AXIS A1601 Network Door Controller

Manuale dell'utente

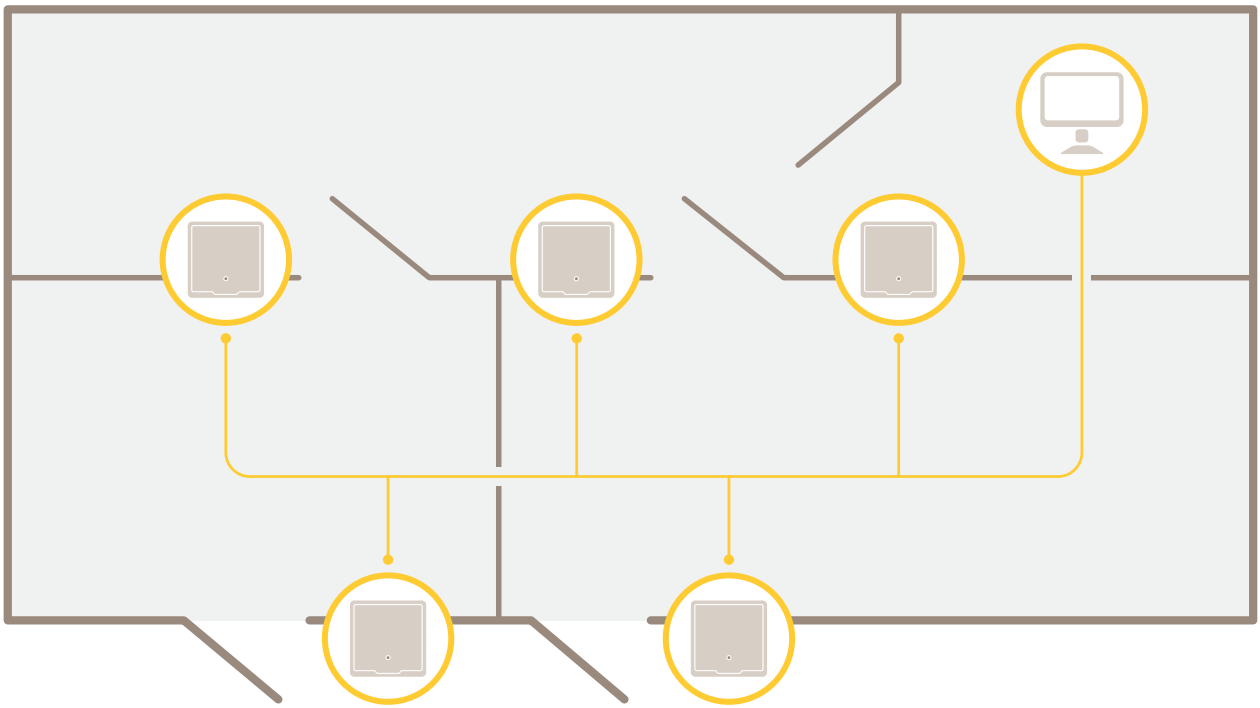
Indice

Panoramica delle soluzioni....5
Panoramica dei prodotti....6
Individuazione del dispositivo sulla rete....7
Accesso al dispositivo....7
Modalità di accesso al dispositivo da Internet....7
Password sicure....7
Come impostare la password root....8
Pagina Panoramica....8
Configurazione di sistema....9
Configurazione: passo - passo....9
Selezioneare una lingua....9
Impostare la data e l'ora....9
Data e ora da un server NTP (Network Time Protocol)....10
Impostazione di data e ora manuali....10
Ottenimento della data e dell'ora dal computer....10
Configurare le impostazioni di rete....10
Configurazione dell'hardware....10
Modalità di importazione di un file di configurazione hardware....11
Creazione di una nuova configurazione dell'hardware....11
Modalità di creazione di una nuova configurazione hardware senza periferiche....12
Come creare una nuova configurazione hardware per i blocchi wireless....15
Come creare una nuova configurazione hardware con il controllo ascensore (AXIS A9188)....16
Modalità di aggiunta e configurazione delle periferiche di rete....16
Verificare i collegamenti hardware....17
Comandi di verifica delle porte....17
Piani dei controlli di verifica....17
Configurare le schede e i formati....18
Descrizioni del formato della scheda....19
Formato tessera....19
Mappe dei campi....19
Configurazione dei servizi....20
SmartIntego....20
Profilo LED OSDP....21
Istruzioni di manutenzione....22
Configurazione evento....24
Visualizza il registro degli eventi....24
Filtri di registro eventi....24
Configurazione del registro eventi....24
Opzioni del registro eventi....24
Modalità di impostazione delle regole di azione....24
Modalità di aggiunta di destinatari....25
Modalità di creazione delle pianificazioni....26
Modalità di impostazione delle ricorrenze....26
Feedback del lettore....27
Opzioni di sistema....28
Sicurezza....28
Utenti....28
ONVIF....28
Filtro indirizzi IP....28
HTTPS....28
IEEE 802.1X....29
Certificati....29
Rete....30

Impostazioni TCP/IP di base 30
Advanced TCP/IP Settings 31
SOCKS 34
QoS (Qualità del servizio) (Quality of Service) 34
SNMP 34
UPnP 35
Bonjour 35
Porte e dispositivi 35
Porte I/O 35
Stato delle porte 35
Manutenzione 35
Supporto 36
Panoramica supporto 36
Panoramica del sistema 36
Registri e report 36
Avanzata 37
Scripting 37
Caricamento di file 37
Risoluzione dei problemi 38
Ripristinare le impostazioni predefinite di fabbrica 38
Modalità di controllo del firmware corrente 38
Modalità di aggiornamento del firmware 38
Sintomi, possibili cause e azioni correttive 39
Dati tecnici 41
..... 41
Indicatori LED 41
Pulsanti 41
Pulsante di comando 41
Connettori 41
Connettore di rete 41
Connettore lettore 42
Connettore porta 43
Connettore relè 44
Connettore ausiliario 45
Connettore esterno 46
Connettore di alimentazione 46
Connettore di input della batteria di backup 46
Informazioni di sicurezza 48
Livelli di pericolo 48
Altri livelli di messaggio 48
Interfaccia Web 49
..... 49
Stato 49
Dispositivo 50
Allarmi 50
Periferiche 51
Lettori 51
Serrature wireless 52
Aggiornamento 52
Sistema 52
Ora e ubicazione 52
Rete 54
Sicurezza 58
Account 62
MQTT 63
Accessori 66

Registri....66
Manutenzione....69

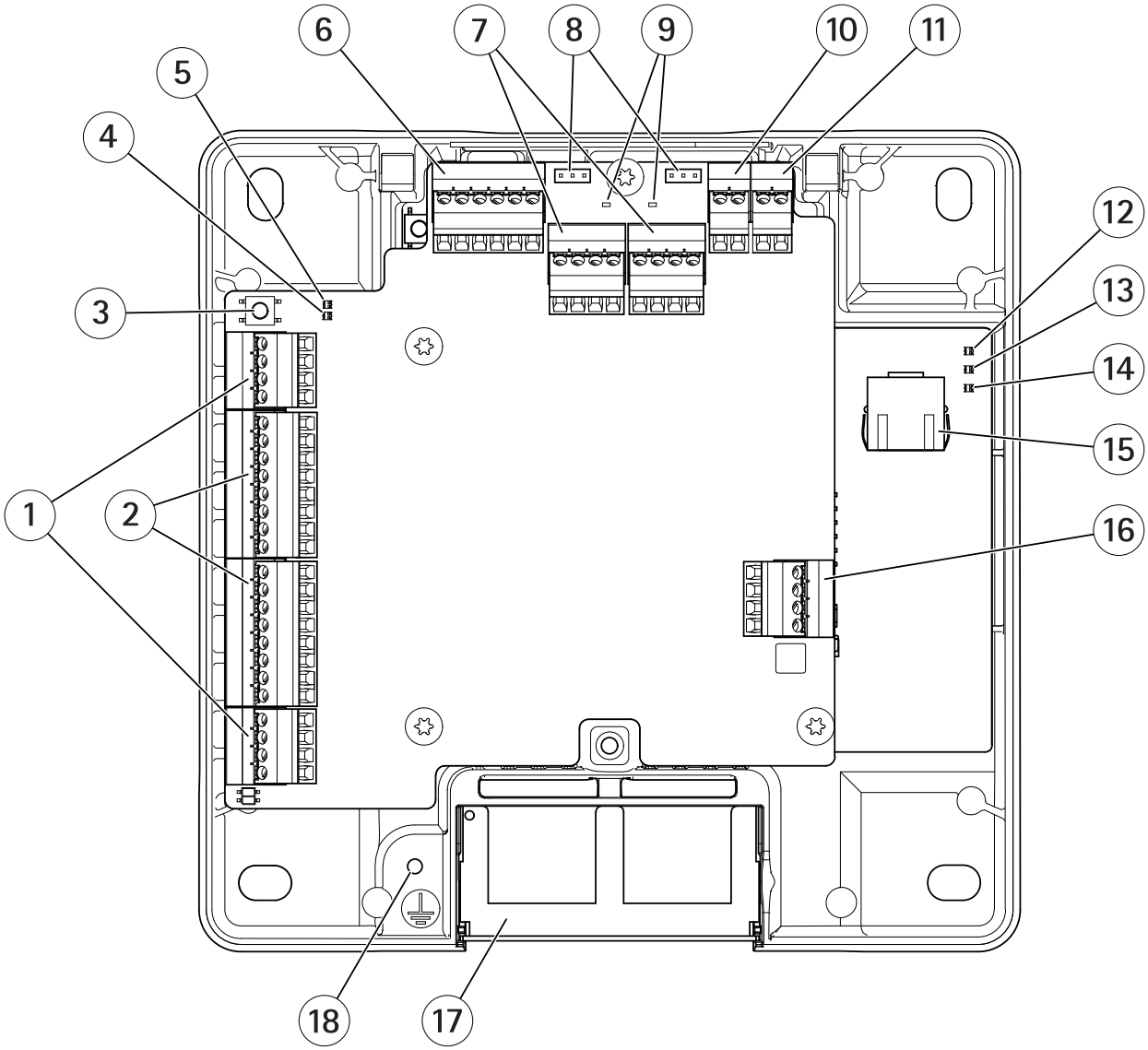
Panoramica delle soluzioni



Il door controller di rete può essere facilmente collegato a e alimentato dalla rete IP esistente senza bisogno di cablaggi speciali.

Ciascun dispositivo di controllo delle porte di rete è un dispositivo intelligente che può essere facilmente montato vicino a una porta. È in grado di alimentare e controllare fino a quattro lettori.

Panoramica dei prodotti



1 *Connettore porta, on page 43 (2x)*
2 *Connettore lettore, on page 42 (2x)*
3 *Pulsante di comando, on page 41*
4 *LED sovracorrente lettore*
5 *LED sovracorrente relè*
6 *Connettore ausiliario, on page 45*
7 *Connettore relè, on page 44 (2x)*
8 *Ponticello relè (2x)*
9 *LED relè (2x)*
10 *Connettore di input della batteria di backup, on page 46*
11 *Connettore di alimentazione, on page 46*
12 *LED di alimentazione*
13 *LED di stato*
14 *LED di rete*
15 *Connettore di rete, on page 41*
16 *Connettore esterno, on page 46*
17 *Coperchio cavi reversibile*
18 *Posizione di messa a terra*

Individuazione del dispositivo sulla rete

Per trovare i dispositivi Axis sulla rete e assegnare loro un indirizzo IP in Windows®, utilizza AXIS IP Utility o AXIS Device Manager. Queste applicazioni sono entrambe gratuite e possono essere scaricate dal sito Web *axis.com/support*.

Per ulteriori informazioni su come trovare e assegnare indirizzi IP, andare alla sezione *Come assegnare un indirizzo IP e accedere al 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. Immettere il nome utente e la password. Se si accede al dispositivo per la prima volta, è necessario impostare la password root. Vedere .
3. La pagina web del dispositivo si apre nel browser. La pagina iniziale è chiamata pagina Overview (Panoramica).

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.

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®.

Password sicure

Importante

Utilizza il protocollo HTTPS (abilitato per impostazione predefinita) per configurare la password o altre configurazioni sensibili tramite la rete. Il protocollo HTTPS abilita collegamenti di rete sicuri e crittografati, garantendo così la protezione dei dati sensibili, come le password.

La password del dispositivo è il sistema di protezione principale dei dati e dei servizi. I dispositivi Axis non impongono criteri relativi alla password poiché i dispositivi potrebbero essere utilizzati in vari tipi di installazioni.

Per proteggere i dati consigliamo vivamente di:

- Utilizzare una password con almeno 8 caratteri, creata preferibilmente da un generatore di password.
- Non mostrare la password.
- Cambiare la password a intervalli regolari, almeno una volta all'anno.

Come impostare la password root

Per accedere al prodotto Axis, è necessario impostare la password per il **root** utente amministratore predefinito. 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 uno scambio di informazioni crittografato. Vedere *HTTPS, on page 28*.

Il **root** nome utente amministratore predefinito è permanente e non è possibile eliminarlo. Se si perde la password del root, il prodotto deve essere ripristinato alle impostazioni di fabbrica predefinite. Vedere *Ripristinare le impostazioni predefinite di fabbrica, on page 38*.

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

Pagina Panoramica

La pagina Panoramica nella pagina Web del dispositivo 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.

La prima volta che si accede al dispositivo Axis, la pagina Panoramica richiederà di configurare l'hardware, impostare la data e l'ora e configurare le impostazioni di rete. Per ulteriori informazioni sulla configurazione del sistema, vedere *Configurazione: passo - passo, on page 9*.

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

Configurazione di 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 riguardanti gli utenti e gli amministratori, vedere *page 28*.

Configurazione: passo - 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 la pagina Web del dispositivo per l'utilizzo di un'altra lingua. Vedere *Selezioneare una lingua, on page 9*.
2. Impostare la data e l'ora. Vedere *page 9*.
3. Configurare le impostazioni di rete. Vedere *page 10*.
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, on page 10*.
5. Verificare i collegamenti hardware. Vedere *page 17*.
6. Configurare le schede e i formati. Vedere *page 18*.

Per maggiori informazioni sui suggerimenti di manutenzione, vedere *Istruzioni di manutenzione, on page 22*.

Selezioneare una lingua

La lingua predefinita della pagina Web del dispositivo 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, la pagina Web del dispositivo torna alla lingua inglese.
- Se si ripristina, si riavvia il dispositivo o si aggiorna il firmware, la pagina Web del dispositivo continuerà a utilizzare la lingua selezionata.

Impostare la data e l'ora

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 *page 10*.
- Impostazione manuale di data e ora. Vedere *page 10*.
- Ottenimento di data e ora dal computer. Vedere *page 10*.

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** (Opzioni di sistema, Data e ora, Impostazione, Configurazione controller 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 maggiori informazioni sulle impostazioni NTP, vedere *NTP Configuration, on page 32*.
Se si utilizza un nome host per il server NTP, deve essere configurato un server DNS. Vedere *DNS Configuration, on page 31*.

Impostazione di data e ora manuali

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. 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.

Configurare le 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 maggiori informazioni sulle impostazioni di rete, vedere *Rete, on page 30*.

Configurazione dell'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 sulla manutenzione, vedere *page 22*.

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

- Importazione di un file di configurazione hardware. Vedere *page 11*.
- Creazione di una nuova configurazione dell'hardware. Vedere *page 11*.

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 maggiori informazioni, vedere *Modalità di esportazione di un file di configurazione hardware, on page 11*.

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, on page 12*
- *Come creare una nuova configurazione hardware per i blocchi wireless, on page 15*
- *Come creare una nuova configurazione hardware con il controllo ascensore (AXIS A9188), on page 16*

Modalità di creazione di una nuova configurazione hardware senza periferiche

1. Selezionare **Setup > Hardware Configuration (Configurazione > Configurazione hardware)** e fare clic su **Start new hardware configuration (Avvia una 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, on page 12*.
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, on page 14*.
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 maggiori informazioni, vedere *Modalità di utilizzo degli input supervisionati, on page 14*.

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.

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.

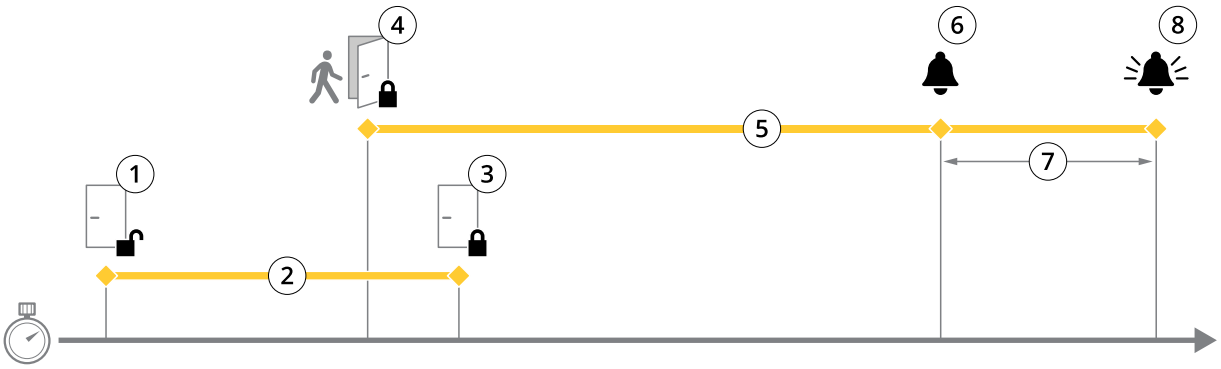
- **Cancel access time once door is opened (Cancella tempo di accesso una volta aperta la porta)**: selezionare questa opzione per prevenire accessi non autorizzati. Il blocco verrà attivato non appena il monitor porte indicherà che la porta è stata aperta.

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.

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 sull'impostazione di una regola di azione, consultare *Modalità di impostazione delle regole di azione, on page 24*.

Informazioni sulle opzioni di blocco

Le opzioni del circuito di blocco disponibili sono:

- **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.
- **None (Nessuno)** – Disponibile solo per il blocco 2. Selezionare se si intende utilizzare 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 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 *page 43*.
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

La funzione seguente supporta gli input supervisionati:

- Monitor porte. Vedere *Connettore porta, on page 43*.

Come creare una nuova configurazione hardware per i blocchi wireless

1. Selezionare **Setup > Hardware Configuration (Configurazione > Configurazione hardware)** e fare clic su **Start new hardware configuration (Avvia una nuova configurazione hardware)**.
2. Inserire 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 blocco, 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 (Configurazione > Riconfigurazione hardware)**, per completare la configurazione, consultare *Aggiunta di dispositivi e porte Assa Aperio™, on page 15*
   - **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 (Fai clic qui per selezionare il gateway wireless e configurare le porte)** per completare la configurazione, consultare *Modalità di configurazione di SmartIntego, on page 21*.

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 **Aggiungi**.

Come creare una nuova configurazione hardware con 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. Nella pagina Web del dispositivo di controllo delle porte di rete, selezionare **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. 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. Inserire 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 **Network Peripherals (Periferiche di rete)** per completare la configurazione consultare *Modalità di aggiunta e configurazione delle periferiche di rete , on page 16* 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 **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 di I/O e relè 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 **Aggiungi**.

Verificare i 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)**.
- **Reader: Feedback (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 maggiori informazioni, vedere *Feedback del lettore, on page 27*. Vedere anche le istruzioni del produttore.
- **Reader: tampering (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)**.
- **Reader: Card swipe (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)**.
- **Elevator Reader: Feedback (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 maggiori informazioni, vedere *Feedback del lettore, on page 27*. Vedere anche le istruzioni del produttore.
- **Elevator Reader: tampering (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)**.

- **Elevator Reader: Card swipe (Lettore ascensore: 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)**.

Configurare le schede e i 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 tessera 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, on page 19*.
4. Fare clic su **Add field map (Aggiungi mappa campo)** e immettere le informazioni necessarie nei campi. Vedere *Mappe dei campi, on page 19*.
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 ,255mm,sfx)=″graphics:graphicFDD764D07E7C241C8A937BCA610A09E0″ e modificare le descrizioni dei formati scheda e le mappe dei campi secondo necessità. Quindi fare clic su **Save (Salva)**.

Per eliminare una mappa di campo nella finestra di dialogo **Edit card format (Modifica formato scheda)** o **Add card format (Aggiungi formato scheda)**, fare clic su ,255mm,sfx)=″graphics:graphic4F71DDC71F74F5FFD775B70D87A3F3B1″

Per eliminare un formato scheda, fare clic su ,255mm,sfx)=″graphics:graphic4F71DDC71F74F5FFD775B70D87A3F3B1″.

Importante

- È possibile abilitare e disabilitare i formati scheda solo se il dispositivo di controllo porta è stato configurato con almeno un lettore. Vedere *Configurazione dell'hardware, on page 10* e *Modalità di configurazione di lettori e dispositivi REX, on page 14*.
- 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.

Formato tessera

Questa funzione è riservata esclusivamente agli utenti esperti. Non appena l'opzione **Card format (Formato scheda)** è attiva:

- Se si utilizza una credenziale a 37 bit, gli ultimi 5 bit vengono rimossi.
- Se si utilizza una credenziale a 64 bit (codice QR), la prima sequenza di 24 bit viene rimossa.

Per visualizzare le credenziali è possibile utilizzare sia i dati campione sia il lettore di schede.

1. Andare ad **Advanced (Avanzate)** > **Card format (Formato scheda)**.
2. Leggere l'avviso e fare clic su **I understand (Ho compreso)** per abilitare **Card format (Formato scheda)**.
3. Nel menu a discesa **Reader data visualization (Visualizzazione dati del lettore)**, scegliere il lettore.
4. Fare clic su **Get reader data (Ottieni dati del lettore)** oppure **Use sample data (Usa dati di esempio)** per generare un output di scheda. Verrà applicata a tutti i titolari di carte presenti sul dispositivo.
5. Attivare l'opzione **Trim reader data (Ritaglia i dati del lettore)** per rimuovere i bit finali delle credenziali della carta.
6. Fare clic su **Enable (Abilita)**.

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 conteggio è già pari, il valore del bit di parità è impostato su 0. Se il conteggio è dispari, il valore del bit di parità pari viene impostato su 1, rendendo il conteggio totale un numero pari.
  - `OddParity`: Anche i bit di disparità assicurano che ci sia un numero dispari di bit nella stringa. Vengono conteggiati i bit che hanno il valore 1. Se il conteggio è già dispari, il valore del bit di parità dispari viene impostato su 0. Se il conteggio è pari, il valore del bit di parità viene impostato su 1, rendendo il conteggio 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 da 0 a 9 e le lettere da a ad f. L'ordine dei bit Little endian significa che il primo bit è il più piccolo (il 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 da 0 a 9 e le lettere da a ad f. L'ordine dei bit Big-endian significa che il primo bit è il più grande (il più significativo).
  - **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.

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.

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, on page 15*.

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. Fai clic su **Browse...**, selezionare il file csv e fare clic su **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. Fai clic su **Browse...**, selezionare il file csv e fare clic su **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.

Profilo LED OSDP

È possibile personalizzare i profili LED del lettore OSDP per definire le luci e i suoni da utilizzare in base ai diversi eventi. Per un elenco completo dei profili, consultare la sezione *Profili LED*.

Impostare i livelli di luce e audio

1. Andare a **Peripherals (Periferiche)** > **Readers (Lettori)** > **OSDP LED profile (Profilo LED OSDP)**.
2. Aprire il menu a discesa **Light and audio levels (Livelli di luce e volume dell'audio)**.
3. Utilizzare il cursore per regolare l'intensità della striscia LED, della retroilluminazione LED e del suono.
4. Fare clic su **Save (Salva)**.

Nota

Quando si effettuano delle modifiche di luminosità e audio, le impostazioni vengono aggiornate per tutti i lettori collegati al controller.

Verificare le impostazioni LED OSDP:

È possibile utilizzare il menu **OSDP LED test (test LED OSDP)** per visualizzare le impostazioni audio e di illuminazione di ogni profilo del lettore.

Per verificare le impostazioni dei profili LED OSDP:

1. Andare a **Peripherals (Periferiche)** > **Readers (Lettori)** > **OSDP LED profile (Profilo LED OSDP)**.
2. Espandere il menu a discesa **OSDP LED test (Test LED OSDP)**.
3. Scegliere una retroazione LED.
4. Scegli il lettore che si desidera testare.
5. Fare clic su **Avvia**.
6. Fare clic su **Edit feedback (Modifica retroazione)** per modificare le impostazioni di luce e audio del profilo.
   - Scegliere un nuovo colore dal menu a discesa **Color (Colore)**.
   - Scegliere una frequenza audio dal menu a discesa **Audio**, se del caso.
   - È inoltre possibile ripristinare le impostazioni del profilo facendo clic su **Reset to default values (Ripristina valori predefiniti)**.
   - Fare clic su **Save (Salva)**.

Modifica delle impostazioni del profilo LED OSDP:

1. Andare a **Peripherals (Periferiche)** > **Readers (Lettori)** > **OSDP LED profile (Profilo LED OSDP)**.
2. Accedere a **OSDP LED profile (Profilo LED OSDP)**.
3. Fare clic su accanto al profilo che si desidera modificare.
4. Modifica delle impostazioni pertinenti:
   - Scegliere il comportamento che i LED dovranno seguire dal menu a discesa **Behavior (Comportamento)**.
   - Scegli il colore dei LED dal menu a discesa **Color (Colore)**.
   - Impostare **Duration on (Durata acceso)** e **Duration off (Durata spento)** per i LED.
   - Impostare la **Recurrence (Periodicità)** della risposta del LED.
   - Dal menu a discesa **Audio**, scegliere **Beep duration, on (Durata del segnale acustico in funzione)** e **Beep duration, off (Durata del segnale acustico spento)**, quindi impostare la **Recurrence (Periodicità)** della risposta acustica. Assicurarsi che la **Beep duration, on (Durata del segnale acustico in funzione)** e **Beep duration, off (Durata del segnale acustico spento)** siano uguali.
5. Fare clic su **Save (Salva)**.

Importare le impostazioni esistenti da un altro controller

1. Andare a **Peripherals (Periferiche)** > **Readers (Lettori)** > **OSDP LED profile (Profilo LED OSDP)**.
2. Fare clic su **Import (Importa)**.
3. Scegliere il file che si desidera caricare.
4. Fare clic su **Import (Importa)**.

Esportare le impostazioni attuali

1. Andare a **Peripherals (Periferiche)** > **Readers (Lettori)** > **OSDP LED profile (Profilo LED OSDP)**.
2. Fare clic su **Export (Esporta**.
3. Scegliere dove si desidera salvare il file JSON e fare clic su **Save (Salva)**.

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, on page 17*.
- 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, on page 17*.

- Se il door controller non funziona come previsto, consultare *Risoluzione dei problemi, on page 38* e *Manutenzione, on page 35* per ulteriori informazioni.

Configurazione evento

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.

- Visualizza il registro degli eventi. Vedere *page 24*.
- Esportare il registro eventi. Vedere .
- Configurazione del registro eventi. Vedere *Configurazione del registro eventi, on page 24*.

Visualizza il registro degli eventi

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

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 maggiori informazioni, vedere *Filtri di registro eventi, on page 24*.

Per l'amministratore potrebbero essere più interessanti alcuni eventi piuttosto che altri. Pertanto, è possibile scegliere quali eventi devono essere registrati. Per maggiori informazioni, vedere *Opzioni del registro eventi, on page 24*.

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.
- Data e ora: filtrare il registro eventi per un intervallo di data e ora.

Configurazione del registro eventi

La pagina di configurazione del registro eventi consente di definire gli eventi che devono essere registrati.

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 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)**: abilita la registrazione degli eventi. L'evento verrà registrato e incluso nel registro eventi.

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. 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 sui trigger e sulle azioni disponibili, vedere la Guida integrata del dispositivo.

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 (Vai 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.

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 .

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** per provare la connessione con il destinatario.
6. Fare clic su **OK**.

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** 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, on page 29*.

Modalità di creazione delle pianificazioni

Le pianificazioni possono essere utilizzate come attivazioni 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	Wiegand LED doppio	Wiegand LED singolo	OSDP	Schema segnale acustico	Stato
Inattivo[1]	Off	Rosso	Rosso	Invisibile	Normale
RequirePIN	Rosso/verde lampeggiante	Rosso/verde lampeggiante	Rosso/verde lampeggiante	Due segnali acustici brevi	PIN obbligatorio
AccessGranted	Verde	Verde	Verde	Bip	Accesso consentito
AccessDenied	Rosso	Rosso	Rosso	Bip	Accesso negato

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.

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

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 è abilitata automaticamente. Utilizzare il nome utente e la password con tutta la comunicazione 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 su **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, on page 29*.

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). Occorrente:

- 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, on page 29*.

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 .

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 dell'autorità di certificazione – 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 su **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 auto firmato, vedere *Modalità di creazione di un certificato autofirmato, on page 30*.
2. Andare su **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 su **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.

Rete

Impostazioni TCP/IP di base

Il dispositivo Axis supporta IP versione 4 (IPv4) e IP versione 6 (IPv6).

Il dispositivo Axis può ottenere un indirizzo IP 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 le impostazioni di fabbrica, vedere *page 38*.

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 dei prodotti, on page 6*) 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.

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 maggiori informazioni, consultare il sito *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.

Advanced TCP/IP Settings

DNS Configuration

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` in cui `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.

NTP Configuration

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.

Host Name Configuration

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.

Link-Local IPv4 Address

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 maggiori informazioni, vedere *HTTPS, on page 28*.

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 abilita il caricamento di nuovi firmware, applicazioni utente, ecc. Si può disattivare il server FTP 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 postazione di gestione che eseguono SNMP. I nomi di 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 HTTPS sia abilitato, vedere *HTTPS, on page 28*. 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 di fabbrica del dispositivo Axis, vedere *Ripristinare le impostazioni predefinite di fabbrica, on page 38*.

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 fornisce quattro porte di input e output configurabili per il collegamento di dispositivi esterni.

Il connettore esterno offre due porte di input e output configurabili per il collegamento di dispositivi esterni.

È possibile configurare le porte I/O 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)**). È possibile assegnare nomi descrittivi alle porte e le opzioni **Normal states (Stati normali)** possono essere configurate 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. Non avrà effetti 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. Il dispositivo Axis può anche essere ripristinato ai valori predefiniti di fabbrica utilizzando il pulsante di comando, vedere *Ripristinare le impostazioni predefinite di fabbrica, on page 38*.

Per informazioni sull'aggiornamento del firmware, vedere *Modalità di aggiornamento del firmware, on page 38*.

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 dei problemi, on page 38*.

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.

Scaricare 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)).

Avanzata

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 Script Editor, andare in **Setup > Additional Controller Configuration > System Options > Advanced > Scripting (Impostazione > Configurazione dispositivo di controllo aggiuntivo > Opzioni di sistema > Avanzate > Scripting)**. Se uno script provoca dei problemi, ripristinare le impostazioni predefinite di fabbrica del dispositivo. Per tale operazione, vedere *page 38*.

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 accedere a un file, andare a **Setup > Additional Controller Configuration > System Options > Advanced > File Upload** (Opzioni di sistema, Avanzate, Caricamento file, Configurazione, Configurazione controller aggiuntivo, Opzioni di sistema, Avanzate, Caricamento file, Preferenze, Configurazione dispositivo aggiuntivo, Opzioni di sistema, Avanzate, Caricamento file).

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

Risoluzione dei problemi

Ripristinare le 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 alle impostazioni predefinite di fabbrica:

1. Scollegare l'alimentazione dal dispositivo.
2. Tenere premuto il pulsante di comando quando si ricollega l'alimentazione. Vedere *Panoramica dei prodotti, on page 6*.
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. La procedura è terminata quando il LED di stato diventa 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 (Configurazione) > Additional Controller Configuration (Configurazione controller aggiuntivo) > Setup (Configurazione) > System Options (Opzioni sistema) > Maintenance (Manutenzione)** e fare clic su **Default (predefinito)**.

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. L'ultima versione potrebbe contenere una correzione che risolve il tuo 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 richiesto dipende dalla quantità di 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 di rilascio disponibili per ogni nuova versione.

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 **Aggiorna**.
6. Attendere circa 5 minuti mentre il dispositivo viene aggiornato e riavviato. Quindi cancellare la cache del browser Web.
7. Accedere al dispositivo.

Sintomi, possibili cause e azioni 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 lunghezza del ping sia impostata su 408. Per le istruzioni, vedere la guida all'installazione presente sulla pagina del prodotto sul sito *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.
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 la risposta ricevuta è `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`, significa che l'indirizzo IP può essere utilizzato con il prodotto 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	Quando HTTPS è abilitato, verifica che sia usato il protocollo giusto (HTTP o HTTPS) quando tenti 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 *Ripristinare le impostazioni predefinite di fabbrica, on page 38*.
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 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 .

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, on page 33*. 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)**.

Dati tecnici

Il testo contrassegnato con **UL** è valido solo per le installazioni UL 293 o UL 294.

Indicatori LED

LED	Colore	Significato
Rete	Verde	Luce fissa per connessione di rete a 100 MBit/s. Lampeggiante per attività di rete.
	Giallo	Luce fissa per connessione di rete a 10 MBit/s. Lampeggiante per attività di rete.
	Spento	Assenza di collegamento di rete.
Stato	Verde	Luce verde fissa in condizioni di normale utilizzo.
	Giallo	Luce fissa durante l'avvio e quando si ripristinano le impostazioni.
	Rosso	Luce lampeggiante lenta per aggiornamento non riuscito.
Potenza	Verde	Funzionamento normale.
	Giallo	Luce lampeggiante verde/gialla durante l'aggiornamento del firmware.
Sovracorrente relè	Rosso	Luce fissa in caso di corto circuito o se è stata rilevata sovracorrente.
	Spento	Funzionamento normale.
Sovracorrente lettore	Rosso	Luce fissa in caso di corto circuito o se è stata rilevata sovracorrente.
	Spento	Funzionamento normale.
Relè	Verde	Relè attivo.[2]
	Spento	Relè inattivo.

Nota

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

Pulsanti

Pulsante di comando

Il pulsante di comando viene utilizzato per:

- Ripristino del dispositivo alle impostazioni predefinite di fabbrica. Vedere *Ripristinare le impostazioni predefinite di fabbrica, on page 38*.

Connettori

Connettore di rete

Connettore Ethernet RJ45 con Power over Ethernet Plus (PoE +).

UL: Power over Ethernet (PoE) deve essere fornito da un UL 294 elencato Power over Ethernet IEEE 802.3af / 802.3at Tipo 1 Classe 3 o Power over Ethernet Plus (PoE+) IEEE 802.3at Tipo 2 Classe 4 iniettore limitato che

2. Il relè è attivo quando COM è connesso a NO.

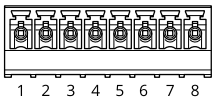
fornisce 44-57 V CC, 15,4 W / 30 W. Power over Ethernet (PoE) è stato valutato da UL con AXIS T8133 Midspan 30 W 1-port.

Connettore lettore

Due morsettiere a 8 pin che supportano i protocolli RS485 e Wiegand per la comunicazione con il lettore.

I valori di output dell'alimentazione specificati vengono condivisi dalle due porte dei lettori. Ciò significa che 486 mA a 12 V CC è riservata a tutti i lettori collegati al dispositivo di controllo delle porte.

Selezionare il protocollo da utilizzare nella pagina Web del dispositivo.



Configurato per RS485

Funzione	Pin	Nota	Dati tecnici
Massa CC (GND)	1		0 V CC
Output CC (+12 V)	2	Fornisce alimentazione al lettore.	12 V CC, Max 486 mA combinata per entrambi i lettori
RX/TX	3-4	Full-duplex: RX. Half-duplex: RX/TX.	
TX	5–6	Full-duplex: TX.	
Configurabile (ingresso o uscita)	7–8	Ingresso digitale - collegare al pin 1 per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo.	Da 0 a max 30 V CC
		Output digitale: se utilizzato con un carico induttivo, ad esempio un relè, collegare un diodo in parallelo al carico per proteggere il dispositivo da sovratensioni.	Da 0 a max 30 V CC, open-drain, 100 mA

Importante

- Quando il lettore è alimentato dal controller, la lunghezza del cavo certificata raggiunge il massimo di 200 m (656 piedi).
- Quando il lettore non è alimentato dal controller, la lunghezza del cavo certificata per i dati del lettore raggiunge il massimo di 1000 m (3280,8 piedi) se sono soddisfatti i seguenti requisiti del cavo: 1 doppino con schermatura, AWG 24, impedenza 120 ohm.

Configurato per Wiegand

Funzione	Pin	Nota	Dati tecnici
Massa CC (GND)	1		0 V CC
Output CC (+12 V)	2	Fornisce alimentazione al lettore.	12 V CC, Max 486 mA combinata per entrambi i lettori
D0	3		

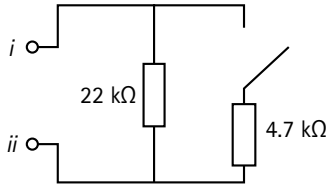
D1	4		
O	5–6	Output digitale, open-drain	
Configurabile (ingresso o uscita)	7–8	Ingresso digitale - collegare al pin 1 per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo.	Da 0 a max 30 V CC
		Output digitale: se utilizzato con un carico induttivo, ad esempio un relè, collegare un diodo in parallelo al carico per proteggere il dispositivo da sovratensioni.	Da 0 a max 30 V CC, open-drain, 100 mA

Importante

- Quando il lettore è alimentato dal controller, la lunghezza del cavo certificata raggiunge il massimo di 150 m (500 piedi).
- Quando il lettore non è alimentato dal controller, la lunghezza del cavo certificata per i dati del lettore raggiunge il massimo di 150 m (500 piedi) se è soddisfatto il seguente requisito del cavo: AWG 22.

Ingressi con supervisione

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



i Ingresso

ii 0 V CC (-)

UL: Gli input supervisionati non sono stati valutati da UL per l'uso di antifurto. Solo il monitor porte e REX supportano la supervisione con resistori di linea.

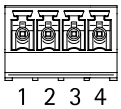
Nota

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

Connettore porta

Due morsettiere a 4 pin utilizzate per i monitor porte (input digitale).

Il monitor porte supporta la supervisione con resistori di linea. Se il collegamento viene interrotto, viene attivato un allarme. Per utilizzare gli input supervisionati, installare resistenze di fine linea. Per gli input supervisionati utilizzare lo schema delle connessioni. Vedere .



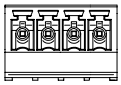
Funzione	Pin	Note	Dati tecnici
Terra CC	1, 3		0 V CC
Ingresso	2, 4	Per comunicare con il monitoraggio porte. Input digitale o input supervisionato: collegare al pin 1 o 3 rispettivamente per attivare oppure lasciare svolazzante (scollegato) per disattivare.	Da 0 a max 30 V CC

Importante

La lunghezza certificata del cavo è massimo fino a 200 m (656 piedi) se è soddisfatto il seguente requisito del cavo: AWG 24.

Connettore relè

Due morsettiere a 4 pin da relè a forma di C che possono essere utilizzati, ad esempio, per controllare un blocco o un'interfaccia di un cancello.



Funzione	Pin	Note	Dati tecnici
Massa CC (GND)	1		0 V CC
NO	2	Normalmente aperto. Per il collegamento di relè. Collegare un blocco di protezione intrinseca tra NO e massa CC. I due pin relè sono separati con isolamento galvanico dal resto dei circuiti se i ponticelli non vengono utilizzati.	Corrente massima = 2 A per relè Tensione max. = 30 V CC
COM	3	Comune	
NC	4	Normalmente chiuso. Per il collegamento di relè. Collegare un blocco di sicurezza intrinseca tra NC e massa CC. I due pin relè sono separati con isolamento galvanico dal resto dei circuiti se i ponticelli non vengono utilizzati.	

Ponticello di alimentazione relè

Quando montato, il ponticello di alimentazione del relè si collega a 12 V CC o 24 V CC al pin COM del relè.

Può essere utilizzato per collegare un blocco tra i pin GND e NO o tra i pin GND e NC.

Sorgente di alimentazione	Potenza massima a 12 V CC[3]	Potenza massima a 24 V CC[3]
IN CC	1.600 mA	800 mA
PoE	800 mA	400 mA

AVVISO

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

3. *L'alimentazione è condivisa tra i due relè e AUX I/O 12 V CC.*

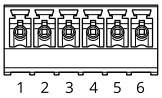
Connettore ausiliario

Utilizzare il connettore ausiliario con dispositivi esterni in combinazione con, ad esempio, rilevamento del movimento, attivazione di eventi e notifiche di allarme. Oltre al punto di riferimento 0 V CC e all'alimentazione (output CC), il connettore ausiliario fornisce l'interfaccia per:

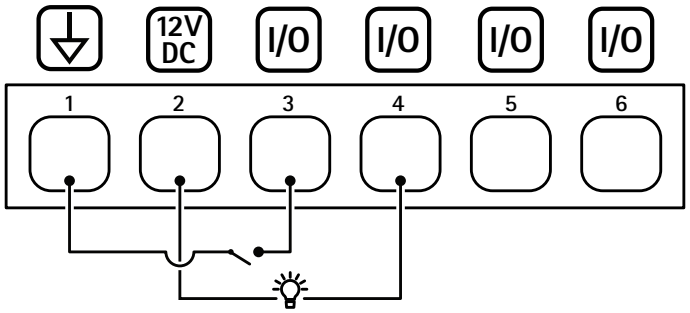
Ingresso digitale – Per il collegamento di dispositivi che possono passare da un circuito chiuso ad uno aperto, ad esempio i sensori PIR, i contatti porta/finestra e i rivelatori di rottura.

Uscita digitale – Per il collegamento di dispositivi esterni come relè e LED. I dispositivi collegati possono essere attivati tramite l'API (interfaccia per la programmazione di applicazioni) VAPIX® oppure dalla pagina Web del dispositivo.

Morsettiera a 6 pin



Funzione	Pin	Note	Dati tecnici
Terra CC	1		0 V CC
Uscita CC	2	Questo terminale può essere utilizzato anche per alimentare una periferica ausiliaria. Nota: questo pin può essere usato solo come uscita alimentazione.	12 V CC Carico max = 50 mA per ciascun I/O
Configurabile (ingresso o uscita)	3–6	Ingresso digitale - collegare al pin 1 per attivarlo oppure lasciarlo isolato (scollegato) per disattivarlo.	Da 0 a max 30 V CC
		Uscita digitale: collegato internamente al pin 1 (terra CC) quando attivo e isolato (scollegato) quando inattivo. Se utilizzata con un carico induttivo, ad esempio un relè, collegare un diodo in parallelo al carico per proteggere il dispositivo da sovratensioni. Ogni I/O è in grado di guidare 12 V CC, 50 mA (max) carico esterno, se si utilizza l'uscita interna 12 V CC (pin 2). In caso di utilizzo di connessioni di scarico aperte in combinazione con un alimentatore esterno, gli I/O possono gestire l'alimentazione CC di 0 – 30 V CC, 100 mA.	Da 0 a max 30 V CC, open-drain, 100 mA

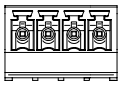


1 *Terra CC*
2 *Output CC 12 V*
3 *I/O configurato come input*
4 *I/O configurato come output*
5 *I/O configurabile*
6 *I/O configurabile*

Connettore esterno

Morsettiera a 4 pin per dispositivi esterni, ad esempio rottura vetri o rivelatori di incendio.

UL: Il connettore non è stato valutato da UL per l'uso di antifurto/allarme antincendio.



Funzione	Pin	Note	Dati tecnici
Terra CC	1, 3		0 V CC
Configurabile (ingresso o uscita)	2, 4	Uscita digitale - Collegare al pin 1 o 3 per attivare, o lasciare flottante (non connesso) per disattivare.	Da 0 a max 30 V CC
		Uscita digitale - Collegare al pin 1 o 3 per attivare, o lasciare flottante (non connesso) per disattivare. Se utilizzata con un carico induttivo, ad esempio un relè, collegare un diodo in parallelo al carico per proteggere il dispositivo da sovratensioni.	Da 0 a max 30 V CC, open-drain, 100 mA

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 uscita nominale limitata a ≤100 W o una corrente nominale di uscita limitata a ≤5 A.



Funzione	Pin	Note	Dati tecnici
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 10,5 a 28 V CC, max. 36 W

UL: L'alimentazione CC deve essere fornita da un alimentatore conforme a UL 294, UL 293 o UL 603, a seconda dell'applicazione, dotato delle classificazioni appropriate.

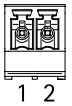
Connettore di input della batteria di backup

Per una soluzione di backup con una batteria che utilizza un caricabatterie integrato. Input 12 V CC.

UL: Il connettore non è stato valutato da UL.

Importante

Quando viene utilizzato l'input batteria, un fusibile 3 A esterno deve essere collegato in serie.



Funzione	Pin	Note	Dati tecnici
0 V CC (-)	1		0 V CC
Input batteria	2	Per alimentare il dispositivo di controllo della porta quando le altre sorgenti di alimentazione non sono disponibili. Nota: questo pin può essere utilizzato come alimentazione della batteria. Solo per il collegamento a UPS.	11– 13,7 V DC, max 36 W

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.

Interfaccia Web

Nota

Questa sezione è valida solo per AXIS A1601 Network Door Controller con AXIS Camera Station Secure Entry firmware.

: Passare da **Device settings (Impostazioni dispositivo)** alla panoramica **Analytics (Analitiche)**.

: Mostra o nascondi il menu principale.

Help (Guida): Accedere alla guida del prodotto, alle note di rilascio e alla guida sul ciclo di vita.

Informazioni:

- **About (Informazioni)**: visualizza le informazioni relative al dispositivo, compresa la versione di AXIS OS e il numero di serie.
- **Legal (Informazioni legali)**: visualizzare informazioni sui cookie e le licenze.
- **Feedback**: condividi qualsiasi feedback per contribuire a rendere migliore la tua esperienza utente.
- **Analytics data (Dati di analisi)**: acconsenti alla condivisione dei dati non personali del browser.
- **Device server report (Report del server dispositivo)**: Scarica il report del server del dispositivo.

Administrator (Amministratore):

- : Informazioni relative all'utente che ha eseguito l'accesso.
- : Modificare la lingua.
- : Imposta il tema chiaro o il tema scuro.
- **Change account (Modifica account)**: Disconnettersi dall'account corrente e accedere a un nuovo account.
- **Log out (Disconnetti)**: Disconnettersi dall'account corrente.

Stato

Stato sincronizzazione ora

Mostra le informazioni di sincronizzazione NTP, inclusa l'eventuale sincronizzazione del dispositivo con un server NTP e il tempo che rimane fino alla sincronizzazione successiva e lo stato PTP.

NTP settings (Impostazioni NTP): visualizza e aggiorna le impostazioni NTP. Conduce l'utente alla pagina **Time and location (Ora e ubicazione)** dove è possibile modificare le impostazioni NTP.

Informazioni sui dispositivi

Mostra le informazioni sul dispositivo, compresa la versione AXIS OS e il numero di serie.

Upgrade AXIS OS (Aggiorna AXIS OS): Aggiorna il software sul dispositivo. Porta l'utente sulla pagina Manutenzione dove è possibile eseguire l'aggiornamento.

Dispositivo

Allarmi

Device motion (Movimento dispositivo): Attivalo per attivare un allarme nel tuo sistema quando rileva un movimento del dispositivo.

Casing open (Apertura alloggiamento): abilitare questa opzione per far scattare un allarme nel sistema quando rileva un alloggiamento del door controller aperto. Disabilitare questa opzione per i door controller barebone.

External tamper (Manomissione esterna): abilitare questa opzione per attivare un allarme nel sistema quando rileva una manomissione esterna. Ad esempio, quando qualcuno apre e chiude l'armadietto esterno.

- **Normal state (Stato normale)**: Fare clic su  per il circuito aperto e su  per il circuito chiuso.
- **Supervised input (Input supervisionato)**: Attivare per il monitoraggio dello stato di input e la configurazione dei resistori end-of-line.
  - Per utilizzare la prima connessione parallela, selezionare **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Prima connessione parallela con un resistore parallelo da 22 KΩ E un resistore seriale da 4,7 KΩ)**.
  - Per utilizzare la prima connessione in serie, selezionare **Serial first connection (Prima connessione in serie)** e selezionare un valore dei resistori dall'elenco a discesa **Resistor values (Valori resistore)**.

Periferiche

Lettori

Add (Aggiungi) : Fare clic per aggiungere un lettore.

Lettori di rete Axis: È possibile aggiungere fino a 16 lettori Bluetooth al controller, senza necessità di licenza.

- **Nome**: inserire un nome per il lettore.
- **Lettore**: selezionare un selezionare dall'elenco a discesa.
- **Indirizzo IP**: immettere manualmente l'indirizzo IP del lettore.
- **Username (Nome utente)**: Inserire il nome utente del lettore.
- **Password**: Inserire la password del lettore.
- **Ignore server certificate verification (Ignora verifica certificato server)**: attivare per ignorare la verifica.
- **Porte I/O e relè**: Espandere per configurare le porte I/O e i relè.
  - **Port (Porta)**: Indica il nome porta.
  - **Direction (Direzione)**: Indica che si tratta di una porta di input o di output.
  - **Normal state (Stato normale)**: Fare clic su  per il circuito aperto e su  per il circuito chiuso.

Intercom di rete Axis (Necessità di riconfigurare in AXIS Camera Station)

- **Nome**: inserire un nome per il lettore.
- **Lettore**: selezionare un selezionare dall'elenco a discesa.
- **Indirizzo IP**: immettere manualmente l'indirizzo IP del lettore.
- **Username (Nome utente)**: Inserire il nome utente del lettore.
- **Password**: Inserire la password del lettore.
- **Ignore server certificate verification (Ignora verifica certificato server)**: attivare per ignorare la verifica.

AXIS License Plate Verifier (Necessaria riconfigurazione in AXIS Camera Station)

- **Nome**: inserire un nome per il lettore.
- **API key (Chiave API**: Inserire la chiave API.
- **Generate (Genera)**: Fare clic per generare la chiave API.
- **Copy API-key** (Copia chiave API): Fare clic per copiare la chiave API e salvare in un luogo sicuro.

AXIS Barcode Reader (Lettore di codici a barre AXIS) (Necessità di riconfigurare in AXIS Camera Station)

- **Nome**: inserire un nome per il lettore.
- **API key (Chiave API**: Inserire la chiave API.
- **Generate (Genera)**: Fare clic per generare la chiave API.
- **Copy API-key** (Copia chiave API): Fare clic per copiare la chiave API e salvare in un luogo sicuro.

Edit (Modifica): Selezionare un lettore e fare clic su **Edit** (Modifica) per apportare modifiche al lettore selezionato.

Elimina; Selezionare i lettori e fare clic su **Delete** (Elimina) per eliminare i lettori selezionati.

Serrature wireless

È possibile collegare fino a 16 blocchi wireless ASSA ABLOY Aperio utilizzando l'hub di comunicazione AH30. Per il blocco wireless è necessaria una licenza.

Nota

È necessario installare l'hub di comunicazione AH30 sul lato sicuro.

Connect communication hub (Connetti hub comunicazioni): Fare clic su per collegare i blocchi wireless.

Aggiornamento

Upgrade readers (Aggiorna lettori): Fare clic per aggiornare il software del lettore. È possibile solo aggiornare i lettori supportati quando sono online.

Upgrade converters (Aggiorna convertitori): Fare clic per aggiornare il software del convertitore. È possibile solo aggiornare i convertitori supportati quando sono online.

Sistema

Ora e ubicazione

Data e ora

Le impostazioni della lingua del browser Web influenzano il formato dell'ora.

Nota

Consigliamo di eseguire la sincronizzazione di data e ora del dispositivo usando un server NTP.

Synchronization (Sincronizzazione): selezionare un'opzione per la sincronizzazione di data e ora del dispositivo.

- **Automatic date and time (PTP) (Data e ora automatiche (PTP))**: Sincronizzare utilizzando il protocollo di tempo di precisione (PTP).
- **Automatic date and time (manual NTS KE servers) (Data e ora automatiche (server NTS KE manuali))**: eseguire la sincronizzazione con i server NTP key establishment sicuri connessi al server DHCP.
  - **Manual NTS KE servers (Server NTS KE manuali)**: inserisci l'indirizzo IP di uno o due server NTP. Quando usi due server NTP, l'ora del dispositivo viene sincronizzata e adattata sulla base dell'input di entrambi.
  - **Trusted NTS KE CA certificates (Certificati CA NTS KE attendibili)**: Selezionare i certificati CA attendibili da utilizzare per la sincronizzazione temporale sicura NTS KE oppure lasciare vuoto.
  - **Max NTP poll time (Tempo massimo poll NTP)**: Selezionare il tempo massimo di attesa del dispositivo prima di eseguire il polling del server NTP per ottenere un'ora aggiornata.
  - **Min NTP poll time (Tempo min poll NTP)**: Selezionare il tempo minimo di attesa del dispositivo prima di eseguire il polling del server NTP per ottenere un'ora aggiornata.
- **Automatic date and time (NTP servers using DHCP) (Data e ora automatiche (server NTP tramite DHCP))**: esegui la sincronizzazione con i server NTP connessi al server DHCP.
  - **Fallback NTP servers (Server NTP di fallback)**: inserisci l'indirizzo IP di uno o due server fallback.
  - **Max NTP poll time (Tempo massimo poll NTP)**: Selezionare il tempo massimo di attesa del dispositivo prima di eseguire il polling del server NTP per ottenere un'ora aggiornata.
  - **Min NTP poll time (Tempo min poll NTP)**: Selezionare il tempo minimo di attesa del dispositivo prima di eseguire il polling del server NTP per ottenere un'ora aggiornata.
- **Automatic date and time (manual NTP servers) (Data e ora automatiche (server NTP manuali))**: esegui la sincronizzazione con i server NTP scelti.
  - **Manual NTP servers (Server NTP manuali)**: inserisci l'indirizzo IP di uno o due server NTP. Quando usi due server NTP, l'ora del dispositivo viene sincronizzata e adattata sulla base dell'input di entrambi.
  - **Max NTP poll time (Tempo massimo poll NTP)**: Selezionare il tempo massimo di attesa del dispositivo prima di eseguire il polling del server NTP per ottenere un'ora aggiornata.
  - **Min NTP poll time (Tempo min poll NTP)**: Selezionare il tempo minimo di attesa del dispositivo prima di eseguire il polling del server NTP per ottenere un'ora aggiornata.
- **Custom date and time (Data e ora personalizzate)**: impostare manualmente la data e l'ora. Per recuperare una volta dal computer o dal dispositivo mobile le impostazioni di data e ora, fare clic su **Get from system (Ottieni dal sistema)**.

Fuso orario: selezionare il fuso orario da utilizzare. L'ora legale e l'ora solare si alterneranno automaticamente.

- **DHCP**: Adotta il fuso orario del server DHCP. Il dispositivo si deve connettere a un server DHCP (v4 o v6) prima di poter selezionare questa opzione. Se entrambe le versioni sono disponibili, il dispositivo predilige i fusi orari IANA rispetto a POSIX e DHCPv4 rispetto a DHCPv6.
  - DHCPv4 utilizza l'opzione 100 per i fusi orari POSIX e l'opzione 101 per i fusi orari IANA.
  - DHCPv6 utilizza l'opzione 41 per POSIX e l'opzione 42 per IANA.
- **Manual (Manuale)**: Selezionare un fuso orario dall'elenco a discesa.

Nota

Il sistema utilizza le impostazioni di data e ora in tutte le registrazioni, i registri e le impostazioni di sistema.

Time sync status (Stato sincronizzazione ora): Mostra le informazioni sulla sincronizzazione NTP e lo stato PTP.

Network time synchronized capture (Acquisizione sincronizzata con l'ora di rete): Attivare per consentire a più telecamere di acquisire immagini simultaneamente.

Rete

Rete

IPv4

Assign IPv4 automatically (Assegna automaticamente IPv4): Selezionare IPv4 automatico (DHCP) per consentire alla rete di assegnare automaticamente l'indirizzo IP, la subnet mask e il router, senza necessità di configurazione manuale. Si consiglia l'uso dell'assegnazione IP automatica (DHCP) per la maggior parte delle reti.

Indirizzo IP: Inserire un indirizzo IP univoco per il dispositivo. Gli indirizzi IP fissi possono essere assegnati casualmente in reti isolate, a condizione che ogni indirizzo sia univoco. Per evitare conflitti, si consiglia di contattare l'amministratore di rete prima di assegnare un indirizzo IP statico.

Subnet mask: Immetti la subnet mask per definire quali indirizzi sono all'interno della rete locale. Qualsiasi indirizzo fuori dalla rete locale passa attraverso il router.

Router: Inserire l'indirizzo IP del router predefinito (gateway) utilizzato per connettere i dispositivi collegati a reti diverse e a segmenti di rete.

Fallback to static IP address if DHCP isn't available (Fallback all'indirizzo IP fisso se DHCP non è disponibile): selezionalo se vuoi aggiungere un indirizzo IP statico da usare come fallback se DHCP non è disponibile e non è possibile assegnare in automatico un indirizzo IP.

Nota

Se DHCP non è disponibile e il dispositivo utilizza un fallback dell'indirizzo statico, l'indirizzo statico viene configurato con un ambito limitato.

IPv6

Assign IPv6 automatically (Assegna automaticamente IPv6): Selezionare questa opzione per attivare IPv6 e consentire al router di rete di assegnare automaticamente un indirizzo IP al dispositivo.

Nome host

Assign hostname automatically (Assegna automaticamente il nome host): Selezionare questa opzione per consentire al router di rete di assegnare automaticamente un nome host al dispositivo.

Nome host: Immetti manualmente il nome host da usare come metodo alternativo per accedere al dispositivo. Il report del server e il registro di sistema utilizzano il nome host. I caratteri consentiti sono A–Z, a–z, 0–9 e -.

Abilitare gli aggiornamenti DNS dinamici: Consentire al proprio dispositivo di aggiornare automaticamente le registrazioni del server dei nomi di dominio ogni volta che cambia l'indirizzo IP.

Registra nome DNS: Inserire un nome dominio univoco che punti all'indirizzo IP del dispositivo. I caratteri consentiti sono A–Z, a–z, 0–9 e -.

TTL: Time To Live (TTL) stabilisce per quanto tempo una registrazione DNS resta valida prima che debba essere aggiornata.

Server DNS

Assign DNS automatically (Assegna automaticamente DNS): Selezionare questa opzione per consentire al server DHCP di assegnare automaticamente i domini di ricerca e gli indirizzi del server DNS al dispositivo. Si consiglia il DNS automatico (DHCP) per la maggior parte delle reti.

Search domains (Domini di ricerca): Quando si utilizza un nome host non completo, fare clic su **Add search domain (Aggiungi dominio di ricerca)** e inserire un dominio in cui cercare il nome host utilizzato dal dispositivo.

DNS servers (Server DNS): Fare clic su **Add DNS server (Aggiungi server DNS)** e inserire l'indirizzo IP del server DNS. Offre la conversione dei nomi host in indirizzi IP nella rete.

Nota

Se il DHCP è disabilitato, le funzionalità che dipendono dalla configurazione automatica della rete, quali nome host, server DNS, NTP e altre, potrebbero smettere di funzionare.

HTTP e HTTPS

HTTPS è un protocollo che fornisce la crittografia per le richieste di pagine da parte di utenti e per le pagine restituite dal server Web. Lo scambio di informazioni crittografate è regolato dall'utilizzo di un certificato HTTPS, che garantisce l'autenticità del server.

Per utilizzare HTTPS nel dispositivo, è necessario installare un certificato HTTPS. Andare a **System > Security (Sistema > Sicurezza)** per creare e installare i certificati.

Allow access through (Consenti l'accesso tramite): Selezionare questa opzione se a un utente è consentito connettersi al dispositivo tramite **HTTP**, **HTTPS** o entrambi i protocolli **HTTP e HTTPS**.

Nota

Se si visualizzano pagine Web crittografate tramite HTTPS, è possibile che si verifichi un calo delle prestazioni, soprattutto quando si richiede una pagina per la prima volta.

HTTP Port (Porta HTTP): inserire la porta HTTP da utilizzare. Il dispositivo consente l'utilizzo della porta 80 o di qualsiasi porta nell'intervallo 1024-65535. Se è stato eseguito l'accesso come amministratore, è possibile immettere qualsiasi porta nell'intervallo da 1 a 1023. Se si utilizza una porta in questo intervallo, viene visualizzato un avviso.

HTTPS Port (Porta HTTPS): inserire la porta HTTPS da utilizzare. Il dispositivo consente l'utilizzo della porta 443 o di qualsiasi porta nell'intervallo 1024-65535. Se è stato eseguito l'accesso come amministratore, è possibile immettere qualsiasi porta nell'intervallo da 1 a 1023. Se si utilizza una porta in questo intervallo, viene visualizzato un avviso.

Certificato: selezionare un certificato per abilitare HTTPS per il dispositivo.

Protocolli di individuazione in rete

Bonjour®: Selezionare per consentire il rilevamento automatico sulla rete.

Nome Bonjour: Inserire un nome descrittivo che deve essere visibile sulla rete. Il nome predefinito è il nome del dispositivo e l'indirizzo MAC.

UPnP®: Selezionare per consentire il rilevamento automatico sulla rete.

UPnP name: Inserire un nome descrittivo che deve essere visibile sulla rete. Il nome predefinito è il nome del dispositivo e l'indirizzo MAC.

WS-Discovery: Selezionare per consentire il rilevamento automatico sulla rete.

LLDP e CDP: Selezionare per consentire il rilevamento automatico sulla rete. Se LLDP e CDP non sono abilitati, ciò può influire sulla negoziazione dell'alimentazione PoE. Per risolvere eventuali problemi con la negoziazione dell'alimentazione PoE, configurare lo switch PoE solo per la negoziazione dell'alimentazione PoE dell'hardware.

Confinanti: Fare clic su questa voce per visualizzare le informazioni sui dispositivi vicini connessi alla stessa rete.

Connessione al cloud con un clic

One-Click Cloud Connect (O3C), utilizzato in combinazione con un servizio O3C, offre un accesso Internet facile e sicuro a video in diretta e registrati, accessibili da qualsiasi ubicazione. Per ulteriori informazioni, vedere *axis.com/end-to-end-solutions/hosted-services*.

Allow O3C (Consenti O3C):

- **One-click**: Questa è l'opzione predefinita. Per connettersi a O3C, premere il pulsante di comando sul dispositivo. A seconda del modello di dispositivo, premere e rilasciare oppure tenere premuto, finché il LED di stato non lampeggia. Registrare il dispositivo con il servizio O3C entro 24 ore per abilitare **Always** (Sempre) e rimanere connessi. Se non si effettua la registrazione, il dispositivo si disconnette da O3C.
- **Sempre**: Il dispositivo tenta continuamente di collegarsi a un servizio O3C via Internet. Una volta registrato il dispositivo, questo rimane connesso. Utilizzare questa opzione se il pulsante di comando non è disponibile.
- **No**: Disabilita il servizio O3C.

Proxy settings (Impostazioni proxy): Se necessario, inserire le impostazioni proxy per collegarsi al server proxy.

Host: Inserire l'indirizzo del server del proxy.

Port (Porta): inserire il numero della porta utilizzata per l'accesso.

Accesso e **Password**: se necessario, immettere un nome utente e una password per il server proxy.

Metodo di autenticazione:

- **Base**: questo metodo è lo schema di autenticazione maggiormente compatibile per HTTP. È meno sicuro del metodo **Digest** perché invia il nome utente e la password non crittografati al server.
- **Digest**: questo metodo è più sicuro perché la password viene sempre trasferita crittografata nella rete.
- **Automatico**: questa opzione consente al dispositivo Axis di selezionare il metodo di autenticazione a seconda dei metodi supportati, dando priorità a **Digest** rispetto al metodo **Base**.

Owner authentication key (OAK) (Chiave di autenticazione proprietario (OAK): Fare clic su **Get key (Ottieni chiave)** per recuperare la chiave di autenticazione proprietaria. Questo è possibile solo se il dispositivo è connesso a Internet senza un firewall o un proxy.

SNMP

SNMP (Simple Network Management Protocol) consente il monitoraggio e la gestione in remoto dei dispositivi di rete.

SNMP: Selezionare la versione di SNMP da utilizzare.

- **v1 and v2c (v1 e v2c)**:
  - **Read community (Comunità con privilegi in lettura)**: Inserire il nome della comunità che dispone solo dell'accesso in lettura a tutti gli oggetti SNMP supportati. Il valore predefinito è **public**.
  - **Write community (Comunità con privilegi in scrittura)**: Specificare il nome della comunità che dispone di accesso in lettura o scrittura a tutti gli oggetti SNMP supportati (ad eccezione degli oggetti in sola lettura). Il valore predefinito è **write**.
  - **Activate traps (Attiva trap)**: Attivare la segnalazione di trap. Il dispositivo utilizza i trap per inviare messaggi per eventi importanti o cambi di stato a un sistema di gestione. Nell'interfaccia Web, è possibile impostare trap per SNMP v1 e v2c. I trap vengono disattivati automaticamente se si cambia in SNMP v3 o si disattiva SNMP. Se si utilizza SNMP v3, è possibile impostare i trap tramite l'applicazione di gestione SNMP v3.
  - **Trap address (Indirizzo trap)**: immettere l'indirizzo IP o il nome host del server di gestione.
  - **Trap community (Comunità trap)**: Immettere la comunità da utilizzare quando il dispositivo invia un messaggio trap al sistema di gestione.
  - **Traps (Trap)**:
    - **Cold start (Avvio a freddo)**: Invia un messaggio di trap all'avvio del dispositivo.
    - **Link up**: invia un messaggio trap quando un collegamento cambia dal basso verso l'alto.
    - **Link down (Collegamento in basso)**: invia un messaggio trap quando un collegamento passa dall'alto al basso.
    - **Autenticazione non riuscita**: invia un messaggio trap quando un tentativo di autenticazione non riesce.

Nota

Tutti i trap Axis Video MIB vengono abilitati quando si attivano i trap SNMP v1 e v2c. Per ulteriori informazioni, vedere *AXIS OS Portal > SNMP (Poortale sistema operativo AXIS > SNMP)*.

- **v3**: SNMP v3 è una versione più sicura che fornisce crittografia e password sicure. Per utilizzare SNMP v3, si consiglia di attivare HTTPS poiché la password verrà successivamente inviata via HTTPS. Ciò impedisce inoltre alle parti non autorizzate di accedere ai trap SNMP v1 e v2c non crittografati. Se si utilizza SNMP v3, è possibile impostare i trap tramite l'applicazione di gestione SNMP v3.
  - **Privacy**: Selezionare la crittografia da utilizzare per proteggere i dati SNMP.
  - **Password for the account "initial" (Password per l'account "iniziale")**: Immettere la password SNMP per l'account denominato "iniziale". Sebbene la password possa essere inviata senza attivare HTTPS, non è consigliabile. La password SNMP v3 può essere impostare solo una volta e preferibilmente solo quando è attivato HTTPS. Una volta impostata la password, il relativo campo non verrà più visualizzato. Per impostare di nuovo la password, il dispositivo deve essere ripristinato alle impostazioni predefinite di fabbrica. Notare che la password deve essere conforme alla politica sulle password, vedere *Account, on page 62*.

Clienti collegati

Mostra il numero di connessioni e client connessi.

View details (Visualizza dettagli): Consente di visualizzare e aggiornare l'elenco dei client connessi. L'elenco mostra l'indirizzo IP, il protocollo, la porta, lo stato e il PID/processo di ogni connessione.

Sicurezza

Certificati

I certificati sono utilizzati per autenticare i dispositivi in una rete. I tipi di certificati supportati da questo dispositivo sono due:

- **Client/server certificates (Certificati client/server)**
  Un certificato client/server convalida l'identità del dispositivo e può essere autofirmato o emesso 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 dell'autorità di certificazione**
  È possibile utilizzare un certificato CA per autenticare un certificato peer, ad esempio per convalidare l'identità di un server di autenticazione nel caso in cui il dispositivo venga collegato a una rete protetta da IEEE 802.1X. Il dispositivo dispone di diversi certificati CA preinstallati.

Questi formati sono supportati:

- Formati certificato.PEM, .CER e.PFX
- Formati delle chiavi private: PKCS#1 e PKCS#12

Importante

Se il dispositivo viene ripristinato alle impostazione di fabbrica, tutti i certificati vengono eliminati. Qualsiasi certificato CA preinstallato viene reinstallato.

Add certificate (Aggiungi certificato): fare clic sull'opzione per aggiungere un certificato. Si apre una guida passo dopo passo.

- **More (Altri)** : mostra altri campi da compilare o selezionare.
- **Secure keystore (Archivio chiavi sicuro)**: selezionare questa opzione per utilizzare **Trusted Execution Environment (SoC TEE)**, **Secure Element** o **Trusted Platform Module 2.0** per archiviare in modo sicuro la chiave privata. Per ulteriori informazioni su quale keystore sicuro selezionare, andare a *help.axis.com/axis-os#cryptographic-support*.
- **Key type (Tipo chiave)**: selezionare l'algoritmo di crittografia predefinito o diverso dall'elenco a discesa per proteggere il certificato.

Il menu contestuale contiene:

- **Certificate information (Informazioni certificato)**: visualizza le proprietà di un certificato installato.
- **Delete certificate (Elimina certificato)**: Elimina il certificato.
- **Create certificate signing request (Crea richiesta di firma certificato)**: Per fare richiesta di un certificato di identità digitale, crea una richiesta di firma del certificato da mandare a un'autorità di registrazione.

Secure keystore (Archivio chiavi sicuro):

- **Trusted Execution Environment (SoC TEE) (Ambito di esecuzione attendibile)**: Selezionare questa opzione per utilizzare SoC TEE per il keystore sicuro.
- **Secure element (Elemento sicuro) (CC EAL6+, FIPS 140-3 Level 3)**: Selezionare questa opzione per utilizzare un elemento sicuro per l'archivio chiavi sicuro.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Level 2)** Selezionare questa opzione per utilizzare TPM 2.0 per il keystore sicuro.

Controllo degli accessi di rete e crittografia

IEEE 802.1x

IEEE 802.1x è uno standard IEEE 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 802.1x, i dispositivi di rete devono autenticarsi. L'autenticazione viene eseguita da un server di autenticazione, generalmente un server RADIUS (ad esempio FreeRADIUS e Microsoft Internet Authentication Server).

IEEE 802.1AE MACsec

IEEE 802.1AE MACsec rappresenta uno standard IEEE per la sicurezza MAC (Media Access Control) che definisce la riservatezza e l'integrità dati senza connessione per i protocolli indipendenti di accesso ai media.

Certificati

Se configurato senza un certificato CA, la convalida del certificato del server verrà disabilitata e il dispositivo cercherà in questo caso di autenticarsi a prescindere dalla rete a cui è connesso.

Nell'implementazione di Axis, quando si utilizza un certificato, il dispositivo e il server di autenticazione si autenticano con certificati digitali mediante EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).

Per consentire al dispositivo di accedere a una rete protetta tramite certificati, è necessario installare un certificato client firmato sul dispositivo.

Metodo di autenticazione: selezionare un tipo EAP impiegato per l'autenticazione.

Client Certificate (Certificato client): selezionare un certificato client per utilizzare IEEE 802.1x. Il server di autenticazione utilizza il certificato per convalidare l'identità del client.

CA Certificates (Certificati CA): selezionare i certificati CA per convalidare l'identità del server di autenticazione. Quando non ne viene selezionato nessun certificato, il dispositivo tenterà di autenticarsi a prescindere dalla rete a cui è connesso.

EAP identity (Identità EAP): Immettere l'identità utente associata al certificato del client.

EAPOL version (Versione EAPOL): Selezionare la versione EAPOL utilizzata nello switch di rete.

Use IEEE 802.1x (Usa IEEE 802.1x): Selezionare questa opzione per utilizzare il protocollo IEEE 802.1x.

Le impostazioni sono a disposizione solo se si usa **IEEE 802.1x PEAP-MSCHAPv2** come metodo di autenticazione:

- **Password**: immettere la password per l'identità utente.
- **Peap version (Versione Peap)**: selezionare la versione Peap utilizzata nello switch di rete.
- **Label (Etichetta)**: Selezionare 1 per utilizzare la codifica EAP del client; selezionare 2 per utilizzare la crittografia PEAP del client. Selezionare l'etichetta usata dallo switch di rete quando si utilizza Peap versione 1.

Le impostazioni sono a disposizione solo se si usa **IEEE 802.1ae MACsec (chiave Static CAK/Pre-Shared)** come metodo di autenticazione:

- **Key agreement connectivity association key name (Nome della chiave di associazione della connettività del contratto chiave)**: immettere il nome dell'associazione della connettività (CKN). Deve essere composto da 2 a 64 caratteri esadecimali (divisibili per 2). Il CKN deve essere configurato manualmente nell'associazione della connettività e deve corrispondere su entrambe le estremità del collegamento per abilitare inizialmente MACsec.
- **Key agreement connectivity association key (Chiave di associazione della connettività del contratto chiave)**: immettere la chiave di associazione della connettività (CAK). Deve essere composta da 32 o 64 caratteri esadecimali. Il CAK deve essere configurato manualmente nell'associazione della

connettività e deve corrispondere su entrambe le estremità del collegamento per abilitare inizialmente MACsec.

Prevenire gli attacchi di forza bruta

Blocking (Blocco): Attiva per bloccare gli attacchi di forza bruta. Un attacco di forza bruta usa tentativi ed errori per indovinare le informazioni di accesso o le chiavi di crittografia.

Blocking period (Periodo di blocco): Immettere il numero di secondi per cui si blocca un attacco di forza bruta.

Blocking conditions (Condizioni di blocco): Immettere il numero di errori di autenticazione consentiti al secondo prima dell'inizio del blocco. È possibile impostare il numero di errori consentiti a livello di pagina e di dispositivo.

Firewall

Firewall (Firewall): Attivare per abilitare il firewall.

Default Policy (Criterio predefinito): Selezionare come si desidera che il firewall gestisca le richieste di connessione non coperte da regole.

- **ACCEPT:** (ACCETTA) Permette tutte le connessioni al dispositivo. Questa opzione è impostata per impostazione predefinita.
- **DROP (BLOCCA):** Blocca tutte le connessioni al dispositivo.

Per eccezioni al criterio predefinito, si può eseguire la creazione di regole che permettono o bloccano le connessioni al dispositivo da indirizzi, protocolli e porte specifici.

+ New rule (+ Nuova regola): Fare clic per la creazione di una regola.

Rule type (Tipo di regola):

- **FILTRO**: Selezionare per consentire o bloccare le connessioni dai dispositivi che corrispondono ai criteri definiti nella regola.
  - **Policy (Criteri)**: Selezionare **Accept (Accetta)** o **Drop (Blocca)** per la regola del firewall.
  - **IP range (Intervallo IP)**: Selezionare per specificare un intervallo di indirizzi da abilitare o bloccare. Utilizzare IPv4/IPv6 in **Start (Inizio)** e **End (Fine)**.
  - **Indirizzo IP**: Immettere l'indirizzo che si desidera abilitare o bloccare. Usare il formato IPv4/IPv6 o CIDR.
  - **Protocol (Protocollo)**: Selezionare un protocollo di rete (TCP, UDP o entrambi) da consentire o bloccare. Se si seleziona un protocollo, è necessario specificare anche una porta.
  - **MAC**: Inserire l'indirizzo MAC di un dispositivo che si desidera abilitare o bloccare.
  - **Intervallo porta**: Selezionare per specificare l'intervallo di porte da abilitare o bloccare. Aggiungerlo in **Start (Inizio)** e **End (Fine)**.
  - **Port (Porta)**: Immettere il numero di porta che si desidera abilitare o bloccare. I numeri di porta devono essere compresi tra 1 e 65535.
  - **Traffic type (Tipo di traffico)**: Selezionare il tipo di traffico che si desidera abilitare o bloccare.
    - **UNICAST**: Traffico da un singolo mittente a un singolo destinatario.
    - **BROADCAST (TRASMISSIONE)**: Traffico da un singolo mittente a tutti i dispositivi della rete.
    - **MULTICAST**: Traffico da uno o più mittenti a uno o più destinatari.
- **LIMIT (LIMITA)**: Selezionare per accettare le connessioni dai dispositivi che soddisfano i criteri definiti nella regola, ma applicare dei limiti per ridurre il traffico eccessivo.
  - **IP range (Intervallo IP)**: Selezionare per specificare un intervallo di indirizzi da abilitare o bloccare. Utilizzare IPv4/IPv6 in **Start (Inizio)** e **End (Fine)**.
  - **Indirizzo IP**: Immettere l'indirizzo che si desidera abilitare o bloccare. Usare il formato IPv4/IPv6 o CIDR.
  - **Protocol (Protocollo)**: Selezionare un protocollo di rete (TCP, UDP o entrambi) da consentire o bloccare. Se si seleziona un protocollo, è necessario specificare anche una porta.
  - **MAC**: Inserire l'indirizzo MAC di un dispositivo che si desidera abilitare o bloccare.
  - **Intervallo porta**: Selezionare per specificare l'intervallo di porte da abilitare o bloccare. Aggiungerlo in **Start (Inizio)** e **End (Fine)**.
  - **Port (Porta)**: Immettere il numero di porta che si desidera abilitare o bloccare. I numeri di porta devono essere compresi tra 1 e 65535.
  - **Unit (Unità)**: Selezionare il tipo di connessioni da abilitare o bloccare.
  - **Period (Periodo)**: Selezionare il periodo di tempo relativo ad **Amount (Quantità)**.
  - **Amount (Quantità)**: Configurare il numero massimo di volte in cui un dispositivo è autorizzato a connettersi entro il **Period** (Periodo) impostato. La quantità massima è 65535.

- **Burst (Eccezione)**: Immettere il numero di connessioni che possono superare la **Amount (Quantità)** una volta durante il **Period (periodo)** impostato. Una volta raggiunto il numero, è consentita solo la quantità impostata durante il periodo stabilito.
- **Traffic type (Tipo di traffico)**: Selezionare il tipo di traffico che si desidera abilitare o bloccare.
  - **UNICAST**: Traffico da un singolo mittente a un singolo destinatario.
  - **BROADCAST (TRASMISSIONE)**: Traffico da un singolo mittente a tutti i dispositivi della rete.
  - **MULTICAST**: Traffico da uno o più mittenti a uno o più destinatari.

Test rules (Testa regole): Fare clic per testare le regole definite.

- **Time in seconds: (Tempo di test in secondi)**: Impostare un limite di tempo al fine di mettere alla prova le regole.
- **Roll back**: Fare clic per riportare il firewall allo stato precedente, prima di aver testato le regole.
- **Apply rules (Applica regole)**: Fare clic su per attivare le regole senza eseguire il test. Si sconsiglia questa procedura.

Certificato AXIS OS con firma personalizzata

Serve un certificato AXIS OS con firma personalizzata per l'installazione di software di prova o software personalizzato di altro tipo di Axis sul dispositivo. Il certificato verifica che il software è stato approvato sia dal proprietario del dispositivo che da Axis. Il software può essere eseguito solo su un dispositivo specifico, identificato da un numero di serie univoco e da un chip ID. Solo Axis può creare certificati AXIS OS firmati in modo personalizzato, poiché possiede la chiave per la firma.

Install (Installa): Fare clic per eseguire l'installazione del certificato. Il certificato deve essere installato prima del software.

Il menu contestuale contiene:

- **Delete certificate (Elimina certificato)**: Elimina il certificato.

Account

Account dispositivo

Account

Add account (Aggiungi account): Fare clic per aggiungere un nuovo account. Puoi aggiungere un massimo di 100 account.

Account: Inserire un nome account univoco.

New password (Nuova password): inserire una password per l'account. La lunghezza delle password deve essere compresa tra 1 e 64 caratteri. La password può contenere solo caratteri ASCII stampabili (codice da 32 a 126), quali lettere, numeri, segni di punteggiatura e alcuni simboli.

Repeat password (Ripeti password): immettere di nuovo la stessa password.

Privileges (Privilegi):

- **Administrator (Amministratore)**: ha accesso completo a tutte le impostazioni. Gli amministratori possono anche aggiungere, aggiornare e rimuovere altri account.
- **Operator (Operatore)**: ha accesso a tutte le impostazioni ad eccezione di:
  - Tutte le impostazioni **System (Sistema)**.
- **Viewer (Visualizzatore)**: non ha l'accesso alla modifica di alcuna impostazioni.

Il menu contestuale contiene:

Update account (Aggiorna account): Modifica le proprietà dell'account.

Delete account (Elimina account): Elimina l'account. Non puoi cancellare l'account root.

MQTT

MQTT (Message Queuing Telemetry Transport) è un protocollo di messaggistica standard per l'Internet of Things (IoT). È stato progettato per un'integrazione IoT semplificata ed è utilizzato in numerosi settori per connettere dispositivi remoti con un'impronta di codice ridotta e una larghezza di banda minima in rete. Il client MQTT nel software del dispositivo Axis può semplificare l'integrazione di dati ed eventi prodotti nel dispositivo con sistemi che non sono software per la gestione video (VMS).

Configurare il dispositivo come client MQTT. La comunicazione MQTT si basa su due entità, i client e il broker. I client possono inviare e ricevere messaggi. Il broker è responsabile del routing dei messaggi tra i client.

Per maggiori informazioni relative a MQTT consultare l'*AXIS OS Knowledge base*.

ALPN (RETE ALPN)

ALPN è un'estensione TLS/SSL che consente la selezione di un protocollo applicativo durante la fase di handshake della connessione tra client e server. Viene utilizzato per abilitare il traffico MQTT sulla stessa porta utilizzata per altri protocolli, ad esempio HTTP. In alcuni casi, potrebbe non esserci una porta dedicata aperta per la comunicazione MQTT. Una soluzione in tali casi consiste nell'utilizzare ALPN per trattare l'uso di MQTT come protocollo applicativo su una porta standard, consentito dai firewall.

Client MQTT

Connect (Connetti): Attivare o disattivare il client MQTT.

Status (Stato): Visualizza lo stato corrente del client MQTT.

Broker

Host: immettere il nome host o l'indirizzo IP del server MQTT.

Protocol (Protocollo): selezionare il protocollo da utilizzare.

Port (Porta): Immettere il numero di porta.

- 1883 è il valore predefinito per **MQTT over TCP (MQTT su TCP)**
- 8883 è il valore predefinito per **MQTT su SSL**
- 80 è il valore predefinito per **MQTT su WebSocket**
- 443 è il valore predefinito per **MQTT su WebSocket Secure**

ALPN protocol (Protocollo ALPN): Inserire il nome del protocollo ALPN fornito dal provider MQTT. Ciò è applicabile solo con MQTT over SSL e MQTT over WebSocket Secure.

Username (Nome utente): inserire il nome utente che il client utilizzerà per accedere al server.

Password: immettere una password per il nome utente.

Client ID (ID client): Immettere un ID client. L'identificativo del client viene inviato al server quando il client si connette.

Clean session (Sessione pulita): Controlla il comportamento al momento della connessione e della disconnessione. Se selezionate, le informazioni sullo stato vengono ignorate al momento della connessione e della disconnessione.

HTTP proxy (proxy HTTP): Un URL dotato di una lunghezza non superiore a 255 byte. È possibile lasciare il campo vuoto se non si vuole usare un proxy HTTP.

HTTPS proxy (proxy HTTPS): Un URL dotato di una lunghezza non superiore a 255 byte. È possibile lasciare il campo vuoto se non si vuole usare un proxy HTTPS.

Keep alive interval (Intervallo keep alive): Consente al client di rilevare quando il server non è più disponibile senza dover attendere il lungo tempo di timeout TCP/IP.

Timeout: L'intervallo di tempo in secondi per consentire il completamento di una connessione. Valore predefinito: 60

Device topic prefix (Prefisso argomento dispositivo): utilizzato nei valori predefiniti per l'argomento nel messaggio di connessione e nel messaggio Ultime volontà e testamento nella scheda **MQTT client (Client MQTT)** e nelle condizioni di pubblicazione nella scheda **MQTT publication (Pubblicazione MQTT)**.

Reconnect automatically (Riconnetti automaticamente): specifica se il client deve riconnettersi automaticamente dopo una disconnessione.

Messaggio connessione

Specifica se un messaggio deve essere inviato quando viene stabilita una connessione.

Send message (Invia messaggio): Attivare per inviare messaggi.

Use default (Usa predefinito): Disattivare per immettere un messaggio predefinito.

Topic (Argomento): Immettere l'argomento per il messaggio predefinito.

Payload: Immettere il contenuto per il messaggio predefinito.

Retain (Conserva): Selezionare questa opzione per mantenere lo stato del client su questo **Topic (Argomento)**

QoS: Cambiare il livello QoS per il flusso di pacchetti.

Messaggio di ultime volontà e testamento

Ultime volontà e testamento consente a un client di fornire un testamento insieme alle proprie credenziali quando si collega al broker. Se il client si disconnette in modo anomalo in un secondo momento (forse perché la sua sorgente di alimentazione non funziona), può lasciare che il broker recapiti un messaggio ad altri client. Questo messaggio Ultime volontà e testamento ha lo stesso formato di un messaggio ordinario e viene instradato tramite la stessa meccanica.

Send message (Invia messaggio): Attivare per inviare messaggi.

Use default (Usa predefinito): Disattivare per immettere un messaggio predefinito.

Topic (Argomento): Immettere l'argomento per il messaggio predefinito.

Payload: Immettere il contenuto per il messaggio predefinito.

Retain (Conserva): Selezionare questa opzione per mantenere lo stato del client su questo **Topic (Argomento)**

QoS: Cambiare il livello QoS per il flusso di pacchetti.

Pubblicazione MQTT

Use default topic prefix (Usa prefisso di argomento predefinito): Selezionare questa opzione per usare il prefisso dell'argomento predefinito, definito nel prefisso argomento dispositivo nella scheda **MQTT client (Client MQTT)**.

Include condition (Includi condizione): selezionare questa opzione per l'inclusione dell'argomento che illustra la condizione nell'argomento MQTT.

Include namespaces (Includi spazi dei nomi): Selezionare questa opzione per includere gli spazi dei nomi degli argomenti di ONVIF nell'argomento MQTT.

Include serial number (Includi numero di serie): selezionare questa opzione per comprendere il numero di serie del dispositivo nel payload MQTT.

Add condition (Aggiungi condizione): fare clic sull'opzione per aggiungere una condizione.

Retain (Conserva): definire quali messaggi MQTT sono inviati come conservati.

- **None (Nessuno)**: inviare tutti i messaggi come non conservati.
- **Property (Proprietà)**: inviare solo messaggi con stato conservati.
- **All (Tutto)**: Invia messaggi sia con che senza stato come conservati.

QoS: Seleziona il livello desiderato per la pubblicazione MQTT.

Sottoscrizioni MQTT

Add subscription (Aggiungi abbonamento): Fai clic per aggiungere una nuova sottoscrizione MQTT.

Subscription filter (Filtro sottoscrizione): Inserisci l'argomento MQTT per il quale desideri eseguire la sottoscrizione.

Nota

Se si modifica al filtro di sottoscrizione, è necessario aggiornare gli eventi collegati.

Use device topic prefix (Usa prefisso argomento dispositivo): Aggiungi il filtro sottoscrizione come prefisso all'argomento MQTT.

Subscription type (Tipo di sottoscrizione):

- **Stateless (Privo di stato)**: Seleziona per convertire i messaggi MQTT in messaggi senza stato.
- **Stateful (Dotato di stato)**: Seleziona per convertire i messaggi MQTT in una condizione. Il payload è usato come stato.

QoS: Seleziona il livello desiderato per la sottoscrizione MQTT.

Accessori

Porte I/O

Utilizzare l'input digitale per collegare i dispositivi esterni che possono passare da un circuito aperto a un circuito chiuso, ad esempio i sensori PIR, i contatti porta o finestra e i rivelatori di rottura del vetro.

Utilizzare l'uscita digitale per collegare dispositivi esterni come relè e LED. È possibile attivare i dispositivi collegati tramite l'API VAPIX® o l'interfaccia Web.

Porta

Nome: modificare il testo per rinominare la porta.

Direction (Direzione):  indica che la porta è una porta di ingresso.  indica che si tratta di una porta di uscita. Se la porta è configurabile, è possibile fare clic sulle icone per passare dall'input all'output.

Normal state (Stato normale): Fare clic su  per il circuito aperto e su  per il circuito chiuso.

Current State (Stato corrente): indica lo stato attuale della porta. L'input e l'output vengono attivati quando lo stato corrente è diverso dallo stato normale. Un input sul dispositivo ha un circuito aperto se disconnesso o in caso di tensione superiore a 1 V CC.

Nota

Durante il riavvio, il circuito di output è aperto. Al completamento del riavvio, il circuito torna alla posizione normale. Se si modificano le impostazioni in questa pagina, i circuiti di output tornano alle relative posizioni normali, indipendentemente dai trigger attivi.

Supervised (Supervisionato): Attivare per rendere possibile il rilevamento e l'attivazione di azioni se qualcuno manomette la connessione ai dispositivi I/O digitali. Oltre a rilevare se un ingresso è aperto o chiuso, è anche possibile rilevare se qualcuno l'ha manomesso (ovvero se è stato tagliato o corto). Per supervisionare la connessione è necessario un ulteriore hardware (resistori terminali) nel loop I/O esterno.

Registri

Report e registri

Report

- **View the device server report (Visualizza il report del server del dispositivo)**: Visualizzare informazioni sullo stato del dispositivo in una finestra pop-up. Il registro degli accessi viene automaticamente incluso nel report del server.
- **Download the device server report (Scarica il report del server del dispositivo)**: Crea un file .zip contenente un file di testo del report del server completo in formato UTF-8. Per includere l'istantanea dell'immagine corrente della visualizzazione in diretta, selezionare **Include image** (Includi immagine). Includere sempre il file .zip del report del server quando si contatta l'assistenza.
- **Download the crash report (Scarica il report dell'arresto anomalo)**: Scaricare un archivio con le informazioni dettagliate sullo stato del server. Il report di arresto anomalo contiene le informazioni presenti nel report del server e le informazioni dettagliate sul debug. Questo report potrebbe contenere informazioni riservate, ad esempio l'analisi della rete. Possono volerci alcuni minuti per generare il report.

Registri

- **View the system log (Visualizza il registro di sistema)**: Fare clic per visualizzare le informazioni sugli eventi di sistema come l'avvio del dispositivo, gli avvisi e i messaggi critici.
- **View the access log (Visualizza il registro degli accessi)**: Fare clic per mostrare tutti i tentativi non riusciti di accedere al dispositivo, ad esempio quando si utilizza una password di accesso errata.
- **View the audit log (Visualizza il registro audit)**: Fare clic su per visualizzare le informazioni relative alle attività utente e di sistema, ad esempio autenticazioni e configurazioni riuscite o fallite.

Analisi della rete

Importante

È possibile che un file di analisi della rete contenga informazioni riservate, ad esempio certificati o password.

Un file di analisi della rete può facilitare la risoluzione dei problemi registrando l'attività sulla rete.

Trace time (Tempo di analisi): Selezionare la durata dell'analisi in secondi o minuti e fare clic su **Download**.

Registro di sistema remoto

Syslog è uno standard per la registrazione dei messaggi. Consente di separare il software che genera messaggi, il sistema che li archivia e il software che li riporta e li analizza. Ogni messaggio è contrassegnato con un codice struttura che indica il tipo di software che genera il messaggio. Inoltre viene assegnato un livello di gravità a tutti i messaggi.



Server: Fare clic per aggiungere un nuovo server.

Host: immettere il nome host o l'indirizzo IP del server proxy.

Format (Formatta): selezionare il formato del messaggio syslog da utilizzare.

- Axis
- RFC 3164
- RFC 5424

Protocol (Protocollo): Selezionare il protocollo da utilizzare:

- UDP (la porta predefinita è 514)
- TCP (la porta predefinita è 601)
- TLS (la porta predefinita è 6514)

Port (Porta): Cambiare il numero di porta per impiegare una porta diversa.

Severity (Gravità): Seleziona quali messaggi inviare al momento dell'attivazione.

Tipo: Selezionare il tipo di log che si desidera inviare.

Test server setup (Test della configurazione del server): Inviare un messaggio di prova a tutti i server prima di salvare le impostazioni.

CA certificate set (Certificato CA impostato): Visualizza le impostazioni correnti o aggiungi un certificato.

Manutenzione

Restart (Riavvia): Riavviare il dispositivo. Non avrà effetti su nessuna delle impostazioni correnti. Le applicazioni in esecuzione verranno riavviate automaticamente.

Restore (Ripristina): Riporta la maggior parte delle impostazioni ai valori predefiniti di fabbrica. In seguito dovrai riconfigurare il dispositivo e le app, reinstallare tutte le app non preinstallate e ricreare eventuali eventi e preset.

Importante

Dopo il ripristino, le uniche impostazioni salvate sono:

- Protocollo di avvio (DHCP o statico)
- Indirizzo IP statico
- Router predefinito
- Subnet mask
- Impostazioni 802.1X
- Impostazioni O3C
- Indirizzo IP server DNS

Factory default (Valori predefiniti di fabbrica): Riporta tutte le impostazioni ai valori predefiniti di fabbrica. Dopo, per rendere accessibile il dispositivo, devi reimpostare l'indirizzo IP.

Nota

Tutti i software per dispositivi Axis sono firmati digitalmente per assicurare di installare solo software verificato sul dispositivo. Ciò aumenta ulteriormente il livello di sicurezza informatica minimo globale dei dispositivi Axis. Per ulteriori informazioni, visitare il white paper "Axis Edge Vault" su *axis.com*.

AXIS OS upgrade (Aggiornamento di AXIS OS): Aggiorna a una versione nuova di AXIS OS. nuove versioni possono contenere funzionalità migliorate, correzioni di bug e funzionalità completamente nuove. Si consiglia di utilizzare sempre l'ultima versione di AXIS OS. Per scaricare l'ultima versione, andare a *axis.com/support*.

Quando conduci l'aggiornamento, puoi scegliere fra tre opzioni:

- **Standard upgrade (Aggiornamento standard)**: Aggiorna a una nuova versione di AXIS OS.
- **Factory default (Valori predefiniti di fabbrica)**: Aggiorna e riporta tutte le impostazioni ai valori predefiniti di fabbrica. Se selezioni questa opzione, dopo l'aggiornamento non puoi eseguire il ripristino della versione precedente di AXIS OS.
- **Rollback automatico**: Aggiorna e conferma l'aggiornamento entro il tempo impostato. Se non dai la conferma, il dispositivo tornerà alla precedente versione di AXIS OS.

AXIS OS rollback (Rollback AXIS OS): Eseguire il ripristino alla versione di AXIS OS installata precedentemente.

T10125657_it

2026-09 (M15.3)

© 2018 – 2026 Axis Communications AB