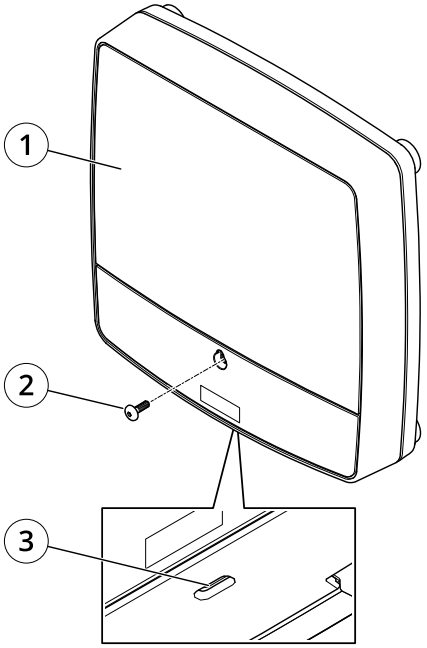
AXIS A1001 & AXIS Entry Manager

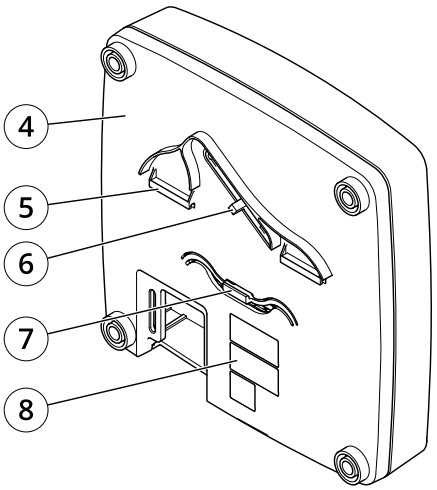
Manuale per l'utente

Sommario

Panoramica del dispositivo

Panoramica del dispositivo

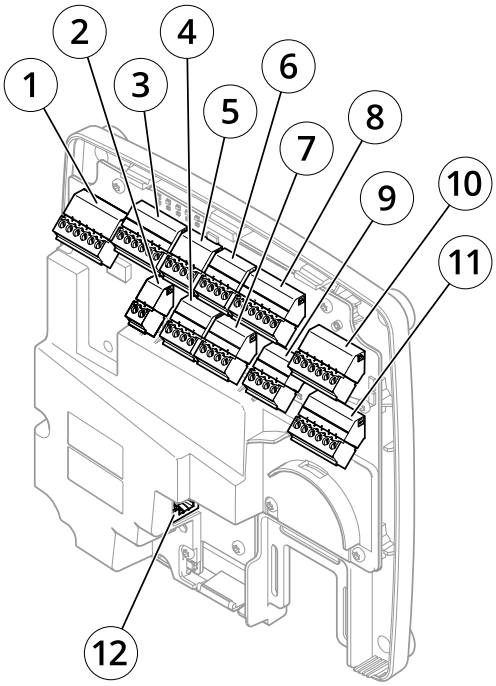




Vista anteriore e posteriore:

1 *Coperchio*
2 *Vite del coperchio*
3 *Slot di rimozione coperchio*
4 *Base*
5 *Clip DIN superiore*
6 *Interruttore allarme anti-manomissione - retro*
7 *Clip DIN inferiore*
8 *Codice dispositivo (N/P) e numero di serie (N/S)*

Panoramica del dispositivo



Interfaccia I/O:

1 Connettore dati lettore (READER DATA 1)
10 Connettore dati lettore (READER DATA 2)
3 Connettore I/O lettore (READER I/O 1)
8 Connettore I/O lettore (READER I/O 2)
4 Connettore porta (DOOR IN 1)
7 Connettore porta (DOOR IN 2)
6 Connettore ausiliario (AUX)
5 Connettore audio (AUDIO) (non utilizzato)

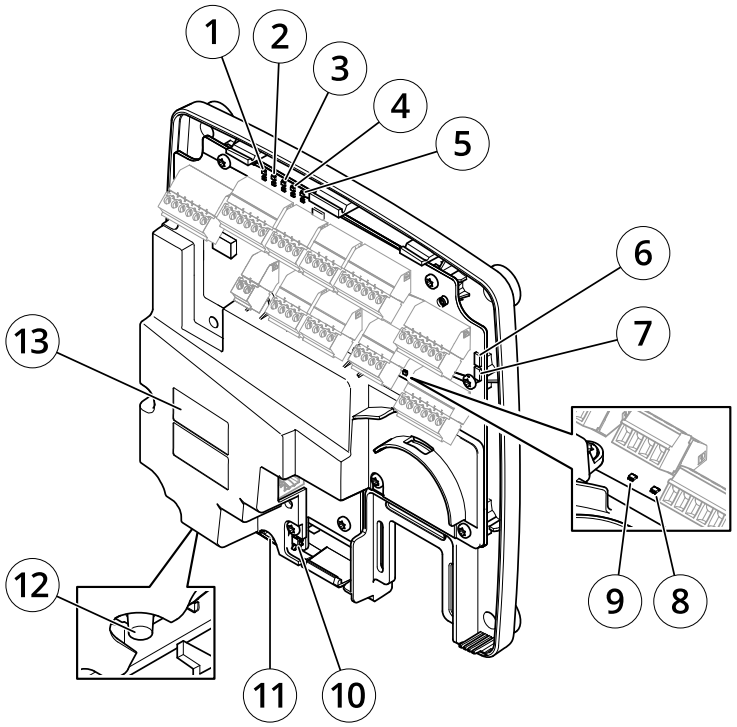
Ingressi alimentazione esterna:

2 Connettore di alimentazione (DC IN)
12 Connettore di rete (PoE)

Uscite alimentazione:

9 Connettore blocco di alimentazione (LOCK)
11 Connettore di alimentazione e relè (PWR, RELAY)

Panoramica del dispositivo



Indicatori LED, pulsanti e altro hardware:

1 *Indicatore LED di alimentazione*
2 *Indicatore LED di stato*
3 *Indicatore LED di rete*
4 *Indicatore LED 2 del lettore (non utilizzato)*
5 *Indicatore LED 1 del lettore (non utilizzato)*
6 *Collettore pin allarmi anti-manomissione - fronte (TF)*
7 *Collettore pin allarmi anti-manomissione - retro (TB)*
8 *Indicatore LED di blocco*
9 *Indicatore LED di blocco*
10 *Sensore allarme anti-manomissione - fronte*
11 *Slot per scheda SD (microSDHC) (non utilizzato)*
12 *Pulsante di comando*
13 *Codice dispositivo (N/P) e numero di serie (N/S)*

Indicatori LED

LED	Colore	Indicazione
Rete	Verde	Luce fissa per connessione di rete a 100 MBit/s. Luce lampeggiante: attività di rete.
	Giallo	Luce fissa per connessione di rete a 10 MBit/s. Luce lampeggiante: attività di rete.
	Spento	Assenza di connessione.
Stato	Verde	Luce verde fissa: condizioni di normale utilizzo.
	Giallo	Fissa durante l'avvio e quando si ripristinano le impostazioni.
	Rosso	Luce lampeggiante lenta: aggiornamento non riuscito.
Alimentazione	Verde	Normale utilizzo.
	Giallo	Luce lampeggiante verde/gialla durante l'aggiornamento del firmware.

Blocco	Verde	Luce fissa: non in tensione.
	Rosso	Luce fissa: in tensione.
	Spento	Isolato.

Nota

- Il LED di stato può essere configurato per lampeggiare quando un evento è attivo.
- Il LED di stato può essere configurato per lampeggiare durante l'identificazione dell'unità. Andare a **Setup > Additional Controller Configuration > System Options > Maintenance (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Manutenzione)**.

Connettori e pulsanti

Interfaccia I/O

Connettori dati lettore
Due morsettiere a 6 pin che supportano protocolli RS485 e Wiegand per la comunicazione con il lettore. Per le specifiche, vedere *pagina 69*.

Connettori I/O lettore
Due morsettiere a 6 pin per l'ingresso e l'uscita del lettore. Oltre al punto di riferimento 0 V CC e all'alimentazione (uscita CC), il connettore I/O lettore fornisce l'interfaccia per:

- Input digitale: ad esempio per il collegamento degli allarmi anti-manomissione del lettore.
- Output digitale – Per collegare ad esempio i suoni acustici e segnali LED del lettore.

Per le specifiche, vedere *pagina 69*.

Connettori porta
Due morsettiere a 4 pin per il collegamento di dispositivi di monitoraggio porta e dispositivi REX (Request to Exit). Per le specifiche, vedere *pagina 70*.

Connettore ausiliario
Morsettiera I/O a 4 pin configurabile. Utilizzare con dispositivi esterni in combinazione con, ad esempio, allarmi antimanomissione, attivazione di eventi e notifiche di allarme. Oltre al punto di riferimento 0 V CC e all'alimentazione (uscita CC), il connettore ausiliario fornisce l'interfaccia per:

- Input digitale: ingresso allarme utilizzabile per collegare i dispositivi, che può passare dal circuito chiuso al circuito aperto, ad esempio i sensori PIR o rilevatori di rottura.
- Output digitale: per collegare dispositivi esterni come allarmi antifurto, sirene o luci. I dispositivi collegati possono essere attivati tramite l'API (interfaccia per la programmazione di applicazioni) VAPIX® oppure tramite una regola di azione.

Per le specifiche, vedere *pagina 71*.

Input alimentazione esterni

AVVISO

Il dispositivo deve essere collegato tramite un cavo di rete schermato (STP). Tutti i cavi che collegano il dispositivo alla rete sono destinati al loro uso specifico. Accertarsi che i dispositivi di rete siano installati secondo le istruzioni del produttore. Per maggiori informazioni sui requisiti normativi, vedere .

Connettore di alimentazione
Morsettiera a 2 pin utilizzata per l'input dell'alimentazione CC. Utilizzare una sorgente di alimentazione limitata (LPS) compatibile con una bassissima tensione di sicurezza (SELV) con una potenza di output nominale limitata a ≤100 W o una corrente nominale di output limitata a ≤5 A. Per le specifiche, vedere *pagina 71*.

Connettore di rete
Connettore Ethernet RJ45. Supporta Power over Ethernet (PoE). Per le specifiche, vedere *pagina 72*.

Output alimentazione

Connettore blocco di alimentazione

Morsettiera a 4 pin per la connessione di uno o due blocchi. Il connettore di blocco può essere usato anche per fornire alimentazione ai dispositivi esterni. Per le specifiche, vedere *pagina 72*.

Connettore del relè e di alimentazione

Morsettiera a 6 pin utilizzata per collegare l'alimentazione e il relè del dispositivo di controllo porte a dispositivi esterni quali blocchi e sensori. Per le specifiche, vedere *pagina 72*.

Pulsanti e altro hardware

Collettore pin allarmi anti-manomissione
Due collettori a due pin per scollegare gli allarmi anti-manomissione anteriore e posteriore. Per le specifiche, vedere *pagina 73*.

Pulsante di comando
Il pulsante di comando viene utilizzato per:

- Ripristino del dispositivo alle impostazioni predefinite di fabbrica. Vedere *pagina 64*.
- Collegarsi a un servizio AXIS Video Hosting System. Vedere *pagina 58*. Per il collegamento, premere e tenere premuto il tasto per circa 1 secondo fino a quando il LED di stato lampeggia in verde.
- Collegamento al AXIS Internet Dynamic DNS Service. Vedere *pagina 58*. Per il collegamento, premere e tenere premuto il tasto per circa 3 secondi.

Installazione

Installazione

Video di installazione del prodotto.

Modalità di accesso al dispositivo

Modalità di accesso al dispositivo

Per installare il dispositivo Axis, vedere la guida all'installazione fornita con il dispositivo.

Accesso al dispositivo

1. Aprire un browser ed inserire il nome di host o l'indirizzo IP del dispositivo Axis.

   Se non si conosce l'indirizzo IP, utilizzare AXIS IP Utility o AXIS Device Manager per individuare il dispositivo sulla rete.

2. Inserire nome utente e password. Se si accede al dispositivo per la prima volta, è necessario impostare la password di default. Vedere .

3. AXIS Entry Manager si apre nel browser. Se si utilizza un computer, verrà visualizzata la pagina Panoramica. Se si utilizza un dispositivo mobile, verrà visualizzata la pagina web in versione mobile.

Informazioni sulla pagina di destinazione del dispositivo mobile

La pagina di destinazione del dispositivo mobile mostra lo stato delle porte e dei blocchi collegati al dispositivo di controllo delle porte. È possibile eseguire la verifica di blocco e sblocco. Aggiornare la pagina per visualizzare il risultato.

Un collegamento indirizzerà ad Axis Entry Manager.

Nota

- Axis Entry Manager non supporta i dispositivi mobili.
- Se si prosegue in Axis Entry Manager, il collegamento alla pagina di destinazione per dispositivi mobili non sarà più disponibile.

Modalità di accesso al dispositivo da Internet

Un router di rete consente ai dispositivi su una rete privata (LAN) di condividere una singola connessione a Internet. Questo avviene inoltrando il traffico di rete da una rete privata a Internet.

La maggior parte dei router è preconfigurata per bloccare i tentativi di accesso alla rete privata (LAN) da una rete pubblica (Internet).

Se il dispositivo Axis si trova su una intranet (LAN) e si desidera renderlo disponibile dall'altro lato (WAN) di un router NAT (Network Address Translator), attivare la funzione **NAT traversal**. Se la funzione è correttamente configurata, tutto il traffico HTTP a una porta HTTP esterna nel router NAT viene inoltrato al dispositivo.

Modalità di attivazione della funzione NAT traversal

- Andare a **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > TCP/IP > Avanzate)**.
- Fare clic su **Enable (Abilita)**.
- Configurare manualmente il router NAT per consentire l'accesso da Internet.

Vedere anche AXIS Internet Dynamic DNS Service all'indirizzo *www.axiscam.net*

Nota

- In questo contesto, il termine "router" fa riferimento a qualsiasi dispositivo di routing di rete come un router NAT, un router di rete, un gateway Internet, un router a banda larga, un dispositivo di condivisione a banda larga o un software, ad esempio un firewall.
- Affinché funzioni, la funzione NAT traversal deve essere supportata dal router. Il router inoltre deve supportare UPnP®.

Modalità di accesso al dispositivo

Come impostare la password root

Per accedere al dispositivo Axis, è necessario impostare la password dell'utente amministratore predefinito **root**. Questa operazione viene effettuata nella finestra di dialogo **Configure Root Password (Configura password root)**, visualizzata quando si accede al dispositivo per la prima volta.

Per evitare intercettazioni sulla rete, la password root può essere impostata tramite una connessione HTTPS crittografata, con un certificato HTTPS. HTTPS (Hypertext Transfer Protocol over SSL) è un protocollo utilizzato per crittografare il traffico tra i browser e i server Web. Il certificato HTTPS assicura lo scambio crittografato di informazioni. Vedere *HTTPS alla pagina 54*.

Il nome utente amministratore predefinito **root** è permanente e non può essere eliminato. Se si smarrisce la password di root, il dispositivo deve essere ripristinato alle impostazioni predefinite di fabbrica. Vedere *Ripristino delle impostazioni predefinite di fabbrica alla pagina 64*.

Per impostare la password, inserirla direttamente nella finestra di dialogo.

Pagina Panoramica

La pagina Panoramica di AXIS Entry Manager visualizza le informazioni relative a: nome del dispositivo di controllo della porta, indirizzo MAC, indirizzo IP e versione del firmware. Consente inoltre di identificare il dispositivo di controllo della porta sulla rete o nel sistema.

La prima volta che si accede al dispositivo Axis, la pagina Panoramica richiederà di configurare l'hardware, per impostare una data e un'ora, per configurare le impostazioni di rete e configurare il dispositivo di controllo della porta come parte di un sistema o un'unità indipendente. Per ulteriori informazioni sulla configurazione del sistema, vedere *Configurazione: passo a passo alla pagina 11*.

Per tornare alla pagina Panoramica dalle altre pagine Web del dispositivo, fare clic su **Overview (Panoramica)** nella barra dei menu.

Configurazione del sistema

Per aprire le pagine di impostazione del dispositivo, fare clic su **Setup (Impostazione)** nell'angolo superiore destro della pagina Panoramica.

Il dispositivo Axis può essere configurato dagli amministratori. Per ulteriori informazioni relative agli utenti e agli amministratori, vedere *pagina 31*, *pagina 40* e *pagina 54*.

Configurazione: passo a passo

Prima di iniziare ad utilizzare il sistema di controllo degli accessi è necessario completare la seguente procedura di configurazione:

1. Se l'inglese non è la lingua madre, è possibile configurare AXIS Entry Manager per l'utilizzo di un'altra lingua. Vedere *Selezione di una lingua alla pagina 11*.
2. Impostare la data e l'ora. Vedere *pagina 11*.
3. Configurare le impostazioni di rete. Vedere *pagina 13*.
4. Configurare il dispositivo di controllo delle porte e i dispositivi collegati quali lettori, blocchi e dispositivi per le richieste di uscita (REX). Vedere *Configurazione dell'hardware alla pagina 13*.
5. Verificare i collegamenti hardware. Vedere *pagina 20*.
6. Configurare le schede e i formati. Vedere *pagina 21*.
7. Configurare il sistema di controllo delle porte. Vedere *Gestione dei dispositivi di controllo porta di rete alla pagina 26*.

Per informazioni su come configurare e gestire porte, pianificazioni, utenti e gruppi del sistema, vedere *Gestione degli accessi alla pagina 31*.

Per informazioni sui consigli per la manutenzione, vedere *Istruzioni di manutenzione alla pagina 29*.

Nota

Per aggiungere o rimuovere i dispositivi di controllo delle porte, per aggiungere, rimuovere o modificare gli utenti oppure per configurare l'hardware, più della metà dei dispositivi di controllo delle porte nel sistema deve essere **online**. Per verificare lo stato del dispositivo di controllo della porta, andare a **Setup > Manage Network Door Controllers in System (Impostazione > Gestisci i dispositivi di controllo delle porte nel sistema)**.

Selezione di una lingua

La lingua predefinita di AXIS Entry Manager è l'inglese ma è possibile passare a qualsiasi altra lingua inclusa nel firmware del dispositivo. Per informazioni sul firmware più recente, vedere *www.axis.com*

È possibile passare a qualsiasi altra lingua in qualsiasi pagina Web del dispositivo.

Per passare a un'altra lingua, fare clic sull'elenco a discesa delle lingue  e selezionare una lingua. Tutte le pagine Web del dispositivo e le pagine della Guida vengono visualizzate nella lingua selezionata.

Nota

- Quando si cambia la lingua, viene modificato anche il formato della data in un formato comunemente utilizzato nella lingua selezionata. Il formato corretto viene visualizzato nei campi dati.
- Se si ripristina il dispositivo alle impostazioni predefinite di fabbrica, AXIS Entry Manager torna alla lingua inglese.
- Se si ripristina il dispositivo, AXIS Entry Manager continuerà ad utilizzare la lingua selezionata.
- Se si riavvia il dispositivo, AXIS Entry Manager continuerà ad utilizzare la lingua selezionata.
- Se si aggiorna il firmware, AXIS Entry Manager continuerà a utilizzare la lingua selezionata.

Impostazione di data e ora

Se il dispositivo di controllo delle porte fa parte di un sistema, le impostazioni di data e ora verranno distribuite a tutti i dispositivi di controllo delle porte. Ciò significa che le impostazioni verranno fornite ad altri dispositivi di controllo nel sistema, indipendentemente dalla sincronizzazione con un server NTP, dall'impostazione di data e ora manualmente o dall'ottenimento di data e ora da un computer. Se non è possibile visualizzare le modifiche, provare ad aggiornare la pagina nel browser. Per ulteriori informazioni sulla gestione di un sistema di dispositivi di controllo delle porte, vedere *Gestione dei dispositivi di controllo porta di rete alla pagina 26*.

Per impostare la data e l'ora del dispositivo Axis, andare a **Setup > Date & Time (Impostazione > Data e ora)**.

È possibile impostare la data e l'ora nei seguenti modi:

- Data e ora da un server NTP (Network Time Protocol). Vedere *pagina 12*.
- Impostare la data e l'ora manualmente. Vedere *pagina 12*.
- Ottenere la data e l'ora dal computer. Vedere *pagina 12*.

Current controller time (Ora attuale dispositivo di controllo) visualizza la data e l'ora correnti del dispositivo di controllo delle porte (formato 24 ore).

Le stesse opzioni per la data e l'ora sono inoltre disponibili nelle pagine Opzioni di sistema. Andare a **Setup > Additional Controller Configuration > System Options > Date & Time (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Data e ora)**.

Data e ora da un server NTP (Network Time Protocol)

1. Andare a **Setup > Date & Time (Impostazione > Data e ora)**.
2. Selezionare **Timezone (Fuso orario)** dall'elenco a discesa.
3. Se nella propria regione è in uso l'ora legale, selezionare **Adjust for daylight saving (Passa all'ora legale)**.
4. Selezionare **Synchronize with NTP (Sincronizza con NTP)**.
5. Selezionare l'indirizzo DHCP predefinito oppure immettere l'indirizzo di un server NTP.
6. Fare clic su **Save (Salva)**.

Quando si esegue la sincronizzazione con un server NTP, la data e l'ora vengono aggiornate continuamente poiché la data viene inoltrata dal server NTP. Per informazioni sulle impostazioni NTP, vedere *Configurazione NTP alla pagina 59*.

Se si utilizza un nome host per il server NTP, deve essere configurato un server DNS. Vedere *Configurazione DNS alla pagina 59*.

Impostazione di data e ora manuali

1. Andare a **Impostazione > Data & ora**.
2. Se nella propria regione è in uso l'ora legale, selezionare **Adjust for daylight saving (Passa all'ora legale)**.
3. Selezionare **Set date & time manually (Imposta data e ora manualmente)**.
4. Immettere la data e l'ora desiderate.
5. Fare clic su **Save (Salva)**.

Quando si impostano la data e l'ora manualmente, queste vengono impostate e non verranno aggiornate manualmente. Ciò significa che se la data e l'ora devono essere aggiornate, le modifiche devono essere eseguite manualmente poiché non esiste nessuna connessione a un server NTP esterno.

Ottenimento della data e dell'ora dal computer

1. Andare a **Setup > Date & Time (Impostazione > Data e ora)**.

2. Se nella propria regione è in uso l'ora legale, selezionare **Adjust for daylight saving (Passa all'ora legale)**.
3. Selezionare **Set date & time manually (Imposta data e ora manualmente)**.
4. Fare clic su **Sync now and save (Sincronizza ora e salva)**.

Quando si utilizza l'ora del computer, la data e l'ora vengono sincronizzati con l'ora del computer una sola volta e non verranno aggiornate automaticamente. Ciò significa che se si modifica la data o l'ora del computer che si utilizzano per gestire il sistema, è necessario effettuare nuovamente la sincronizzazione.

Configurazione delle impostazioni di rete

Per configurare le impostazioni di rete di base, andare a **Setup > Network Settings (Impostazione > Impostazioni di rete)** o a **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > TCP/IP > Base)**.

Per ulteriori informazioni sulle impostazioni di rete, vedere *Rete alla pagina 56*.

Configurazione dell'hardware

Per poter gestire le porte e i piani, è necessario configurare l'hardware nelle pagine Configurazione hardware.

È possibile collegare lettori, blocchi e altri dispositivi al dispositivo Axis prima di completare la configurazione hardware. Tuttavia, sarà più semplice collegare i dispositivi dopo aver completato la configurazione dell'hardware. Ciò è dovuto al fatto che al termine della configurazione è disponibile uno schema dei pin hardware che funge da guida per connettere i pin e può essere utilizzato come scheda di riferimento per la manutenzione. Per le istruzioni di manutenzione, vedere *pagina 29*.

Se si configura l'hardware per la prima volta, selezionare uno dei seguenti metodi:

- Importare un file di configurazione hardware. Vedere *pagina 13*.
- Creare una nuova configurazione dell'hardware. Vedere *pagina 14*.

Nota

Se l'hardware del dispositivo non è stato configurato prima o è stato cancellato, l'opzione **Hardware Configuration (Configurazione hardware)** sarà disponibile nel pannello delle notifiche della pagina Overview (Panoramica).

Modalità di importazione di un file di configurazione hardware

La configurazione hardware del dispositivo Axis può essere completata più rapidamente importando un file di configurazione hardware.

Quando si esporta il file da un dispositivo per importarlo in altri dispositivi, è possibile eseguire più copie della stessa configurazione hardware senza dover ripetere la stessa procedura ogni volta. È anche possibile archiviare i file esportati come backup e utilizzarli per ripristinare configurazioni hardware precedenti. Per ulteriori informazioni, vedere *Modalità di esportazione di un file di configurazione hardware alla pagina 14*.

Per importare un file di configurazione hardware:

1. Andare a **Setup > Hardware Configuration (Impostazione > Configurazione hardware)**.
2. Fare clic sul pulsante **Import hardware configuration (Importa configurazione hardware)** o, se già esiste una configurazione, sul pulsante **Reset and import hardware configuration (Reimposta e importa configurazione hardware)**.
3. Nella finestra di dialogo del browser visualizzata, individuare e selezionare il file di configurazione hardware (*.json) sul computer.
4. Fare clic su **OK**.

Modalità di esportazione di un file di configurazione hardware

La configurazione hardware del dispositivo Axis può essere esportata per effettuare più copie della stessa impostazione dell'hardware. È anche possibile archiviare i file esportati come backup e utilizzarli per ripristinare configurazioni hardware precedenti.

Nota

La configurazione hardware dei piani non può essere esportata.

Le impostazioni di blocco wireless non sono incluse nell'esportazione della configurazione hardware.

Per esportare un file di configurazione hardware:

1. Andare a **Setup > Hardware Configuration (Impostazione > Configurazione hardware)**.
2. Fare clic su **Export hardware configuration (Esporta configurazione hardware)**.
3. A seconda del browser, potrebbe essere necessario esplorare una finestra di dialogo per completare l'esportazione.

   Se non diversamente specificato, il file esportato (*.json) viene salvato nella cartella di download predefinita. È possibile selezionare una cartella di download nelle impostazioni utente del browser Web.

Creazione di una nuova configurazione dell'hardware

Attenersi alla seguente procedura a seconda delle esigenze:

- *Modalità di creazione di una nuova configurazione hardware senza periferiche alla pagina 14*
- *Come creare una nuova configurazione hardware per i blocchi wireless alla pagina 18*
- *Modalità di creazione di una nuova configurazione hardware tramite il controllo ascensore (AXIS A9188) alla pagina 19*

Modalità di creazione di una nuova configurazione hardware senza periferiche

1. Andare a **Setup > Hardware Configuration (Configurazione > Configurazione hardware)** e fare clic sul pulsante **Start new hardware configuration (Avvia nuova configurazione hardware)**.
2. Inserire un nome per il dispositivo Axis.
3. Selezionare il numero di porte collegate e fare clic su **Next (Avanti)**.
4. Configurare i monitor porte (i sensori di posizione delle porte) e i blocchi secondo le proprie necessità, quindi fare clic su **Next (Avanti)**. Per ulteriori informazioni sulle opzioni disponibili, vedere *Modalità di configurazione di monitor porte e blocchi alla pagina 14*.
5. Configurare i lettori e i dispositivi REX che verranno utilizzati e fare clic sul pulsante **Finish (Fine)**. Per ulteriori informazioni sulle opzioni disponibili, vedere *Modalità di configurazione di lettori e dispositivi REX alla pagina 17*.
6. Fare clic su **Close (Chiudi)** oppure sul collegamento per visualizzare lo schema dei pin hardware.

Modalità di configurazione di monitor porte e blocchi

Una volta selezionata un'opzione porta nella nuova configurazione hardware, è possibile configurare i monitor porte e i blocchi.

1. Se viene utilizzato un monitor porte, selezionare **Door monitor (Monitor porte)**, quindi selezionare l'opzione che corrisponde alla modalità di connessione dei circuiti del monitor porte.
2. Se il blocco deve attivarsi immediatamente dopo l'apertura della porta, selezionare **Cancel access time once door is opened (Cancella tempo di accesso una volta aperta la porta)**.

   Se si desidera ritardare la nuova chiusura, impostare il tempo di ritardo in millisecondi in **Relock time (Tempo di nuova chiusura)**.

3. Specificare le opzioni di tempo del monitor porte o, se non verrà utilizzato alcun monitor porte, le opzioni di tempo del blocco.
4. Selezionare le opzioni che corrispondono alla modalità di collegamento dei circuiti di blocco.
5. Se viene utilizzato un monitor blocco, selezionare **Lock monitor (Monitor blocco)**, quindi selezionare le opzioni che corrispondono alla modalità di collegamento dei circuiti del monitor blocco.
6. Se le connessioni di input da lettori, dispositivi REX e monitor porte devono essere supervisionate, selezionare **Enable supervised inputs (Abilita input supervisionati)**.

   Per ulteriori informazioni, vedere *Modalità di utilizzo degli input supervisionati alla pagina 17*.

Nota

- La maggior parte delle opzioni relative a blocchi, monitor porte e lettore può essere modificata senza reimpostare e avviare una nuova configurazione hardware. Andare a **Setup > Hardware Reconfiguration (Impostazione > Riconfigurazione hardware)**.
- È possibile collegare un monitor blocco per dispositivo di controllo porte. Quindi, se si utilizzano porte con doppio blocco, solo uno dei blocchi può avere un monitor blocco. Se due porte sono collegate allo stesso dispositivo di controllo porte, non è possibile utilizzare monitor blocco.
- È necessario configurare i blocchi motorizzati come blocchi secondari.

Informazioni sulle opzioni relative al monitor porte e all'orario

Per il monitor porte le opzioni disponibili sono le seguenti:

- **Door monitor (Monitor porte)**: selezionato per impostazione predefinita. Ciascuna porta ha il proprio monitor porte che, ad esempio, segnalerà quando la porta è stata forzata o aperta troppo a lungo. Deselezionare questa opzione in caso non sia utilizzato alcun monitor porte.
  - **Open circuit = Closed door (Circuito aperto = Porta chiusa)**: selezionare questa opzione in caso il circuito del monitor porte sia normalmente aperto. Il monitor porte emette il segnale di porta aperta quando il circuito è chiuso. Il monitor porte emette il segnale di porta chiusa quando il circuito è aperto.
  - **Open circuit = Open door (Circuito aperto = Porta aperta)**: selezionare questa opzione in caso il monitor porte sia normalmente chiuso. Il monitor porte emette il segnale di porta aperta quando il circuito è aperto. Il monitor porte emette il segnale di porta chiusa quando il circuito è chiuso.
- **Cancel access time once door is opened (Cancella tempo di accesso una volta aperta la porta)**: selezionare questa opzione per prevenire accessi non autorizzati. Il blocco verrà attivato non appena il monitor porte indicherà che la porta è stata aperta.

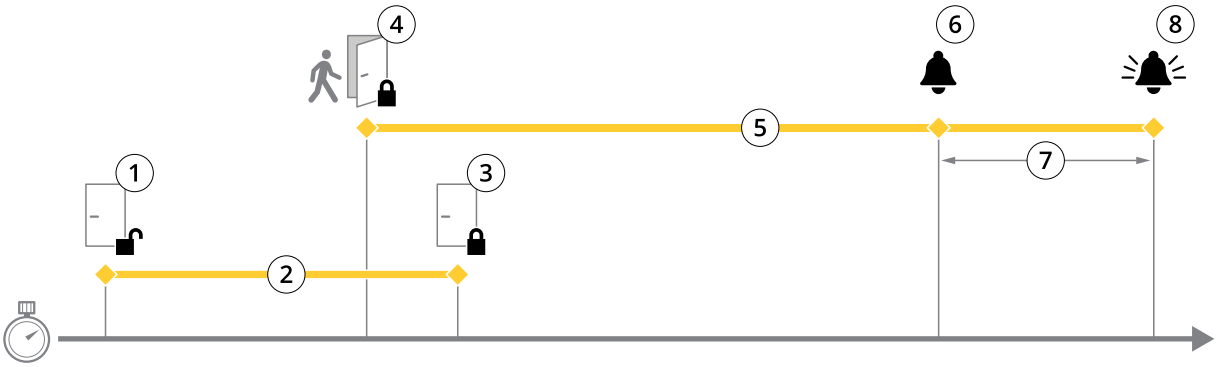
Per il tempo delle porte le seguenti opzioni sono sempre disponibili:

- **Access time (Tempo di accesso)**: impostare il numero di secondi per cui la porta deve rimanere sbloccata dopo aver consentito l'accesso. La porta rimane sbloccata fino a quando la porta è aperta o finché è stato raggiunto il tempo prestabilito. La porta si bloccherà alla chiusura indipendentemente dal fatto che sia trascorso o meno il tempo di accesso.
- **Long access time (Ora di accesso prolungata)**: impostare il numero di secondi per cui la porta deve rimanere sbloccata dopo aver concesso l'accesso. L'opzione Ora di accesso prolungata sovrascrive il tempo di accesso già impostato e verrà abilitata per gli utenti con ora di accesso prolungata selezionata, vedere *Credenziali dell'utente alla pagina 40*

Selezionare **Door monitor (Monitor porte)** per rendere disponibili le seguenti opzioni:

- **Open too long time (Tempo di apertura eccessivo)**: impostare il numero di secondi per cui la porta può rimanere aperta. Se la porta è ancora aperta quando è stato raggiunto il tempo prestabilito, viene attivato l'allarme porta aperta troppo a lungo. Impostare una regola di azione per configurare l'azione che verrà attivata dall'evento porta aperta troppo a lungo.
- **Pre-alarm time (Tempo di pre-allarme)**: un pre-allarme è un segnale di avviso che viene attivato prima che il tempo di porta aperta troppo a lungo sia stato raggiunto. A seconda di come la regola di azione è stata impostata, informa l'amministratore e avvisa la persona che oltrepassa la porta che la porta deve essere chiusa per evitare che scatti l'allarme di porta aperta troppo a lungo. Impostare il numero di secondi precedenti all'attivazione dell'allarme porta aperta troppo a

lungo durante i quali il sistema darà il segnale di avvertimento pre-allarme. Per disabilitare il pre-allarme, impostare il tempo di pre-allarme su 0.



1 *Accesso consentito: la serratura si sblocca*
2 *Tempo di accesso*
3 *Nessuna azione compiuta: la serratura si blocca*
4 *Azione compiuta (porta aperta): la serratura si blocca o rimane sbloccata finché non si chiude la porta*
5 *Tempo di apertura eccessivo*
6 *Scatta il pre-allarme*
7 *Tempo di pre-allarme*
8 *Scatta l'allarme porta aperta troppo a lungo*

Per informazioni su come impostare una regola di azione, vedere *Modalità di impostazione delle regole di azione alla pagina 46*.

Informazioni sulle opzioni di blocco

Le opzioni del circuito di blocco disponibili sono:

- 12 V
  - **Fail-secure (Protezione intrinseca)**: selezionare questa opzione per le serrature che rimangono bloccate in caso di interruzione dell'alimentazione elettrica. Una volta ripristinata la corrente elettrica, la serratura si sblocca.
  - **Fail-safe (Sicurezza intrinseca)**: selezionare questa opzione per le serrature che si sbloccano durante le interruzioni dell'alimentazione. Una volta ripristinata la corrente elettrica, la serratura si blocca.
- **Relay (Relè)**: questa opzione può essere utilizzata solo su un blocco per dispositivo di controllo porta. Se due porte sono collegate al dispositivo di controllo porta, sul blocco della seconda porta può essere usato solo un relè.
  - **Relay open = Locked (Relè aperto = bloccato)**: selezionare questa opzione per le serrature che rimangono bloccate quando il relè è aperto (protezione intrinseca). Quando si chiude il relè, si sblocca la serratura.
  - **Relay open = Unlocked (Relè aperto = sbloccato)**: selezionare questa opzione per le serrature che si sbloccano durante le interruzioni dell'alimentazione (sicurezza intrinseca). Quando si chiude il relè, si blocca la serratura.
- **None (Nessuno)**: disponibile solo per la serratura 2. Selezionare se verrà utilizzato un solo blocco.

Le seguenti opzioni di monitor blocco sono disponibili per le configurazioni a singola porta:

- **Lock monitor (Monitoraggio blocco)**: selezionare questa opzione per rendere disponibili i controlli del monitor blocco. Quindi, selezionare il blocco che deve essere monitorato. Un monitor blocco può essere utilizzato solo su porte con doppio blocco e non può essere utilizzato se due porte sono collegate al dispositivo di controllo porta.
  - **Open circuit = Locked (Circuito aperto = bloccato)**: selezionare questa opzione se il circuito di monitor blocco è normalmente chiuso. Il monitor blocco emette il segnale di porta sbloccata quando il circuito è chiuso. Il monitor blocco emette il segnale di porta bloccata quando il circuito è aperto.

- **Open circuit = Unlocked (Circuito aperto = sbloccato)**: selezionare questa opzione se il circuito di monitor blocco è normalmente aperto. Il monitor blocco emette il segnale di porta sbloccata quando il circuito è aperto. Il monitor blocco emette il segnale di porta bloccata quando il circuito è chiuso.

Modalità di configurazione di lettori e dispositivi REX

Una volta configurati i monitor porte e i blocchi nella nuova configurazione hardware, è possibile configurare i lettori e richiedere di uscire dai dispositivi (REX).

1. Se un lettore verrà utilizzato, selezionare la casella di controllo, quindi selezionare le opzioni che corrispondono al protocollo di comunicazione del lettore.
2. Se verrà utilizzato un dispositivo REX, ad esempio un pulsante, un sensore o un maniglione, selezionare la casella di controllo, quindi selezionare l'opzione che corrisponde alla modalità di collegamento dei circuiti del dispositivo REX.

   Se il segnale REX non influenza l'apertura della porta (ad esempio per porte con maniglie meccaniche o maniglioni), selezionare **REX does not unlock door (REX non sblocca la porta)**.
3. In caso di connessione di più lettori o dispositivi REX al dispositivo di controllo porta, eseguire nuovamente i due passaggi precedenti finché ogni lettore o dispositivo REX non presenterà le impostazioni corrette.

Informazioni sulle opzioni del lettore e del dispositivo REX

Sono disponibili le opzioni relative al lettore riportate di seguito:

- **Wiegand (Wiegand)**: selezionare questa opzione per i lettori che utilizzano i protocolli Wiegand. Quindi, selezionare il controllo LED che è supportato dal lettore. I lettori con controllo LED singolo generalmente passano dal rosso al verde e viceversa. I lettori con controllo LED doppio utilizzano cavi diversi per i LED rossi e verdi. Questo significa che i LED sono controllati indipendentemente l'uno dall'altro. Se entrambi i LED sono accesi, la luce sarà gialla. Vedere le informazioni fornite dal produttore sul controllo LED supportato dal lettore.
- **OSDP, RS485 half-duplex (OSDP, RS485 half-duplex)**: selezionare l'opzione per i lettori RS485 con supporto half-duplex. Vedere le informazioni fornite dal produttore sul protocollo supportato dal lettore.

Sono disponibili le opzioni relative al dispositivo REX riportate di seguito:

- **Active low (Attivo basso)**: selezionare questa opzione se l'attivazione del dispositivo REX chiude il circuito.
- **Active high (Attivo alto)**: selezionare questa opzione se l'attivazione del dispositivo REX apre il circuito.
- **REX does not unlock door (REX non sblocca la porta)**: selezionare questa opzione se il segnale REX non influisce sull'apertura della porta (ad esempio per porte con maniglie meccaniche o maniglioni). L'allarme di porta forzata non verrà attivato se l'utente apre la porta nell'intervallo di tempo previsto per l'accesso. Deselezionare l'opzione se la porta deve sbloccarsi automaticamente quando l'utente attiva il dispositivo REX.

Nota

La maggior parte delle opzioni relative a blocchi, monitor porte e lettore può essere modificata senza reimpostare e avviare una nuova configurazione hardware. Andare a **Setup > Hardware Reconfiguration (Impostazione > Riconfigurazione hardware)**.

Modalità di utilizzo degli input supervisionati

Gli input supervisionati forniscono informazioni sullo stato della connessione tra il dispositivo di controllo porta e i lettori, i dispositivi REX e i monitor porte. Se il collegamento viene interrotto, viene attivato un evento.

Per utilizzare gli input supervisionati:

1. Installare resistori terminali su tutti gli input supervisionati utilizzati. Vedere lo schema delle connessioni in *pagina 74*.
2. Andare a **Setup > Hardware Reconfiguration (Impostazione > Riconfigurazione hardware)** e selezionare **Enable supervised inputs (Abilita input supervisionati)**. È inoltre possibile abilitare gli input supervisionati durante la configurazione dell'hardware.

Informazioni sulla compatibilità dell'input supervisionato

I connettori seguenti supportano gli input supervisionati:

- Connettore I/O lettore: segnale anti-manomissione. Vedere *pagina 69*.
- Connettore porta. Vedere *pagina 70*.

I lettori e gli switch che possono essere utilizzati con input supervisionati includono:

- Lettori e switch con pull-up interno da 1kΩ a 5 V.
- Lettori e switch senza pull-up interno.

Come creare una nuova configurazione hardware per i blocchi wireless

1. Andare a **Setup > Hardware Configuration (Configurazione > Configurazione hardware)** e fare clic sul pulsante **Start new hardware configuration (Avvia nuova configurazione hardware)**.
2. Immettere un nome per il dispositivo Axis.
3. Nell'elenco delle periferiche, selezionare un produttore per un gateway wireless.
4. Se si desidera collegare una porta cablata, selezionare la casella di controllo **1 Door (1 porta)** e fare clic su **Next (Avanti)**. Se non è inclusa nessuna porta, fare clic su **Finish (Fine)**.
5. In base al produttore della serratura, procedere in base a uno dei punti riportati di seguito:
   - **ASSA Aperio**: Fare clic sul collegamento per visualizzare lo schema dei pin hardware oppure fare clic su **Close (Chiudi)** e andare in **Setup > Hardware Reconfiguration (Impostazione > Riconfigurazione hardware)**, per completare la configurazione vedere *Aggiunta di dispositivi e porte Assa Aperio™ alla pagina 18*
   - **SmartIntego**: Fare clic sul collegamento per visualizzare lo schema dei pin hardware oppure fare clic su **Click here to select wireless gateway and configure doors (Fare clic qui per selezionare il gateway wireless e configurare le porte)**, per completare la configurazione vedere *Modalità di configurazione di SmartIntego alla pagina 26*.

Aggiunta di dispositivi e porte Assa Aperio™

Prima di aggiungere una porta wireless al sistema è necessario associarla all'hub di comunicazione Assa Aperio collegato, utilizzando Aperio PAP (lo strumento di applicazione di programmazione di Aperio).

Per aggiungere una porta wireless:

1. Selezionare **Setup (Impostazione)** > **Hardware Reconfiguration (Riconfigurazione hardware)**.
2. In Wireless Doors and Devices (Dispositivi e porte wireless) fare clic su **Add door (Aggiungi porta)**.
3. Nel campo **Nome porta**: immettere un nome descrittivo.
4. Nel campo **ID** in **Blocco**: immettere l'indirizzo composto da sei caratteri del dispositivo che si desidera aggiungere. L'indirizzo del dispositivo è stampato sull'etichetta del dispositivo.
5. Facoltativamente, in **Sensore di posizione delle porte**: Selezionare **Sensore di posizione delle porte incorporato** o **Sensore di posizione delle porte esterno**.

Nota

Se si utilizza un sensore di posizione delle porte esterno (DPS) assicurarsi che il dispositivo di blocco Aperio includa il supporto per la gestione del rilevamento dello stato prima di configurarlo.

6. Facoltativamente, nel campo **ID** in **Sensore di posizione delle porte**: immettere l'indirizzo composto da sei caratteri del dispositivo che si desidera aggiungere. L'indirizzo del dispositivo è stampato sull'etichetta del dispositivo.

7. Fare clic su **Add (Aggiungi)**.

Modalità di creazione di una nuova configurazione hardware tramite il controllo ascensore (AXIS A9188)

Importante

Prima di creare una configurazione HW è necessario aggiungere un utente in AXIS A9188 Network I/O Relay Module. Andare all'interfaccia Web A9188 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Preferenze > Configurazione dispositivo aggiuntivo > Configurazione di base > Utenti > Aggiungi > Configurazione utente)**.

Nota

È possibile configurare un massimo di 2 AXIS 9188 Network I/O Relay Modules per ciascun Axis Network Door Controller

1. In A1001, andare a **Setup > Hardware Configuration (Configurazione > Configurazione hardware)** e fare clic sul pulsante **Start new hardware configuration (Avvia nuova configurazione hardware)**.
2. Immettere un nome per il dispositivo Axis.
3. Nell'elenco delle periferiche, selezionare **Elevator control (Controllo ascensore)** per includere un AXIS A9188 Network I/O Relay Module e fare clic su **Next (Avanti)**.
4. Immettere un nome per il lettore connesso.
5. Selezionare il protocollo del lettore che verrà utilizzato e fare clic su **Finish (Fine)**.
6. Fare clic su **Periferiche di rete** per completare la configurazione; vedere *Modalità di aggiunta e configurazione delle periferiche di rete alla pagina 19* oppure fare clic sul collegamento per passare allo schema dei pin hardware.

Modalità di aggiunta e configurazione delle periferiche di rete

Importante

- Prima di configurare le periferiche di rete è necessario aggiungere un utente in AXIS A9188 Network I/O Relay Module. Andare all'interfaccia web AXIS A9188 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Preferenze > Configurazione dispositivo aggiuntivo > Configurazione di base > Utenti > Aggiungi > Configurazione utente)**.
- Non aggiungere un altro AXIS A1001 Network Door Controller come periferica di rete.

1. Andare a **Setup > Network Periphals (Configurazione > Periferiche di rete)** per aggiungere un dispositivo
2. Trovare i dispositivi in **Discovered devices (Dispositivi rilevati)**.
3. Fare clic su **Add this device (Aggiungi questo dispositivo)**
4. Immettere un nome per il dispositivo
5. Immettere il nome utente e la password per AXIS A9188
6. Fare clic su **Add (Aggiungi)**.

Nota

È possibile aggiungere manualmente le periferiche di rete inserendo l'indirizzo MAC o l'indirizzo IP nella finestra di dialogo **Manually add device (Aggiungi dispositivo manualmente)**.

Importante

Se si desidera eliminare una pianificazione, assicurarsi innanzitutto che non sia utilizzata dal modulo relè I/O di rete.

Modalità di configurazione dei relè I/O nelle periferiche di rete

Importante

Prima di configurare le periferiche di rete è necessario aggiungere un utente in AXIS A9188 Network I/O Relay Module. Andare all'interfaccia web AXIS A9188 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Preferenze > Configurazione dispositivo aggiuntivo > Configurazione di base > Utenti > Aggiungi > Configurazione utente)**.

1. Andare a **Setup > Network Periphals (Configurazione > Periferiche di rete)** e fare clic sulla riga **Added devices (Dispositivi aggiunti)**.
2. Scegliere quali dispositivi I/O e relè impostare come piani.
3. Fare clic su **Set as floor (Imposta come piano)** e immettere un nome.
4. Fare clic su **Add (Aggiungi)**.

Il piano sarà ora visibile nella scheda **Floor (Piano)** sotto **Access Management (Gestione degli accessi)**.

Nota

In AXIS Entry Manager è possibile aggiungere un massimo di 16 piani.

Verifica dei collegamenti hardware

Una volta completate l'installazione e la configurazione dell'hardware, e in qualsiasi momento per tutta la durata del dispositivo di contro porta, è possibile verificare la funzione di monitor porte collegati, moduli relè I/O di rete, blocchi e lettori.

Per verificare la configurazione e l'accesso ai controlli di verifica, andare a **Setup > Hardware Connection Verification (Impostazione > Verifica connessione hardware)**.

Comandi di verifica delle porte

- **Stato porta**: verificare lo stato corrente del monitor porte, degli allarmi della porta e dei blocchi. Fare clic su **Get current state (Ottieni stato corrente)**.
- **Blocca**: attivare manualmente il blocco. Ne verranno influenzati i blocchi primari e secondari, se presenti. Fare clic sul pulsante **Lock (Blocca)** o **Unlock (Sblocca)**.
- **Blocca**: attivare manualmente il blocco per consentire l'accesso. Ne verranno influenzati solo i blocchi primari. Fare clic su **Access (Accesso)**.
- **Lettore: feedback**: verificare il feedback del lettore, ad esempio i suoni e i segnali LED per comandi differenti. Selezionare il comando e fare clic sul pulsante **Test (Test)**. I tipi di feedback disponibili dipendono dal lettore. Per ulteriori informazioni, vedere *Feedback del lettore alla pagina 51*. Vedere anche le istruzioni del produttore.
- **Lettore: manomissione**: ottenere le informazioni sull'ultimo tentativo di manomissione. Il primo tentativo di manomissione verrà registrato quando viene installato il lettore. Fare clic su **Get last tampering (Ottieni ultima manomissione)**.
- **Lettore: passaggio carta**: acquisire le informazioni relative all'ultimo passaggio della carta oppure a un altro tipo di token utente accettato dal lettore. Fare clic su **Get last credential (Ottieni ultime credenziali)**.
- **REX**: ottenere informazioni sull'ultimo orario in cui è stata premuta la richiesta di uscita dal dispositivo (REX). Fare clic su **Get last REX (Ottieni ultimo REX)**.

Piani dei controlli di verifica

- **Stato del piano**: verificare lo stato corrente dell'accesso al piano. Fare clic su **Get current state (Ottieni stato corrente)**.
- **Blocco e sblocco piano**: attivare manualmente l'accesso al piano. Ne verranno influenzati i blocchi primari e secondari, se presenti. Fare clic sul pulsante **Lock (Blocca)** o **Unlock (Sblocca)**.

- **Accesso al piano**: concedere manualmente l'accesso temporaneo al piano. Ne verranno influenzati solo i blocchi primari. Fare clic su **Access (Accesso)**.
- **Lettore ascensore: Feedback**: verificare il feedback del lettore, ad esempio i suoni e i segnali LED per comandi differenti. Selezionare il comando e fare clic sul pulsante **Test (Test)**. I tipi di feedback disponibili dipendono dal lettore. Per ulteriori informazioni, vedere *Feedback del lettore alla pagina 51*. Vedere anche le istruzioni del produttore.
- **Lettore ascensore: Manomissione**: ottenere le informazioni sull'ultimo tentativo di manomissione. Il primo tentativo di manomissione verrà registrato quando viene installato il lettore. Fare clic su **Get last tampering (Ottieni ultima manomissione)**.
- **Lettore ascensore: Passaggio scheda**: acquisire le informazioni relative all'ultimo passaggio della scheda oppure a un altro tipo di token utente accettato dal lettore. Fare clic su **Get last credential (Ottieni ultime credenziali)**.
- **REX**: ottenere informazioni sull'ultimo orario in cui è stata premuta la richiesta di uscita dal dispositivo (REX). Fare clic su **Get last REX (Ottieni ultimo REX)**.

Configurazione di schede e formati

Il dispositivo di controllo porta dispone di alcuni formati scheda comunemente utilizzati, predefiniti, che è possibile utilizzare così come sono o modificati secondo necessità. È possibile inoltre creare formati scheda personalizzati. Ciascun formato di scheda dispone di un set di regole diverso, mappe di campi, riguardanti il modo in cui le informazioni presenti nella scheda sono archiviate. Definendo un formato scheda si indica al sistema come interpretare le informazioni che il dispositivo di controllo ottiene dal lettore. Per informazioni sui formati di scheda supportati dal lettore, vedere le istruzioni del produttore.

Per abilitare i formati di scheda:

1. Andare a **Setup > Configure cards and formats (Impostazione > Configura schede e formati)**.
2. Selezionare uno o più formati scheda che corrispondono al formato scheda utilizzato dai lettori collegati.

Per creare nuovi formati scheda:

1. Andare a **Setup > Configure cards and formats (Impostazione > Configura schede e formati)**.
2. Fare clic su **Add card format (Aggiungi formato scheda)**.
3. Nella finestra di dialogo **Add card format (Aggiungi formato scheda)** immettere un nome, una descrizione e la lunghezza in bit del formato della scheda. Vedere *Descrizioni del formato della scheda alla pagina 22*.
4. Fare clic su **Add field map (Aggiungi mappa campo)** e immettere le informazioni necessarie nei campi. Vedere *Mappe dei campi alla pagina 22*.
5. Per aggiungere più mappe di campo, ripetere il passaggio precedente.

Per espandere un elemento dell'elenco **Card formats (Formati scheda)** e visualizzare le descrizioni del formato scheda e le mappe dei campi, fare clic su .

Per modificare un formato scheda, fare clic su  e modificare le descrizioni dei formati scheda e le mappe dei campi secondo necessità. Quindi fare clic su **Save (Salva)**.

Per eliminare una mappa del campo nella finestra di dialogo **Edit card format (Modifica formato scheda)** o **Add card format (Aggiungi formato scheda)**, fare clic su 

Per eliminare un formato scheda, fare clic su .

Importante

- Tutte le modifiche apportate ai formati tessera si applicano all'intero sistema di dispositivi di controllo porta.
- È possibile abilitare e disabilitare formati scheda solo se almeno un dispositivo di controllo porta nel sistema è stato configurato con almeno un lettore. Vedere *Configurazione dell'hardware alla pagina 13* e *Modalità di configurazione di lettori e dispositivi REX alla pagina 17*.
- Non è possibile che due formati scheda con la stessa lunghezza in bit possano essere attivi contemporaneamente. Ad esempio, se sono stati definiti due formati scheda da 32 bit, "Formato A" e "Formato B" e "Formato A" è stato abilitato, non è possibile abilitare "Formato B" senza disabilitare prima "Formato A".
- Se nessun formato scheda è stato abilitato, è possibile utilizzare i tipi di identificazione **Card raw only (Solo scheda dati non elaborati)** e **Card raw and PIN (Dati non elaborati e PIN)** per identificare una scheda e consentire l'accesso agli utenti. Tuttavia, questo non è consigliabile poiché produttori di lettori diversi o impostazioni del lettore diverse possono generare schede dati non elaborati diverse.

Descrizioni del formato della scheda

- **Name (Nome)** (obbligatorio): immettere un nome descrittivo.
- **Description (Descrizione)**: immettere le informazioni aggiuntive desiderate. Queste informazioni sono visibili soltanto nelle finestre di dialogo **Edit card format (Modifica formato scheda)** e **Add card format (Aggiungi formato scheda)**.
- **Bit length (Lunghezza in bit)** (obbligatorio): immettere la lunghezza in bit del formato della scheda. Deve essere un numero compreso tra 1 e 1000000000.

Mappe dei campi

- **Name (Nome)** (obbligatorio): immettere il nome della mappa del campo senza spazi, ad esempio `OddParity`.

  Esempi di mappe dei campi comuni includono:

  - `Parity`: i bit di parità vengono utilizzati per il rilevamento di errori. I bit di parità vengono di norma aggiunti all'inizio o alla fine di una stringa di codice binario e indicano se il numero di bit è pari o dispari.
  - `EvenParity`: Anche i bit di parità assicurano che ci sia un numero pari di bit nella stringa. Vengono conteggiati i bit che hanno il valore 1. Se il numero è già pari, il valore di bit di parità è impostato su 0. Se il numero è dispari, il valore di bit di parità pari è impostato su 1, rendendo il numero totale un numero pari.
  - `OddParity`: i bit di parità dispari assicurano un numero di bit dispari nella stringa. Vengono conteggiati i bit che hanno il valore 1. Se il numero è già dispari, il valore di bit di parità dispari è impostato su 0. Se il numero è pari, il valore di bit di parità è impostato su 1, rendendo il numero totale un numero dispari.
  - `FacilityCode`: i codici struttura vengono talvolta utilizzati per verificare che il token corrisponda al batch di credenziali dell'utente finale ordinato. Nei sistemi di controllo degli accessi precedenti, il codice struttura è stato utilizzato per una convalida ridotta, che consente l'accesso di tutti i dipendenti al batch di credenziali che è stato codificato con un codice sito corrispondente. Questo nome di mappa del campo, che fa distinzione tra maiuscole e minuscole, è necessario per la convalida del dispositivo con il codice struttura.
  - `CardNr`: il codice carta o l'ID utente è l'elemento più comunemente convalidato nei sistemi di controllo degli accessi. Questo nome di mappa del campo, che fa distinzione tra maiuscole e minuscole, è necessario per la convalida del dispositivo con il codice carta.
  - `CardNrHex`: i dati binari del codice carta sono codificati come caratteri esadecimali minuscoli nel dispositivo. Sono utilizzati principalmente per la risoluzione di problemi quando non si ottiene il codice carta previsto dal lettore.

- **Range (Intervallo)** (obbligatorio): immettere l'intervallo di bit della mappa del campo, ad esempio 1, 2-17, 18-33 e 34.
- **Encoding (Codifica)** (obbligatorio): selezionare il tipo di codifica di ogni mappa del campo.

  - **BinLE2Int**: i dati binari sono codificati come numeri interi nell'ordine dei bit little endian. Numero intero significa che deve essere un numero intero (senza decimali). Ordine dei bit little endian significa che il primo bit è il più piccolo (meno significativo).

- **BinBE2Int**: i dati binari sono codificati come numeri interi nell'ordine dei bit big endian. Numero intero significa che deve essere un numero intero (senza decimali). Ordine dei bit big endian significa che il primo bit è il più grande (più importante).
- **BinLE2Hex**: i dati binari sono codificati come numeri esadecimali minuscoli nell'ordine dei bit little endian. Il sistema esadecimale, noto anche come sistema numerico in base 16, è composto da 16 simboli univoci: i numeri 0-9 e le lettere a-f. Ordine dei bit little endian significa che il primo bit è il più piccolo (meno significativo).
- **BinBE2Hex**: i dati binari sono codificati come numeri esadecimali minuscoli nell'ordine dei bit big endian. Il sistema esadecimale, noto anche come sistema numerico in base 16, è composto da 16 simboli univoci: i numeri 0-9 e le lettere a-f. Ordine dei bit big endian significa che il primo bit è il più grande (più importante).
- **BinLEIBO2Int**: i dati binari sono codificati come per BinLE2Int, ma i dati non elaborati della scheda vengono letti con ordine dei byte invertito in una sequenza di più byte prima che le mappe dei campi vengano estratte per essere codificate.
- **BinBEIBO2Int**: i dati binari sono codificati come per BinBE2Int, ma i dati non elaborati della scheda vengono letti con ordine dei byte invertito in una sequenza di più byte prima che le mappe dei campi vengano estratte per essere codificate.

Per informazioni sulle mappe dei campi che utilizza il formato della scheda, vedere le istruzioni del produttore.

Codice struttura predefinito

I codici struttura vengono utilizzati a volte per verificare che il token corrisponda al sistema di controllo degli accessi della struttura. Spesso tutti token emessi per una singola struttura hanno lo stesso codice struttura. Immettere un codice struttura preset per consentire una più semplice registrazione manuale di un insieme di schede. Il codice struttura preset viene automaticamente compilato quando si aggiungono gli utenti, vedere *Credenziali dell'utente alla pagina 40*

Per configurare un codice struttura preset:

1. Andare a **Setup > Configure cards and formats (Impostazione > Configura schede e formati)**.
2. In **Preset facility code (Codice struttura preset)**: Inserire un codice struttura.
3. Fare clic su **Set facility code (Imposta codice struttura)**.

Configurazione dei servizi

L'opzione Configura servizi nella pagina Impostazione viene utilizzata per accedere alla configurazione dei servizi esterni che può essere utilizzata con un dispositivo di controllo delle porte.

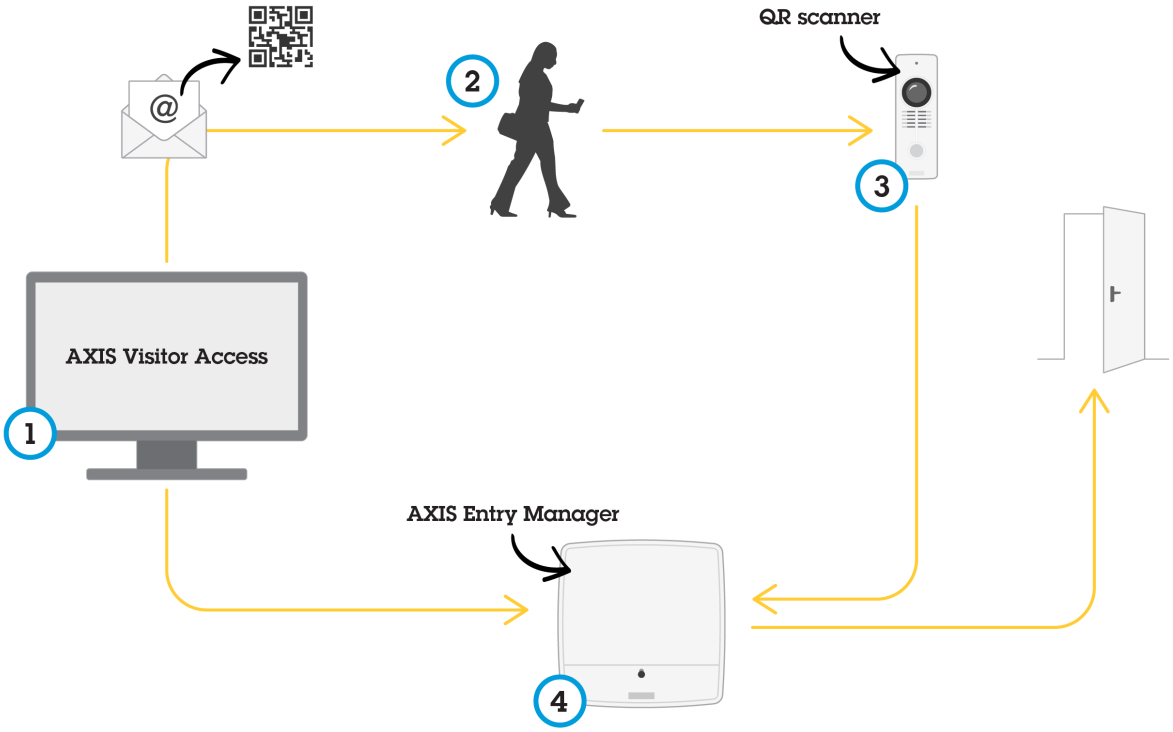
Axis Visitor Access

Con Axis Visitor Access, le credenziali temporanee possono essere create sotto forma di un codice QR. Una telecamera di rete Axis o un videocitofono collegato al sistema di controllo degli accessi esegue la scansione del codice QR.

Il servizio è composto da:

- un Axis door controller con AXIS Entry Manager e versione firmware 1.65.2 o successiva
- Una telecamera di rete Axis o una door station, con l'applicazione scanner QR installata
- un PC Windows® con l'applicazione AXIS Visitor Access installata

Configurazione del sistema



Utilizzo del servizio di Axis Visitor Access

L'utente crea un invito in Axis Visitor Access e manda l'invito all'indirizzo email del visitatore. Allo stesso tempo, le credenziali per sbloccare la porta vengono create e memorizzate nel controller della porta Axis collegato. Il visitatore mostra il codice QR incluso nell'invito sulla telecamera di rete o sul posto esterno, che chiede al controllore della porta di sbloccare la porta per il visitatore.

Il codice QR è un marchio registrato di Denso Wave, inc.

Prerequisiti AXIS Visitor Access

Prima di poter utilizzare il servizio AXIS Visitor Access, è necessario:

- configurare l'hardware del dispositivo di controllo delle porte
- una telecamera di rete Axis o un videocitofono collegati alla stessa rete del dispositivo di controllo delle porte e posizionata in modo accessibile per il visitatore
- Il pacchetto di installazione di AXIS Visitor Access. È possibile trovarlo su *axis.com*
- due account utente aggiuntivi nel dispositivo di controllo delle porte, da utilizzare solo tramite il servizio AXIS Visitor Access. È necessario disporre di un'applicazione AXIS Visitor Access e un'altra applicazione QR scanner. Per informazioni sulla creazione degli account utente, vedere *Utenti alla pagina 54*.

Importante

- È possibile collegare il servizio AXIS Visitor Access a un singolo dispositivo di controllo delle porte nell'intero sistema.
- Con il servizio AXIS Visitor Access, è possibile gestire solo le porte controllate dal dispositivo di controllo delle porte collegato. Non è possibile gestire le altre porte del sistema.
- Utilizzare l'applicazione AXIS Visitor Access per modificare ed eliminare i visitatori. Non utilizzare AXIS Entry Manager.
- Se si modifica la password dell'account utente utilizzato per AXIS Visitor Access, è necessario aggiornarlo anche in AXIS Visitor Access.
- Se si modifica la password dell'account utente utilizzato per l'applicazione QR scanner, è necessario impostare nuovamente il QR scanner.

Imposta Axis Visitor Access

Si installa l'applicazione scanner QR sulla telecamera di rete Axis o sul posto esterno quando si imposta il servizio AXIS Visitor Access. Non è necessario effettuare alcuna installazione separata.

1. Nella pagina Web del dispositivo di controllo delle porte, andare a **Setup > Configure Services > Settings (Impostazione > Configura servizi > Impostazioni)**.
2. Fare clic su **Start a new setup (Avvia una nuova configurazione)**.
3. Seguire le istruzioni per finalizzare la configurazione.

Importante

Se si desidera applicare HTTPS, assicurarsi che il dispositivo di controllo delle porte comunichi tramite HTTPS. In caso contrario l'applicazione non sarà in grado di comunicare con il dispositivo di controllo delle porte.

4. Sul computer che verrà utilizzato per creare credenziali temporanee, installare e configurare l'applicazione AXIS Visitor Access.

SmartIntego

SmartIntego è una soluzione wireless che aumenta il numero di porte che possono essere gestiste da un dispositivo di controllo porte.

Prerequisiti SmartIntego

I seguenti prerequisiti devono essere soddisfatti prima di procedere con la configurazione SmartIntego:

- Deve essere creato un file csv. Il file csv contiene informazioni sul GatewayNode e le porte utilizzate nella soluzione SmartIntego. Il file viene creato in un software indipendente fornito da un partner SimonsVoss.
- La configurazione hardware di SmartIntego è stata eseguita, vedere *Come creare una nuova configurazione hardware per i blocchi wireless alla pagina 18*.

Nota

- È necessario disporre della versione 2.1.6452.23485, build 2.1.6452.23485 (31/08/2017 13:02:50) o successive dello strumento di configurazione SmartIntego.
- Lo standard AES (Advanced Encryption Standard) non è supportato per SmartIntego e deve pertanto essere disabilitato nello strumento di configurazione SmartIntego.

Modalità di configurazione di SmartIntego

Nota

- Verificare di aver soddisfatto i prerequisiti elencati.
- Per una migliore visibilità dello stato della batteria, andare a **Setup (Configurazione)** > **Configure event and alarms logs (Configura registri allarmi ed eventi)**, quindi aggiungere **Door — Battery alarm (Porta: allarme batteria)** o **IdPoint — Battery alarm (IdPoint: allarme batteria)** come allarme.
- Le impostazioni dei monitor porte derivano dal file CSV. Non è necessario modificare questa impostazione in una normale installazione.

1. Fare clic sul pulsante **Browse...(Sfoglia...)**, selezionare il file csv e fare clic su **Upload file (Carica file)**.
2. Selezionare un GatewayNode e fare clic su **Next (Avanti)**.
3. Viene visualizzata un'anteprima della nuova configurazione. Disattivare i monitor porte se necessario.
4. Fare clic sul pulsante **Configure (Configura)**.
5. Viene visualizzata una panoramica delle porte incluse nella configurazione. Fare clic su **Settings (Impostazioni)** per configurare ogni porta singolarmente.

Modalità di riconfigurazione di SmartIntego

1. Fare clic su **Setup (Impostazione)** nel menu di livello superiore.
2. Fare clic su **Configure Services (Configura servizi)** > **Settings (Impostazioni)**.
3. Fare clic su **Re-configure (Riconfigura)**.
4. Fare clic sul pulsante **Browse...(Sfoglia...)**, selezionare il file csv e fare clic su **Upload file (Carica file)**.
5. Selezionare un GatewayNode e fare clic su **Next (Avanti)**.
6. Viene visualizzata un'anteprima della nuova configurazione. Disattivare i monitor porte se necessario.

Nota

Le impostazioni dei monitor porte derivano dal file CSV. Non è necessario modificare questa impostazione in una normale installazione.

7. Fare clic sul pulsante **Configure (Configura)**.
8. Viene visualizzata una panoramica delle porte incluse nella configurazione. Fare clic su **Settings (Impostazioni)** per configurare ogni porta singolarmente.

Gestione dei dispositivi di controllo porta di rete

La pagina Gestisci i dispositivi di controllo delle porte nel sistema fornisce informazioni sul dispositivo di controllo porta, il relativo stato di sistema e gli altri dispositivi di controllo porta che fanno parte del sistema. Inoltre, consente all'amministratore di modificare l'impostazione del sistema aggiungendo e rimuovendo i dispositivi di controllo porta.

Importante

Tutti i dispositivi di controllo delle porte devono essere collegati alla stessa rete ed essere configurati per l'uso su un unico sito.

Per gestire i dispositivi di controllo porta, andare a **Setup > Manage Network Door Controllers in System (Impostazione > Gestisci i dispositivi di controllo porta nel sistema)**.

La pagina Gestisci i dispositivi di controllo delle porte nel sistema include i pannelli seguenti:

- **System status of this controller (Stato sistema di questo dispositivo di controllo)**: mostra lo stato del sistema del dispositivo di controllo porta e consente il passaggio tra le modalità sistema e indipendente. Per ulteriori informazioni, vedere *Stato del sistema del dispositivo di controllo porta alla pagina 27*.
- **Network door controllers in system (Dispositivi di controllo delle porte di rete nel sistema)**: mostra informazioni sui dispositivi di controllo porta nel sistema e include controlli per l'aggiunta e la rimozione di un dispositivo di controllo dal sistema. Per ulteriori informazioni, vedere *Dispositivi di controllo porta collegati nel sistema alla pagina 27*.

Stato del sistema del dispositivo di controllo porta

Lo stato del sistema indica se un dispositivo di controllo porta può fare parte o meno di un sistema di dispositivi di controllo porta. Lo stato del sistema del dispositivo di controllo porta viene visualizzato nel pannello **System status for this controller (Stato sistema di questo dispositivo di controllo)**.

Se il dispositivo di controllo porta non è in modalità indipendente e si desidera impedire che venga aggiunto a un sistema, fare clic su **Activate standalone mode (Attiva modalità indipendente)** per attivare la modalità indipendente.

Se il dispositivo di controllo porta è in modalità indipendente, ma si intende aggiungerlo a un sistema, fare clic su **Deactivate standalone mode (Disattiva modalità indipendente)** per lasciare la modalità indipendente.

Modalità di sistema

- **This controller is not part of a system and not in standalone mode (Questo dispositivo di controllo non fa parte di un sistema e non in modalità indipendente)**: il dispositivo di controllo non è stato configurato come parte di un sistema e non è in modalità indipendente. Ciò significa che il dispositivo di controllo delle porte è aperto e può essere aggiunto a un sistema da qualsiasi altro dispositivo di controllo delle porte all'interno della stessa rete. Per evitare che il dispositivo di controllo delle porte venga aggiunto a un sistema, attivare la modalità indipendente.
- **This controller is set to standalone mode (Questo dispositivo di controllo non fa parte di un sistema e non in modalità indipendente)**: il dispositivo di controllo delle porte non fa parte di un sistema. Non può essere aggiunto a un sistema da altri dispositivi di controllo delle porte nella rete o aggiunto ad altri dispositivi di controllo delle porte. La modalità standalone viene generalmente utilizzata in piccole configurazioni con un controller di porta e una o due porte. Per consentire al dispositivo di controllo delle porte di essere aggiunto in un sistema, disattivare la modalità indipendente.
- **This controller is part of a system (Questo dispositivo di controllo delle porte fa parte di un sistema)**. il dispositivo di controllo delle porte fa parte di un sistema distribuito. Nel sistema distribuito, gli utenti, i gruppi, le porte e le pianificazioni vengono condivisi tra i dispositivi di controllo collegati.

Dispositivi di controllo porta collegati nel sistema

Nel pannello **Network door controllers in system (Dispositivi di controllo delle porte di rete nel sistema)** vengono forniti controlli per le modifiche del sistema seguenti:

- Aggiungere un dispositivo di controllo porta a un sistema. A tale scopo, vedere *Aggiunta di dispositivi di controllo porta al sistema alla pagina 28*.
- Rimuovere un dispositivo di controllo porta da un sistema. A tale scopo, vedere *Rimozione dei dispositivi di controllo porta dal sistema alla pagina 28*.

Elenco dei dispositivi di controllo delle porte collegati

Il pannello **Network door controllers in system (Dispositivi di controllo delle porte di rete nel sistema)** include anche un elenco che mostra le seguenti informazioni di stato e relative all'ID sui dispositivi di controllo delle porte nel sistema:

- **Name (Nome)**: il nome del dispositivo di controllo delle porte definito dall'utente. Se l'amministratore di un nome non ha impostato un nome durante la configurazione dell'hardware, verrà visualizzato il nome predefinito.
- **IP address (Indirizzo IP)**
- **MAC address (Indirizzo MAC)**

- **Status (Stato)**: il dispositivo di controllo delle porte da cui si accede al sistema mostrerà lo stato **This controller (Questo dispositivo di controllo)**. Gli altri dispositivi di controllo delle porte avranno lo stato **Online (In linea)**.
- **Firmware version (Versione del firmware)**

Per aprire le pagine Web di un altro dispositivo di controllo delle porte, fare clic sull'indirizzo IP del dispositivo di controllo delle porte.

Per aggiornare l'elenco, fare clic su **Refresh the list of controllers (Aggiorna l'elenco dei dispositivi di controllo delle porte)**.

Nota

Tutti i dispositivi di controllo delle porte in un sistema devono avere sempre la stessa versione del firmware. Utilizzare Axis Device Manager per eseguire un aggiornamento del firmware in parallelo su tutti i dispositivi di controllo nell'intero sistema.

Aggiunta di dispositivi di controllo porta al sistema

Importante

Durante l'associazione dei dispositivi di controllo porta, tutte le impostazioni di gestione degli accessi sul dispositivo di controllo porta aggiunto verranno eliminate e sovrascritte dalle impostazioni di gestione degli accessi del sistema.

Per aggiungere un dispositivo di controllo porta al sistema dall'elenco dei dispositivi di controllo porta:

1. Andare a **Setup > Manage Network Door Controllers in System (Impostazione > Gestisci i dispositivi di controllo porta nel sistema)**.
2. Fare clic su **Add controllers to system from list (Aggiungi dispositivi di controllo porta al sistema dall'elenco)**.
3. Selezionare il dispositivo di controllo porta che si desidera aggiungere.
4. Fare clic su **Add (Aggiungi)**.
5. Per aggiungere altri dispositivi di controllo porta, ripetere i passaggi precedenti.

Per aggiungere un dispositivo di controllo porta al sistema mediante il relativo indirizzo IP o indirizzo MAC noto:

1. Andare a **Manage Devices (Gestisci dispositivi)**.
2. Fare clic su **Add controller to system by IP or MAC address (Aggiungi dispositivo di controllo al sistema mediante indirizzo IP o MAC)**.
3. Immettere l'indirizzo IP o MAC.
4. Fare clic su **Add (Aggiungi)**.
5. Per aggiungere altri dispositivi di controllo porta, ripetere i passaggi precedenti.

Una volta completata l'associazione, tutti gli utenti, le porte, le pianificazioni e i gruppi vengono condivisi da tutti i dispositivi di controllo porta nel sistema.

Per aggiornare l'elenco, fare clic su **Refresh the list of controllers (Aggiorna elenco dei dispositivi di controllo)**.

Rimozione dei dispositivi di controllo porta dal sistema

Importante

- Prima di rimuovere un dispositivo di controllo porta dal sistema, ripristinarne la configurazione hardware. Se si salta questo passaggio, tutte le porte correlate al dispositivo di controllo porta rimosso rimarranno nel sistema e non potranno essere eliminate.
- Quando si rimuove un dispositivo di controllo porta da un sistema a due dispositivi di controllo, entrambi i dispositivi di controllo porta passano automaticamente alla modalità indipendente.

Per rimuovere un dispositivo di controllo porta dal sistema:

1. Accedere al sistema tramite il dispositivo di controllo porta che si desidera rimuovere e andare a **Setup > Hardware Configuration (Impostazione > Configurazione hardware)**.
2. Fare clic su **Reset hardware configuration (Ripristina configurazione hardware)**.
3. Una volta ripristinata la configurazione dell'hardware, andare a **Setup > Manage Network Door Controllers in System (Impostazione > Gestisci i dispositivi di controllo porta nel sistema)**.
4. Nell'elenco **Network door controllers in system (Dispositivi di controllo porta di rete nel sistema)** identificare il dispositivo di controllo porta che si desidera rimuovere e fare clic su **Remove from system (Rimuovi dal sistema)**.
5. Viene visualizzata una finestra di dialogo che indica di ripristinare la configurazione hardware del dispositivo di controllo. Fare clic su **Remove controller (Rimuovi dispositivo di controllo)** per confermare.
6. Viene visualizzata una finestra di dialogo che richiede di confermare l'intenzione di rimuovere il dispositivo di controllo porta. Fare clic su **OK** per confermare. Il dispositivo di controllo porta rimosso ora è disponibile in modalità indipendente.

Nota

- Quando un dispositivo di controllo porta viene rimosso dal sistema, vengono eliminate tutte le relative impostazioni di gestione degli accessi.
- Possono essere rimossi solo i dispositivi di controllo porta online.

Modalità di configurazione

La modalità di configurazione è la modalità standard quando si accede al dispositivo per la prima volta. Quando la modalità di configurazione viene disabilitata la maggior parte delle funzionalità di configurazione del dispositivo sono nascoste.

Importante

Per disabilitare la modalità di configurazione non deve essere considerata come funzionalità di sicurezza. È ideato per interrompere gli errori di configurazione e non per interrompere la modifica delle impostazioni critiche da parte di utenti non autorizzati.

Modalità di disabilitazione della modalità di configurazione

1. Andare a **Setup (Impostazione)** > **Disable Configuration Mode (Disabilita modalità di configurazione)**.
2. Immettere un PIN e selezionare **OK**.

Nota

Il PIN non è obbligatorio.

Modalità di abilitazione della modalità di configurazione

1. Andare a **Setup (Impostazione)** > **Enable Configuration Mode (Abilita modalità di configurazione)**.
2. Immettere il PIN e selezionare **OK**.

Nota

Se non si ricorda il PIN è possibile abilitare la modalità di configurazione digitando `http://[IP-address]/webapp/pacs/index.shtml#resetConfigurationMode`.

Istruzioni di manutenzione

Per tenere il sistema di controllo degli accessi in buono stato di funzionamento, Axis ne consiglia la regolare manutenzione, che deve includere door controller e dispositivi collegati.

Effettuare la manutenzione almeno una volta all'anno. Le procedure di manutenzione consigliate, includono, a titolo esemplificativo, i passaggi seguenti:

- Verificare che tutti i collegamenti tra il door controller e i dispositivi esterni siano ben saldi.
- Verificare tutti i collegamenti hardware. Vedere *Comandi di verifica delle porte alla pagina 20*.
- Verificare che il sistema, inclusi i dispositivi esterni collegati, funzioni correttamente.
  - Passare una tessera e testare i lettori, le porte e le serrature.
  - Se nel sistema sono inclusi dispositivi REX, sensori o altri dispositivi, testare anche quelli.
  - Se attivati, testare gli allarmi anti-manomissione.

Se i risultati di qualsiasi passaggio precedente indicano problemi o comportamenti imprevisti:

- Testare i segnali dei cavi con attrezzatura appropriata e controllare se i cavi sono in qualche modo danneggiati.
- Sostituire tutti i cavi danneggiati o difettosi.
- Dopo aver sostituito i cavi, verificare nuovamente tutti i collegamenti hardware. Vedere *Comandi di verifica delle porte alla pagina 20*.

- Verificare che tutte le pianificazioni accessi, le porte, i gruppi e gli utenti siano aggiornati.
- Se il door controller funziona in modo diverso dal previsto, vedere *Risoluzione di problemi alla pagina 66* e *Manutenzione alla pagina 62* per ulteriori informazioni.

Gestione degli accessi

Informazioni sugli utenti

In AXIS Entry Manager, gli utenti sono le persone registrate come proprietari di uno o più token (tipi di identificazione). Ciascun utente deve disporre di un profilo utente univoco per poter accedere alle porte nel sistema di controllo degli accessi. Il profilo utente è composto da credenziali che indicano al sistema chi è l'utente e quando e come può accedere alle porte. Per ulteriori informazioni, vedere *Creazione e modifica di utenti alla pagina 40*.

Gli utenti in questo contesto non devono essere confusi con gli amministratori. Gli amministratori hanno accesso illimitato a tutte le impostazioni. Nell'ambito della gestione del sistema di controllo degli accessi, nelle pagine Web del dispositivo (AXIS Entry Manager), gli amministratori vengono spesso indicati come utenti. Per ulteriori informazioni, vedere *Utenti alla pagina 54*.

Pagina Gestione degli accessi

La pagina Gestione degli accessi consente di configurare e gestire gli utenti, i gruppi, le porte e le pianificazioni del sistema. Per aprire la pagina Gestione degli accessi, fare clic su **Access Management (Gestione degli accessi)**.

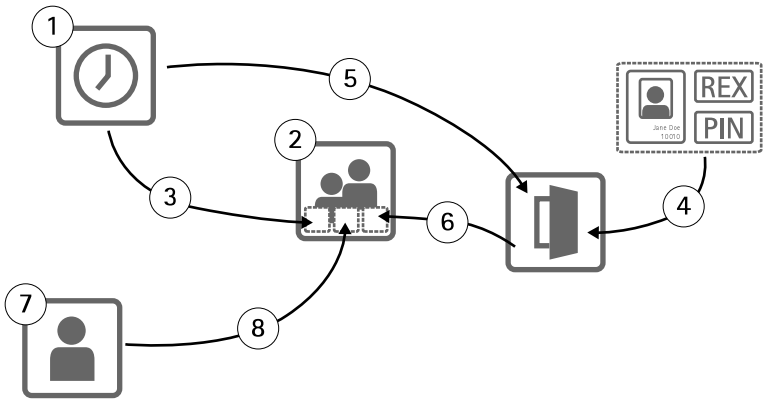
Per aggiungere utenti ai gruppi e applicare le porte e le pianificazioni degli accessi, trascinare gli elementi alle loro rispettive destinazioni negli elenchi **Groups (Gruppi)** e **Doors (Porte)**.

Nota

I messaggi che richiedono azioni vengono visualizzati in rosso.

Scelta di un flusso di lavoro

La struttura di gestione degli accessi è flessibile consentendo all'utente di sviluppare un flusso di lavoro più adatto alle proprie esigenze. Di seguito è riportato un esempio di flusso di lavoro:



1. Creazione di pianificazioni degli accessi. Vedere *pagina 32*.
2. Creazione di gruppi. Vedere *pagina 34*.
3. Applicazione di pianificazioni degli accessi ai gruppi.
4. Aggiunta di tipi di identificazione per porte o piani. Vedere *pagina 34* e *pagina 35*.
5. Applicazione delle pianificazioni degli accessi a ciascun tipo di identificazione.
6. Applicazione di porte o piani ai gruppi.
7. Creazione di utenti. Vedere *pagina 40*.

8. Aggiunta di utenti ai gruppi.

Per gli esempi di applicazione di questo flusso di lavoro, vedere *Esempi di combinazioni di pianificazioni degli accessi alla pagina 42*.

Creazione e modifica delle pianificazioni degli accessi

Le pianificazioni degli accessi vengono utilizzate per definire regole generali in merito a quando è possibile o non è possibile accedere alle porte. Vengono inoltre utilizzate per definire regole relative a quando i gruppi possono e non possono accedere alle porte nel sistema. Per ulteriori informazioni, vedere *Tipi di pianificazioni degli accessi alla pagina 32*.

Per creare una nuova pianificazione degli accessi:

1. Andare ad **Access Management (Gestione degli accessi)**.
2. Nella scheda **Access Schedules (Pianificazioni accessi)** fare clic su **Add new schedule (Aggiungi nuova pianificazione)**.
3. Nella finestra di dialogo **Add access schedule (Aggiungi pianificazione accessi)** immettere il nome della pianificazione.
4. Per creare una pianificazione degli accessi normale, selezionare **Addition Schedule (Pianificazione aggiunta)**.

   Oppure per creare una pianificazione di sottrazione, selezionare **Subtraction Schedule (Pianificazione sottrazione)**.

   Per ulteriori informazioni, vedere *Tipi di pianificazioni degli accessi alla pagina 32*.
5. Fare clic su **Save (Salva)**.

Per espandere un elemento nell'elenco **Access Schedules (Pianificazioni accessi)**, fare clic su . Le pianificazioni di aggiunta vengono visualizzate in verde e le pianificazioni di sottrazione vengono visualizzate in rosso scuro.

Per visualizzare il calendario di una pianificazione degli accessi, fare clic su .

Per modificare il nome di una pianificazione degli accessi o un elemento della pianificazione, fare clic su e apportare le modifiche. Quindi fare clic su **Save (Salva)**.

Per eliminare una pianificazione degli accessi, fare clic su .

Nota

Il dispositivo di controllo porte ha alcune pianificazioni degli accessi comunemente utilizzate, predefinite, che possono essere usate come esempi o modificate secondo necessità. Tuttavia, la pianificazione degli accessi predefinita **Always (Sempre)** non può essere modificata o eliminata.

Tipi di pianificazioni degli accessi

Esistono due tipi di pianificazioni degli accessi:

- **Pianificazione di aggiunta**: pianificazioni degli accessi normali che definiscono quando è possibile accedere alle porte. Le pianificazioni di aggiunta tipiche sono orario di ufficio, orario lavorativo, straordinario o orario notturno.
- **Pianificazione di sottrazione**: eccezioni alle pianificazioni degli accessi normali. In genere vengono utilizzate per limitare l'accesso durante uno specifico periodo di tempo che si verifica durante il periodo di tempo di una pianificazione normale (pianificazione di aggiunta). Le pianificazioni di sottrazione, ad esempio, possono essere utilizzate per rifiutare l'accesso degli utenti all'edificio durante le festività che si verificano nei giorni della settimana.

Entrambi i tipi di pianificazione degli accessi possono essere utilizzate a due livelli:

- **Pianificazioni del tipo di identificazione**: determinano quando e come i lettori concedono agli utenti l'accesso a una porta. Ogni tipo di identificazione deve essere collegato a una pianificazione degli accessi che indica al sistema quando concedere l'accesso agli utenti con tale tipo di identificazione. A ogni tipo di identificazione possono essere aggiunte più pianificazioni di aggiunta e sottrazione. Per informazioni sui tipi di identificazione, vedere *pagina 35*.

- **Pianificazioni gruppo**: determina quando, ma non come, viene concesso l'accesso a una porta ai membri di un gruppo. Ogni gruppo deve essere collegato a uno o più pianificazioni degli accessi che indicano al sistema quando concedere l'accesso ai membri. A ogni gruppo possono essere aggiunte più pianificazioni di aggiunta e sottrazione. Per informazioni sui gruppi, vedere *pagina 34*.

Le pianificazioni di gruppo possono limitare i diritti di accesso in ingresso, ma non estendere i diritti di accesso in ingresso o in uscita oltre quanto consentito dalle pianificazioni del tipo di identificazione. In altre parole, se una pianificazione del tipo di identificazione limita l'accesso in ingresso o in uscita a determinati orari, una pianificazione dei gruppi non può sovrascrivere tale pianificazione del tipo di identificazione. Tuttavia, se una pianificazione di gruppo è più rigorosa in merito all'accesso rispetto alla pianificazione del tipo di identificazione, la pianificazione di gruppo sovrascrive la pianificazione del tipo di identificazione.

Le pianificazioni dei tipi di identificazione e le pianificazioni dei gruppi possono essere combinate in diversi modi per ottenere risultati diversi. Per esempi di combinazioni di pianificazioni degli accessi, vedere *pagina 42*.

Aggiunta di elementi di pianificazione

Entrambe le pianificazioni di aggiunta e di sottrazione possono essere eventi occasionali (singoli) o eventi ricorrenti.

Per aggiungere un elemento di pianificazione a una pianificazione degli accessi:

1. Espandere la pianificazione degli accessi nell'elenco **Access Schedules (Pianificazioni accessi)**.
2. Fare clic su **Add schedule item (Aggiungi elemento di pianificazione)**.
3. Immettere il nome dell'elemento pianificato.
4. Selezionare **One time (Una volta)** o **Recurrence (Ricorrenza)**.
5. Impostare la durata nei campi dell'ora. Vedere *Opzioni relative all'orario alla pagina 33*.
6. Per gli eventi con pianificazione ricorrente, selezionare i parametri **Recurrence pattern (Schema di ricorrenza)** e **Range of recurrence (Intervallo di ricorrenza)**. Vedere *Opzioni dello schema di ricorrenza alla pagina 33* e *Opzioni dell'intervallo di ricorrenza alla pagina 33*.
7. Fare clic su **Save (Salva)**.

Opzioni relative all'orario

Sono disponibili le opzioni relative all'orario riportate di seguito:

- **All day (Tutti i giorni)**: selezionare questa opzione per gli eventi la cui durata si protrae per tutte le 24 ore del giorno. Quindi immettere la data di **inizio** desiderata.
- **Start (Inizio)**: fare clic sul campo dell'ora e selezionare l'opzione desiderata. Se necessario, fare clic sul campo della data e selezionare il mese, il giorno e l'anno desiderati. È inoltre possibile immettere la data direttamente nel campo.
- **End (Fine)**: fare clic sul campo dell'ora e selezionare l'opzione desiderata. Se necessario, fare clic sul campo della data e selezionare il mese, il giorno e l'anno desiderati. È inoltre possibile immettere la data direttamente nel campo.

Opzioni dello schema di ricorrenza

Le opzioni dello schema di ricorrenza disponibili sono:

- **Yearly (Annuale)**: selezionare questa opzione per ripetere l'evento ogni anno.
- **Weekly (Settimanale)**: selezionare questa opzione per ripetere l'evento ogni settimana.
- Si verifica ogni settimana di **Monday (Lunedì)**, **Tuesday (Martedì)**, **Wednesday (Mercoledì)**, **Thursday (Giovedì)**, **Friday (Venerdì)**, **Saturday (Sabato)** e **Sunday (Domenica)**: selezionare il giorno in cui si desidera che si ripeta l'evento.

Opzioni dell'intervallo di ricorrenza

Le opzioni dell'intervallo di ricorrenza disponibili sono:

- **First occurrence (Prima occorrenza)**: fare clic sul campo della data e selezionare mese, giorno e anno desiderati. È inoltre possibile immettere la data direttamente nel campo.
- **No end date (Nessuna data di fine)**: selezionare questa opzione per ripetere l'occorrenza all'infinito.
- **End by (Data di fine)**: fare clic sul campo della data e selezionare il mese, il giorno e l'anno desiderati. È inoltre possibile immettere la data direttamente nel campo.

Creazione e modifica di gruppi

I gruppi consentono di gestire gli utenti e i rispettivi diritti di accesso collettivamente e in modo efficiente. Un gruppo è costituito da credenziali che indicano al sistema quali utenti fanno parte del gruppo e quando e come viene consentito l'accesso alle porte ai membri del gruppo.

Ogni utente deve appartenere a uno o più gruppi. Per aggiungere un utente a un gruppo, trascinare e rilasciare l'utente nel gruppo desiderato nell'elenco **Groups (Gruppi)**. Per ulteriori informazioni, vedere *Creazione e modifica di utenti alla pagina 40*.

Per creare un nuovo gruppo:

1. Andare ad **Access Management (Gestione degli accessi)**.
2. Nella scheda **Groups (Gruppi)** fare clic su **Add new group (Aggiungi nuovo gruppo)**.
3. Nella finestra di dialogo **Add Group (Aggiungi gruppo)** immettere le credenziali del gruppo. Vedere *Credenziali di gruppo alla pagina 34*.
4. Fare clic su **Save (Salva)**.

Per espandere un elemento nell'elenco **Groups (Gruppi)** e visualizzarne i membri, i diritti di accesso alle porte e le pianificazioni, fare clic su  .

Per modificare il nome di un gruppo o la data di validità, fare clic su  e apportare le modifiche. Quindi fare clic su **Save (Salva)**.

Per verificare quando e come un gruppo possa accedere a determinate porte, fare clic su  .

Per eliminare un gruppo o i membri del gruppo, le porte o le pianificazioni di un gruppo, fare clic su  .

Credenziali di gruppo

Per i gruppi sono disponibili le seguenti credenziali:

- **Name (Nome)** (obbligatorio)
- **Valid from (Valido da)** e **Valid to (Valido fino a)**: immettere le date entro le quali le credenziali del gruppo devono essere valide. Fare clic sul campo della data e selezionare il mese, il giorno e l'anno desiderati. È inoltre possibile immettere la data direttamente nel campo.
- **Whitelist (Whitelist)**: gli utenti nel gruppo whitelist possono accedere sempre alle porte nel gruppo, anche in caso di errore di rete o di alimentazione. Poiché gli utenti nel gruppo hanno sempre accesso alle porte, le pianificazioni o le opzioni Valido da e Valido fino a non si applicano. Ora di accesso prolungata non è supportata per un utente che apre una porta in un gruppo whitelist. Al gruppo possono essere aggiunte solo le porte con blocchi wireless che supportano la funzionalità whitelist.

Nota

- Per poter salvare il gruppo, è necessario immettere il **Name (Nome)** del gruppo.
- Le opzioni Valido fino a e Valido da per un utente non si applicano quando si aggiunge l'utente al gruppo whitelist.
- La sincronizzazione delle credenziali aggiunte alla whitelist ad un blocco wireless richiede del tempo e interferisce sulle normali procedure di apertura delle porte. Evitare l'aggiunta o la rimozione di un numero elevato di credenziali in un sistema durante le ore di picco. Quando viene eseguita la sincronizzazione delle credenziali aggiornate per il blocco, il registro eventi indicherà `SyncOngoing: false` per il blocco.

Gestione delle porte

Le regole generali per ogni porta vengono gestite nella scheda **Doors (Porte)**. Le regole includono l'aggiunta di tipi di identificazione che determinano in che modo agli utenti verrà concesso l'accesso alla porta e le pianificazioni degli accessi che determinano in quale momento è valido ogni tipo di identificazione. Per ulteriori informazioni, vedere *Tipi di identificazione alla pagina 35* e *Creazione e modifica delle pianificazioni degli accessi alla pagina 32*.

Prima di poter gestire una porta, è necessario aggiungerla al sistema di controllo degli accessi completando la configurazione dell'hardware. A tale scopo, vedere *Configurazione dell'hardware alla pagina 13*.

Per gestire una porta:

1. Andare ad **Access Management (Gestione degli accessi)** e selezionare la scheda **Doors (Porte)**.
2. Nell'elenco **Doors (Porte)** fare clic su accanto alla porta che si desidera modificare.
3. Trascinare la porta in almeno un gruppo. Se l'elenco **Groups (Gruppi)** è vuoto, creare un nuovo gruppo. Vedere *Creazione e modifica di gruppi alla pagina 34*.
4. Fare clic su **Add identification type (Aggiungi tipo di identificazione)** e selezionare le credenziali che l'utente deve presentare al lettore per poter accedere alla porta. Vedere *Tipi di identificazione alla pagina 35*.

   Aggiungere almeno un tipo di identificazione a ogni porta.
5. Per aggiungere più tipi di identificazione, ripetere il passaggio precedente.

   Se vengono aggiunti entrambi i tipi di identificazione **Card number only (Solo numero scheda)** e **PIN only (Solo PIN)**, gli utenti possono scegliere di strisciare la scheda oppure immettere il PIN per accedere alla porta. Se invece viene aggiunto un solo tipo di identificazione **Card number and PIN (Numero scheda e PIN)**, l'utente deve strisciare la scheda e immettere il PIN per accedere alla porta.
6. Per definire il momento in cui le credenziali sono valide, trascinare una pianificazione per ogni tipo di identificazione.

Per sbloccare le porte, chiuderle o concedere l'accesso temporaneo manualmente, fare clic su una delle azioni porta manuali richieste. Vedere *Utilizzo di azioni porta manuali alla pagina 36*.

Nota

I controlli per sbloccare e bloccare manualmente le porte o concedervi l'accesso temporaneo non sono disponibili per porte/dispositivi wireless.

Per espandere un elemento nell'elenco **Doors (Porte)**, fare clic su .

Per modificare il nome di una porta o di un lettore, fare clic su e apportare le modifiche. Quindi fare clic su **Save (Salva)**.

Per verificare il lettore, il tipo di identificazione e le combinazioni di pianificazione degli accessi, fare clic su .

Per verificare la funzione dei blocchi collegati alle porte, fare clic sui controlli di verifica. Vedere *Comandi di verifica delle porte alla pagina 20*.

Per eliminare i tipi di identificazione o le pianificazioni degli accessi, fare clic su .

Tipi di identificazione

I tipi di identificazione sono dispositivi di archiviazione di credenziali portatili, informazioni memorizzate o varie combinazioni di questi due elementi che determinano il modo in cui agli utenti viene concesso l'accesso alla porta. Tipi di identificazione comuni comprendono token quali schede o portachiavi, numeri di identificazione personale (PIN) e richieste di uscita da dispositivi (REX).

Per ulteriori informazioni sulle credenziali, vedere *Credenziali dell'utente alla pagina 40*.

Sono disponibili i tipi di identificazione elencati di seguito:

- **Solo codice struttura**: l'utente può accedere alla porta utilizzando una scheda o un altro token con il codice struttura accettato dal lettore.
- **Solo numero scheda**: l'utente può accedere alla porta solo tramite una scheda o altri token accettati dal lettore. Il codice carta è un numero univoco generalmente stampato sulla scheda. Vedere le informazioni fornite dal produttore della scheda per scoprire dove trovare il codice carta. Il numero della scheda può essere recuperato dal sistema. Strisciare la scheda su un lettore collegato, selezionare il lettore dall'elenco e fare clic su **Retrieve (Recupera)**.
- **Solo scheda dati non elaborati**: l'utente può accedere alla porta solo tramite una scheda o altri token accettati dal lettore. Le informazioni vengono archiviate come dati non elaborati sulla scheda. I dati non elaborati sulla scheda possono essere recuperati dal sistema. Strisciare la scheda su un lettore collegato, selezionare il lettore dall'elenco e fare clic su **Retrieve (Recupera)**. Utilizzare questo tipo di identificazione solo se non è possibile individuare un codice carta.
- **Solo PIN**: l'utente può accedere alla porta solo tramite un PIN (Personal Identification Number) a quattro cifre.
- **Codice struttura e PIN**: l'utente necessita della scheda o di un altro token con il codice della struttura accettato dal lettore e un PIN per accedere alla porta. L'utente deve inserire le credenziali nell'ordine indicato (prima la scheda, poi il PIN).
- **Numero scheda e PIN**: l'utente necessita della scheda o dell'altro token accettato dal lettore e di un PIN per accedere alla porta. L'utente deve inserire le credenziali nell'ordine indicato (prima la scheda, poi il PIN).
- **Scheda dati non elaborati e PIN**: l'utente necessita della scheda o dell'altro token accettato dal lettore e di un PIN per accedere alla porta. Utilizzare questo tipo di identificazione solo se non è possibile individuare un codice carta. L'utente deve inserire le credenziali nell'ordine indicato (prima la scheda, poi il PIN).
- **REX**: l'utente può accedere alla porta tramite l'attivazione di una richiesta di uscita dal dispositivo (REX), ad esempio un pulsante, un sensore o un maniglione.
- **Solo targa**: l'utente può accedere alla porta utilizzando solo il numero di targa di un veicolo.

Aggiunta di stati di sblocco pianificati

Per mantenere sbloccata una porta automaticamente per una durata di tempo specifica, è possibile aggiungere uno stato **Scheduled unlock (Sblocco pianificato)** a una porta e applicarvi una pianificazione degli accessi.

Ad esempio, per mantenere una porta sbloccata durante l'orario di ufficio:

1. Andare ad **Access Management (Gestione degli accessi)** e selezionare la scheda **Doors (Porte)**.
2. Fare clic su  accanto alla voce dell'elenco **Doors (Porte)** che si desidera modificare.
3. Fare clic su **Add scheduled unlock (Aggiungi sblocco pianificato)**.
4. Selezionare **Unlock state (Stato sblocco)** (**sbloccato** o **sblocca entrambi i blocchi** a seconda che la porta abbia un blocco o due).
5. Fare clic su **OK**.
6. Applicare la pianificazione degli accessi predefinita **Office hours (Orario di ufficio)** nello stato **Scheduled unlock (Sblocco pianificato)**.

Per verificare se la porta è sbloccata, fare clic su  .

Per eliminare uno stato di sblocco pianificato o una pianificazione degli accessi, fare clic su  .

Utilizzo di azioni porta manuali

Le porte possono essere sbloccate o bloccate e può essere consentito l'accesso temporaneo nella scheda **Doors (Porte)** in **Manual door actions (Azioni porte manuali)**. Le azioni porta manuali disponibili per una porta specifica dipendono da come è stata configurata la porta.

Per utilizzare le azioni porta manuali:

1. Andare ad **Access Management (Gestione degli accessi)** e selezionare la scheda **Doors (Porte)**.
2. Nell'elenco **Doors (Porte)**, fare clic su ▶ accanto alla porta che si desidera controllare.
3. Fare clic sull'azione richiesta per la porta. Vedere *Azioni porta manuali alla pagina 37*.

Nota

Per utilizzare le azioni porta manuali, è necessario aprire la pagina Gestione degli accessi tramite il dispositivo di controllo delle porte a cui è collegata la porta specifica. Se si apre la pagina Gestione degli accessi tramite un dispositivo di controllo delle porte differente, al posto delle azioni porta manuali esisterà un collegamento alla pagina Panoramica del dispositivo di controllo delle porte a cui la porta specifica è collegata. Fare clic sul collegamento, andare ad **Access Management (Gestione degli accessi)** e selezionare la scheda **Doors (Porte)**.

Azioni porta manuali

Sono disponibili le seguenti azioni manuali per le porte:

- **Get door status (Ottieni stato porta)**: verificare lo stato corrente del monitor porte, degli allarmi porta e dei blocchi.
- **Access (Accesso)**: consente agli utenti l'accesso alla porta. Si applica il tempo di accesso specificato. Vedere *Modalità di configurazione di monitor porte e blocchi alla pagina 14*.
- **Unlock (Sblocca)** (un blocco) o **Unlock both locks (Sblocca entrambi i blocchi)** (due blocchi): sblocca la porta. La porta rimane sbloccata finché non si preme **Lock (Blocca)** o **Lock both locks (Blocca entrambi i blocchi)**, viene attivato uno stato porta pianificato o il dispositivo di controllo della porta viene riavviato.
- **Lock (Blocco)** (un blocco) o **Lock both locks (Blocca entrambi i blocchi)** (due blocchi): blocca la porta.
- **Unlock second lock and lock primary (Sblocca secondo blocco e blocca primario)**: questa opzione è disponibile solo se la porta è stata configurata con un blocco secondario. Sblocca la porta. Il blocco secondario rimane sbloccato finché non si preme **Double lock (Blocco doppio)** oppure quando viene attivato uno stato porta pianificato.

Gestione dei piani

Se AXIS 9188 Network I/O Relay Module è stato installato nel proprio sistema, i piani possono essere gestiti con una modalità simile a quella della gestione delle porte.

Nota

Se si utilizza A1001 in modalità cluster con eventi globali abilitati, verificare di utilizzare nomi descrittivi univoci per ciascun piano. Ad esempio *"Ascensore A, Piano 1"*.

Nota

È possibile configurare max 2 moduli AXIS 9188 Network I/O Relay per ciascun A1001 Network Door Controller.

Le regole generali per ciascun piano sono gestite nella scheda **Floors (Piani)**. Le regole includono l'aggiunta di tipi di identificazione che determinano la modalità con cui verrà garantito l'accesso agli utenti al piano e alle pianificazioni dell'accesso che determinano quando ciascun tipo di identificazione è valido. Per ulteriori informazioni, vedere *Piani dei tipi di identificazione alla pagina 38* e *Creazione e modifica delle pianificazioni degli accessi alla pagina 32*.

Prima di poter gestire un piano, è necessario aggiungerlo al sistema di controllo degli accessi completando la configurazione dell'hardware, vedere *Configurazione dell'hardware alla pagina 13*.

Per gestire un piano:

1. Andare a **Access Management (Gestione degli accessi)** e selezionare la scheda **Floors (Piani)**.
2. Nell'elenco **Floors (Piani)**, fare clic su ▶ accanto al piano che si desidera modificare.

3. Trascinare il piano su almeno un gruppo. Se l'elenco **Groups (Gruppi)** è vuoto, creare un nuovo gruppo. Vedere *Creazione e modifica di gruppi alla pagina 34*.
4. Fare clic su **Add identification type (Aggiungi tipo di identificazione)** e selezionare quali credenziali l'utente deve presentare al lettore affinché venga garantito l'accesso al piano. Vedere *Piani dei tipi di identificazione alla pagina 38*.

   Aggiungere almeno un tipo di identificazione a ciascun piano.
5. Per aggiungere più tipi di identificazione, ripetere il passaggio precedente.

   Se vengono aggiunti entrambi i tipi di identificazione **Card number only (Solo numero scheda)** e **PIN only (Solo PIN)**, gli utenti possono scegliere di strisciare la scheda oppure immettere il PIN per accedere alla porta. Se invece viene aggiunto un solo tipo di identificazione **Card number and PIN (Numero scheda e PIN)**, l'utente deve strisciare la scheda e immettere il PIN per accedere alla porta.
6. Per definire quando le credenziali sono valide, trascinare una pianificazione su ciascun tipo di identificazione.

Per sbloccare, bloccare o concedere accesso temporaneo manualmente ai piani fare clic su una delle azioni manuali della porta come richiesto. Vedere *Utilizzo di azioni per i piani manuali alla pagina 39*.

Nota

I comandi per sbloccare, bloccare o garantire accesso temporaneo manualmente i piani non sono disponibili per i dispositivi o le porte wireless.

Per espandere una voce nell'elenco **Floors (Piani)**, fare clic su  .

Per modificare un piano o un nome del lettore, fare clic su  ed effettuare le modifiche. Quindi, fare clic su **Save (Salva)**.

Per verificare il lettore, il tipo di identificazione e le combinazioni di pianificazione degli accessi, fare clic su  .

Per verificare la funzione dei blocchi collegati ai piani, fare clic sui comandi di verifica. Vedere *Piani dei controlli di verifica alla pagina 20*.

Per eliminare i tipi di identificazione o le pianificazioni degli accessi, fare clic su  .

Piani dei tipi di identificazione

I tipi di identificazione sono dispositivi di archiviazione di credenziali portatili, alcune informazioni memorizzate o varie combinazioni di questi due elementi che determinano il modo in cui gli utenti ricevono accesso al piano. Tipi di identificazione comuni comprendono token quali schede o portachiavi, numeri di identificazione personale (PIN) e richieste di uscita da dispositivi (REX).

Per ulteriori informazioni sulle credenziali, vedere *Credenziali dell'utente alla pagina 40*.

Sono disponibili i tipi di identificazione elencati di seguito:

- **Solo codice struttura**: l'utente può accedere al piano utilizzando una scheda o un altro token con il codice struttura accettato dal lettore.
- **Solo numero scheda**: l'utente può accedere al piano solo tramite una scheda o altri token accettati dal lettore. Il codice carta è un numero univoco generalmente stampato sulla scheda. Vedere le informazioni fornite dal produttore della scheda per scoprire dove trovare il codice carta. Il numero della scheda può essere recuperato dal sistema. Strisciare la scheda su un lettore collegato, selezionare il lettore dall'elenco e fare clic su **Retrieve (Recupera)**.
- **Solo scheda dati non elaborati**: l'utente può accedere al piano solo tramite una scheda o altri token accettati dal lettore. Le informazioni vengono archiviate come dati non elaborati sulla scheda. I dati non elaborati sulla scheda possono essere recuperati dal sistema. Strisciare la scheda su un lettore collegato, selezionare il lettore dall'elenco e fare clic su **Retrieve (Recupera)**. Utilizzare questo tipo di identificazione solo se non è possibile individuare un codice carta.
- **Solo PIN**: l'utente può accedere al piano solo tramite un PIN (Personal Identification Number) a quattro cifre.
- **Codice struttura e PIN**: l'utente necessita della scheda o di un altro token con il codice della struttura accettato dal lettore e un PIN per accedere al piano. L'utente deve inserire le credenziali nell'ordine indicato (scheda prima, quindi PIN).

- **Numero scheda e PIN**: l'utente necessita della scheda o dell'altro token accettato dal lettore e di un PIN per accedere al piano. L'utente deve inserire le credenziali nell'ordine indicato (scheda prima, quindi PIN).
- **Scheda dati non elaborati e PIN**: l'utente necessita della scheda o dell'altro token accettato dal lettore e di un PIN per accedere al piano. Utilizzare questo tipo di identificazione solo se non è possibile individuare un codice carta. L'utente deve inserire le credenziali nell'ordine indicato (scheda prima, quindi PIN).
- **REX**: l'utente può accedere al piano tramite una richiesta di uscita dal dispositivo (REX), ad esempio un pulsante, un sensore o un maniglione.

Aggiunta di stati di sblocco pianificati

Per mantenere automaticamente un piano accessibile a chiunque per una durata di tempo specifica, è possibile aggiungere uno stato di **Scheduled unlock (Sblocco pianificato)** ad un piano ed applicare una pianificazione di accesso.

Ad esempio, per mantenere un piano accessibile a chiunque durante le ore di ufficio:

1. Andare a **Access Management (Gestione degli accessi)** e selezionare la scheda **Floors (Piani)**.
2. Fare clic su  accanto alla voce dell'elenco **Floors (Piani)** che si desidera modificare.
3. Fare clic su **Add scheduled unlock (Aggiungi sblocco pianificato)**.
4. Selezionare lo **Unlock state (Stato sblocco)** (**sbloccato** o **sblocca entrami i blocchi** dipendentemente dal fatto che il piano abbia un blocco o due).
5. Fare clic su **OK**.
6. Applicare la pianificazione di accesso predefinita **Office hours (Orario di ufficio)** allo stato **Scheduled unlock (Sblocco pianificato)**.

Per verificare se il piano è accessibile, fare clic su  .

Per eliminare uno stato di sblocco pianificato o una pianificazione di accesso, fare clic su  .

Utilizzo di azioni per i piani manuali

I piani possono avere accessibilità diverse, limitate o accessibili per tutti gli utenti. L'accesso temporaneo può essere garantito nella scheda **Floors (Piani)** tramite **Manual floor actions (Azioni piani manuali)**. Le azioni disponibili per i piani manuali per un piano specifico dipendono da come è stato configurato il piano.

Per utilizzare le azioni per i piani manuali:

1. Andare a **Access Management (Gestione degli accessi)** e selezionare la scheda **Floors (Piani)**.
2. Nell'elenco **Floors (Piani)**, fare clic su  accanto al piano che si desidera controllare.
3. Fare clic sull'azione richiesta per il piano. Vedere *Azioni piano manuali alla pagina 39*.

Nota

Per utilizzare le azioni per i piani manuali, è necessario aprire la pagina Gestione degli accessi tramite il dispositivo di controllo dei piani a cui è collegata la porta specifica. Se si apre la pagina Gestione degli accessi tramite un dispositivo di controllo dei piani differente, al posto delle azioni per i piani manuali esisterà un collegamento alla pagina Panoramica del dispositivo di controllo dei piani a cui il piano specifico è collegato. Fare clic sul collegamento, andare a **Access Management (Gestione degli accessi)** e selezionare la scheda **Floors (Piani)**.

Azioni piano manuali

Sono disponibili le seguenti azioni per i piani manuali:

- **Get floor status (Ottieni stato piano)**: verificare lo stato corrente del relè collegato al piano.

- **Access (Accesso)**: consente agli utenti l'accesso al piano. Si applica il tempo di accesso specificato. Vedere *Modalità di configurazione di monitor porte e blocchi alla pagina 14*.
- **Unlock (Sblocca)**: il piano diventa completamente accessibile a tutti finché non si preme il pulsante **Lock (Blocca)**. Viene attivato uno stato piano pianificato oppure il dispositivo di controllo delle porte viene riavviato.
- **Lock (Blocca)**: il piano diventa completamente inaccessibile a tutti finché non si preme il pulsante **Unlock (Sblocca)**. Viene attivato uno stato piano pianificato oppure il dispositivo di controllo delle porte viene riavviato.

Creazione e modifica di utenti

Ciascun utente deve disporre di un profilo utente univoco per poter accedere alle porte nel sistema di controllo degli accessi. Il profilo utente è composto da credenziali che indicano al sistema chi è l'utente e quando e come può accedere alle porte.

Per poter gestire in modo efficace i diritti di accesso utente, ogni utente deve appartenere a uno o più gruppi. Per ulteriori informazioni, vedere *Creazione e modifica di gruppi*.

Per creare un nuovo profilo utente:

1. Andare ad **Access Management (Gestione degli accessi)**.
2. Selezionare la scheda **Users (Utenti)** e fare clic su **Add new user (Aggiungi nuovo utente)**.
3. Nella finestra di dialogo **Add User (Aggiungi utente)** immettere le credenziali dell'utente. Vedere *Credenziali dell'utente alla pagina 40*.
4. Fare clic su **Save (Salva)**.
5. Trascinare l'utente in uno o più gruppi nell'elenco **Groups (Gruppi)**. Se l'elenco **Groups (Gruppi)** è vuoto, creare un nuovo gruppo. Vedere *Creazione e modifica di gruppi alla pagina 34*.

Per espandere un elemento nell'elenco **Users (Utenti)** e visualizzare le credenziali di un utente, fare clic su  .

Per trovare un utente specifico, immettere un filtro nel campo del filtro degli utenti. Per ottenere corrispondenze esatte, racchiudere il testo del filtro tra virgolette doppie, ad esempio "John" o "potter, virginia".

Per modificare le credenziali di un utente, fare clic su  e modificare le credenziali secondo necessità. Quindi, fare clic su **Save (Salva)**.

Per eliminare un utente, fare clic su  .

Importante

Se un utente è stato creato tramite AXIS Visitor Manager, non modificarlo o eliminarlo in AXIS Entry Manager. Per ulteriori informazioni su AXIS Visitor Manager e il servizio di lettore di codici QR, vedere *Axis Visitor Access alla pagina 23*.

Credenziali dell'utente

Per gli utenti sono disponibili le seguenti credenziali:

- **Nome** (obbligatorio)
- **Cognome**
- **Valido da** e **Valido fino a**: immettere le date entro le quali le credenziali dell'utente devono essere valide. Fare clic sul campo della data e selezionare il mese, il giorno e l'anno desiderati. È inoltre possibile immettere la data direttamente nel campo.
- **Sospendi credenziali**: selezionare questa opzione per sospendere le credenziali. Una volta sospese, le credenziali non potranno essere utilizzate dall'utente per accedere ad alcuna porta nel sistema. Deselezionare l'opzione per concedere di nuovo l'accesso all'utente. La sospensione è progettata per essere temporanea. Se è necessario rifiutare l'accesso all'utente in modo permanente, si consiglia di eliminare il profilo utente.

- **PIN** (obbligatorio in caso non sia disponibile un codice carta o una scheda di dati non elaborati): immettere il numero di identificazione personale a quattro cifre (PIN) selezionato dall'utente o assegnato all'utente.
- **Codice struttura**: immettere un codice per verificare il sistema di controllo degli accessi della struttura. Se si immette un codice struttura preset, questo campo viene riempito automaticamente. A tale scopo, vedere *Codice struttura predefinito alla pagina 23*
- **Numero di schede** (obbligatorio in caso di PIN o scheda dati non elaborati non disponibile): immettere il numero della scheda. Vedere le informazioni fornite dal produttore della scheda per scoprire dove trovare il codice carta. Il numero della scheda può essere recuperato dal sistema. Strisciare la scheda su un lettore collegato, selezionare il lettore dall'elenco e fare clic su **Retrieve (Recupera)**.
- **Scheda dati non elaborati** (obbligatorio in caso di PIN o codice carta non disponibile): immettere i dati non elaborati della scheda. I dati possono essere recuperati dal sistema. Strisciare la scheda su un lettore collegato, selezionare il lettore dall'elenco e fare clic su **Retrieve (Recupera)**. Utilizzare questo tipo di identificazione solo se non è possibile individuare un codice carta.
- **Ora di accesso prolungata**: selezionare questa opzione per sovrascrivere l'ora di accesso esistente e consentire l'apertura della porta per l'ora di accesso prolungata per l'utente. Vedere *Informazioni sulle opzioni relative al monitor porte e all'orario alla pagina 15*
- **Targa** (queste credenziali non sono disponibili in un'installazione del dispositivo di controllo porta predefinito): quando queste credenziali sono attivata dal software sviluppato da partner, immettere il numero di targa per il veicolo dell'utente. Questo tipo di credenziali può essere usato solo con un software partner Axis e una telecamera con il software di riconoscimento targhe. Per ulteriori informazioni, contattare il partner Axis o il rappresentante vendite Axis locale.

Nota

Il pulsante **Retrieve (Recupera)** è disponibile solo se è stata completata la configurazione dell'hardware e uno o più lettori sono collegati al dispositivo di controllo.

Importazione degli utenti

Gli utenti possono essere aggiunti al sistema mediante l'importazione di un file di testo con valori separati da virgola (CSV). Si consiglia di importare utenti quando è necessario aggiungere molti utenti alla volta.

Prima di poter importare gli utenti, è necessario creare e salvare un file (*.csv o *.txt) nel formato CSV corretto. Separare i valori con virgola, senza spazi e separare ogni utente con un'interruzione di riga.

Esempio

```
jane,doe,1234,12345678,abc123
john,doe,5435,87654321,cde321
```

Per importare utenti:

1. Andare a **Setup > Import Users (Impostazione > Importa utenti)**.
2. Individuare e selezionare il file *.csv o *.txt che contiene l'elenco degli utenti.
3. Selezionare l'opzione delle credenziali corretta per ogni colonna.
4. Per importare gli utenti nel sistema, fare clic su **Import users (Importa utenti)**.
5. Verificare che ogni colonna contenga il tipo di credenziali corretto.
6. Se le colonne sono corrette, fare clic su **Start importing users (Avvia importazione utenti)**. Se le colonne non sono corrette, fare clic su **Cancel (Annulla)** e iniziare di nuovo.
7. Al termine dell'importazione, fare clic su **OK**.

Sono disponibili le opzioni delle credenziali riportate di seguito:

- **First name (Nome)**

- **Last name (Cognome)**
- **PIN code (Codice PIN)**
- **Card number (Codice carta)**
- **License plate (Targa)**
- **Unassigned (Non assegnati)**: i valori che non verranno importati. Selezionare questa opzione per ignorare una determinata colonna.

Per ulteriori informazioni sulle credenziali, vedere *Creazione e modifica di utenti*.

Esportazione degli utenti

La pagina di esportazione mostra un elenco con valori separati da virgola (CSV) di tutti gli utenti nel sistema. L'elenco può essere utilizzato per importare gli utenti in un altro sistema.

Per esportare l'elenco degli utenti:

1. Aprire un editor di testo normale e creare un nuovo documento.
2. Andare a **Setup > Export Users (Impostazione > Esporta utenti)**
3. Selezionare tutti i valori nella pagina e copiarli.
4. Incollare i valori nel documento di testo.
5. Salvare il documento come file con valori delimitati da virgole (*.csv) o come file di testo (*.txt).

Esempi di combinazioni di pianificazioni degli accessi

Le pianificazioni dei tipi di identificazione e le pianificazioni dei gruppi possono essere combinate in diversi modi per ottenere risultati diversi. Gli esempi riportati qui sotto seguono il flusso di lavoro descritto in *pagina 31*.

Esempio

Per creare una combinazione di pianificazioni che

- conceda ai sorveglianti di accedere a una porta in qualsiasi momento,
  - con la propria tessera durante il turno di lavoro diurno (lunedì - venerdì, dalle 06.00 alle 16.00) e
  - con la propria tessera e il PIN prima e dopo il turno di lavoro diurno. Questo
- consente al personale del turno diurno di accedere alla stessa porta,
  - con la propria tessera solo durante l'orario lavorativo diurno:

1. Creare una **pianificazione aggiuntiva** chiamata **Orario turno diurno**. Vedere *pagina 32*.
2. Creare un turno lavorativo diurno **Schedule item (Elemento pianificazione)** che si ripete dal lunedì al venerdì, dalle 06.00 alle 16.00.
3. Creare due gruppi, un **gruppo** chiamato **Sorveglianti** e un **gruppo** chiamato **Personale turno diurno**. Vedere *pagina 34*.
4. Trascinare la pianificazione degli accessi **Always (Sempre)** predefinita nel gruppo **Sorveglianti**.
5. Trascinare la pianificazione degli accessi **Turno di lavoro diurno** nel gruppo **Personale turno diurno**.
6. Aggiungere i tipi di identificazione **Card number and PIN (Numero scheda e PIN)** e **Card number only (Solo numero scheda)** al lettore della porta.
7. Trascinare la pianificazione degli accessi **Always (Sempre)** predefinita nel tipo di identificazione **Card number and PIN (Numero scheda e PIN)**.

8. Trascinare la pianificazione degli accessi **Turno di lavoro diurno** nel tipo di identificazione **Card number only (Solo numero scheda)**.
9. Trascinare la porta su entrambi i gruppi. Quindi, aggiungere utenti ai gruppi, come richiesto. Vedere *pagina 40*.

Esempio

Per creare una combinazione di pianificazioni che

- conceda ai sorveglianti di accedere a una porta in qualsiasi momento,
  - con la propria tessera durante il turno di lavoro diurno (lunedì - venerdì, dalle 06.00 alle 16.00) e
  - con la propria tessera e il PIN prima e dopo il turno di lavoro diurno. Questo
- consente l'accesso del personale del turno diurno alla stessa porta ogni giorno tra le 06.00 e le 16.00,
  - con la propria tessera durante l'orario lavorativo diurno e
  - con la propria tessera e il PIN durante la notte e nei fine settimana:

1. Creare una **pianificazione aggiuntiva** chiamata **Orario turno diurno**. Vedere *pagina 32*.
2. Creare un turno lavorativo diurno **Schedule item (Elemento pianificazione)** che si ripete dal lunedì al venerdì, dalle 06.00 alle 16.00.
3. Creare una **pianificazione di sottrazione** chiamata **Notti e fine settimana**.
4. Creare un **elemento di pianificazione** per notti e fine settimana che si ripete dal lunedì alla domenica, dalle 16.00 alle 06.00.
5. Trascinare la pianificazione **Always (Sempre)** predefinita e la pianificazione degli accessi **Notte e fine settimana** sul gruppo **Personale turno diurno**.
6. Creare due gruppi, un **gruppo** chiamato **Sorveglianti** e un **gruppo** chiamato **Personale turno diurno**. Vedere *pagina 34*.
7. Trascinare la pianificazione degli accessi **Always (Sempre)** predefinita nel gruppo **Sorveglianti** e nel gruppo **Personale turno diurno**.
8. Trascinare la pianificazione degli accessi **Notti e fine settimana** nel gruppo **Personale turno diurno**.
9. Aggiungere i tipi di identificazione **Card number and PIN (Numero scheda e PIN)** e **Card number only (Solo numero scheda)** al lettore della porta.
10. Trascinare la pianificazione degli accessi **Always (Sempre)** predefinita nel tipo di identificazione **Card number and PIN (Numero scheda e PIN)**.
11. Trascinare la pianificazione degli accessi **Turno di lavoro diurno** nel tipo di identificazione **Card number only (Solo numero scheda)**.
12. Trascinare la porta su entrambi i gruppi. Quindi, aggiungere utenti ai gruppi, come richiesto. Vedere *pagina 40*.

Configurazione di allarmi ed eventi

Gli eventi che si verificano nel sistema, ad esempio quando un utente striscia una scheda o quando viene attivato un dispositivo REX, vengono registrati nel registro eventi. Gli eventi registrati possono essere configurati per attivare allarmi e tali allarmi vengono registrati nel registro allarmi.

- Visualizzare il registro eventi. Vedere *pagina 44*.
- Esportare il registro eventi. Vedere *pagina 44*
- Visualizzare il registro allarmi. Vedere *pagina 45*.
- Configurare i registri eventi e allarmi. Vedere *pagina 45*.

Anche gli allarmi possono essere configurati per attivare azioni come le notifiche e-mail. Per ulteriori informazioni, vedere *Modalità di impostazione delle regole di azione alla pagina 46*.

Visualizzazione del registro eventi

Per visualizzare gli eventi registrati, andare a **Event Log (Registro eventi)**.

Se gli eventi globali sono abilitati, è possibile aprire il registro eventi da qualsiasi dispositivo di controllo porte nel sistema. Per ulteriori informazioni sugli eventi globali, vedere *Configurazione dei registri eventi e allarmi alla pagina 45*.

Per espandere un elemento nel registro eventi e visualizzare i dettagli degli eventi, fare clic su  .

L'applicazione di filtri al registro eventi rende più semplice individuare eventi specifici. Per filtrare l'elenco, selezionare uno o più filtri del registro eventi e fare clic su **Apply filters (Applica filtri)**. Per ulteriori informazioni, vedere *Filtri di registro eventi alla pagina 44*.

Per l'amministratore potrebbero essere più interessanti alcuni eventi piuttosto che altri. Pertanto, è possibile scegliere gli eventi che devono essere registrati e i relativi dispositivi di controllo. Per ulteriori informazioni, vedere *Opzioni del registro eventi alla pagina 45*.

Filtri di registro eventi

È possibile restringere l'ambito del registro eventi selezionando uno o più filtri seguenti:

- Utenti: filtrare per eventi correlati a un utente selezionato.
- Porta e piano: filtrare per eventi correlati a una porta o a un piano specifici.
- Argomento: filtrare per tipo di eventi.
- Origine: filtrare per gli eventi da un dispositivo di controllo selezionato. Disponibile solo in un dispositivo di controllo cluster e quando sono abilitati eventi globali.
- Data e ora: filtrare il registro eventi per un intervallo di data e ora.

Esportazione del registro eventi

Per esportare gli eventi registrati, andare a **Event Log (Registro eventi)**:

1. Fare clic su  .
2. Selezionare il formato di esportazione dal menu a comparsa per avviare l'esportazione.

Nota

Il formato CSV è supportato da tutti i browser, il formato XLSX è supportato in Chrome™ e Internet Explorer®.

Nota

Al termine di un'esportazione, il pulsante di esportazione si modifica da  in  . Per avviare un'altra esportazione, aggiornare la pagina Web. Il pulsante Esporta torna a  .

Visualizzazione del registro allarmi

Per visualizzare gli allarmi attivati, andare a **Alarm Log (Registro allarmi)**. Se gli eventi globali sono abilitati, è possibile aprire il registro allarmi da qualsiasi dispositivo di controllo porte nel sistema. Per ulteriori informazioni sugli eventi globali, vedere *Configurazione dei registri eventi e allarmi alla pagina 45*.

Per espandere un elemento nel registro allarmi e visualizzare i dettagli dell'allarme, ad esempio identità porta e stato della porta, fare clic su  .

Per rimuovere un allarme dall'elenco dopo aver verificato la causa dell'allarme, fare clic su **Acknowledge (Conferma)**. Rimuovere tutti gli allarmi, fare clic su **Acknowledge all alarms (Conferma tutti gli allarmi)**.

Come amministratore, potrebbe essere necessario che alcuni eventi attivino allarmi. Pertanto, è possibile scegliere gli eventi che devono attivare allarmi e per quali dispositivi di controllo. Per ulteriori informazioni, vedere *Opzioni registro allarmi alla pagina 46*.

Configurazione dei registri eventi e allarmi

La pagina Configura registri allarmi ed eventi consente di definire gli eventi da registrare e attiva gli allarmi.

Per condividere eventi e allarmi tra tutti i dispositivi di controllo collegati, selezionare **Global events (Eventi globali)**. Quando gli eventi globali sono abilitati, è necessario solo aprire una pagina Registro eventi e una pagina Registro allarmi per gestire contemporaneamente gli eventi e gli allarmi di tutti i dispositivi di controllo porta nel sistema. Eventi globali è abilitato per impostazione predefinita.

Se si disabilitano gli eventi globali, sarà necessario aprire una pagina Registro eventi e una pagina Registro allarmi per ogni dispositivo di controllo di ogni porta e gestire i relativi eventi e allarmi separatamente.

Importante

Ogni volta che si abilitano o si disabilitano gli eventi globali, il registro eventi viene cancellato. Questo significa che tutti gli eventi precedenti a quel momento vengono rimossi e il registro eventi riprenderà da tale momento.

Anche gli allarmi possono essere configurati per attivare azioni come le notifiche e-mail. Per ulteriori informazioni, vedere *Modalità di impostazione delle regole di azione alla pagina 46*.

Opzioni del registro eventi

Per definire gli eventi che è possibile includere nel registro eventi, andare a **Setup > Configure Event and Alarm Logs (Impostazione > Configura registri allarmi ed eventi)**.

Sono disponibili le seguenti opzioni per la registrazione degli eventi:

- **No logging (Nessuna registrazione)**: disattiva la registrazione degli eventi. L'evento non verrà registrato o incluso nel registro eventi.
- **Log for all sources (Registra per tutte le sorgenti)**: abilitare la registrazione degli eventi in tutti i dispositivi di controllo delle porte. L'evento verrà registrato per tutti i dispositivi di controllo delle porte e incluso nel registro eventi.
- **Log for selected sources (Registra per sorgenti selezionate)**: abilitare la registrazione degli eventi nei dispositivi di controllo delle porte selezionati. L'evento verrà registrato per tutti i dispositivi di controllo delle porte selezionati e incluso nel registro eventi. Selezionare questa opzione per gli eventi che verranno combinato con l'opzione di registro allarmi **No alarms (Nessun allarme)** oppure **Log alarm for selected controllers (Registra allarme per i dispositivi di controllo delle porte selezionati)**.

Nell'elenco **Configure event logging (Configura registrazione eventi)**, fare clic su **Select controllers (Seleziona dispositivi di controllo)** nella voce di registro degli eventi che si desidera abilitare. Viene visualizzata la finestra di dialogo **Device Specific Event Logging (Registrazione eventi specifici del dispositivo)**. In **Log event (Registra evento)**, selezionare i dispositivi di controllo delle porte che devono avere la registrazione degli allarmi abilitata e fare clic su **Save (Salva)**.

Opzioni registro allarmi

Per definire gli eventi che devono attivare un allarme, andare a **Setup > Configure Event and Alarm Logs (Impostazione > Configura registro allarmi ed eventi)**.

Sono disponibili le seguenti opzioni per l'attivazione e la registrazione degli allarmi:

- **No alarms (Nessun allarme)**: disattivare la registrazione degli allarmi. L'evento non attiverà nessun allarme oppure non verrà incluso in nessun registro allarmi.
- **Log alarm for all sources (Registra allarme per tutte le sorgenti)**: abilitare la registrazione degli allarmi per tutti i dispositivi di controllo delle porte. L'evento attiverà un allarme e verrà incluso nel registro allarmi.
- **Log alarm for selected sources (Registra allarme per le sorgenti selezionate)**: abilitare la registrazione degli allarmi nei dispositivi di controllo delle porte selezionati. L'evento attiverà un allarme e verrà incluso nel registro allarmi.

  Nell'elenco **Configure alarm logging (Configura registrazione allarmi)**, fare clic su **Select sources (Seleziona sorgenti)** nella voce di registro allarmi che si desidera abilitare. Viene aperta la finestra di dialogo **Device Specific Alarm Triggering (Attivazione allarmi specifica del dispositivo)**. In **Trigger alarm (Attiva allarme)**, selezionare i dispositivi di controllo delle porte che devono avere la registrazione degli allarmi abilitata e fare clic su **Save (Salva)**.

Modalità di impostazione delle regole di azione

Le pagine di eventi consentono di configurare il dispositivo Axis affinché esegua azioni quando si verificano eventi diversi. Ad esempio, il dispositivo può inviare una notifica e-mail o attivare una porta di output quando viene attivato un allarme. Il set di condizioni che definisce come e quando viene attivata l'azione è detto regola di azione. Se vengono definite più condizioni, devono essere tutte soddisfatte per attivare l'azione.

Per ulteriori informazioni sulle azioni e sui trigger disponibili, vedere *Trigger alla pagina 47* e *Azioni alla pagina 49*.

In questo esempio viene descritto come impostare una regola di azione per inviare una notifica e-mail quando viene attivato un allarme.

1. Configurare gli allarmi. Vedere *Configurazione dei registri eventi e allarmi alla pagina 45*.
2. Andare a **Setup > Additional Controller Configuration > Events > Action Rules (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Eventi > Regole di azione)** e fare clic su **Add (Aggiungi)**.
3. Selezionare **Enable rule (Abilita regola)** e immettere un nome descrittivo per la regola.
4. Selezionare **Event Logger (Registro eventi)** dall'elenco a discesa **Trigger (Trigger)**.
5. Facoltativamente, è possibile selezionare una **pianificazione** e **condizioni aggiuntive**. Vedere di seguito.
6. In **Actions (Azioni)** selezionare **Send Notification (Invia notifica)** dall'elenco a discesa **Type (Tipo)**.
7. Selezionare un destinatario e-mail dall'elenco a discesa. Vedere *Modalità di aggiunta di destinatari alla pagina 50*.

In questo esempio viene descritto come impostare una regola di azione per attivare una porta di output quando la porta è stata forzata.

1. Andare a **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Porte e dispositivi > Porte I/O**.
2. Selezionare **Output (Output)** dall'elenco a discesa **I/O Port Type (Tipo di porta I/O)** desiderato e immettere un **nome**.
3. Selezionare **Normal state (Stato normale)** per la porta I/O e fare clic su **Save (Salva)**.
4. Andare a **Events > Action Rules (Eventi > Regole di azione)** e fare clic su **Add (Aggiungi)**.

5. Selezionare **Door (Porta)** dall'elenco a discesa **Trigger (Trigger)**.
6. Selezionare **Door Alarm (Allarme porta)** dall'elenco a discesa.
7. Selezionare la porta desiderata dall'elenco a discesa.
8. Selezionare **DoorForcedOpen (DoorForcedOpen)** dall'elenco a discesa.
9. Facoltativamente, è possibile selezionare una **pianificazione** e **condizioni aggiuntive**. Vedere di seguito.
10. In **Actions (Azioni)** selezionare **Output Port (Porta di output)** dall'elenco a discesa **Type (Tipo)**.
11. Selezionare la porta di output desiderata dall'elenco a discesa **Port (Porta)**.
12. Impostare lo stato **Active (Attivo)**.
13. Selezionare **Duration (Durata)** e **Go to opposite state after (Andare allo stato opposto dopo)**. Quindi, immettere la durata desiderata dell'azione.
14. Fare clic su **OK**.

Per utilizzare più trigger per la regola di azione, selezionare **Additional conditions (Condizioni aggiuntive)** e fare clic su **Add (Aggiungi)** per aggiungere ulteriori trigger. Quando si utilizzano condizioni aggiuntive, tutte le condizioni devono essere soddisfatte per attivare l'azione.

Per impedire che un'azione venga attivata ripetutamente, è possibile impostare un intervallo di tempo nel campo **Wait at least (Attendi almeno)**. Immettere l'intervallo di tempo in ore, minuti e secondi, durante il quale il trigger deve essere ignorato prima che la regola di azione possa essere nuovamente attivata.

Per ulteriori informazioni, vedere la Guida integrata del dispositivo.

Trigger

I **trigger** e le **condizioni** delle regola di azione disponibili includono:

- **Access point**
  - **Access Point abilitato**: attiva una regola di azione quando viene configurato un dispositivo access point, quale un lettore o un dispositivo REX, ad esempio quando si completa la configurazione hardware o si aggiunge un tipo di identificazione.
- **Configurazione**
  - **Access point modificato**: attiva una regola di azione quando viene modificata la configurazione di un dispositivo access point quale un lettore o un dispositivo REX, ad esempio quando si configura l'hardware o si modifica un tipo di identificazione modificando le modalità di accesso a una porta.
  - **Access point rimosso**: attiva una regola di azione quando viene reimpostata la configurazione hardware di un dispositivo access point, quale un lettore o un dispositivo REX.
  - **Area modificata**: non supportata da questa versione di AXIS Entry Manager. Questa opzione deve essere configurata da un client, ad esempio un sistema di gestione degli accessi, tramite l'API (interfaccia per la programmazione di applicazioni) VAPIX® che supporta questa funzione e utilizza i dispositivi in grado di fornire i segnali necessari. Attiva la regola di azione quando un'area di accesso viene modificata.
  - **Area rimossa**: non supportata da questa versione di AXIS Entry Manager. Questa opzione deve essere configurata da un client, ad esempio un sistema di gestione degli accessi, tramite l'API (interfaccia per la programmazione di applicazioni) VAPIX® che supporta questa funzione e utilizza i dispositivi in grado di fornire i segnali necessari. Attiva la regola di azione quando un'area di accesso viene rimossa dal sistema.
  - **Porta modificata**: attiva una regola di azione quando vengono modificate le impostazioni di configurazione della porta, ad esempio il nome della porta, oppure quando viene aggiunta una porta al sistema. Questa opzione può essere utilizzata, ad esempio, per inviare una notifica quando una porta è installata e configurata.

- **Porta rimossa**: attiva una regola di azione quando una porta viene rimossa dal sistema. Questa opzione può essere utilizzata, ad esempio, per inviare una notifica quando una porta viene rimossa dal sistema.

- **Porta**
  - **Allarme batteria**: attiva una regola di azione quando una batteria wireless della porta è scarica e in esaurimento.
  - **Allarme porta**: attiva una regola di azione quando il monitor porte indica che la porta è stata forzata, è restata aperta troppo a lungo o non funziona correttamente. Questa opzione può essere utilizzata, ad esempio, per inviare una notifica quando qualcuno sta forzando un'entrata.
  - **Monitoraggio doppio blocco della porta**: attiva una regola di azione solo quando lo stato del blocco secondario diventa bloccato o sbloccato.
  - **Monitoraggio blocco della porta**: attiva una regola di azione solo quando lo stato del blocco normale diventa bloccato o sbloccato. Ad esempio, un malfunzionamento viene attivato quando il monitoraggio della porta rileva che la porta è aperta nonostante il blocco sia chiuso.
  - **Modalità porta**: attiva una regola di azione quando lo stato della porta cambia, ad esempio quando una porta viene oltrepassata o bloccata oppure quando è in modalità di blocco. Per ulteriori dettagli su queste modalità, vedere la Guida in linea.
  - **Monitoraggio porta**: attiva una regola di azione quando cambia lo stato del monitoraggio della porta. Questa opzione può essere utilizzata, ad esempio, per inviare una notifica quando un monitoraggio di una porta indica che la porta è aperta o chiusa.
  - **Manomissione porta**: attiva una regola di azione quando il monitoraggio della porta rileva che la connessione è stata interrotta, ad esempio quando qualcuno taglia i cavi del monitor della porta. Per usare questo trigger, accertarsi che **Enable supervised inputs (Abilita input supervisionati)** sia selezionato e i resistori terminali siano installati sulle relative porte di input del connettore della porta. Per ulteriori informazioni, vedere *Modalità di utilizzo degli input supervisionati alla pagina 17*.
  - **Avviso porta**: attiva una regola di azione prima che scatti l'allarme di porta aperta troppo a lungo. Utilizzare questo trigger, ad esempio, per inviare un segnale di avviso in modo che il dispositivo di controllo della porta invii un allarme reale, l'allarme di porta aperta troppo a lungo, se la porta non viene chiusa entro il tempo specificato dall'opzione di porta aperta troppo a lungo. Per ulteriori informazioni sull'opzione di porta aperta troppo a lungo, vedere *Modalità di configurazione di monitor porte e blocchi alla pagina 14*.
  - **Blocco chiuso**: attiva una regola di azione quando il blocco di una porta wireless è fisicamente chiuso.

- **Registro eventi**: tiene traccia di tutti gli eventi nel dispositivo di controllo della porta, ad esempio quando un utente passa una tessera o apre una porta. Se l'opzione **Eventi globali** è abilitata, il registro eventi tiene traccia di tutti gli eventi in ciascun dispositivo di controllo nel sistema. Per impostare gli allarmi e gli eventi che possono attivare una regola di azione, andare a **Impostazione > Configura registri allarmi ed eventi**. Il registro eventi viene condiviso dal sistema e può archiviare fino a 30.000 eventi. Al raggiungimento del limite, il registro eventi utilizza la regola FIFO (First In, First Out). Ciò significa che il primo evento registrato sarà il primo a essere sovrascritto.
  - **Allarme**: attiva una regola di azione quando uno degli allarmi specificati viene attivato. L'amministratore del sistema può configurare gli eventi più importanti rispetto agli altri e selezionare se un evento specificato deve attivare un allarme o meno.
  - **Allarmi eliminati**: attiva una regola di azione quando i nuovi record di allarme non possono essere scritti nei registri allarme, ad esempio quando si verificano così tanti allarmi simultaneamente che il registro eventi non riesce a tenere il passo. Quando un allarme viene eliminato, è possibile inviare una notifica all'operatore.
  - **Eventi eliminati**: attiva una regola di azione quando nuovi record di eventi non possono essere scritti nei registri eventi, ad esempio quando si verificano così tanti eventi simultaneamente che il registro eventi non riesce a tenere il passo. Quando un evento viene eliminato, è possibile inviare una notifica all'operatore.

- **Hardware**
  - **Rete**: attiva una regola di azione quando il collegamento di rete viene interrotto. Selezionare **Yes (Sì)** per attivare la regola di azione quando il collegamento di rete viene interrotto. Selezionare **No (No)** per attivare la regola di azione quando il collegamento di rete viene ripristinato. Selezionare **IPv4/v6 address removed**

(Indirizzo IPv4/v6 rimosso) oppure **New IPv4/v6 address (Nuovo indirizzo IPv4/v6)** per attivare un'azione quando cambia l'indirizzo IP.

- **Connessione peer-to-peer**: attiva una regola di azione quando il dispositivo Axis ha stabilito un collegamento a un altro dispositivo di controllo porta, se viene perso il collegamento di rete tra i dispositivi o se l'associazione dei dispositivi di controllo porta non è riuscita. Questa opzione può essere utilizzata, ad esempio per inviare una notifica in merito a un dispositivo di controllo porta che ha perso il collegamento di rete.

- **Segnale di input**
  - **Porta di input digitale**: attiva una regola di azione quando una porta I/O riceve un segnale da un dispositivo connesso. Vedere *Porte I/O alla pagina 62*.
  - **Attivazione manuale**: attiva una regola di azione quando l'attivazione manuale viene attivata. Questa opzione può essere utilizzata da un client, ad esempio un sistema di gestione degli accessi, tramite l'API (interfaccia per la programmazione di applicazioni) VAPIX® che avvia o arresta manualmente la regola di azione.
  - **Input virtuali**: attiva una regola di azione quando uno degli input virtuali cambia stato. Questo trigger può essere utilizzato da un client, ad esempio un sistema di gestione degli accessi, tramite l'API (interfaccia per la programmazione di applicazioni) VAPIX® che attiva le azioni. Gli input virtuali possono, ad esempio, essere connessi ai pulsanti dell'interfaccia utente del sistema di gestione.
- **Pianificazione**
  - **Intervallo**: attiva una regola di azione all'ora di inizio della pianificazione, che resta attiva fino al raggiungimento dell'ora di fine della pianificazione.
  - **Impulso**: attiva una regola di azione quando si verifica un evento singolo, ossia un evento che avviene in un dato momento e non presenta durata.
- **Sistema**
  - **Pronto all'uso**: attiva una regola di azione quando il sistema è pronto all'uso. Ad esempio, il dispositivo Axis è in grado di rilevare lo stato del sistema e inviare una notifica quando il sistema è stato avviato.

    Selezionare **Sì** per attivare la regola di azione quando il dispositivo si trova nello stato Pronto. La regola si attiverà solo quando tutti i servizi necessari, ad esempio un sistema di eventi, sono stati avviati.
- **Ora**
  - **Ricorrenza**: attiva una regola di azione monitorando le ricorrenze create. È possibile utilizzare questo trigger per avviare azioni ricorrenti, ad esempio l'invio di notifiche ogni ora. Selezionare un criterio di ricorrenza o crearne uno nuovo. Per ulteriori informazioni relative all'impostazione di un criterio di ricorrenza, vedere *Modalità di impostazione delle ricorrenze alla pagina 51*.
  - **Pianificazione di utilizzo**: attiva una regola di azione in base alla pianificazione selezionata. Vedere *Modalità di creazione delle pianificazioni alla pagina 51*.

Azioni

È possibile configurare varie azioni:

- **Porta di output**: attivare una porta I/O per controllare un dispositivo esterno.
- **Invia notifica**: inviare un messaggio di notifica a un destinatario.
- **LED di stato**: il LED di stato può essere impostato in modo da lampeggiare per la durata della regola di azione o per un determinato numero di secondi. Il LED di stato può essere utilizzato durante l'installazione e la configurazione per convalidare visivamente se le impostazioni dei trigger funzionano correttamente, ad esempio il trigger che segnala una porta aperta per troppo tempo. Per impostare il colore di lampeggiamento del LED di stato, selezionare **LED Color (Colore del LED)** dall'elenco a discesa.

Modalità di aggiunta di destinatari

Il dispositivo può inviare messaggi di notifica ai destinatari in relazione a eventi e allarmi. Ma prima che il dispositivo possa inviare messaggi di notifica, è necessario definire uno o più destinatari. Per informazioni sulle opzioni disponibili, vedere *Tipi di destinatari alla pagina 50*.

Per aggiungere un destinatario:

1. Andare a **Setup > Additional Controller Configuration > Events > Recipients (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Eventi > Destinatari)** e fare clic su **Add (Aggiungi)**.
2. Immettere un nome descrittivo.
3. Selezionare un **tipo** di destinatario.
4. Immettere le informazioni necessarie per il tipo di destinatario.
5. Fare clic su **Test (Test)** per verificare la connessione con il destinatario.
6. Fare clic su **OK**.

Tipi di destinatari

Sono disponibili i tipi di destinatari elencati di seguito:

HTTP

HTTPS

Email (E-mail)

TCP

Modalità di impostazione dei destinatari e-mail

I destinatari e-mail possono essere configurati selezionando uno dei provider e-mail elencati, o specificando il server SMTP, la porta e l'autenticazione utilizzati, ad esempio, da un server e-mail aziendale.

Nota

Alcuni provider e-mail hanno filtri di sicurezza che impediscono agli utenti di ricevere o visualizzare allegati di grandi dimensioni, ad esempio e-mail pianificate e simili. Controllare i criteri di sicurezza del provider e-mail per evitare problemi di consegna e account e-mail bloccati.

Per impostare un destinatario e-mail utilizzando uno dei provider elencati:

1. Andare a **Events > Recipients (Eventi > Destinatari)** e fare clic su **Add (Aggiungi)**.
2. Immettere un **nome** e selezionare **E-mail** dall'elenco **Type (Tipo)**.
3. Immettere gli indirizzi e-mail a cui inviare messaggi nel campo **To (A)**. Utilizzare la virgola per separare più indirizzi.
4. Selezionare il provider e-mail dall'elenco **Provider (Provider)**.
5. Immettere l'ID utente e la password per l'account e-mail.
6. Fare clic su **Test (Test)** per inviare un messaggio e-mail di testo.

Per impostare un destinatario e-mail, ad esempio un server e-mail aziendale, seguire le istruzioni indicate in precedenza, ma selezionare **User defined (Definito dall'utente)** come **Provider (Provider)**. Immettere l'indirizzo e-mail affinché venga visualizzato come mittente nel campo **From (Da)**. Selezionare **Advanced settings (Impostazioni avanzate)** e specificare l'indirizzo del server SMTP, la porta e il metodo di autenticazione. In alternativa, selezionare **Use encryption (Usa crittografia)** per inviare messaggi e-mail tramite una connessione crittografata. Il certificato server può essere convalidato utilizzando i certificati disponibili nel dispositivo Axis. Per informazioni su come caricare i certificati, vedere *Certificati alla pagina 55*.

Modalità di creazione delle pianificazioni

Le pianificazioni possono essere utilizzate come trigger della regola di azione o come condizioni aggiuntive. Utilizzare una delle pianificazioni predefinite o crearne una nuova come descritto di seguito.

Per creare una nuova pianificazione:

1. Andare a **Setup > Additional Controller Configuration > Events > Schedules (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Eventi > Pianificazioni)** e fare clic su **Add (Aggiungi)**.
2. Immettere un nome descrittivo e le informazioni necessarie per una pianificazione giornaliera, settimanale, mensile o annuale.
3. Fare clic su **OK**.

Per utilizzare la pianificazione in una regola di azione, selezionare la pianificazione dall'elenco a discesa **Schedule (Pianificazione)** nella pagina Impostazione della regola di azione.

Modalità di impostazione delle ricorrenze

Le ricorrenze sono utilizzate per attivare ripetutamente le regole di azione, ad esempio ogni 5 minuti o ogni ora.

Per impostare una ricorrenza:

1. Andare a **Setup > Additional Controller Configuration > Events > Recurrences (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Eventi > Ricorrenze)** e fare clic su **Add (Aggiungi)**.
2. Immettere un nome descrittivo e uno schema di ricorrenza.
3. Fare clic su **OK**.

Per utilizzare la ricorrenza in una regola di azione, selezionare prima **Time (Ora)** dall'elenco a discesa **Trigger (Trigger)** nella pagina Impostazione della regola di azione, quindi selezionare la ricorrenza dal secondo elenco a discesa.

Per modificare o rimuovere le ricorrenze, selezionare la ricorrenza in **Recurrences List (Elenco ricorrenze)** e fare clic su **Modify (Modifica)** o **Remove (Rimuovi)**.

Feedback del lettore

I lettori utilizzano LED e segnali acustici per inviare messaggi di feedback all'utente (la persona che accede o tenta di accedere alla porta). Il dispositivo di controllo porta può attivare un numero di messaggi di feedback, alcuni dei quali sono preconfigurati nel dispositivo di controllo porta e supportati dalla maggior parte dei lettori.

I lettori hanno diversi comportamenti LED, ma in genere utilizzano diverse sequenze di luci fisse e lampeggianti di colore rosso, verde e giallo.

I lettori, inoltre, possono utilizzare cicalini per inviare messaggi, utilizzando sequenze diverse di segnali acustici brevi e lunghi.

Nella tabella seguente sono mostrati gli eventi preconfigurati nel dispositivo di controllo porta per attivare un feedback del lettore e i segnali di feedback tipici del lettore. I segnali di feedback per i lettori AXIS vengono presentati nella Guida all'installazione fornita con il lettore AXIS.

Evento	LED doppio Wiegand	LED singolo Wiegand	OSDP	Schema segnale acustico	Stato
Idle (Inattivo)[1]	Spento	Rosso	Rosso	Invisibile	Normale
RequirePIN	Rosso/verde lampeggiante	Rosso/verde lampeggiante	Rosso/verde lampeggiante	Due segnali acustici brevi	PIN obbligatorio
AccessGranted	Verde	Verde	Verde	Segnale acustico	Accesso consentito
AccessDenied	Rosso	Rosso	Rosso	Segnale acustico	Accesso negato

1. Lo stato Inattivo viene attivato quando la porta è chiusa e il blocco è chiuso.

Messaggi di feedback diversi da quelli precedenti devono essere configurati da un client, ad esempio un sistema di gestione degli accessi, tramite l'API (interfaccia per la programmazione di applicazioni) VAPIX® che supporta questa funzione e utilizza i lettori in grado di fornire i segnali necessari. Per ulteriori informazioni, vedere le informazioni utente fornite dallo sviluppatore del sistema di gestione degli accessi e dal produttore del lettore.

Report

La pagina Report consente di visualizzare, stampare ed esportare report che contengono diversi tipi di informazioni relative al sistema. Per ulteriori informazioni sui report disponibili, vedere *Tipi di report alla pagina 53*.

Visualizzazione, stampa ed esportazione dei report

Per aprire la pagina Report, fare clic su **Reports (Report)**.

Per visualizzare un report, fare clic su **View and print (Visualizza e stampa)**.

Per stampare un report:

1. Fare clic su **View and print (Visualizza e stampa)**.
2. Selezionare le colonne che devono essere incluse nel report. Tutte le colonne sono selezionate per impostazione predefinita.
3. Se si desidera restringere lo scopo del report, immettere un filtro nel relativo campo del filtro. Ad esempio, è possibile filtrare gli utenti a seconda del gruppo a cui appartengono, le porte a seconda delle pianificazioni oppure i gruppi a seconda delle porte a cui hanno accesso.

   Per ottenere corrispondenze esatte, racchiudere il testo del filtro tra virgolette doppie, ad esempio "John".
4. Se si desidera ordinare le voci del report in un ordine diverso, fare clic su nella relativa colonna. Per passare dall'ordine standard a quello inverso, attivare i pulsanti di ordinamento.

   Mostra le voci nell'ordine standard (crescente).

   Mostra le voci nell'ordine inverso (discendente).
5. Fare clic su **Print selected columns (Stampa colonne selezionate)**.

Per esportare un report, fare clic su **Export CSV file (Esporta file CSV)**.

Il report viene esportato sotto forma di file con valori delimitati da virgole (CSV) e include tutte le colonne e le voci possibili per il tipo di report. Se non diversamente specificato, il file esportato (*.csv) viene salvato nella cartella di download predefinita. È possibile selezionare una cartella di download nelle impostazioni utente del browser Web.

Nota

Nei report vengono visualizzati solo gli utenti che dispongono di credenziali.

Tipi di report

Sono disponibili i tipi di report elencati di seguito:

- Pianificazioni di accesso. Per ulteriori informazioni sui tipi di pianificazione degli accessi e di opzioni, vedere *pagina 32* e *pagina 33*.
- Gruppi. Per ulteriori informazioni sulle credenziali del gruppo, vedere *pagina 34*.
- Porte. Per ulteriori informazioni sui tipi di porte e di identificazione, vedere *pagina 34* e *pagina 35*.
- Utenti. Per ulteriori informazioni sulle credenziali utente, vedere *pagina 40*.
- Dispositivi di controllo delle porte. Per ulteriori informazioni sui dispositivi di controllo collegati e i tipi di ID, vedere *pagina 27*. Per ulteriori informazioni sulle opzioni relative agli orari del monitor porte, vedere *pagina 16*.

Opzioni di sistema

Sicurezza

Utenti

Il controllo degli accessi utente è abilitato per impostazione predefinita e può essere configurato in **Setup > Additional Controller Configuration > System Options > Security > Users (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Sicurezza > Utenti)**. L'amministratore può impostare altri utenti fornendo loro nomi utente e password.

Nell'elenco degli utenti sono visualizzati i gruppi di utenti e gli utenti autorizzati (livelli di accesso):

- Gli **amministratori** hanno accesso illimitato a tutte le impostazioni. L'amministratore può aggiungere, modificare e rimuovere altri utenti.

Nota

Quando l'opzione **Encrypted & unencrypted (Crittografata e non crittografata)** è selezionata, il server Web codificherà la password. Questa è l'opzione predefinita per un'unità nuova o un'unità di cui sono state ripristinate le impostazioni predefinite di fabbrica.

In **HTTP/RTSP Password Settings (Impostazioni password HTTP/RTSP)**, selezionare il tipo di password da consentire. Potrebbe essere necessario consentire password non crittografate se sono disponibili client di visualizzazione che non supportano la crittografia, o se è stato aggiornato il firmware e i client esistenti supportano la crittografia, tuttavia devono accedere di nuovo ed essere configurati per utilizzare questa funzione.

ONVIF

ONVIF è un forum di settore aperto che fornisce e promuove interfacce standardizzate per un'interoperabilità efficace dei dispositivi di sicurezza fisica basati su IP.

Con la creazione di un utente, la comunicazione ONVIF viene abilitata automaticamente. Utilizzare il nome utente e la password in tutte le comunicazioni ONVIF con il dispositivo. Per ulteriori informazioni, vedere il sito Web *www.onvif.org*

Filtro indirizzi IP

Il filtro degli indirizzi IP è abilitato nella pagina **Setup > Additional Controller Configuration > System Options > Security > IP Address Filter (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Sicurezza > Filtro indirizzi IP)**. Una volta abilitato, all'indirizzo IP elencato viene consentito o rifiutato l'accesso al dispositivo Axis. Selezionare **Allow (Consenti)** o **Deny (Rifiuta)** dall'elenco e fare clic su **Apply (Applica)** per abilitare il filtro degli indirizzi IP.

L'amministratore può aggiungere fino a 256 voci di indirizzi IP all'elenco (una singola voce può contenere più indirizzi IP).

HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer o HTTP over SSL) è un protocollo Web che consente la navigazione crittografata. Il protocollo HTTPS può anche essere utilizzato da utenti e client per verificare che venga eseguito l'accesso al dispositivo corretto. Il livello di sicurezza fornito da HTTPS è considerato adeguato per la maggior parte degli scambi commerciali.

Il dispositivo Axis può essere configurato per richiedere ad HTTPS quando gli amministratori eseguono l'accesso.

Per utilizzare HTTPS, è necessario installare prima un certificato HTTPS. Andare a **Setup > Additional Controller Configuration > System Options > Security > Certificates (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Sicurezza > Certificati)** per installare e gestire certificati. Vedere *Certificati alla pagina 55*.

Per abilitare HTTPS nel dispositivo Axis:

1. Andare a **Setup > Additional Controller Configuration > System Options > Security > HTTPS (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Sicurezza > HTTPS)**

2. Selezionare un certificato HTTPS dall'elenco di certificati installati.
3. In alternativa, fare clic su **Ciphers (Crittografie)** e selezionare gli algoritmi di crittografia da utilizzare per SSL.
4. Impostare il **criterio di connessione HTTPS** per i diversi gruppi di utenti.
5. Fare clic su **Save (Salva)** per abilitare le impostazioni.

Per accedere al dispositivo Axis tramite il protocollo desiderato, nel campo degli indirizzi di un browser, immettere `https://` per il protocollo HTTPS e `http://` per il protocollo HTTP.

La porta HTTPS può essere modificata nella pagina **System Options > Network > TCP/IP > Advanced (Opzioni di sistema > Rete > TCP/IP > Avanzate)**.

IEEE 802.1X

IEEE 802.1X è uno standard per il controllo di ammissione alla rete in base alla porta che fornisce un'autenticazione sicura di dispositivi di rete cablati e wireless. IEEE 802.1X è basato su EAP (Extensible Authentication Protocol).

Per accedere a una rete protetta da IEEE 802.1 X, è necessario autenticare i dispositivi. L'autenticazione viene eseguita da un server di autenticazione, generalmente un **server RADIUS**, di cui FreeRADIUS e Microsoft Internet Authentication Service sono un esempio.

Nell'implementazione di Axis, il dispositivo Axis e il server di autenticazione si identificano con certificati digitali mediante EAP-TLS (Extensible Authentication Protocol - Transport Layer Security). I certificati sono forniti da un'**autorità di certificazione** (CA).
È necessario:

- un certificato CA per autenticare il server di autenticazione.
- Un certificato client firmato dalla CA per autenticare il dispositivo Axis.

Per creare e installare certificati, andare a **Setup > Additional Controller Configuration > System Options > Security > Certificates (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Sicurezza > Certificati)**. Vedere *Certificati alla pagina 55*.

Per consentire al dispositivo di accedere a una rete protetta da IEEE 802.1 X:

1. Andare a **Setup > Additional Controller Configuration > System Options > Security > IEEE 802.1X (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Sicurezza > IEEE 802.1X)**.
2. Selezionare un **certificato CA** e un **certificato client** dagli elenchi dei certificati installati.
3. In **Settings (Impostazioni)**, selezionare la versione EAPOL e fornire l'identità EAP associata al certificato client.
4. Selezionare la casella per abilitare IEEE 802.1 X e fare clic su **Save (Salva)**.

Nota

Per un corretto funzionamento dell'autenticazione, le impostazioni della data e dell'ora nel dispositivo Axis devono essere sincronizzate con un server NTP. Vedere *Data e ora alla pagina 56*.

Certificati

I certificati sono utilizzati per autenticare i dispositivi in una rete. Le applicazioni tipiche includono la navigazione Web crittografata (HTTPS), la protezione di rete tramite IEEE 802.1 X e i messaggi di notifica, ad esempio tramite e-mail. Con il dispositivo Axis possono essere utilizzati due tipi di certificati:

Certificati server e client – Per autenticare il dispositivo Axis. Un certificato **Server/Client** può essere autofirmato o rilasciato da un'autorità di certificazione (CA). Un certificato autofirmato offre una protezione limitata e può essere utilizzato prima che sia stato ottenuto un certificato emesso da un'autorità di certificazione.

Certificati CA – Per autenticare certificati peer, ad esempio il certificato di un server di autenticazione nel caso in cui il dispositivo Axis sia collegato a una rete protetta da IEEE 802.1X. Un dispositivo Axis dispone di diversi certificati CA preinstallati.

Nota

- Se il dispositivo viene ripristinato ai valori predefiniti di fabbrica, tutti i certificati, ad eccezione dei certificati CA preinstallati, verranno cancellati.
- Se il dispositivo viene ripristinato ai valori predefiniti di fabbrica, tutti i certificati CA preinstallati che sono stati eliminati verranno reinstallati.

Modalità di creazione di un certificato autofirmato

1. Andare a **Setup > Additional Controller Configuration > System Options > Security > Certificates (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Sicurezza > Certificati)**.
2. Fare clic su **Create self-signed certificate (Crea certificato autofirmato)** e fornire le informazioni richieste.

Modalità di creazione e installazione di un certificato firmato dalla CA

1. Per la creazione di un certificato autofirmato, vedere .
2. Andare a **Setup > Additional Controller Configuration > System Options > Security > Certificates (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Sicurezza > Certificati)**.
3. Fare clic su **Create certificate signing request (Crea richiesta di firma del certificato)** e fornire le informazioni necessarie.
4. Copiare la richiesta formattata PEM e inviarla alla CA scelta.
5. Quando il certificato firmato viene restituito, fare clic su **Install certificate (Installazione certificato)** e caricare il certificato.

Modalità di installazione dei certificati CA

1. Andare a **Setup > Additional Controller Configuration > System Options > Security > Certificates (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Sicurezza > Certificati)**.
2. Fare clic su **Install certificate (Installa certificato)** e caricare il certificato.

Data e ora

Le impostazioni di data e ora del dispositivo Axis sono configurate in **Setup > Additional Controller Configuration > System Options > Date & Time (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Data e ora)**.

Ora server corrente mostra la data e l'ora correnti (formato di 24 ore).

Per modificare le impostazioni di data e ora, selezionare l'opzione **Time mode (Modalità ora)** preferita in **New Server Time (Nuova ora server)**:

- **Sincronizza con l'ora del computer server**: imposta data e ora in base all'orologio del computer. Con questa opzione data e ora vengono impostate una sola volta e non verranno aggiornate automaticamente.
- **Sincronizza con server NTP**: ottiene data e ora da un server NTP. Con questa opzione, le impostazioni di data e ora vengono aggiornate continuamente. Per informazioni sulle impostazioni NTP, vedere *Configurazione NTP alla pagina 59*.

  Se si utilizza un nome host per il server NTP, deve essere configurato un server DNS. Vedere *Configurazione DNS alla pagina 59*.
- **Imposta manualmente**: consente di impostare manualmente la data e l'ora.

Se si utilizza un server NTP, selezionare il **fuso orario** dall'elenco a discesa. Se richiesto, selezionare **Automatically adjust for daylight saving time changes (Passa automaticamente all'ora legale)**.

Rete

Impostazioni TCP/IP di base

Il dispositivo Axis supporta IP versione 4 (IPv4).

Il dispositivo Axis può ottenere un indirizzo IPv4 nei seguenti modi:

- **Indirizzo IP dinamico:Obtain IP address via DHCP (Ottieni indirizzo IP tramite DHCP)** è selezionato per impostazione predefinita. Ciò significa che il dispositivo Axis è impostato per ottenere l'indirizzo IP automaticamente tramite il protocollo DHCP (Dynamic Host Configuration Protocol).

  DHCP consente agli amministratori di rete di gestire e automatizzare l'assegnazione degli indirizzi IP centralmente.

- **Indirizzo IP statico**: per utilizzare un indirizzo IP statico, selezionare **Use the following IP address (Usa il seguente indirizzo IP)** e specificare l'indirizzo IP, la subnet mask e il router predefinito. Quindi fare clic su **Save (Salva)**.

DHCP deve essere abilitato solo se si utilizza una notifica per l'indirizzo IP dinamica oppure se il protocollo DHCP è in grado di aggiornare un server DNS che permette di accedere al dispositivo Axis tramite il nome (nome host).

Se il protocollo DHCP è abilitato e il dispositivo non è accessibile, eseguire AXIS IP Utility affinché cerchi i dispositivi Axis collegati in rete oppure ripristinare le impostazioni predefinite di fabbrica del dispositivo, quindi eseguire nuovamente l'installazione. Per informazioni su come ripristinare i valori predefiniti di fabbrica, vedere *pagina 64*.

ARP/Ping

È possibile assegnare l'indirizzo IP del dispositivo tramite ARP e Ping. Per le istruzioni, vedere *Assegnazione di un indirizzo IP tramite ARP/Ping alla pagina 57*.

Il servizio ARP/Ping è abilitato per impostazione predefinita, ma viene disabilitato automaticamente due minuti dopo l'avvio del dispositivo o dopo l'assegnazione di un indirizzo IP. Per riassegnare l'indirizzo IP tramite ARP/Ping, è necessario riavviare il dispositivo per abilitare ARP/Ping per altri due minuti.

Per disabilitare il servizio, andare a **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > TCP/IP > Base)** e deselezionare l'opzione **Enable ARP/Ping setting of IP address (Abilita impostazione ARP/Ping dell'indirizzo IP)**.

Il ping del dispositivo è ancora possibile quando il servizio è disabilitato.

Assegnazione di un indirizzo IP tramite ARP/Ping

È possibile assegnare l'indirizzo IP del dispositivo tramite ARP/Ping. È necessario inviare il comando entro 2 minuti dal collegamento all'alimentazione.

1. Acquisire un indirizzo IP statico libero sullo stesso segmento di rete del computer.
2. Individuare il numero di serie indicato sull'etichetta del dispositivo.
3. Aprire il prompt dei comandi e digitare i seguenti comandi:

   Sintassi Linux/Unix

   ```
   arp -s <indirizzo IP> <numero di serie> temp
   ping -s 408 <indirizzo IP>
   ```

   Esempio Linux/Unix

   ```
   arp -s 192.168.0.125 00:40:8c:18:10:00 temp
   ping -s 408 192.168.0.125
   ```

   Sintassi Windows (può richiedere l'esecuzione della finestra MS-DOS come amministratore)

   ```
   arp -s <indirizzo IP> <numero di serie>
   ```

```
ping -l 408 -t <indirizzo IP>
```

Esempio Windows (può richiedere l'esecuzione della finestra MS-DOS come amministratore)

```
arp -s 192.168.0.125 00-40-8c-18-10-00
ping -l 408 -t 192.168.0.125
```

4. Riavviare il dispositivo scollegando e ricollegando il connettore di rete.
5. Chiudere il prompt dei comandi appena viene visualizzato il messaggio `Reply from 192.168.0.125:...` o un messaggio simile.
6. Aprire un browser e digitare `http://<IP address>` nel campo dell'indirizzo.

Per altri metodi di assegnazione dell'indirizzo IP, vedere *Modalità di assegnazione di un indirizzo IP e accesso al dispositivo* all'indirizzo *www.axis.com/support*

Nota

- Per aprire un prompt dei comandi in Windows, aprire il menu **Start (Start)** e cercare `cmd`.
- Per usare il comando ARP in Windows 8/Windows 7/Windows Vista, fare clic con il pulsante destro del mouse sull'icona del prompt dei comandi e selezionare **Run as administrator (Esegui come amministratore)**.
- Per aprire un prompt dei comandi in Mac OS X, aprire l'**Terminal utility (utility Terminal)** in **Application > Utilities (Applicazione > Utilità)**.

AXIS Video Hosting System (AVHS)

AVHS, utilizzato in combinazione con un servizio AVHS, offre un accesso Internet facile e sicuro alla gestione e a registri del dispositivo di controllo accessibili da qualsiasi ubicazione. Per ulteriori informazioni su come trovare un fornitore di servizi AVHS locale, vedere la pagina www.axis.com/hosting

Le impostazioni di AVHS sono configurate in **Setup > Additional Controller Configuration > System Options > Network > TCP IP > Basic (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > TCP IP > Base)**. La possibilità di connettersi a un servizio AVHS è abilitata per impostazione predefinita. Per disabilitarla, deselezionare la casella **Enable AVHS (Abilita AVHS)**.

One-click enabled (Abilitazione con un clic) – Premere e tenere premuto il pulsante di comando del dispositivo (vedere *Panoramica del dispositivo alla pagina 3*) per circa 3 secondi per connettersi a un servizio AVHS via Internet. Una volta eseguita la registrazione, **Always (Sempre)** sarà abilitato e il dispositivo Axis rimarrà collegato al servizio AVHS. Se il dispositivo non viene registrato entro 24 dalla pressione del pulsante, il dispositivo si disconnetterà dal servizio AVHS.

Always (Sempre) – Il dispositivo Axis tenterà costantemente di connettersi al servizio AVHS via Internet. Una volta registrato, il dispositivo rimarrà connesso al servizio. Questa opzione può essere utilizzata quando il dispositivo è già installato e non è comodo o possibile utilizzare l'installazione con un clic.

Nota

Il supporto di AVHS dipende dalla disponibilità di sottoscrizioni dai fornitori di servizi.

AXIS Internet Dynamic DNS Service

AXIS Internet Dynamic DNS Service assegna un nome host per semplificare l'accesso al dispositivo. Per ulteriori informazioni, vedere la pagina *www.axiscam.net*

Per registrare il dispositivo Axis con AXIS Internet Dynamic DNS Service, andare a **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > TCP/IP > Base)**. In **Services (Servizi)** fare clic sul pulsante **Settings (Impostazioni)** di AXIS Internet Dynamic DNS Service (richiede l'accesso a Internet). Il nome di dominio attualmente registrato in AXIS Internet Dynamic DNS Service per il dispositivo può essere rimosso in qualsiasi momento.

Nota

AXIS Internet Dynamic DNS Service richiede IPv4.

Impostazioni TCP/IP avanzate

Configurazione DNS

DNS (Domain Name Service) fornisce la conversione di nomi host in indirizzi IP. Le impostazioni DNS sono configurate in **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > TCP/IP > Avanzate)**.

Selezionare **Obtain DNS server address via DHCP (Ottieni indirizzo server DNS tramite DHCP)** per utilizzare le impostazioni DNS fornite dal server DHCP.

Per effettuare impostazioni manuali, selezionare **Use the following DNS server address (Usa il seguente indirizzo server DNS)** e specificare quanto segue:

Nome dominio – Immettere i domini per la ricerca del nome host utilizzato dal dispositivo Axis. I diversi domini possono essere separati da punto e virgola. Il nome host è sempre la prima parte di un nome di dominio completo, ad esempio, `myserver` è il nome host del nome di dominio completo `myserver.mycompany.com` dove `mycompany.com` è il nome di dominio.

Server DNS primario/secondario – Immettere gli indirizzi IP dei server DNS principale e secondario. Il server DNS secondario è facoltativo e verrà utilizzato se il primario non è disponibile.

Configurazione NTP

Il protocollo NTP (Network Time Protocol) è utilizzato per sincronizzare gli orari degli orologi dei dispositivi in una rete. Le impostazioni NTP sono configurate in **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > TCP/IP > Avanzate)**.

Selezionare **Obtain NTP server address via DHCP (Ottieni indirizzo server NTP tramite DHCP)** per utilizzare le impostazioni NTP fornite dal server DHCP.

Per effettuare impostazioni manuali, selezionare **Use the following NTP server address (Usa il seguente indirizzo server NTP)** e immettere il nome host o l'indirizzo IP del server NTP.

Configurazione del nome host

È possibile accedere al dispositivo Axis utilizzando un nome host anziché un indirizzo IP. Il nome host corrisponde in genere al nome DNS assegnato. Il nome host è configurato in **Setup > Additional Controller Configuration> System Options > Network > TCP/IP > Advanced (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > TCP/IP > Avanzate)**.

Selezionare **Obtain host name via IPv4 DHCP (Ottieni nome host tramite IPv4 DHCP)** per utilizzare il nome host fornito dal server DHCP in esecuzione su IPv4.

Selezionare **Use the host name (Usa il nome host)** per impostare manualmente il nome host.

Selezionare **Enable dynamic DNS updates (Abilita aggiornamenti DNS dinamici)** per aggiornare in modo dinamico i server DNS locali ogni volta che cambia l'indirizzo IP del dispositivo Axis. Per ulteriori informazioni, vedere la Guida in linea.

Indirizzo IPv4 di collegamento locale

L'opzione **Link-Local Address (Indirizzo di collegamento locale)** è abilitata per impostazione predefinita e assegna al dispositivo Axis un indirizzo IP aggiuntivo che può essere utilizzato per accedere al dispositivo da altri host sullo stesso segmento della rete locale. Il dispositivo può avere un indirizzo IP di collegamento locale e un indirizzo IP statico o DHCP allo stesso tempo.

La funzione può essere disabilitata in **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > TCP/IP > Avanzate)**.

HTTP

La porta HTTP utilizzata dal dispositivo Axis può essere modificata in **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema >**

Rete > TCP/IP > Avanzate). Oltre all'impostazione predefinita, ovvero 80, è possibile utilizzare qualsiasi porta nell'intervallo compreso tra 1024 e 65535.

HTTPS

La porta HTTPS utilizzata dal dispositivo Axis può essere modificata in **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > TCP/IP > Avanzate)**. Oltre all'impostazione predefinita, ovvero 443, è possibile utilizzare qualsiasi porta nell'intervallo compreso tra 1024 e 65535.

Per abilitare HTTPS, andare a **Setup > Additional Controller Configuration > System Options > Security > HTTPS (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Sicurezza > HTTPS)**. Per ulteriori informazioni, vedere *HTTPS alla pagina 54*.

NAT traversal (mappatura delle porte) per IPv4

Un router di rete consente ai dispositivi su una rete privata (LAN) di condividere una singola connessione a Internet. Questo avviene inoltrando il traffico di rete da una rete privata "all'esterno", ovvero, a Internet. La sicurezza della rete privata (LAN) è aumentata poiché la maggior parte dei router è preconfigurata per bloccare i tentativi di accesso alla rete privata (LAN) dalla rete pubblica (Internet).

Utilizzare **NAT traversal** quando il dispositivo Axis si trova su una intranet (LAN) e si desidera renderlo disponibile dall'altro lato (WAN) di un router NAT. Se la funzione è correttamente configurata, tutto il traffico HTTP a una porta HTTP esterna nel router NAT viene inoltrato al dispositivo.

La funzione NAT traversal viene configurata in **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > TCP/IP > Avanzate)**.

Nota

- Affinché possa essere utilizzata correttamente, la funzionalità NAT traversal deve essere supportata dal router. Il router inoltre deve supportare UPnP®.
- In questo contesto, il termine "router" fa riferimento a qualsiasi dispositivo di routing di rete come un router NAT, un router di rete, un gateway Internet, un router a banda larga, un dispositivo di condivisione a banda larga o un software, ad esempio un firewall.

Abilitazione/Disabilitazione – Una volta abilitato, il dispositivo Axis tenta di configurare la mappatura delle porte in un router NAT sulla rete, utilizzando UPnP. UPnP deve essere abilitato nel dispositivo (vedere **Setup > Additional Controller Configuration > System Options > Network > UPnP (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > UPnP)**).

Utilizzo di un router NAT selezionato manualmente – Selezionare questa opzione per selezionare un router NAT manualmente e immettere l'indirizzo IP del router nel campo. Se non viene specificato alcun router, il dispositivo cerca automaticamente i router NAT sulla rete in uso. Se vengono individuati più router, viene selezionato il router predefinito.

Porta HTTP alternativa – Selezionare questa opzione per definire manualmente una porta HTTP esterna. Immettere una porta nell'intervallo compreso tra 1024 e 65535. Se il campo della porta è vuoto o contiene l'impostazione predefinita, che è 0, viene selezionato automaticamente un numero di porta quando si abilita NAT trasversal.

Nota

- Una porta HTTP alternativa può essere utilizzata o essere attiva anche se la funzionalità NAT trasversal è disabilitata. Questo è utile se il router NAT non supporta UPnP ed è necessario configurare manualmente il port forwarding nel router NAT.
- Se si tenta di inserire manualmente una porta che è già in uso, viene selezionata automaticamente un'altra porta disponibile.
- Quando la porta è selezionata automaticamente, viene visualizzata in questo campo. Per modificarla, immettere un nuovo numero di porta e fare clic su **Save (Salva)**.

FTP

Il server FTP in esecuzione nel dispositivo Axis consente il caricamento del nuovo firmware, delle applicazioni utente, ecc. Il server FTP può essere disabilitato in **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > TCP/IP > Avanzate)**.

RTSP

Il server RTSP in esecuzione nel dispositivo Axis consente a un client di connessione di avviare un flusso di eventi. Il numero di porta RTSP può essere modificato in **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > TCP/IP > Avanzate)**. La porta predefinita è 554.

Nota

I flussi di eventi non saranno disponibili se il server RTSP è disabilitato.

SOCKS

SOCKS è un protocollo di rete proxy. Il dispositivo Axis può essere configurato per l'utilizzo di un server SOCKS per raggiungere le reti sull'altro lato di un firewall o di un server proxy. Questa funzione è utile se il dispositivo Axis si trova su una rete locale dietro un firewall e le notifiche, i caricamenti, gli allarmi e così via devono essere inviati a una destinazione al di fuori della rete locale (ad esempio Internet).

SOCKS è configurato in **Setup > Additional Controller Configuration > System Options > Network > SOCKS (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > SOCKS)**. Per ulteriori informazioni, vedere la Guida in linea.

QoS (Qualità del servizio) (Quality of Service)

QoS (Qualità del servizio) (Quality of Service) garantisce un determinato livello di una risorsa specificata al traffico selezionato su una rete. Una rete QoS dà priorità al traffico di rete e offre una maggiore affidabilità della rete, controllando la quantità di larghezza di banda che un'applicazione può utilizzare.

Le impostazioni di QoS sono configurate in **Setup > Additional Controller Configuration > System Options > Network > QoS (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > QoS)**. Utilizzando i valori DSCP (Differentiated Services Codepoint), il dispositivo Axis può contrassegnare il traffico di evento/allarme e il traffico di gestione.

SNMP

SNMP (Simple Network Management Protocol) consente il monitoraggio e la gestione in remoto dei dispositivi di rete. Una comunità SNMP è il gruppo formato dai dispositivi e dalla stazione di gestione che eseguono SNMP. I nomi delle comunità sono utilizzati per identificare i gruppi.

Per abilitare e configurare SNMP nel dispositivo Axis, andare alla pagina **Setup > Additional Controller Configuration > System Options > Network > SNMP (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > SNMP)**.

A seconda del livello di sicurezza necessario, selezionare la versione da utilizzare su SNMP.

I trap sono utilizzati dal dispositivo Axis per inviare messaggi a un sistema di gestione in merito a modifiche dello stato ed eventi importanti. Selezionare **Enable traps (Abilita trap)** e immettere l'indirizzo IP a cui deve essere inviato il messaggio trap e la **comunità trap** che deve ricevere il messaggio.

Nota

Se HTTPS è abilitato, SNMP v1 e SNMP v2c devono essere disabilitati.

I **trap per SNMP v1/v2** sono utilizzati dal dispositivo Axis per inviare messaggi a un sistema di gestione in merito a modifiche dello stato ed eventi importanti. Selezionare **Enable traps (Abilita trap)** e immettere l'indirizzo IP a cui deve essere inviato il messaggio trap e la **comunità trap** che deve ricevere il messaggio.

Sono disponibili i seguenti trap:

- Avvio a freddo
- Avvio a caldo
- Link up
- Autenticazione non riuscita

SNMP v3 offre crittografia e password sicure. Per utilizzare i trap con SNMP v3, è necessaria un'applicazione di gestione SNMP v3.

Per utilizzare SNMP v3, è necessario che il protocollo HTTPS sia abilitato. A tale scopo, vedere *HTTPS alla pagina 54*. Per abilitare SNMP v3, selezionare la casella e fornire la password iniziale dell'utente.

Nota

La password iniziale può essere impostata solo una volta. Se si smarrisce la password, è necessario ripristinare le impostazioni predefinite di fabbrica del dispositivo. A tale scopo, vedere *Ripristino delle impostazioni predefinite di fabbrica alla pagina 64*.

UPnP

Il dispositivo Axis include il supporto per UPnP®. UPnP è abilitato per impostazione predefinita e il dispositivo viene automaticamente rilevato dai sistemi operativi e dai client che supportano questo protocollo.

UPnP può essere disabilitato in **Setup > Additional Controller Configuration > System Options > Network > UPnP (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > UPnP)**.

Bonjour

Il dispositivo Axis include il supporto per Bonjour. Bonjour è abilitato per impostazione predefinita e il dispositivo viene automaticamente rilevato dai sistemi operativi e dai client che supportano questo protocollo.

Bonjour può essere disabilitato in **Setup > Additional Controller Configuration > System Options > Network > Bonjour (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > Bonjour)**.

Porte e dispositivi

Porte I/O

Il connettore ausiliario sul dispositivo Axis offre due porte di input e output configurabili per il collegamento di dispositivi esterni. Per informazioni su come collegare dispositivi esterni, vedere la Guida all'installazione, disponibile all'indirizzo *www.axis.com*

Le porte I/O sono configurate in **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Porte e dispositivi > Porte I/O)**. Selezionare la direzione della porta (**Input (Input)** o **Output (Output)**). Alle porte possono essere assegnati nomi descrittivi e i loro **stati normali** possono essere configurati come **Open circuit (Circuito aperto)** o **Grounded circuit (Circuito a terra)**.

Stato delle porte

L'elenco nella pagina **System Options > Ports & Devices > Port Status (Opzioni di sistema > Porte e dispositivi > Stato porta)** mostra lo stato delle porte di input e output del dispositivo.

Manutenzione

Il dispositivo Axis offre diverse funzioni di manutenzione. Queste sono disponibili in **Setup > Additional Controller Configuration > System Options > Maintenance (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Manutenzione)**.

Fare clic su **Restart (Riavvio)** per eseguire un riavvio corretto se il dispositivo Axis non funziona nel modo previsto. Questa operazione non avrà alcun effetto sulle impostazioni correnti.

Nota

Un riavvio cancella tutte le voci nel report del server.

Fare clic su **Restore (Ripristino)** per ripristinare le impostazioni predefinite di fabbrica. Le seguenti impostazioni non vengono modificate:

- il protocollo di avvio (DHCP o statico)
- l'indirizzo IP statico
- il router predefinito
- la subnet mask
- l'ora di sistema
- le impostazioni 802.1X IEEE

Fare clic su **Default (Predefinito)** per ripristinare tutte le impostazioni predefinite di fabbrica, incluso l'indirizzo IP. Questo pulsante deve essere utilizzato con cautela. I valori predefiniti di fabbrica del dispositivo Axis possono essere ripristinati anche utilizzando il pulsante di comando. A tale scopo, vedere *Ripristino delle impostazioni predefinite di fabbrica alla pagina 64*.

Per informazioni sull'aggiornamento del firmware, vedere *Modalità di aggiornamento del firmware alla pagina 66*.

Backup dei dati dell'applicazione

Andare a **Setup > Create a backup (Configurazione > Crea un backup)** per creare un backup dei dati dell'applicazione. I dati sottoposti a backup includono utenti, credenziali, gruppi e pianificazioni. Quando si crea un backup, un file contenente i dati viene salvato localmente sul computer.

Andare a **Setup > Upload a backup (Configurazione > Caricare un backup)** per utilizzare un file di backup creato in precedenza per ripristinare i dati dell'applicazione. Prima di poter caricare il file di backup, è necessario ripristinare le impostazioni predefinite di fabbrica del dispositivo. Per le istruzioni, vedere *Ripristino delle impostazioni predefinite di fabbrica alla pagina 64*.

Supporto

Panoramica supporto

La pagina **Setup > Additional Controller Configuration > System Options > Support > Support Overview (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Supporto > Panoramica supporto)** fornisce informazioni sulla risoluzione dei problemi e informazioni di contatto, nel caso in cui sia necessaria assistenza tecnica.

Vedere anche *Risoluzione di problemi alla pagina 66*.

Panoramica del sistema

Per ottenere una panoramica delle impostazioni e dello stato del dispositivo Axis, andare a **Setup > Additional Controller Configuration > System Options > Support > System Overview (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Supporto > Panoramica di sistema)**. Le informazioni che possono essere reperite qui includono la versione del firmware, l'indirizzo IP, le impostazioni di rete e di sicurezza, le impostazioni di eventi e le recenti voci di registro.

Registri e report

La pagina **Setup > Additional Controller Configuration > System Options > Support > Logs & Reports (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Supporto > Registri e report)** genera registri e report utili per l'analisi del sistema e per la risoluzione di problemi. Qualora si contatti l'assistenza Axis, fornire un report del server insieme alla richiesta.

Registro di sistema – Fornisce informazioni sugli eventi di sistema.

Registro degli accessi – Elenca tutti i tentativi non riusciti di accesso al dispositivo. Il registro degli accessi può inoltre essere configurato per elencare tutte le connessioni al dispositivo (vedere di seguito).

Visualizza report del server – Fornisce informazioni sullo stato del dispositivo in una finestra pop-up. Il registro degli accessi viene automaticamente incluso nel report del server.

Scarica report del server – Crea un file .zip contenente un file di testo del report del server completo in formato UTF-8. Selezionare l'opzione **Include snapshot from Live View (Includi istantanea da visualizzazione in diretta)** per includere un'istantanea della visualizzazione in diretta del dispositivo. Il file .zip deve essere sempre incluso quando si contatta l'assistenza.

Elenco dei parametri – Mostra i parametri del dispositivo e le relative impostazioni correnti. Potrebbe rivelarsi utile nella risoluzione di problemi o quando si contatta l'assistenza Axis.

Elenco delle connessioni – Elenca tutti i client che accedono correntemente ai flussi multimediali.

Report di arresto anomalo – Genera un archivio con le informazioni sul debug. La creazione del report dura alcuni minuti.

I livelli dei registri per i registri di sistema e degli accessi vengono impostati in **Setup > Additional Controller Configuration > System Options > Support > Logs & Reports > Configuration (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Supporto > Registri e report > Configurazione)**. Il registro degli accessi può essere configurato affinché elenchi tutti i collegamenti al dispositivo (selezionare Critical (Critico), Warnings & Info (Avvisi e informazioni)).

Avanzate

Scripting

Scripting consente agli utenti esperti di personalizzare e utilizzare i propri script.

AVVISO

L'utilizzo non corretto può causare un comportamento imprevisto e perdita di contatto con il dispositivo Axis.

Axis consiglia vivamente di non utilizzare questa funzione a meno che non se ne conoscano le conseguenze. L'assistenza Axis non fornisce supporto per problemi relativi a script personalizzati.

Per aprire l'editor di script, andare a **Setup > Additional Controller Configuration > System Options > Advanced > Scripting (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Avanzate > Scripting)**. Se uno script crea problemi, ripristinare le impostazioni predefinite di fabbrica del dispositivo. A tale scopo, vedere *pagina 64*.

Per ulteriori informazioni, vedere *www.axis.com/developer*.

Caricamento di file

I file, ad esempio le pagine Web e le immagini, possono essere caricati nel dispositivo Axis e utilizzati come impostazioni personalizzate. Per caricare un file, andare a **Setup > Additional Controller Configuration > System Options > Advanced > File Upload (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Avanzate > Caricamento file)**.

I file caricati sono accessibili tramite `http://<ip address>/local/<user>/<file name>` dove `<user>` è il gruppo di utenti selezionati (amministratore) per il file caricato.

Ripristino delle impostazioni predefinite di fabbrica

Importante

Il ripristino dei valori predefiniti di fabbrica deve essere effettuato con cautela. Tale operazione consentirà di ripristinare i valori predefiniti di fabbrica per tutte le impostazioni, incluso l'indirizzo IP.

Per ripristinare il dispositivo ai valori predefiniti di fabbrica:

1. Scollegare l'alimentazione dal dispositivo.

2. Tenere premuto il pulsante di comando quando si ricollega l'alimentazione. Vedere *Panoramica del dispositivo alla pagina 3* .
3. Tenere premuto il pulsante di comando per 25 secondi finché l'indicatore LED di stato non emette nuovamente una luce gialla.
4. Rilasciare il pulsante di comando. Il processo è completo quando il LED di stato diventerà verde. Il dispositivo è stato reimpostato alle impostazioni di fabbrica predefinite. Se nessun server DHCP è disponibile sulla rete, l'indirizzo IP predefinito è `192.168.0.90`.
5. Utilizzare gli strumenti per l'installazione e la gestione del software per assegnare un indirizzo IP, impostare la password e accedere al dispositivo.

È anche possibile reimpostare i valori predefiniti di fabbrica dei parametri mediante l'interfaccia Web. Andare in **Setup > Additional Controller Configuration > Setup > System Options > Maintenance (Configurazione > Configurazione dispositivo di controllo aggiuntivo > Configurazione > Opzioni di sistema > Manutenzione)** e fare clic su **Default (Predefinito)**.

Risoluzione di problemi

Modalità di controllo del firmware corrente

Il firmware è il software che determina la funzionalità dei dispositivi di rete. Una delle prime azioni quando si risolve un problema deve essere la verifica della versione firmware corrente. La versione più recente può contenere una correzione che risolve il particolare problema.

La versione del firmware corrente nel dispositivo Axis è visualizzata nella pagina Panoramica.

Modalità di aggiornamento del firmware

Importante

- Il rivenditore si riserva il diritto di addebitare eventuali riparazioni attribuibili ad aggiornamenti errati dell'utente.
- Le impostazioni preconfigurate e personalizzate vengono salvate quando il firmware viene aggiornato, a condizione che le funzionalità siano disponibili nel nuovo firmware, sebbene non sia garantito da Axis Communications AB.
- Se si installa una versione del firmware precedente, è necessario ripristinare le impostazioni predefinite di fabbrica del dispositivo in un secondo momento.

Nota

- Dopo aver completato la procedura di aggiornamento, il dispositivo viene riavviato automaticamente. Se si riavvia il dispositivo manualmente dopo l'aggiornamento, attendere 5 minuti anche se si sospetta che l'aggiornamento non sia riuscito.
- Dal momento che il database di utenti, gruppi, credenziali e altri dati viene aggiornato dopo un aggiornamento firmware, il completamento del primo avvio potrebbe richiedere alcuni minuti. Il tempo necessario dipende dalla quantità dei dati.
- Quando viene aggiornato con il firmware più recente, il dispositivo Axis riceve le ultime funzioni disponibili. Prima di aggiornare il firmware, leggere sempre le istruzioni di aggiornamento e le note sulla versione disponibili per ogni nuova versione.

Dispositivi di controllo porta indipendenti:

1. Scaricare il file del firmware più recente nel computer, disponibile gratuitamente all'indirizzo Web *www.axis.com/support*
2. Andare a **Setup > Additional Controller Configuration > Maintenance (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Manutenzione)** nelle pagine Web del dispositivo.
3. In **Upgrade Server (Aggiorna server)** fare clic su **Choose file (Scegli file)** e individuare il file nel computer.
4. Se si desidera che il dispositivo esegua automaticamente il ripristino delle impostazioni predefinite di fabbrica dopo l'aggiornamento, selezionare la casella di controllo **Default (Predefinito)**.
5. Fare clic su **Upgrade (Aggiorna)**.
6. Attendere circa 5 minuti mentre il dispositivo viene aggiornato e riavviato. Quindi cancellare la cache del browser Web.
7. Accedere al dispositivo.

Dispositivi di controllo porta in un sistema:

È possibile utilizzare AXIS Device Manager o AXIS Camera Station per aggiornare tutti i dispositivi di controllo porta in un sistema. Per ulteriori informazioni, vedere *www.axis.com*.

Importante

- Non selezionare un aggiornamento sequenziale.

Nota

- Tutti i dispositivi di controllo in un sistema devono avere sempre la stessa versione del firmware.
- Aggiornare tutti i dispositivi di controllo di un sistema contemporaneamente, utilizzando l'opzione parallela in AXIS Device Manager o AXIS Camera Station.

Procedura di recupero di emergenza

Se il collegamento di rete o dell'alimentazione viene interrotto durante l'aggiornamento, il processo ha esito negativo e il dispositivo potrebbe non rispondere. L'indicatore di stato rosso lampeggiante indica un aggiornamento non riuscito. Per ripristinare il dispositivo, attenersi alla procedura seguente. Il numero di serie si trova sull'etichetta del dispositivo.

1. In **UNIX/Linux** digitare quanto segue dalla riga di comando:

   ```
   arp -s <IP address> <serial number> temp
   ping -l 408 <IP address>
   ```

   In **Windows**, digitare quanto segue da un prompt dei comandi/DOS (questa operazione può richiedere l'esecuzione del prompt dei comandi come amministratore):

   ```
   arp -s <IP address> <serial number>
   ping -l 408 -t <IP address>
   ```

2. Se il dispositivo non risponde entro 30 secondi, riavviarlo e attendere una risposta. Premere CTRL+C per interrompere la funzione Ping.
3. Aprire un browser e digitare l'indirizzo IP del dispositivo. Nella pagina visualizzata utilizzare il pulsante **Browse (Sfoglia)** per selezionare il file di aggiornamento da utilizzare. Fare clic su **Load (Carica)** per riavviare la procedura di aggiornamento.
4. Una volta terminato l'aggiornamento (1-10 minuti), il dispositivo viene riavviato automaticamente e l'indicatore di stato diventa di colore verde fisso.
5. Reinstallare il dispositivo, facendo riferimento alla Guida all'installazione.

Se la procedura di recupero di emergenza non fa sì che il dispositivo torni a funzionare correttamente, contattare l'assistenza Axis all'indirizzo *www.axis.com/support*

Sintomi, cause possibili e misure correttive

Problemi durante l'aggiornamento del firmware	
Errore durante l'aggiornamento del firmware	Se l'aggiornamento del firmware non riesce, il dispositivo ricarica il firmware precedente. Controllare il file del firmware e riprovare.

Problemi durante l'impostazione dell'indirizzo IP	
Quando si utilizza ARP/Ping	Provare a eseguire nuovamente l'installazione. L'indirizzo IP deve essere impostato entro due minuti dal collegamento del dispositivo all'alimentazione. Assicurarsi che la durata del Ping sia impostata su 408. Per istruzioni, vedere la Guida all'installazione nella pagina del dispositivo all'indirizzo *axis.com*.
Il dispositivo si trova in una subnet diversa	Se l'indirizzo IP destinato al dispositivo e l'indirizzo IP del computer utilizzato per accedere al dispositivo si trovano in subnet diverse, non sarà possibile impostare l'indirizzo IP. Contattare l'amministratore di rete per ottenere un indirizzo IP.

Risoluzione di problemi

L'indirizzo IP è già utilizzato da un altro dispositivo	Scollegare il dispositivo Axis dalla rete. Eseguire il comando Ping (in una finestra di comando/DOS digitare `ping` e l'indirizzo IP del dispositivo): • Se si riceve: `Reply from <IP address>: bytes=32; time=10...` significa che l'indirizzo IP potrebbe già essere utilizzato da un altro dispositivo nella rete. Ottenere un nuovo indirizzo IP dall'amministratore di rete e reinstallare il dispositivo. • Se si riceve: `Request timed out (Timeout della richiesta)` significa che l'indirizzo IP può essere utilizzato con il dispositivo Axis. Controllare tutti i cablaggi e reinstallare il dispositivo.
Possibile conflitto dell'indirizzo IP con un altro dispositivo nella stessa subnet	L'indirizzo IP statico del dispositivo Axis viene utilizzato prima che il server DHCP imposti un indirizzo dinamico. Ciò significa che se lo stesso indirizzo IP statico viene utilizzato anche da un altro dispositivo, si potrebbero verificare dei problemi durante l'accesso al dispositivo.

Impossibile accedere al dispositivo da un browser

Impossibile eseguire l'accesso	Se HTTPS è abilitato, assicurarsi di utilizzare il protocollo corretto (HTTP o HTTPS) quando si tenta di eseguire l'accesso. Potrebbe essere necessario digitare manualmente `http` o `https` nel campo dell'indirizzo del browser. Se si smarrisce la password root utente, il dispositivo deve essere ripristinato alle impostazioni predefinite di fabbrica. Vedere *Ripristino delle impostazioni predefinite di fabbrica alla pagina 64*.
L'indirizzo IP è stato modificato dal server DHCP	Gli indirizzi IP ottenuti da un server DHCP sono dinamici e potrebbero cambiare. Se l'indirizzo IP è stato modificato, utilizzare AXIS IP Utility o AXIS Device Manager per individuare il dispositivo sulla rete. Identificare il dispositivo utilizzando il relativo numero di serie o di modello oppure il nome DNS (se è stato configurato). Se necessario, è possibile assegnare manualmente un indirizzo IP statico. Per istruzioni, vedere il documento che illustra la *modalità di assegnazione di un indirizzo IP e di accesso al proprio dispositivo* nella pagina del dispositivo all'indirizzo *axis.com*
Errore del certificato durante l'utilizzo di IEEE 802.1X	Per un corretto funzionamento dell'autenticazione, le impostazioni della data e dell'ora nel dispositivo Axis devono essere sincronizzate con un server NTP. Vedere *Data e ora alla pagina 56*.

L'accesso al dispositivo può essere eseguito localmente ma non esternamente

Configurazione del router	Per configurare il router in modo da consentire il traffico di dati in entrata verso il dispositivo Axis, abilitare la funzione di attraversamento NAT che tenterà di configurare automaticamente il router per permettere l'accesso al dispositivo Axis, vedere *NAT traversal (mappatura delle porte) per IPv4 alla pagina 60*. Il router deve supportare UPnP®.
Protezione del firewall	Controllare il firewall Internet con l'amministratore di rete.
Router predefinito richiesto	Controllare se è necessario configurare le impostazioni del router da **Setup > Network Settings (Impostazione > Impostazioni di rete)** o **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Rete > TCP/IP > Base)**.

I LED relativi a stato e rete sono di colore rosso e lampeggiano rapidamente

Errore hardware	Contattare il rivenditore Axis.

Il dispositivo non si avvia

Il dispositivo non si avvia	Se il dispositivo non si avvia, mantenere collegato il cavo di rete e reinserire il cavo di alimentazione nel midspan.

Specifiche

Connettori

Per informazioni sulle posizioni dei connettori, vedere .

Per gli schemi di connessione e le informazioni sullo schema dei pin hardware generato tramite la configurazione dell'hardware, vedere *Schemi delle connessioni alla pagina 73* e *Configurazione dell'hardware alla pagina 13*.

Nella sezione seguente vengono descritte le specifiche tecniche dei connettori.

Connettore dati lettore

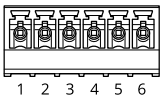
Morsettiera a 6 pin che supporta i protocolli RS485 e Wiegand per la comunicazione con il lettore.

Le porte RS485 supportano:

- RS485 a due fili, half-duplex
- RS485 a quattro fili, full-duplex

Le porte Wiegand supportano:

- Wiegand a due fili



Funzione		Pin	Note
RS485	A-	1	Per RS485 full duplex Per RS485 half duplex
	B+	2	
RS485	A-	3	Per RS485 full duplex Per RS485 half duplex
	B+	4	
Wiegand	D0 (Dati 0)	5	Per Wiegand
	D1 (Dati 1)	6	

Importante

Le porte RS485 hanno una velocità di trasmissione fissa di 9600 Bit/s.

Importante

La lunghezza cavo massima consigliata è di 30 m.

Importante

I circuiti di output in questa sezione sono di Classe 2 con potenza limitata.

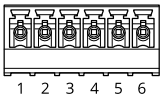
Connettore I/O lettore

Morsettiera a 6 pin per:

- Alimentazione ausiliaria (uscita CC)
- Input digitale

- Output digitale
- 0 V CC (-)

Il pin 3 sui connettori I/O lettore può essere supervisionato. Se il collegamento viene interrotto, viene attivato un evento. Per utilizzare input supervisionati, installare resistori terminali. Per gli input supervisionati utilizzare lo schema delle connessioni. Vedere *pagina 74*.



Funzione	Pin	Nota	Specifiche
0 V CC (-)	1		0 V CC
Output CC	2	Per alimentare periferiche ausiliarie. Nota: questo pin può essere usato solo come uscita alimentazione.	12 V CC Carico massimo = 300 mA
Configurabile (ingresso o uscita)	3–6	Input digitale: collegare al pin 1 per attivare oppure lasciare isolato (scollegato) per disattivare.	Da 0 a max 40 V CC
		Output digitale: collegare al pin 1 per attivare oppure lasciare isolato (scollegato) per disattivare. Se utilizzata con un carico induttivo, ad esempio un relè esterno, è necessario collegare un diodo in parallelo al carico per proteggere il dispositivo da sovratensioni.	Da 0 a max 40 V CC, open-drain, 100 mA

Importante

La lunghezza cavo massima consigliata è di 30 m.

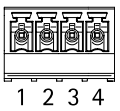
Importante

I circuiti di output in questa sezione sono di Classe 2 con potenza limitata.

Connettore porta

Due morsettiere a 4 pin utilizzate per i dispositivi di monitoraggio porte (ingresso digitale).

Tutti i pin di ingresso porte possono essere supervisionati. Se il collegamento viene interrotto, viene attivato un allarme. Per utilizzare input supervisionati, installare resistori terminali. Per gli input supervisionati utilizzare lo schema delle connessioni. Vedere *pagina 74*.



Funzione	Pin	Nota	Specifiche
0 V CC (-)	1, 3		0 V CC
Input	2, 4	Per comunicare con il monitor della porta. Input digitale - Collegare al pin 1 o 3 rispettivamente per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo. Nota: usare questo pin solo come ingresso.	Da 0 a max 40 V CC

Importante

La lunghezza cavo massima consigliata è di 30 m.

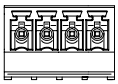
Specifiche

Connettore ausiliario

Morsettiera I/O a 4 pin configurabile per:

- Alimentazione ausiliaria (uscita CC)
- Input digitale
- Output digitale
- 0 V CC (-)

Per un esempio di schema delle connessioni, vedere *Schemi delle connessioni alla pagina 73*.



Funzione	Pin	Note	Specifiche
0 V CC (-)	1		0 V CC
Output CC	2	Per alimentare periferiche ausiliarie. Nota: questo pin può essere usato solo come uscita alimentazione.	3,3 V CC Carico massimo = 100 mA
Configurabile (ingresso o uscita)	3–4	Input digitale: collegare al pin 1 per attivare oppure lasciare isolato (scollegato) per disattivare.	Da 0 a max 40 V CC
		Output digitale: collegare al pin 1 per attivare oppure lasciare isolato (scollegato) per disattivare. Se utilizzata con un carico induttivo, ad esempio un relè esterno, è necessario collegare un diodo in parallelo al carico per proteggere il dispositivo da sovratensioni.	Da 0 a max 40 V CC, open-drain, 100 mA

Importante

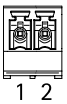
La lunghezza cavo massima consigliata è di 30 m.

Importante

I circuiti di output in questa sezione sono di Classe 2 con potenza limitata.

Connettore di alimentazione

Morsettiera a 2 pin per ingresso alimentazione CC. Utilizzare una sorgente di alimentazione limitata (LPS) compatibile con una bassissima tensione di sicurezza (SELV) con una potenza di output nominale limitata a ≤100 W o una corrente nominale di output limitata a ≤5 A.



Funzione	Pin	Note	Specifiche
0 V CC (-)	1		0 V CC
Input CC	2	Per l'alimentazione del controller quando non si utilizza Power over Ethernet. Nota: Questo pin può essere usato solo come alimentazione.	Da 10 a 28 V CC, max 36 W Carico massimo in uscita = 14 W

Specifiche

Connettore di rete

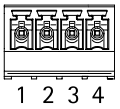
Connettore Ethernet RJ45. Usare cavi di Categoria 5e o superiore.

Funzione	Specifiche
Alimentazione e Ethernet	Power over Ethernet IEEE 802.3af/802.3at Tipo 1 Classe 3, 44-57 V CC Carico massimo in uscita = 7,5 W

Connettore blocco di alimentazione

Morsettiera a 4 pin per l'alimentazione di uno o due blocchi (output CC). Il connettore di blocco può essere usato anche per fornire alimentazione ai dispositivi esterni.

Collegare blocchi e carichi ai pin in base allo schema dei pin hardware generato tramite la configurazione dell'hardware.



Funzione	Pin	Nota	Specifiche
0 V CC (-)	1, 3		0 V CC
0 V CC, isolato o 12 V CC	2, 4	Per controllare fino a due blocchi da 12 V. Usare lo schema dei pin hardware. Vedere *Configurazione dell'hardware alla pagina 13*.	12 V CC Carico massimo totale = 500 mA

AVVISO

Se il blocco non è polarizzato, si consiglia di aggiungere un diodo di ritorno esterno.

Importante

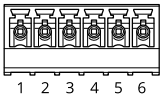
I circuiti di output in questa sezione sono di Classe 2 con potenza limitata.

Connettore del relè e di alimentazione

Morsettiera a 6 pin con relè integrato per:

- Dispositivi esterni
- Alimentazione ausiliaria (uscita CC)
- 0 V CC (-)

Collegare blocchi e carichi ai pin in base allo schema dei pin hardware generato tramite la configurazione dell'hardware.



Funzione	Pin	Nota	Specifiche
0 V CC (-)	1, 4		0 V CC

Relè	2–3	Per il collegamento di relè. Usare lo schema dei pin hardware. Vedere *Configurazione dell'hardware alla pagina 13*. I due pin relè sono separati con isolamento galvanico dal resto dei circuiti.	Corrente max = 700 mA Tensione max = +30 V CC
12 V CC	5	Per alimentare periferiche ausiliarie. Nota: questo pin può essere usato solo come uscita alimentazione.	Tensione massima = +12 V CC Carico massimo = 500 mA
24 V CC	6	Non utilizzato	

AVVISO

Se il blocco non è polarizzato, si consiglia di aggiungere un diodo di ritorno esterno.

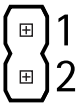
Importante

I circuiti di output in questa sezione sono di Classe 2 con potenza limitata.

Collettore pin allarmi anti-manomissione

Due collettori a 2 pin per escludere:

- Allarme anti-manomissione posteriore (TB)
- Allarme anti-manomissione anteriore (TF)



Funzione	Pin	Note
Allarme anti-manomissione posteriore	1–2	Per escludere contemporaneamente l'allarme anti-manomissione anteriore e posteriore, collegare i ponticelli, rispettivamente, tra TB 1, TB 2 e TF 1, TF 2. Se si escludono gli allarmi anti-manomissione, il sistema non identificherà alcun tentativo di manomissione.
Allarme anti-manomissione anteriore	1–2	

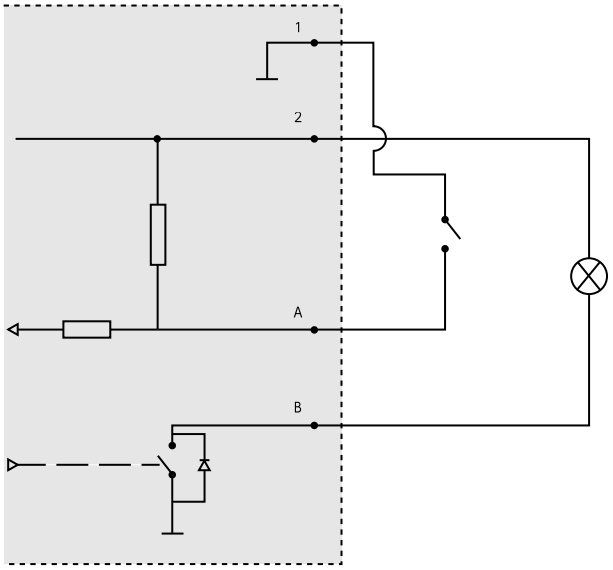
Nota

Gli allarmi anti-manomissione anteriore e posteriore sono collegati per impostazione predefinita. È possibile configurare il trigger di apertura della struttura in modo che esegua un'azione se il dispositivo di controllo porte viene aperto o rimosso dalla parete o dal soffitto. Per informazioni sulla configurazione di allarmi ed eventi, vedere *Configurazione di allarmi ed eventi alla pagina 44*.

Schemi delle connessioni

Collegare i dispositivi in base allo schema dei pin hardware generato tramite la configurazione dell'hardware. Per ulteriori informazioni sulla configurazione dell'hardware e lo schema dei pin hardware, vedere *Configurazione dell'hardware alla pagina 13*.

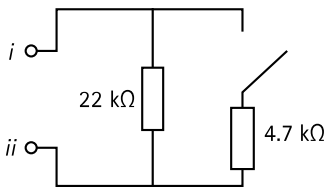
Connettore ausiliario



1 *0 V CC (-)*
2 *Output CC: 3,3 V max 100 mA*
A *I/O configurato come input*
B *I/O configurato come output*

Ingressi supervisionati

Per utilizzare gli input supervisionati, installare resistori terminali in base al diagramma di seguito riportato.



i *Input*
ii *0 V CC (-)*

Nota

Si consiglia l'uso di cavi intrecciati e schermati. Connetti schermatura a 0 V CC.

Informazioni di sicurezza

Livelli di pericolo

⚠PERICOLO

Indica una situazione pericolosa che, se non evitata, provoca morte o lesioni gravi.

⚠AVVISO

Indica una situazione pericolosa che, se non evitata, potrebbe provocare la morte o lesioni gravi.

⚠ATTENZIONE

Indica una situazione pericolosa che, se non evitata, potrebbe provocare lesioni medie o minori.

AVVISO

Indica una situazione che, se non evitata, potrebbe danneggiare la proprietà.

Altri livelli di messaggio

Importante

Indica informazioni importanti, essenziali per il corretto funzionamento del dispositivo.

Nota

Indica informazioni utili che aiutano a ottenere il massimo dal dispositivo.

Manuale per l'utente
AXIS A1001 & AXIS Entry Manager

Ver. M25.2
Data: Dicembre 2023
Codice art. T10010336