Assegnare a questi controllori indirizzi IP statici.

? Aggiungere manualmente questi controllori secondari nell'applicazione di gestione Web invece di usare Discovery.

Vedere Rete 103 per ulteriori informazioni o per apportare modifiche in un secondo momento.

## Pagina 8: Revisione

Tutte le voci vengono visualizzate per essere esaminate. Fare clic su "Indietro" o su "Completa impostazione".

# 7 Riferimento

Materiale di riferimento:



## 7.1 Glossario

**Livello di accessoUn** insieme di coppie porta/schedario che definisce l'accesso a quelle porte durante gli orari associati.

**Riconosciuto** Quando un utente è a conoscenza di un allarme, ma non è stato fatto nulla al riguardo.

**Camera di compensazione** Una regola che si applica a più porte in un'area e che limita le porte che possono essere aperte contemporaneamente.

**Allarme** Innescato da un evento, un allarme è come una copia dell'evento che può cambiare stato da Nuovo a Riconosciuto a Risolto, allo scopo di rendere gli utenti consapevoli del problema e di tenere traccia di se e quali sono stati risolti.

**Attivazione dell'allarme** Attiva un allarme da un evento

**Anti-passback** Una regola che impedisce o rileva il "passing-back" di una credenziale da una persona a un'altra, l'utilizzo della stessa credenziale per due volte di seguito presso la stessa Porta o l'accesso alla stessa Area.

**Audit** Una registrazione di una modifica apportata al sistema da un utente o di un comando manuale eseguito da un utente.

**Monitoraggio batteriaUn** ingresso di un controllore configurato per rilevare se una batteria è collegata o meno.

**Biometrico** Una caratteristica di una persona che può essere utilizzata come credenziale per l'identificazione o la verifica, come un'impronta digitale.

**Tessera**

La tessera è una credenziale codificata con un numero utilizzata per il controllo elettronico degli accessi. Può essere disponibile anche in altre forme, come un fob.

Conosciuto anche come "Distintivo".

**Design della tesseraUn** design grafico, comprendente elementi di immagine e di testo, alcuni dei quali provenienti dal record dell'utente, che può essere utilizzato per stampare sulla superficie di una tessera. Conosciuto anche come "Design del badge".

**Punto di registrazione della carta** Un lettore configurato non per il controllo degli accessi, ma per ottenere il numero della carta a scopo di registrazione.

Formato **della** cartaSpecifica tecnica del formato dei bit di dati codificati su una carta, tra cui numero di carta, codice di struttura e parità. Diversi fornitori forniscono carte diverse codificate con formati diversi.

**Numero della cartaLa** parte dei bit di dati codificati su una carta che corrisponde a un numero unico e identificativo.

**Controllore** Dispositivo fisico elettronico che controlla gli ingressi e le uscite per il controllo degli accessi. I controllori della serie Atlas possono essere controllori primari o secondari.

**CSV** Valori separati da virgola. Un formato di file di testo che può essere importato o esportato da Microsoft Excel e altri programmi di fogli di calcolo per ufficio.

**DHCP** Dynamic Host Configuration Protocol. Un'opzione di rete in cui un dispositivo ottiene il proprio indirizzo IP e altre impostazioni di rete automaticamente da un router, un gateway o un altro dispositivo di rete.

**Porta** Una combinazione di lettori, ingressi e uscite che controlla elettronicamente l'accesso a una porta fisica o a qualcosa di funzionalmente simile a una porta, come un cancello di parcheggio. Conosciuto anche come "Punto di accesso" o "Portale".

**Modalità portaLa** modalità di funzionamento di una porta, che specifica se la porta è semplicemente sbloccata, se è bloccata e non disponibile per l'accesso, o bloccata e richiede la presentazione di credenziali per sbloccarla.
La modalità comprende anche quali tipi di credenziali (carta, PIN, biometrica) sono richieste.

**Modalità porta**

**Programma** Una pianificazione con una serie di intervalli di tempo (compresi i giorni della settimana).

e i tipi di giorno speciale), in cui ogni intervallo di tempo può essere associato a

con una modalità porta. La programmazione della modalità porta può essere associata a una porta per modificare automaticamente la modalità della porta in base alla programmazione.

**Sensore di portaUn** ingresso cablato per rilevare se una porta è aperta o chiusa. Conosciuto anche come "contatto porta" o "interruttore di posizione porta".

**Modello di portaUn** insieme di proprietà della porta che può essere associato a più porte per riutilizzare combinazioni comuni di proprietà senza doverle inserire nuovamente. Utilizzato anche per modificare le proprietà di più porte contemporaneamente, semplicemente cambiando il modello di porta associato.

**PIN di emergenza Un** codice PIN alternativo utilizzato per segnalare una condizione di emergenza. L'accesso viene concesso e negato normalmente come se fosse stato utilizzato il PIN normale. Quando l'accesso viene concesso utilizzando un PIN di costrizione, viene generato un evento Accesso consentito (costrizione), che attiva un allarme all'interno del software, per impostazione predefinita.

Codice **di emergenzaUn** codice PIN che deve essere utilizzato dal personale di emergenza o di alta sicurezza in una situazione di emergenza per accedere a una porta, indipendentemente dalla modalità della porta (compreso il blocco).

**Evento** Registrazione di un evento all'interno del sistema. Include attività hardware e di accesso. Conosciuto anche come "transazione".

**Pulsante di uscitaUn** ingresso cablato per rilevare che la porta deve essere sbloccata per uscire. Generalmente si trova sul lato non sicuro della porta (il lato verso cui ci si rivolge quando si esce). Può essere un pulsante o un altro tipo di dispositivo, come un sensore di movimento. Conosciuto anche come "Richiesta di uscita (REX)".

**Codice** strutturaUn numero codificato su una tessera oltre al numero di tessera, utilizzato per identificare una struttura, un cliente o un lotto di tessere. Una singola azienda spesso ordina carte con lo stesso Facility Code. La lunghezza esatta e la posizione del Facility Code all'interno dei bit di dati della carta possono essere specificate nei

Formati della carta e il valore effettivo del Facility Code previsto può essere specificato anche lì.

**Codice antincendioLe leggi** e le norme di un determinato Paese o regione che specificano come gli edifici, i sistemi di allarme antincendio e altri sistemi elettronici devono essere progettati, costruiti, configurati e gestiti ai fini della sicurezza della vita.

| | |
|---|---|
| **Firmware** | Software che gira su un dispositivo incorporato, come un controller. |
| **Apertura forzataUna** | condizione in cui una porta è stata fisicamente aperta (secondo il sensore di porta), ma è ancora bloccata. Cioè, è stata aperta senza un accesso valido, una richiesta di uscita, un comando manuale o una modalità porta che ne consenta l'apertura. |
| **Modello di hardware** | Un insieme di proprietà del controllore che può essere associato a più controllori per riutilizzare combinazioni comuni di proprietà senza doverle reinserire. Si usa anche per modificare le proprietà di più controllori contemporaneamente, cambiando semplicemente il modello di controllore associato. |
| **Tenuto apertoUna** | condizione in cui una porta è stata aperta, ma non chiusa entro un determinato periodo di tempo. |
| **HTTPS** | Un protocollo per la comunicazione tra un browser web e un server web, protetto dalla crittografia. |
| **In (Porta)** | Una porta configurata per entrare (In). Può essere abbinata a una porta di uscita, nel qual caso la porta di ingresso controlla gli ingressi e le uscite condivisi. |
| **Entrata/Uscita** | Una configurazione su un controllore con 2 porte, una per l'ingresso (In) e una per l'uscita (Out). Queste due porte rappresentano due lati della porta fisica. |
| **Ingresso** | Ingresso elettronico di un controllore in grado di rilevare un circuito attivo o inattivo. |
| **Indirizzo IP** | Un indirizzo numerico per i dispositivi e i computer di una rete. |
| **Ubicazione** | Un'etichetta che indica il nome di una posizione, che può essere disposta in una gerarchia per organizzare Hardware, Porte, Aree e Mappe. |
| **Serratura** | Un'uscita di un controllore configurata per il collegamento a una serratura elettronica fisica della porta. Conosciuto anche come "apriporta". |
| **Blocco** | Uno stato di emergenza per una porta o un controllore in cui la porta (o tutte le porte associate al controllore) sono bloccate e negano l'accesso a tutte le credenziali (con alcune eccezioni). Il |

blocco non è influenzato dalle modifiche programmate della modalità porta e dai normali comandi manuali.

**Comando manualeUn** comando eseguito da un utente nell'applicazione web o nell'app mobile che influisce su una porta o su un controllore. Ad esempio, consente l'accesso momentaneo a una porta o modifica la modalità di u n a porta.

**Mappa** Un layout grafico di una struttura, spesso con una planimetria, che mostra la posizione delle porte e dei controllori, con il loro stato.

**Accesso multiutenteRegole** che richiedono l'accesso a una porta da parte di più utenti di più gruppi di utenti.

**Muster** Un rapporto che mostra l'ultimo accesso conosciuto di ciascun utente, se non si tratta dell'accesso alle aree Global Out o Muster.

**Punto di raccoltaUna** porta utilizzata semplicemente per registrare che un utente ha raggiunto l'area di raccolta, ai fini del rapporto di raccolta.

**Normalmente chiuso (NC)** Un tipo di configurazione di ingresso in cui la condizione normale, "inattiva", dell'ingresso è la chiusura del circuito. Gli ingressi normalmente chiusi sono il sensore porta, il tamper, il monitor di alimentazione e il monitor batteria.

**Normalmente aperto (NO)** Un tipo di configurazione di ingresso in cui la condizione normale, "inattiva", dell'ingresso è la chiusura del circuito. Gli ingressi normalmente chiusi sono il sensore di porta, il tamper, il monitor di alimentazione e il monitor della batteria.

**Notifica** Una copia all'interno dell'applicazione di determinati eventi sottoscritti da ciascun utente. Una copia delle notifiche può anche essere configurata per essere inviata via e-mail.

**NTP** Network Time Protocol. Protocollo per la sincronizzazione dell'ora di computer e dispositivi su una rete o su Internet. I server NTP forniscono un'ora affidabile e precisa ai dispositivi e ai computer che si iscrivono ai loro servizi.

**OSDP** Open Supervised Device Protocol. Protocollo standard per il collegamento dei lettori ai controllori tramite RS-485.

Una porta configurata per l'uscita (**Out** ), che è sempre abbinata a una porta per l'ingresso (In). La porta In è quella che controlla gli ingressi e le uscite condivise.

| | |
|---|---|
| **Uscita** | Un'uscita elettronica su un controller che funziona come un interruttore elettronico e può controllare altri dispositivi, come un lucchetto. |
| **Parità** | Un tipo di bit di dati all'interno di un formato di scheda utilizzato per garantire l'integrità dei dati letti. Un bit di parità funge da controllo su un insieme di valori binari, calcolati in modo tale che il numero di 1 nell'insieme più il bit di parità sia sempre pari (o occasionalmente, sia sempre dispari). |
| **PDF** | Formato di documento portatile. Un formato utilizzato per documenti o rapporti che possono essere facilmente visualizzati o stampati su un PC. |
| **PIN** | Numero di identificazione personale. Credenziale costituita da un codice numerico da inserire sulla tastiera di un lettore a scopo di identificazione o verifica. |
| **Politica** | Una regola che collega eventi e condizioni ad azioni o output. Conosciuta anche come "collegamento". |
| **Power MonitorUn** | ingresso di un controllore configurato per rilevare se l'alimentazione principale è collegata o meno. |
| Controllore **primarioII** | controllore della serie Atlas del sistema che mantiene l'intera configurazione del sistema e ospita l'applicazione web utilizzata per accedere, configurare e monitorare il sistema. Un controllore primario può gestire più controllori secondari. |
| **Lettore** | Legge le carte o le credenziali, tra cui eventualmente la carta, il PIN o la biometria. |
| **Risolto** | Lo stato di un allarme che significa che è stato completamente risolto, cioè che non è più un problema che richiede attenzione o che deve essere visibile. |
| **RS-485** | Protocollo di comunicazione seriale utilizzato per le comunicazioni tra dispositivi, compresi i controllori e i lettori. OSDP utilizza ad esempio il protocollo RS-485. |
| **Programmazione** | Un insieme di intervalli di tempo (compresi i giorni della settimana e i tipi di giorni speciali), utilizzati per regolare l'accesso allo sportello in base all'orario. |

| | |
|---|---|
| **Controllore secondario** | Un controllore della serie Atlas che ottiene la propria configurazione da un controllore primario |
| **Codice di accesso condivisoUn** | codice PIN condiviso da un gruppo di persone, utilizzato per accedere a una porta. |
| **Server SMTP** | Un server di posta elettronica per l'invio di e-mail |
| **Giorno specialeUn** | giorno del calendario (ad esempio un giorno festivo) in cui il normale accesso alla porta non è consentito per impostazione predefinita, a meno che il Programma non indichi esplicitamente che i giorni speciali sono consentiti. |
| **Tipo di giornata speciale** | Una categoria o un raggruppamento di giorni speciali. |
| **SSL** | Un altro termine per TLS, un protocollo di crittografia di rete. |
| **Sottocontrollore** | Un tipo di controllore che gestisce gli ingressi e le uscite (I/O) ma non prende decisioni di accesso o di altro tipo da solo. In alcuni sistemi, questi subcontrollori sono dispositivi fisici separati. Nella serie Atlas, sono integrati nei controllori. |
| **Tamper** | Un ingresso di un controllore configurato per rilevare la manomissione fisica di una custodia, di un involucro, ecc. |
| **TLS** | Un protocollo di crittografia di rete |
| **Ruolo dell'utenteUn** | insieme di autorizzazioni per ciò che un utente può o non può fare quando è connesso all'applicazione web o all'applicazione mobile. |
| **Gruppo di utenti** | Una classificazione o un raggruppamento di utenti utilizzato per l'accesso multiutente. |
| **Wiegand** | Protocollo standard per il collegamento dei lettori ai controllori. |

## 7.2 Categorie e tipi di eventi

Colori dell'evento:

- Rosso: L'evento è anche un trigger di allarme per impostazione predefinita. Se si creano trigger di allarme aggiuntivi, tali eventi appariranno rossi nell'applicazione di gestione

Web. Se si rimuovono i trigger integrati, gli eventi appariranno gialli.

- Giallo: Avvertenze
- Verde: Accesso normale concesso

- Bianco: Informativo

## Sistema

| | |
|---|---|
| Accesso riuscito | Un utente accede con successo all'applicazione |
| Accesso non riuscito | Un utente tenta senza successo di accedere all'applicazione - generica |
| Firmato in uscita | Un utente esce dall'applicazione Il |
| Avvio del controllore | controllore si avvia |
| Risincronizzazione del controllore | I dati risincronizzati su un Controllore La pianificazione diventa attiva |
| Programmazione attiva | Il programma diventa inattivo |
| Programmazione inattiva | |
| Accesso non riuscito (inattivo) | Un utente tenta senza successo di accedere all'applicazione - inattivo |
| Accesso non riuscito (non ancora efficace) | Un utente tenta senza successo di accedere all'applicazione - non ancora effettivo |
| Accesso non riuscito (scaduto) | Un utente tenta senza successo di accedere all'applicazione - scaduto |
| Accesso non riuscito (nessun privilegio) | Un utente tenta senza successo di accedere all'applicazione - nessun ruolo dell'utente |
| Accesso non riuscito (fuori programma) | Un utente tenta senza successo di accedere all'applicazione - al di fuori dell'orario previsto. |

| | |
|---|---|
| Firmware di lettura della scheda (registrazione) aggiornato | Una scheda è stata letta su un punto di registrazione.<br>Firmware aggiornato |
| Aggiornamento del firmware non riuscito | Aggiornamento del firmware non riuscito |
| Backup del database | Base di dati ripristinata |

| | |
|---|---|
| Backup del database non riuscito | Backup del database non riuscito |

## Accesso consentito

| | |
|---|---|
| Accesso consentito | Generico |
| Accesso consentito (porta già aperta) | Porta già aperta |

## Accesso negato

| | |
|---|---|
| Accesso | Generic |
| Accesso negato | Scheda |
| Accesso negato (non ancora | Prima della validità |
| Accesso negato | Dopo la validazione |
| Accesso negato (nessun | Nessun livello di accesso o porta/schema corrispondente |
| Accesso negato (fuori programma) | Corrisponde al livello di accesso o all'assegnazione della porta, |
| Accesso negato (numero di carta | Numero di carta |
| Accesso negato (formato | Lo schema dei bit di dati sulla scheda non è |
| Accesso negato (PIN unico | PIN sconosciuto utilizzato per il solo PIN o per il primo PIN |
| Accesso negato (codice struttura | Formato carta riconosciuto, ma Codice struttura |
| Accesso negato (nessun | La modalità della porta è |
| Accesso negato (nessun accesso | La modalità porta non consente l'uso della scheda, ma la scheda |

| | |
|---|---|
| Accesso negato (nessun accesso al PIN) | La modalità porta non consente l'uso del PIN, ma il PIN è stato presentato. |
| Accesso negato (non è stato definito un PIN di conferma) | La modalità porta richiede un PIN, ma l'utente non ha un PIN definito |
| Accesso negato (nessun biometrico definito) | La modalità porta richiede la biometria, ma l'utente non è registrato. |
| Accesso negato (PIN di conferma errato) | La modalità porta richiede la conferma del PIN, ma il PIN inserito non corrisponde a quello di conferma. |
| Accesso negato (nessun accesso biometrico) | La modalità porta non consente la biometria, ma la biometria presentata è un'altra. |
| Accesso negato (biometrico sconosciuto) | Biometrico sconosciuto presentato in modalità solo biometrica o biometrico presentato per primo (verifica biometrica uno a molti) |
| Accesso negato (biometria errata) | Biometria errata o non valida presentata (verifica biometrica uno a uno) |
| Accesso negato (lettura biometrica errata) | È stato presentato un dato biometrico, ma non è stato possibile leggerlo/elaborarlo. |
| Accesso negato (Anti-passback) | Violazione dell 'Anti-passback |
| Accesso negato (blocco) | La modalità porta è blocco |
| Accesso negato (non è stato presentato il PIN) | La modalità porta richiede il PIN, ma non viene presentato alcun PIN |
| Accesso negato (incompleto) | Credenziali presentate in modo incompleto (ad esempio cifre parziali del PIN) |

| | |
|---|---|
| Accesso negato (nessun biometrico presentato) | La modalità porta richiede la biometria, ma non viene presentata alcuna biometria. |
| Accesso negato (nessuna carta presentata) | La modalità porta richiede la carta, ma non è stata presentata alcuna carta. |

| | |
|---|---|
| Accesso negato (carta errata) | La modalità porta richiede/consente alla scheda di essere presentato dopo un PIN o un dato |
| Accesso negato (camera di | Le regole della camera d'equilibrio verrebbero violate dalla accesso (un'altra porta nell'area |
| Accesso negato (nessuna credenziale multipla) | La regola multi-credenziale è in vigore, ma la regola |

## Comunicazioni

| | |
|---|---|
| Controllore online | Controllore online (controllore secondario, sottocontrollore (I/O)) |
| Controllore offline | Controllore online (controllore secondario, sottocontrollore (I/O)) |
| Lettore | onlineLettore online (OSDP, ZKTeco RS-485) |
| Lettore offline | Lettore offline (OSDP, ZKTeco RS-485) |

## Porta

| | |
|---|---|
| Porta aperta forzatamente | Porta aperta senza essere sbloccata |
| Porta forzata aperta ripristinata | La condizione di apertura forzata della porta non è presente o non è più presente. |
| Porta tenuta aperta | La porta è rimasta aperta troppo a lungo dopo essere stata aperta |
| Ripristino della porta aperta | La condizione di porta aperta non è presente o non è più presente. |
| Porta porta) | apertaPorta aperta (secondo il sensore di |

Porta chiusaPorta chiusa (secondo il sensore porta)

Modalità porta: SbloccatoIndicazione modalità porta

Modalità porta: Nessun accessoIndicazione modalità porta

Modalità porta: Solo cartaIndicazione modalità porta

Modalità porta: Indicazione della modalità carta e PINDella modalità porta

Modalità porta: Solo PINIndicazione della modalità porta

Modalità porta: Indicazione modalità porta: carta o PIN

| | |
|---|---|
| Modalità porta: Sbloccato | Indicazione della |
| Modalità porta: Blocco | Indicazione della |

Modalità porta: Solo scheda (primo sblocco)Indicazione modalità porta

Modalità porta: Indicazione della modalità porta: carta e biometrica

Modalità porta: Indicazione della modalità porta: tessera, biometrica e PINDoor

Modalità porta: Solo biometricoIndicazione modalità porta

Modalità porta: Indicazione biometrica e PINDella modalità porta

Modalità porta: Indicazione biometrica o PINModalità porta

Modalità porta: Scheda o biometricaIndicazione della modalità porta

Modalità porta: Biometrico, scheda o PINIndicazione della modalità porta

Uscita richiestaPulsante di uscita attivo, che attiva l'accesso all'uscita

| | |
|---|---|
| Porta momentaneamente | Accesso momentaneo Comando manuale inviato |
| Avviso di porta aperta | Avvertenza prima che la porta venga tenuta aperta troppo a lungo dopo essere stata aperta |
| Modalità porta: Nessun accesso, nessun porta | pulsante di uscitaIndicazione della modalità |
| Uscita richiesta (porta già aperta) | Pulsante di uscita attivo, che attiva l'accesso all'uscita - Porta già aperta |

| | |
|---|---|
| Porta momentaneamente sbloccata (porta già aperta) | Accesso momentaneo Comando manuale inviato dall'applicazione - La porta è già aperta |
| Richiesta di uscita negata | Pulsante di uscita attivo, ma accesso all'uscita non attivato - generico |
| Porta Accesso momentaneo negato | Accesso momentaneo Comando manuale inviato dall'applicazione - non eseguito (negato) - generico |
| Richiesta di uscita negata (camera di compensazione occupata) | Pulsante di uscita attivo, ma accesso all'uscita non attivato perché violerebbe le regole della camera di compensazione (un'altra porta nell'area configurata per la camera di compensazione è sbloccata/aperta). |
| Accesso momentaneo alla porta negato (camera di compensazione occupata) | Comando manuale di accesso momentaneo inviato dall'applicazione - non eseguito (negato), perché violerebbe le regole della camera di compensazione (un'altra porta nell'area configurata per la camera di compensazione è sbloccata/aperta). |
| Modalità porta:Scheda e PIN (primo sblocco) | Indicazione della modalità porta |
| Modalità porta: Solo PIN (primo sblocco) | Indicazione modalità porta |
| Modalità porta: Carta o PIN (primo sblocco) | Indicazione modalità porta |
| Modalità porta: Scheda e biometrica (primo sblocco) | Indicazione della modalità della porta |
| Modalità porta: Scheda, biometrica e PIN (primo sblocco) | Indicazione della modalità della porta |
| Modalità porta: Solo biometrico (primo sblocco) | Indicazione della modalità porta (primo sblocco) |
| Modalità porta: Biometrico e PIN | |

Indicazione della modalità della porta

Modalità porta: Biometrico o PIN (primo sblocco)Indicazione modalità porta

Modalità porta: Scheda o biometrica (primo sblocco) Indicazione della modalità della porta

| | |
|---|---|
| Modalità porta: Biometrico, scheda o PIN (primo sblocco) | Indicazione della modalità della porta |
| Modalità di accesso al controller: Sbloccato (emergenza) | Sblocco di emergenza a livello di controllore |
| Modalità di accesso del controllore: Blocco | Blocco a livello di controllore |
| Modalità di accesso del controllore: Nessuno | Sblocco o blocco di emergenza a livello di controllore abilitato |
| Costrizione | Costrizione (è stato inserito il PIN di costrizione) |
| Codice di emergenza presentato | Codice di emergenza presentato |
| Modalità di accesso globale: Sbloccato (emergenza) | Sblocco di emergenza a livello globale |
| Modalità di accesso globale: Blocco | Blocco a livello globale |
| Modalità di accesso globale: Nessuno | Sblocco o blocco di emergenza a livello globale autorizzato |

## Ingresso/uscita

| | |
|---|---|
| Uscita | inattivaUscita inattiva |
| Uscita | attivaUscita attiva |
| Ingresso | inattivoOutput inattivo |
| Ingresso | AttivoIngresso inattivo |

## Tamper/potenza

| | |
|---|---|
| Su | Alimentazione principaleL'ingresso di monitoraggio |
| Spento Alimentazione principale | L'ingresso Power Monitor è attivo |
| dell'alimentazione è inattivo | |

| | | |
|---|---|---|
| Batteria ripristinata | | L'ingresso di monitoraggio della batteria è inattivo. |
| Guasto della batteria | | L'ingresso Battery Monitor è attivo |

| | |
|---|---|
| Tamper ripristinato | L'ingresso Tamper è inattivo |
| TamperL'ingresso | Tamper è attivo |

## 7.3 Modalità della porta

La modalità della porta determina se la porta si trova in uno stato immutabile (sbloccato, sbloccato (emergenza), non accessibile, bloccato) o in uno stato di accesso controllato, che richiede la presentazione di credenziali per l'accesso. Quando sono richieste le credenziali, la modalità della porta determina anche quali tipi di credenziali sono necessari.

Quando la modalità porta è impostata inizialmente per una porta, o cambia, viene generato un evento corrispondente (vedere: Categorie e tipi di eventi) 134 . Ad esempio, se la modalità della porta diventa **Solo carta**, viene generato un evento: **Modalità porta: Solo scheda**.

La modalità predefinita di una porta è impostata nella schermata Porte. nella schermata Porte.

Le pianificazioni delle modalità porta possono essere utilizzate per cambiare automaticamente le modalità porta in base a una pianificazione.

Comandi manuali 115 possono essere utilizzati per impostare la modalità porta.

La modalità della porta viene visualizzata anche in Stato porta e ovunque lo stato di una porta sia mostrato (Porte 73 , 82 ). Mappe

La maggior parte delle modalità di porta ad accesso controllato ha una variante **(Primo sblocco)**. Vedere Primo sblocco della credenziale per i dettagli.

Di seguito sono elencate tutte le modalità di una porta:

Sbloccato

Sbloccato (emergenza)

Nessun accesso

Blocco

Accesso vietato, uscita vietata

Solo con tessera

Solo carta (primo

sblocco) Carta e PIN

Carta e PIN (primo sblocco)

Solo PIN

Solo Pin (primo sblocco)

Carta o PIN

Scheda o PIN (primo sblocco)

Scheda e biometrica

Scheda e biometrica (primo

sblocco) Scheda e biometrica e PIN

Carta, biometrica e PIN (primo sblocco) Solo

biometrica

Solo biometrico (primo

sblocco) Biometrico e PIN

Biometrico e PIN (primo sblocco)

Biometrico o PIN

Biometrico o PIN (primo sblocco)

Scheda o biometrico

Scheda o biometrico (primo

sblocco) Biometrico o scheda o PIN

Biometrico, carta o PIN (primo sblocco)

Si noti che un controllore può essere posto in una modalità porta speciale durante il blocco globale e lo sblocco di emergenza[113]. Gli eventi generati per questo a livello globale sono:

**- Modalità di accesso globale: Sbloccato (emergenza)**

- **Modalità di accesso globale: Blocco**
- **Modalità di accesso globale: Nessuno**

Gli eventi generati per questo a livello di controllore (secondario) sono:

- **Modalità di accesso al controller: Sbloccato (emergenza)**
- **Modalità di accesso del controllore: Blocco**
- **Modalità di accesso del controllore: Nessuno**

## Argomenti correlati

- Porte 73
- Orari della modalità porta 150
- Comandi manuali 115
- Primo sblocco delle credenziali 146
- Blocco 111
- Sblocco di emergenza 120
- Eventi 22
- Categorie e tipi di eventi 134

# Indice

## - F -

www.zkteco.eu