

AXIS Camera Station S1232 Tower Recording Server

Indice

Informazioni sul dispositivo	4
Impostazioni preliminari	5
Installare il dispositivo.....	6
Operazioni preliminari all'installazione	6
Configurare il dispositivo	7
Configurazione iniziale del registratore Axis.....	7
Configurazione di AXIS Camera Station Pro.....	7
Avviare il video management system	8
Aggiunta di dispositivi.....	8
Configura metodo di registrazione.....	8
Visualizzazione del video in diretta	8
Visualizzazioni registrate	8
Aggiunta di segnalibri	8
Esportazione delle registrazioni.....	9
Riproduzione e verifica delle registrazioni in AXIS File Player.....	9
Configurazione di rete.....	9
Configurazione della porta del server.....	10
Considerazioni sulla protezione.....	10
Ottenimento di una licenza per un sistema online.....	10
Ottenimento di una licenza per un sistema offline	10
Gestire gli account utente di Windows® locali	12
Creare un account utente.....	12
Crea un account amministratore.....	12
Creare un gruppo di utenti locale.....	12
Eliminare un account utente	12
Modificare la password di un account utente	13
Creare un disco di reimpostazione della password per un account utente.....	13
Gestire gli account utente di AXIS Camera Station Pro.....	14
Autorizzazioni utente	14
Aggiunta di utenti o gruppi	14
Privilegi utente o di gruppo	15
Gestire il dispositivo.....	18
Aggiornare i certificati Secure Boot.....	18
Verificare lo stato del certificato	18
Azioni consigliate	19
Aggiornare il certificato tramite il BIOS.....	19
Aggiornare il certificato tramite Windows Update.....	19
Controllo della versione corrente del BIOS.....	19
Aggiornare il BIOS.....	19
Aggiornare Windows®	20
Configurazione delle impostazioni di Windows® Update.....	20
Aggiunta di un disco rigido.....	21
Flusso di lavoro	21
Installa un disco rigido hot-swap	21
Modifica del RAID.....	22
Crea un nuovo array RAID.....	23
Configura Microsoft Windows®.....	24
Configurazione di iDRAC.....	25
Cyber security.....	26
Secure Boot	26
Trusted Platform Module (TPM).....	26
Servizio di notifica di sicurezza Axis	26
Gestione delle vulnerabilità	26

Funzionamento sicuro dei dispositivi Axis.....	26
Risoluzione dei problemi.....	27
Esecuzione della diagnostica	27
Eseguire un ripristino del sistema.....	27
Ripristino interno	27
Ripristino esterno	27
Esportazione di una raccolta SupportAssist	28
Risoluzione dei problemi relativi all'unità di alimentazione	29
Risoluzione dei problemi relativi agli errori di memoria	29
Risoluzione di problemi per AXIS Camera Station Pro	29
Panoramica dei prodotti	30
Parte anteriore e posteriore	30
Dati tecnici.....	31
.....	31
Bisogno di assistenza?.....	34
Link utili.....	34
Contattare l'assistenza.....	34

Informazioni sul dispositivo

La serie AXIS Camera Station S12 Recorder comprende server rack e stazioni di lavoro già predisposte per l'uso omologati per una sorveglianza affidabile ad alta definizione fino a 4K. Per un'installazione rapida e semplice, la serie di registratori è preconfigurata e precaricata con il software per la gestione di video AXIS Camera Station Pro, comprendente le licenze e tutto il software di sistema necessario. La configurazione di sistema può essere importata facilmente da AXIS Site Designer e AXIS Camera Station Pro consente di trarre vantaggio dall'ampia gamma di dispositivi di sorveglianza video di Axis. Con dischi rigidi di livello Enterprise, sistema operativo memorizzato su unità SSD, la serie di registratori offre elevate prestazioni e alta affidabilità per il sistema.

Impostazioni preliminari

Il flusso di lavoro standard per configurare un server di registrazione AXIS Camera Station Pro è:

1. *Installare il dispositivo.*
2. Configurazione iniziale di Windows®: Dopo aver installato il dispositivo, la configurazione guidata consentirà l'impostazione di regione, lingua, layout della tastiera, account amministratore e relativa password.
3. Configurazione iniziale del registratore Axis: dopo la configurazione iniziale di Windows, AXIS Recorder Toolbox viene aperto e si verrà guidati attraverso alcuni passaggi per impostare le impostazioni di base e necessarie, ad esempio, nome del computer, data, ora e rete. Vedere *Configurazione iniziale del registratore Axis, on page 7*.
4. Configurare Windows®. Si consiglia di:
 - Aggiornare Windows® alla versione più recente. Vedere *Aggiornare Windows®, on page 20*.
 - Creare un account utente standard. Vedere *Creare un account utente, on page 12*.
5. Aggiornare AXIS Camera Station Pro alla versione più recente.
 - Se il sistema è online: aprire l'applicazione AXIS Recorder Toolbox e fare clic su **Update AXIS Camera Station Pro (Aggiorna AXIS Camera Station Pro)**.
 - Se il sistema è offline: andare in *axis.com* e scaricare l'ultima versione.
6. Avviare il client AXIS Camera Station Pro.
7. *Connessione al server AXIS Camera Station Pro.*
8. *Configurazione di AXIS Camera Station Pro, on page 7.*

Installare il dispositivo

Operazioni preliminari all'installazione

- Preparare gli accessori aggiuntivi utilizzati per l'installazione: monitor, mouse, tastiera e cavo di rete.
- Comprensione dell'uso di account utente diversi.

La tabella seguente elenca gli account utente che possono essere utilizzati per l'installazione, la configurazione e l'utilizzo del sistema Axis.

Account utente	Descrizione	Nota
MyAxis	Utilizzato per scaricare il software più recente, accedere al sistema di licenza, ad Axis Secure Remote Access e al monitoraggio dell'integrità del sistema.	Registrato da <i>my.axis.com</i> .
Windows®		
Amministratore Windows®	Privilegi di amministratore Windows®. Si consiglia di non utilizzarlo come amministratore di AXIS Camera Station Pro.	Creato durante l'impostazione iniziale di Windows®.
Utente Windows® con privilegi di amministratore di AXIS Camera Station Pro	Un utente Windows® con privilegi di amministratore in AXIS Camera Station Pro per l'utilizzo da parte di un integratore di sistema o da un amministratore di sistema per la configurazione o la risoluzione dei problemi.	Creato nelle impostazioni di Windows®.
Utente di Windows® con privilegi di operatore o visualizzatore in AXIS Camera Station Pro	Un utente Windows® con privilegi di operatore o visualizzatore in AXIS Camera Station Pro.	Creato nelle impostazioni di Windows®.
Gestione hardware		
iDRAC	Utilizzato per accedere allo strumento iDRAC (Integrated Dell Remote Access Controller).	Nome utente: root Password: disponibile sul retro dell'etichetta delle informazioni.
Dispositivo		
Amministratore dispositivo	Utilizzato dall'amministratore per accedere alla telecamera dal Video Management System o dalla pagina Web del dispositivo.	Creato dalla pagina Web del dispositivo o quando si aggiunge il dispositivo ad AXIS Camera Station Pro.

Configurare il dispositivo

Configurazione iniziale del registratore Axis

Dopo aver configurato Windows®, AXIS Recorder Toolbox viene aperto automaticamente e si avvia l'assistente alla configurazione iniziale. Con questo assistente alla configurazione, è possibile configurare diverse impostazioni di base e necessarie prima della gestione del dispositivo in AXIS Recorder Toolbox.

1. Seleziona il tema **Light (Chiaro)** o **Dark (Scuro)** e fai clic su **Next (Avanti)** (se è disponibile per il tuo dispositivo).
2. Se si desidera, cambiare il nome del computer e fare clic su **Next (Avanti)**.
3. In **Date and time (Data e ora)**, configurare le seguenti impostazioni e fare clic su **Next (Avanti)**.
 - Selezionare un fuso orario.
 - Per impostare un server NTP, selezionare **NTP server (Server NTP)** e immettere l'indirizzo del server NTP.
 - Per l'impostazione manuale, selezionare **Manual (Manuale)** e selezionare una data e un'ora.
4. In **Network settings (Impostazioni di rete)**, configurare le seguenti impostazioni e fare clic su **Next (Avanti)**.
 - Le opzioni **Use automatic IP settings (DHCP) (Utilizza impostazioni IP automatiche (DHCP))** e **Use automatic DNS settings (Utilizza le impostazioni DNS automatiche)** sono attivate per impostazione predefinita.
 - Se il dispositivo è connesso a una rete con un server DHCP, vengono visualizzati automaticamente l'indirizzo IP assegnato, la subnet mask, il gateway e il DNS preferito.
 - Se il dispositivo non è connesso a una rete o non è disponibile alcun server DHCP, immettere manualmente l'indirizzo IP, la subnet mask, il gateway e il DNS preferito in base ai requisiti di rete.
5. Fare clic su **Finish (Fine)**. Se è stato modificato il nome del computer, AXIS Recorder Toolbox richiederà di riavviare il dispositivo.

Configurazione di AXIS Camera Station Pro

Operazioni preliminari:

- Configurare la rete a seconda dell'installazione. Vedere *Configurazione di rete*.
- Se necessario, configurare le porte del server. Vedere *Configurazione della porta del server*.
- Valutare eventuali problemi di sicurezza. Vedere *Considerazioni sulla protezione*.

Dopo aver effettuato le necessarie configurazioni, è possibile iniziare a lavorare con AXIS Camera Station Pro.

1. *Avviare il video management system*
2. *Aggiunta di dispositivi*
3. *Configura metodo di registrazione, on page 8*
4. *Visualizzazione del video in diretta, on page 8*
5. *Visualizzazioni registrate, on page 8*
6. *Aggiunta di segnalibri, on page 8*
7. *Esportazione delle registrazioni, on page 9*
8. *Riproduzione e verifica delle registrazioni in AXIS File Player., on page 9*

Avviare il video management system

Fare doppio clic sull'icona del client AXIS Camera Station Pro per avviare il client. Quando viene avviato per la prima volta, il client tenta di accedere al server AXIS Camera Station Pro installato nello stesso computer del client.

È possibile collegarsi a più server di AXIS Camera Station Pro in modi diversi.

Aggiunta di dispositivi

La prima volta che si avvia AXIS Camera Station S1232 Tower Recording Server, si apre la pagina **Add devices (Aggiungi dispositivi)**, che esegue una ricerca nella rete per individuare i dispositivi da aggiungere.

1. Selezionare i dispositivi che si desidera aggiungere dall'elenco. Se non si riesce a trovare un dispositivo, fare clic su **Manual search** (Ricerca manuale) oppure digitare il filtro.
2. Fare clic su **Aggiungi**.
3. Fare clic su **Close (Chiudi)** per saltare la configurazione e proseguire in un secondo momento. Per proseguire con la configurazione a questo punto:
 - 3.1. Scegliere **Quick configuration** (Configurazione rapida) oppure **Site Designer configuration** (Configurazione Site designer). Per ulteriori informazioni, vedere .
 - 3.2. Selezionare **Add image overlay for date, time, and text** (Aggiungi sovrapposizione di immagine per data, ora e testo) per aggiungere sovrapposizioni a qualsiasi telecamera Axis che non ne dispone già.
 - 3.3. Fare clic su **Next (Avanti)**.
 - 3.4. Selezionare la preferenza del **Recording method** (Metodo di registrazione).
 - 3.5. Fare clic su **Next (Avanti)**.
 - 3.6. Scegliere il **Retention time** (Tempo di archiviazione), il **Recording storage** (Archiviazione registrazione) e fare clic su **Finish** (Fine) per applicare la configurazione.

Configura metodo di registrazione

1. Andare a **Configuration (Configurazione) > Registrazione ed eventi > Metodo di registrazione**.
2. Selezionare una telecamera
3. Attivare l'opzione **Motion detection** (Rilevamento movimento) o **Continuous** (Continua) o entrambe.
4. fare clic su **Applica**;

Visualizzazione del video in diretta

1. Aprire una scheda **Live view** (Visualizzazione in diretta).
2. Selezionare una telecamera per visualizzarne il video in diretta.

Visualizzazioni registrate

1. Aprire una scheda **Recordings** (Registrazioni).
2. Selezionare la telecamera da cui visualizzare le registrazioni.

Aggiunta di segnalibri

1. Andare alla registrazione.
2. Nella sequenza temporale, ingrandire e ridurre e spostare la sequenza temporale per posizionare l'indicatore nella posizione desiderata.
3. Fare clic su  .

4. Immettere un nome e una descrizione per il segnalibro. Utilizzare le parole chiave per rendere il segnalibro facile da trovare.
5. Selezionare **Impedisci eliminazione registrazione** per proteggere la registrazione.

Nota

Per rimuovere la protezione della registrazione, deselezionare **Prevent recording deletion (Impedisci rilevamento registrazione)** o eliminare il segnalibro.

6. Fare clic su **OK** per salvare il segnalibro.

Esportazione delle registrazioni

1. Aprire una scheda **Recordings (Registrazioni)**.
2. Selezionare la telecamera da cui esportare le registrazioni.
3. Fare clic su  per visualizzare i marcatori di selezione.
4. Trascinare gli indicatori per includere le registrazioni che si desidera esportare.
5. Fare clic su  per aprire la scheda **Export (Esporta)**.
6. Fare clic su **Export...(Esporta)**

Riproduzione e verifica delle registrazioni in AXIS File Player.

1. Andare alla cartella con le registrazioni esportate.
2. Fare doppio clic su **AXIS File Player**.
3. Fare clic su  per visualizzare le note della registrazione.
4. Per verificare la firma digitale:
 - 4.1. Andare a **Tools > Verify digital signature (Strumenti > Verifica firma digitale)**.
 - 4.2. Selezionare **Validate with password (Convalida con password)** e immettere la password.
 - 4.3. Fare clic su **Verify (Verifica)** per visualizzare i risultati della verifica.

Nota

- Una firma digitale differisce dal video firmato. Un video firmato consente di risalire alla telecamera da cui proviene la registrazione, in modo da poter verificare che non sia stata sottoposta a manomissione. Vedi *Video firmato* e il manuale per l'utente della telecamera per maggiori informazioni.
- Se i file memorizzati non sono collegati a un database di AXIS Camera Station (file non indicizzati), è necessario convertirli per renderli riproducibili in AXIS File Player. Contattare l'assistenza tecnica Axis per ricevere supporto riguardo la conversione dei file.

Configurazione di rete

Configurare le impostazioni del proxy o del firewall prima di utilizzare AXIS Camera Station S1232 Tower Recording Server se il client, il server e i dispositivi di rete collegati si trovano su reti diverse.

Impostazioni proxy client

Se un server proxy si trova tra il client e il server, configurare le impostazioni proxy in Windows sul computer client. Contattare il supporto Axis per ulteriori informazioni.

Impostazioni proxy del server

Se il server proxy si trova tra il dispositivo di rete e il server, è necessario configurare le impostazioni proxy in Windows sul server. Contattare il supporto Axis per ulteriori informazioni.

NAT and Firewall (NAT e Firewall)

Quando un NAT o un firewall separa il client e il server, configurarlo per garantire che la porta HTTP, la porta TCP e la porta di streaming specificate in AXIS Camera Station S1232 Tower Recording Server Service Control possano passare attraverso di esso. Rivolgersi al proprio amministratore della rete per ricevere assistenza.

Configurazione della porta del server

Il server AXIS Camera Station S1232 Tower Recording Server usa le porte 55752 (HTTP), 55754 (TCP), 55756 (comunicazione mobile) e 55757 (mobile streaming) per la comunicazione tra il server e client. Se necessario, le porte possono essere cambiate in AXIS Camera Station Service Control.

Considerazioni sulla protezione

Per impedire l'accesso non autorizzato alle telecamere e alle registrazioni:

- Usare password complesse per tutti i dispositivi di rete (telecamere, video encoder e dispositivi ausiliari).
- Installare il server AXIS Camera Station S1232 Tower Recording Server, le telecamere, i video encoder e i dispositivi ausiliari su una rete protetta separata da una rete d'ufficio. È possibile installare il client AXIS Camera Station S1232 Tower Recording Server su un computer in un'altra rete, ad esempio una rete con accesso a Internet.
- Assicurarsi che tutti gli utenti dispongano di password complesse.

Ottenimento di una licenza per un sistema online

Per utilizzare la licenza automatica, è necessario registrare il proprio sistema e connetterlo a un'organizzazione.

1. Andare a **Configuration (Configurazione) > Licenses (Licenze) > Management (Gestione)**.
2. Verificare che l'opzione **Automatic licensing (Licenza automatica)** sia attiva.
3. Fare clic su **Register... (Registra...)**.
4. Eseguire l'accesso usando il proprio account My Axis e seguire le istruzioni sullo schermo.
5. Fare clic su **Go to AXIS License Manager (Vai ad AXIS License Manager)** per la gestione delle licenze. Per saperne di più, leggere il *manuale per l'utente My Systems su help.axis.com*.

Ottenimento di una licenza per un sistema offline

Per l'ottenimento manuale di una licenza per il sistema:

1. Andare a **Configuration (Configurazione) > Licenses (Licenze) > Management (Gestione)**.
2. Disattivare **Automatic licensing (Concessione automatica delle licenze)**.
3. Fare clic su **Export system file... (Esporta file di sistema...)** e salvare il file sul computer.

Nota

Per eseguire l'accesso ad AXIS License Manager è necessaria una connessione Internet. Se il computer client non ha Internet, copiare il file di sistema su un computer che lo ha.

4. Aprire *AXIS License Manager*.
5. In *AXIS License Manager*:
 - 5.1. Selezionare l'organizzazione giusta o crearne una se necessario. Per saperne di più, leggere il *manuale per l'utente My Systems su help.axis.com*.
 - 5.2. Andare a **System setup (Configurazione del sistema)**.
 - 5.3. Fare clic su **Upload system file (Carica file di sistema)**.
 - 5.4. Fare clic su **Upload system file (Carica file di sistema)** e selezionare il proprio file di sistema.
 - 5.5. Fare clic su **Upload system file (Carica file di sistema)**.
 - 5.6. Fare clic su **Download license file (Scarica il file di licenza)**.
6. Tornare al client AXIS Camera Station S1232 Tower Recording Server.

7. Fare clic su **Import license file...** (Importa file di licenza...) e selezionare il proprio file di licenza.
8. Fare clic su **Go to AXIS License Manager** (Vai ad AXIS License Manager) per la gestione delle licenze.

Gestire gli account utente di Windows® locali

Creare un account utente

Per incrementare la sicurezza dei dati personali e delle informazioni, consigliamo di aggiungere una password per ogni account locale.

Importante

Una volta creata una password per un account locale, non dimenticarla. Se si perde la password per un account locale, è impossibile recuperarla.

1. Andare a **Settings (Impostazioni) > Accounts (Account) > Other users (Altri Utenti) > Add other user (Aggiungi altro utente)** e fare clic su **Add account (Aggiungi account)**.
2. Fare clic su **I don't have this person's sign-in information (Non ho le informazioni di accesso di questa persona)**.
3. Fare clic su **Add a user without a Microsoft account (Aggiungi un utente senza un account Microsoft)**.
4. Immettere un nome utente, una password e un suggerimento per la password.
5. Fare clic su **Next (Avanti)** e seguire le istruzioni.

Crea un account amministratore

1. Andare a **Settings > Accounts > Other people (Impostazioni > Account > Altre persone)**.
2. Accedere all'account che si desidera modificare e fare clic su **Change account type (Cambia tipo di account)**.
3. Andare a **Account type (Tipo di account)** e selezionare **Administrator (Amministratore)**.
4. Fare clic su **OK**.
5. Riavviare il dispositivo e accedere con il nuovo account amministratore.

Creare un gruppo di utenti locale

1. Andare a **Computer Management (Gestione del computer)**.
2. Andare a **Local Users and Groups > Group (Utenti e gruppi locali > Gruppo)**.
3. Fare clic con il pulsante destro del mouse su **Group (Gruppo)** e selezionare **New Group (Nuovo gruppo)**.
4. Immettere un nome per il gruppo e una descrizione.
5. Aggiungere membri al gruppo:
 - 5.1. Fare clic su **Aggiungi**.
 - 5.2. fare clic su **Avanzate**;
 - 5.3. Individuare gli account utente che si desidera aggiungere al gruppo e fare clic su **OK**.
 - 5.4. Fare di nuovo clic su **OK**.
6. Fare clic su **Create (Crea)**.

Eliminare un account utente

Importante

Quando si elimina un account, si rimuove l'account utente dalla schermata di accesso. Inoltre saranno rimossi tutti i file, le impostazioni e i dati dei programmi memorizzati nell'account utente.

1. Andare a **Settings > Accounts > Other people (Impostazioni > Account > Altre persone)**.
2. Accedere all'account che si desidera rimuovere e fare clic su **Remove (Rimuovi)**.

Modificare la password di un account utente

1. Accedere con un account amministratore.
2. Andare a **User Accounts > User Accounts > Manage another account in sequence** (Account utente > Account utente > Gestire un altro account in sequenza).
Verrà visualizzato un elenco di tutti gli account utente nel dispositivo.
3. Selezionare l'account utente di cui si desidera modificare la password.
4. Fare clic su **Change the password** (Modifica la password).
5. Immettere la nuova password e fare clic su **Change password** (Cambia password).

Creare un disco di reimpostazione della password per un account utente.

Si consiglia di creare un disco di reimpostazione della password su un'unità flash USB. Così si può reimpostare la password. Senza un disco di reimpostazione password, non è possibile reimpostare la password.

Nota

Se si utilizza Windows® 10 o versione successiva, è possibile aggiungere domande di sicurezza all'account locale nel caso in cui la password venga dimenticata, in modo da non dover creare un disco di reimpostazione della password. Per fare questo, andare su **Start** e fare clic su **Settings > Sign-in options > Update your security questions** (Impostazioni > Opzioni di accesso > Aggiorna le domande di sicurezza).

1. Accedere al dispositivo con un account utente locale. Non è possibile creare un disco di reimpostazione della password per un account connesso.
2. Collegare un'unità flash USB vuota al dispositivo.
3. Dal campo di ricerca di Windows®, andare su **Create a password reset disk** (Creare un disco di reimpostazione della password).
4. Nell'assistente di configurazione **Forgotten Password** (Password dimenticata), fare clic su **Next** (Avanti).
5. Selezionare l'unità flash USB e fare clic su **Next** (Avanti).
6. Digitare la password attuale e fare clic su **Next** (Avanti).
7. Seguire le istruzioni visualizzate.
8. Rimuovere l'unità flash USB e conservarla in un luogo sicuro. Non è necessario creare un nuovo disco quando si modifica la password, anche se la si modifica più volte.

Gestire gli account utente di AXIS Camera Station Pro

Autorizzazioni utente

Andare a **Configuration > Security > User permissions (Configurazione, Sicurezza, Autorizzazioni utente)** per vedere gli utenti e i gruppi che esistono in AXIS Camera Station S1232 Tower Recording Server.

Nota

Agli amministratori del computer su cui viene eseguito il server AXIS Camera Station S1232 Tower Recording Server vengono assegnati determinati privilegi di amministratore in AXIS Camera Station S1232 Tower Recording Server. Non è possibile cambiare o rimuovere i privilegi del gruppo degli Amministratori.

Prima di poter aggiungere un utente o un gruppo, controllare che siano registrati sul computer locale o che dispongano di un account utente di Windows® Active Directory. Per aggiungere utenti o gruppi, vedere *Aggiunta di utenti o gruppi*.

Quando un utente appartiene a un gruppo, gli vengono assegnate le autorizzazioni relative al ruolo più elevato tra quelle attribuite a lui individualmente e quelle attribuite al gruppo. Ad esempio, un utente che ha accesso alla telecamera X e che appartiene anche a un gruppo con accesso alle telecamere Y e Z ha accesso a tutte e tre le telecamere.

	Indica se la voce si riferisce a un utente singolo.
	Indica che la voce rappresenta un gruppo.
Nome	Il nome utente visualizzato nel computer locale o in Active Directory.
Dominio	Il dominio di cui fa parte l'utente o il gruppo.
Ruolo	Il ruolo di accesso assegnato all'utente o gruppo. I possibili valori sono: Amministratore, Operatore e Visualizzatore.
Dettagli	Informazioni dettagliate sull'utente come visualizzate sul computer locale o in Active Directory.
Server	Il server di cui fa parte l'utente o il gruppo.

Aggiunta di utenti o gruppi

Microsoft Windows® e i gruppi e gli utenti di Active Directory possono accedere a AXIS Camera Station S1232 Tower Recording Server. Per aggiungere un utente a AXIS Camera Station S1232 Tower Recording Server, è necessario aggiungere utenti o un gruppo a Windows®.

Per aggiungere un utente in Windows® 10 e 11:

- Premere il tasto Windows + X e selezionare **Computer Management (Gestione computer)**.
- Nella finestra **Computer Management (Gestione computer)**, spostarsi su **Local Users and Groups (Utenti e gruppi locali) > Users (Utenti)**.
- Fare clic con il tasto destro del mouse su **Users (Utenti)** e selezionare **New user (Nuovo utente)**.
- Nella finestra di dialogo a scomparsa, inserire i dettagli del nuovo utente e annullare **User must change password at next login** (L'utente deve modificare la password all'accesso successivo).
- Fare clic su **Create (Crea)**.

Se si usa un dominio di Active Directory, consultare l'amministratore di rete.

Aggiunta di utenti o gruppi

1. Andare in **Configuration (Configurazione) > Security (Sicurezza) > User permissions (Autorizzazioni utente)**.
2. Fare clic su **Aggiungi**. Gli utenti e i gruppi disponibili vengono visualizzati nell'elenco.

3. In **Scope (Ambito)**, scegliere dove si devono cercare utenti e gruppi.
4. In **Show (Mostra)**, selezionare per mostrare utenti o gruppi. I risultati della ricerca potrebbero non essere visualizzati se il numero di utenti o gruppi è troppo elevato. Utilizzare il filtro per restringere i risultati.
5. Selezionare gli utenti o i gruppi e fare clic su **Aggiungi**.

Ambito	
Server	Selezionare per cercare utenti o gruppi sul computer locale.
Dominio	Selezionare per eseguire la ricerca di utenti o gruppi Active Directory.
Server selezionato	Quando si è connessi a più server AXIS Camera Station S1232 Tower Recording Server, selezionare un server per cercare utenti o gruppi su quel server.

Configurare un utente od un gruppo

1. Selezionare un utente o un gruppo nell'elenco.
2. In **Role (Ruolo)**, selezionare **Administrator (Amministratore)**, **Operator (Operatore)** o **Viewer (Visualizzatore)**.
3. Se si è selezionato **Operator (Operatore)** o **Viewer (Visualizzatore)**, è possibile configurare i privilegi utente o gruppo. Vedere *Privilegi utente o di gruppo*.
4. Fare clic su **Save (Salva)**.

Rimuovere un utente od un gruppo

1. Selezionare utente o gruppo.
2. Fare clic su **Remove (Rimuovi)**.
3. Nella finestra a comparsa, fare clic su **OK** per rimuovere l'utente o il gruppo.

Privilegi utente o di gruppo

Sono disponibili tre ruoli che si possono assegnare a un utente o a un gruppo. Per le modalità di definizione del ruolo per un utente o un gruppo, vedere *Aggiunta di utenti o gruppi*.

Amministratore – accesso completo all'intero sistema, incluso l'accesso ai video in diretta e registrati di tutte le telecamere, tutte le porte I/O e le viste. Questo ruolo è necessario per accedere alla configurazione del sistema.

Operatore – Selezionare telecamere, viste e porte I/O per ottenere l'accesso alle immagini dal vivo e al video registrate. Un operatore ha pieno accesso a tutte le funzionalità di AXIS Camera Station S1232 Tower Recording Server ad eccezione della configurazione del sistema.

Utente – Accesso a video dal vivo di telecamere, porte I/O e viste selezionate. Un visualizzatore non ha accesso ai video registrati o alla configurazione di sistema.

Telecamere

Per utenti o gruppi con ruolo **Operator (Operatore)** o **Viewer (Visualizzatore)** sono disponibili i seguenti privilegi di accesso.

Accesso	consente l'accesso alla telecamera e a tutte le relative funzioni.
Video	consente l'accesso al video dal vivo dalla telecamera.

Ascolta con audio	consente l'accesso per ascoltare l'audio dalla telecamera.
Parla con audio	consente l'accesso per parlare alla telecamera.
Registrazione manuale	Consentire l'avvio e l'interruzione delle registrazioni in modo manuale.
PTZ meccanico	consente accesso ai comandi PTZ meccanici. Disponibile solo per telecamere con PTZ meccanico.
Priorità PTZ	imposta la priorità PTZ. Un numero inferiore indica una priorità più alta. Nessuna priorità assegnata è impostata su 0. Un amministratore ha la priorità più alta. Quando un ruolo con una priorità più elevata opera una telecamera PTZ, gli altri non possono utilizzare la stessa telecamera per 10 secondi per impostazione predefinita. Disponibile solo per telecamere con PTZ meccanico e che hanno Mechanical PTZ (PTZ meccanico) selezionato.

Viste

Per utenti o gruppi con ruolo **Operator (Operatore)** o **Viewer (Visualizzatore)** sono disponibili i seguenti privilegi di accesso. È possibile selezionare più viste e impostare i privilegi di accesso.

Accesso	Consentire l'accesso alle viste in AXIS Camera Station S1232 Tower Recording Server.
Modifica	Consente la modifica delle viste in AXIS Camera Station S1232 Tower Recording Server.

I/O

Per utenti o gruppi con ruolo **Operator (Operatore)** o **Viewer (Visualizzatore)** sono disponibili i seguenti privilegi di accesso.

Accesso	consente l'accesso completo alla porta I/O.
Leggi I'	Consente di visualizzare lo stato della porta I/O senza effettuare alcuna modifica.
Scrittura	Consente di effettuare una modifica dello stato della porta I/O.

Sistema

Non si può eseguire la configurazione dei privilegi di accesso visualizzati in grigio nella lista. Un segno di spunta indica che l'utente o il gruppo ha questo privilegio per impostazione predefinita.

Per utenti o gruppi con ruolo **Operator (Operatore)** sono disponibili i seguenti privilegi di accesso. **Take snapshots (Acquisisci istantanee)** è anche disponibile per il ruolo **Viewer (Visualizzatore)**.

Acquisisci istantanee	Consente di scattare istantanee in modalità di visualizzazione in diretta e in modalità di registrazione.
Esportazione delle registrazioni	consente di esportare le registrazioni.
Genera report dell'incidente	consente di generare i report dell'incidente.

Prevent access to recordings older than (Impedisci accesso a registrazioni precedenti a)	impedisce di accedere alle registrazioni precedenti al numero di minuti specificato. Gli utenti non possono trovare queste registrazioni quando effettuano una ricerca.
Accedi ad allarmi, attività e registri	Ricevere notifiche di allarme e permettere l'accesso alla barra Alarms and tasks (Allarmi e attività) e alla scheda Logs (Registri).
Access data search (Ricerca dati di accesso)	Consente di cercare i dati per tenere traccia di quanto è successo al momento di un evento.
Aggiungere categorie agli eventi	Consente l'aggiunta di categorie agli eventi nella scheda Recordings (Registrazioni).
Rimuovere le categorie dall'evento	Consente la rimozione di categorie dagli eventi nella scheda Recordings (Registrazioni).

Controllo accessi

Per utenti o gruppi con ruolo **Operator (Operatore)** sono disponibili i seguenti privilegi di accesso. **Access Management** (Gestione degli accessi) è a disposizione anche per il ruolo **Viewer (Visualizzatore)**.

Configurazione controllo degli accessi	Permette di configurare porte e zone, profili di identificazione, formati tessera, PIN, comunicazione criptata e multiserver.
Gestione degli accessi	Permette la gestione degli accessi e l'accesso alle impostazioni di Active Directory.

Per utenti o gruppi con ruolo **Viewer (Visualizzatore)** sono disponibili i seguenti privilegi di accesso.

Monitoraggio dell'integrità del sistema

Per utenti o gruppi con ruolo **Operator (Operatore)** sono disponibili i seguenti privilegi di accesso. **Access to system health monitoring** (Accesso a monitoraggio dell'integrità del sistema) è a disposizione anche per il ruolo **Viewer (Visualizzatore)**.

Configurazione di Monitoraggio dell'integrità del sistema	Consente la configurazione di monitoraggio dell'integrità del sistema.
Accesso a monitoraggio dell'integrità del sistema	Consente l'accesso al monitoraggio dell'integrità del sistema.

Gestire il dispositivo

Aggiornare i certificati Secure Boot

Microsoft ritirerà i certificati Secure Boot del 2011 nel giugno 2026 e li sostituirà con i nuovi certificati del 2023. Per garantire la sicurezza dell'unità di registrazione, installare i certificati del 2023 prima di tale data.

L'installazione dei certificati 2023 richiede Windows 10 LTSC (Long-Term Servicing Channel) o Windows 11 LTSC. Se il dispositivo è ancora in garanzia ma utilizza Windows 10 SAC (Semi-Annual Channel) anziché una versione LTSC, contattare l'assistenza tecnica di Axis. Possono indicarle se è possibile effettuare l'aggiornamento a una versione LTSC prima di aggiornare il BIOS o effettuare eventuali modifiche ai certificati.

Nota

Dopo giugno 2026, i dispositivi sprovvisti dei certificati del 2023 continueranno a funzionare normalmente, ma non riceveranno nuove protezioni di sicurezza per la fase iniziale di avvio, compresi gli aggiornamenti di Windows Boot Manager e gli elenchi di revoca relativi alle nuove vulnerabilità.

Verificare lo stato del certificato

Per verificare che i certificati del 2023 siano stati installati e che il bootloader di Windows sia stato aggiornato, utilizzare uno dei seguenti metodi:

Metodo 1:

1. Aprire Registry Editor (Editor di registro).
2. Andare a HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing.
3. Controllare il valore UEFICA2023Status. Se il valore indica **Updated (Aggiornato)**, il certificato del 2023 è installato.

 (Default)	REG_SZ	(value not set)
 BucketHash	REG_SZ	5a3041a8e6c7476f988f369de06e65e224df7d53cf7f9...
 ConfidenceLevel	REG_SZ	No Data Observed - Action Required
 ConfidenceUpdateType	REG_DWORD	0x00000000 (0)
 LastParsedBucketDataVersion	REG_DWORD	0x0000000c (12)
 UEFICA2023Status	REG_SZ	Updated
 WindowsUEFICA2023Capable	REG_DWORD	0x00000002 (2)

Metodo 2:

1. Aprire Windows Security.
2. Andare a Device security (Sicurezza dispositivo).
3. Andare a Secure boot (Avvio sicuro), controllare il messaggio di stato. Se il certificato è aggiornato, la scheda mostra: "Secure Boot è attivo e sono stati applicati tutti gli aggiornamenti necessari al certificato. Non sono necessarie ulteriori modifiche al certificato."

Secure boot

Secure Boot is on and all required certificate updates have been applied.
No further certificate changes are needed.

Nota

Windows Security mostra lo stato del certificato solo se sul dispositivo è effettuata l'installazione dell'aggiornamento cumulativo del 14 aprile 2026 o una versione successiva. Se non viene visualizzato alcun messaggio relativo allo stato del certificato, aggiornare Windows oppure utilizzare il Metodo 1.

Azioni consigliate

Un aggiornamento del BIOS aggiorna il firmware con i certificati del 2023 in modo permanente. È il metodo più affidabile e lo consigliamo anche se è stata già effettuata l'installazione dei certificati tramite Windows Update.

Importante

Se si installano i certificati esclusivamente tramite Windows Update e successivamente si ripristinano le impostazioni di fabbrica delle chiavi di Secure Boot nel BIOS, i certificati andranno persi e il dispositivo non si avvierà con Secure Boot attivo. Aggiornare il BIOS per rendere permanenti i certificati prima di reimpostare le chiavi del Secure Boot.

Aggiornare il certificato tramite il BIOS

Per le serie AXIS S12 e S93, aggiornare il BIOS dal sito Dell anziché da Axis.com. Consultare la pagina *Aggiornare il BIOS, on page 19*.

Ulteriori informazioni:

- *Dell: Scadenza del certificato Secure Boot di Microsoft del 2011.*
- *Dell: Linee guida per l'aggiornamento del BIOS dei server PowerEdge per il Secure Boot.*

Aggiornare il certificato tramite Windows Update

Se per il proprio modello non è ancora disponibile un aggiornamento del BIOS, è possibile ottenere i certificati del 2023 tramite Windows Update.

Importante

I certificati installati in questo modo vengono memorizzati nel database Secure Boot corrente, non nel firmware. Se si reimpostano le chiavi Secure Boot del BIOS alle impostazioni di fabbrica, si perdono i certificati e il dispositivo potrebbe non essere in grado di avviarsi con Secure Boot attivo. Installare un aggiornamento del BIOS non appena ne sarà disponibile uno per il proprio modello, anche se ha già utilizzato questo metodo.

Per utilizzare questo percorso:

1. Controllare che il dispositivo utilizzi Windows 10 LTSC o Windows 11 LTSC.
2. Installare tutti gli aggiornamenti di Windows rilasciati il 14 aprile 2026 o successivamente.
3. Andare a **Windows Security (Sicurezza di Windows) > Device security (Sicurezza del dispositivo) > Secure Boot (Avvio sicuro)** per verificare lo stato del proprio certificato.
4. Se il certificato non viene aggiornato dopo l'installazione degli ultimi aggiornamenti, controllare il valore di registro **UEFICA2023Status**. Se il dispositivo continua a non essere idoneo all'aggiornamento automatico, aggiornare il BIOS oppure contattare l'assistenza tecnica di Axis.

Importante

Non revocare manualmente il certificato del 2011 finché non avrà verificato che tutti i supporti di ripristino, gli ambienti di avvio e i driver presenti nell'ambiente siano firmati con il certificato del 2023. Se si revoca il certificato del 2011 troppo in anticipo, il dispositivo non sarà in grado di avviarsi con la funzione Secure Boot attivata.

Controllo della versione corrente del BIOS

Per controllare il BIOS corrente:

1. Accendi il dispositivo e premi ripetutamente F2 fino a quando non viene visualizzato il logo Axis.
2. Il numero di versione è mostrato come prima voce su **Overview (Panoramica)**.

Aggiornare il BIOS

1. Andare alla pagina *dell'assistenza Dell*.

2. Nel campo **Tag di servizio**, inserire le ultime 7 cifre del numero di serie del dispositivo. Per esempio, HW030ABC1234.
3. Andare alla pagina **Driver & Downloads (Driver e download)** e cercare "BIOS".
4. Se non viene visualizzata una versione più recente per il nome del prodotto OEM (ad esempio, "OEMR XL R760xs"), effettuare una nuova ricerca utilizzando il nome generico della piattaforma Dell anziché il numero di serie (ad esempio, "R760xs").
5. Scaricare e installare l'ultima versione del BIOS rilasciata dopo aprile 2026.

Aggiornare Windows®

Windows® controlla periodicamente la disponibilità degli aggiornamenti. Quando è disponibile un aggiornamento, il dispositivo lo scarica automaticamente, ma è necessario installarlo manualmente.

Nota

La registrazione verrà interrotta durante un riavvio pianificato del sistema.

Per verificare manualmente la disponibilità di aggiornamenti:

1. Andare a **Settings (Impostazioni) > Windows Update (Aggiornamento Windows)**.
2. Fare clic su **Check for updates (Controlla aggiornamenti)**.

Configurazione delle impostazioni di Windows® Update

Si può modificare come e quando Windows® esegue gli aggiornamenti secondo le proprie esigenze.

Nota

Tutte le registrazioni in corso si interrompono durante un riavvio pianificato del sistema.

1. Aprire l'app **Esegui**.
 - Andare a **Windows System > Run (Sistema Windows > Esegui)** o
2. Digitare `gpedit.msc` e fare clic su **OK**. Si apre l'Editor criteri gruppi locali.
3. Andare a **Computer Configuration > Administrative Templates > Windows Components > Windows Update (Configurazione computer > Modelli amministrativi > Componenti di Windows > Windows Update)**.
4. Configurare le impostazioni in base alle esigenze, vedere esempio.

Esempio:

Per scaricare e installare automaticamente gli aggiornamenti senza alcuna interazione dall'utente e fare in modo che il dispositivo venga riavviato, se necessario, fuori dall'orario di ufficio, utilizzare la configurazione seguente:

1. Aprire **Always automatically restart at the scheduled time (Riavvia sempre all'ora pianificata)** e selezionare:
 - 1.1. **Attivato**
 - 1.2. **The restart timer will give users this much time to save their work (minutes) (Il timer di riavvio darà agli utenti questo tempo per salvare il loro lavoro (minuti))**: 15.
 - 1.3. Fare clic su **OK**.
2. Aprire **Configure Automatic Updates (Configurare aggiornamenti automatici)** e selezionare:
 - 2.1. **Attivato**
 - 2.2. **Configure Automatic updates (Configurare aggiornamenti automatici)**: Download automatico e pianificazione dell'installazione
 - 2.3. **Schedule Install day (Pianifica giorno di installazione)**: Ogni domenica
 - 2.4. **Schedule Install time (Pianifica l'ora di installazione)**: 00:00
 - 2.5. Fare clic su **OK**.

3. Aprire **Allow Automatic Updates immediate installation** (Consenti installazione immediata di aggiornamenti automatici) e selezionare:
 - 3.1. **Attivato**
 - 3.2. Fare clic su **OK**.

Aggiunta di un disco rigido

Lo spazio di archiviazione necessario può variare. Il tempo di conservazione dei dati memorizzati o l'archiviazione di registrazioni ad alta risoluzione determinano la stessa situazione: la necessità di installare una maggiore quantità di memoria. Questa sezione illustra in che modo espandere la serie AXIS S12 con ulteriori dischi rigidi e come aggiungerli alla tua configurazione RAID 5.

Nota

Le istruzioni seguenti devono essere utilizzate quando si aggiunge ulteriore spazio di archiviazione a certi modelli della serie AXIS S12. Queste istruzioni sono così come sono e Axis Communications AB non si assume alcuna responsabilità per la perdita di dati e/o per la configurazione errata durante questi passaggi. Rispettare le precauzioni standard quando si esegue il backup di dati critici per l'azienda. La seguente procedura di espansione dell'archiviazione non sarà supportata dall'assistenza tecnica Axis.

Nota

Per evitare scariche elettrostatiche, si consiglia di utilizzare sempre un tappetino statico e un cinturino statico mentre si lavora su componenti all'interno del sistema.

Garanzia

Informazioni dettagliate sulla garanzia sono disponibili all'indirizzo: www.axis.com/support/warranty.

Flusso di lavoro

1. *Installa un disco rigido hot-swap, on page 21*
 - 1.1. *Rimozione della mascherina, on page 21*
 - 1.2. *Rimuovi il disco rigido vuoto, on page 21*
 - 1.3. *Installazione del disco rigido, on page 22*
2. *Crea un nuovo array RAID, on page 23*
 - 2.1. *Entra nel Dell PERC 11 Configuration Utility, on page 23*
 - 2.2. *Crea un array di archiviazione RAID, on page 23*
 - 2.3. *Riconfigurazione di un array di archiviazione RAID, on page 23*
- 3.

Installa un disco rigido hot-swap

Rimozione della mascherina

1. Individuare la chiave della mascherina.
2. Sbloccare la mascherina usando la chiave.
3. Far scorrere il fermo di sgancio verso l'alto e tirare l'estremità sinistra della mascherina.
4. Sganciare l'estremità destra e rimuovere la mascherina.

Rimuovi il disco rigido vuoto

- Premi il pulsante di rilascio sul davanti del disco rigido vuoto e fallo scorrere fuori dallo slot.

Installazione del disco rigido

▲ ATTENZIONE

- Utilizza solo dischi rigidi che sono stati testati e approvati per l'uso con la serie AXIS S12.
 - Quando si installa un disco rigido, assicurarsi che le unità adiacenti siano completamente installate. L'inserimento di un supporto per disco rigido e il tentativo di bloccare la rispettiva maniglia accanto a un supporto parzialmente installato possono danneggiare la molla della protezione del supporto parzialmente installato e renderla inutilizzabile.
 - La combinazione di dischi rigidi SAS e SATA nello stesso volume RAID non è supportata.
1. Se nello slot del disco rigido è installato un disco rigido vuoto, rimuovilo.
 2. Installare un disco rigido nel supporto per disco rigido.
 3. Premere il pulsante di rilascio nella parte anteriore del supporto per disco rigido e aprire la maniglia di tale supporto.
 4. Inserire il supporto per disco rigido nello slot del disco rigido fino a quando il supporto non si collega con il backplane.
 5. Chiudere la maniglia del supporto per disco rigido per bloccare il disco.

Modifica del RAID

▲ ATTENZIONE

La modifica del RAID comporta l'eliminazione di tutti i dati dai dischi.

1. Avviare Lifecycle Controller:
 - 1.1. Accendere il dispositivo.
 - 1.2. Quando viene visualizzata la schermata iniziale di AXIS, premere F10.
2. In Lifecycle Controller passare a **Hardware Configuration > Configuration Wizards (Configurazione hardware > Configurazioni guidate)** e selezionare **RAID Configuration (Configurazione RAID)**.
3. Selezionare il **RAID Controller (Controller RAID)** su cui si desidera creare il RAID. I dettagli di tutti i dischi virtuali disponibili sul controller selezionato verranno visualizzati nella tabella mostrata nella pagina sotto l'elenco dei controller. Verrà visualizzata l'opzione Foreign Configuration (Configurazione esterna) se sul server sono disponibili HDD esterni o non inizializzati.

Nota

- L'opzione Clear Foreign Configuration (Cancella configurazione esterna) consente di cancellare tutti gli HDD esterni disponibili sul controller RAID selezionato.
 - L'opzione Ignore Foreign Configuration (Ignora configurazione esterna) consente di ignorare gli HDD esterni disponibili sul controller RAID durante la creazione del RAID.
4. Cancellare o ignorare gli HDD esterni e quelli non inizializzati.
Se lo si desidera, è possibile inizializzare i dischi non inizializzati:
 - 4.1. Nell'elenco di tutti gli HDD (non inizializzati) non RAID, selezionare gli HDD che si desidera convertire in RAID (inizializzare) e fare clic su **Next (Avanti)** per iniziarli.
 - 4.2. Selezionare l'opzione corrispondente nella pagina Configuration Wizards: RAID Configuration (Procedure guidate di configurazione: Configurazione RAID).
 5. Selezionare un livello RAID.
 6. Selezionare i dischi fisici dalla tabella e fare clic su **Next (Avanti)**.
Se è stata selezionata l'opzione **Ignore foreign configuration (Ignora configurazione esterna)**, gli HDD esterni non sono visualizzati nella tabella.
 7. Immettere gli attributi del disco virtuale.
 8. Fare clic su **Next (Avanti)**.
 9. riesaminare le impostazioni e fare clic su **Fine**.

10. Lifecycle Controller visualizza un messaggio per indicare che tutti i dati correnti riguardanti i dischi virtuali disponibili nel controller andranno persi. Fare clic su **OK** per continuare.
11. Fare clic su **OK** e su **Finish (Fine)**.
12. Uscire dalla procedura guidata e riavviare il sistema.

Crea un nuovo array RAID

L'utilità di configurazione Human Interface Infrastructure (HII) è un'applicazione per la gestione dell'archiviazione integrata nel BIOS del sistema. Viene utilizzata per configurare e gestire i controller, le unità disco virtuali e le unità disco fisiche. Questa utility è indipendente dal sistema operativo.

Entra nel Dell PERC 11 Configuration Utility

1. Accendi il sistema.
2. Durante l'avvio del sistema, premere F2 per accedere alle impostazioni di sistema.
3. Fai clic su **Device Settings (Impostazioni dispositivo)** per la visualizzazione di tutti i controller RAID nel sistema.

Crea un array di archiviazione RAID

1. *Entra nel Dell PERC 11 Configuration Utility, on page 23.*
2. Fai clic su **Main Menu > Configuration Management > Create Virtual Disk (Menu principale > Gestione configurazione > Crea disco virtuale)** e definisci i seguenti parametri per il disco virtuale.
 - **Seleziona livello RAID:** Scegliere il livello RAID.
 - **Seleziona dischi fisici:** Seleziona i dischi fisici da cui si creano i dischi virtuali. Questa opzione è mostrata se selezioni **Unconfigured Capacity (Capacità non configurata)** come capacità di disco fisico.
 - **Configura disco virtuale:** Configura i seguenti parametri per il disco virtuale.
 - **Nome disco virtuale:** Immetti il nome del disco virtuale.
I caratteri consentiti sono solo A-Z, a-z, 0-9, trattino basso (_) e trattino (-).
 - **Dimensione disco virtuale:** Imposta la capacità per il disco virtuale.
3. Fai clic su **Create Virtual Disk (Crea disco virtuale)**.

⚠ ATTENZIONE

Sono disponibili altri parametri da modificare. Tuttavia, Axis Communications AB non si assume la responsabilità per eventuali errori di configurazione che possano verificarsi nell'ambito della modifica di quei parametri. Usa sempre molta cautela quando modifichi i parametri.

Riconfigurazione di un array di archiviazione RAID

Un disco virtuale online si può riconfigurare in modi che ne ampliano la capacità e ne modificano il livello RAID.

⚠ ATTENZIONE

- I dischi virtuali con spanning, come RAID 50 e 60, non si possono riconfigurare.
 - Riconfigurare i dischi virtuali influisce generalmente sulle prestazioni del disco finché l'operazione di riconfigurazione non è completata. Il tempo di completamento può differire notevolmente e arrivare fino a diversi giorni. Consigliamo vivamente di eseguire la procedura nel corso di una finestra di manutenzione.
 - Crea sempre un backup convalidato dei tuoi dati prima di intraprendere qualsiasi azione.
1. *Entra nel Dell PERC 11 Configuration Utility, on page 23.*
 2. Fai clic su **Main Menu > Virtual Disk Management (Menu principale > Gestione dischi virtuali)**. Tutti i dischi virtuali associati al dispositivo di controllo RAID sono visualizzati.
 3. Per visualizzare le proprietà, fai clic sul disco virtuale.

4. Nell'elenco a discesa **Operations (Operazioni)**, seleziona **Reconfigure Virtual Disks (Riconfigura dischi virtuali)** e premi **GO (VAI)**.
5. Seleziona **RAID Level (Livello RAID)** e premi **Choose the Operation (Scegli l'operazione)**.
6. Seleziona i dischi da aggiungere al disco virtuale e premi **Apply Changes (Applica modifiche)**.
7. Conferma l'operazione e fai clic su **YES (Sì)**.
8. Fai clic su **Start Operation (Avvia operazione)**.
9. Fare clic su **OK**.

Nella pagina Gestione disco virtuale, puoi visualizzare lo stato della ricostruzione sul disco virtuale modificato.

Una volta avviata la ricostruzione, il sistema si può lasciare nella Dell PERC 11 Configuration Utility fino al completamento o può essere riavviato nel sistema operativo.

Se il sistema viene riavviato nel sistema operativo, le prestazioni del sistema saranno influenzate fino al completamento della ricostruzione.

NON è inoltre possibile estendere il disco in Windows® fino al completamento della ricostruzione.

▲ ATTENZIONE

Il tempo di ricostruzione differisce da un sistema all'altro e può necessitare di un massimo di diversi giorni.

Configura Microsoft Windows®

Per la configurazione di un nuovo volume:

1. Fai clic con il pulsante destro del mouse sul menu **Avvio** e seleziona **Disk Management (Gestione disco)**.
2. Fai clic con il pulsante destro del mouse su una regione non allocata del tuo disco rigido e seleziona **New Simple Volume (Nuovo volume semplice)**.
3. In **New Simple Volume Wizard (Procedura guidata nuovo volume semplice)**, fai clic su **Next (Avanti)**.
4. Immetti la dimensione del volume che vuoi creare in megabyte (MB) o accetta la dimensione predefinita massima e fai clic su **Next (Avanti)**.
5. Accetta la lettera di unità predefinita o scegli una lettera di unità diversa per identificare la partizione e fai clic su **Next (Avanti)**.
6. Nella finestra di dialogo **Formatta partizione**:
 - Se non vuoi eseguire subito la formattazione del volume, seleziona **Do not format this volume (Non formattare questo volume)** e fai clic su **Next (Avanti)**.
 - Per eseguire la formattazione del volume con le impostazioni predefinite, fai clic su **Next (Avanti)**.
7. Rivedi le tue scelte e fai clic su **Finish (Fine)**.
Gestione disco mostra ora il nuovo volume. Ora puoi chiudere Gestione disco e il sistema è pronto per usare il nuovo volume.

Per la configurazione di un volume esistente:

1. Fai clic con il pulsante destro del mouse sul menu **Avvio** e seleziona **Disk Management (Gestione disco)**.
2. Fai clic con il pulsante destro del mouse sul volume e seleziona **Extend Volume (Estendi volume)**.
3. In **Extend Volume Wizard (Procedura guidata estendi volume)**, fai clic su **Next (Avanti)**.
4. Selezionare il disco con spazio inutilizzato e fare clic su **Next (Avanti)**. Normalmente ciò è selezionato per impostazione predefinita.
5. Rivedi le tue scelte e fai clic su **Finish (Fine)**.
Gestione disco mostra ora il volume esteso. Ora puoi chiudere Gestione disco e il sistema è pronto per usare il nuovo volume.

Configurazione di iDRAC

iDRAC9 (Integrated Dell Remote Access Controller 9) con Lifecycle Controller è progettato per rendere gli amministratori di sistema più produttivi e migliorare la disponibilità generale dei sistemi Dell. iDRAC notifica gli amministratori in merito ai problemi relativi al sistema, consente loro di eseguire la gestione remota del sistema e riduce la necessità di accesso fisico al sistema. È necessario configurare le impostazioni di rete iniziali in base all'infrastruttura di rete in modo da abilitare la comunicazione da e verso iDRAC.

1. Premere F10 durante il test di alimentazione POST (Power-On Self-Test).

Nota

L'installazione guidata iniziale di Lifecycle Controller verrà visualizzata solo per la prima volta. Utilizzare l'installazione guidata iniziale per selezionare la lingua e la tastiera, configurare le impostazioni di rete, le impostazioni di rete iDRAC, la configurazione delle credenziali e visualizzare il riepilogo delle impostazioni. Per apportare modifiche alla configurazione successivamente, selezionare **Settings (Impostazioni)** dalla pagina iniziale di Lifecycle Controller.

2. Configurare la lingua e la tastiera e fare clic su **Next (Avanti)**.
3. Controllare la panoramica del dispositivo e fare clic su **Next (Avanti)**.
4. Configurare le impostazioni di rete Lifecycle Controller:
 - 4.1. Dall'elenco a discesa **NIC Card (Scheda NIC)**, seleziona la porta NIC da configurare.
 - 4.2. Dall'elenco a discesa **IPv4 Network Settings > IP Address Source (Impostazioni di rete IPv4 > Indirizzo IP origine)**, seleziona una delle seguenti opzioni:
 - **DHCP:** indica che la NIC deve essere configurata utilizzando un indirizzo IP di un server DHCP. DHCP è l'opzione predefinita e l'indirizzo IP DHCP viene visualizzato nella pagina Impostazioni di rete.
 - **Static IP: (IP statico)** indica che il valore NIC deve essere configurato utilizzando un IP statico. Digitare le proprietà dell'indirizzo IP, tra cui **IP Address (Indirizzo IP)**, **Subnet mask (Maschera di sottorete)**, **Default Gateway (Gateway predefinito)**, e **DNS Address (Indirizzo DNS)**. Se non si dispone di queste informazioni, contattare l'amministratore di rete.
 - **No Configuration: (Nessuna configurazione)** indica che non è necessario configurare il valore NIC.
 - 4.1. Se viene utilizzata la VLAN, fare clic su **Enabled (Abilitato)** e digitare **VLAN ID (ID VLAN)** e **Priority (Priorità)** in **Lifecycle Controller VLAN Settings (Impostazioni VLAN Lifecycle Controller)** per configurare le impostazioni VLAN di un NIC.
 - 4.2. Fare clic su **Next (Avanti)**. Se le impostazioni di Lifecycle Controller non sono configurate correttamente, viene visualizzato un messaggio di errore.
5. Configurare le credenziali e la rete iDRAC:
 - 5.1. Andare a **IPv4 Configuration > IP Address Source (Configurazione IPv4 > Indirizzo IP origine)** e selezionare una delle seguenti opzioni:
 - **Static: (statico)** indica che la rete deve essere configurata utilizzando un IP statico. Digitare le proprietà dell'indirizzo IP, tra cui **IP Address (Indirizzo IP)**, **Subnet mask (Maschera di sottorete)**, **Default Gateway (Gateway predefinito)**, e **DNS Address Source (Indirizzo DNS sorgente)** e **DNS Address (Indirizzo DNS)**. Se non si dispone di queste informazioni, contattare l'amministratore di rete.
 - **DHCP:** indica che la NIC deve essere configurata utilizzando un indirizzo IP di un server DHCP. DHCP è l'opzione predefinita e l'indirizzo IP DHCP viene visualizzato nella pagina Impostazioni di rete.
 - 5.1. In **Credentials (Credenziali)**, immettere **Account Username (Nome utente account)** e **Password** per accedere alla rete iDRAC.
 - 5.2. Fare clic su **Next (Avanti)**.
6. Verificare il riepilogo della configurazione di rete Lifecycle Controller e iDRAC e fare clic su **Finish (Fine)**.

Cyber security

Per informazioni specifiche sulla cybersecurity (sicurezza informatica), consultare la scheda tecnica del dispositivo su axis.com.

Per informazioni approfondite sulla cybersecurity in AXIS OS, leggere la guida *AXIS OS Hardening*.

Secure Boot

Avvio sicuro è una funzione che impedisce che malware e software non sicuri siano eseguiti sul sistema. Questa funzione viene eseguita all'avvio del sistema e utilizza le firme digitali per verificare i certificati del software e del sistema operativo. Solo software e sistemi operativi attendibili possono essere eseguiti sul sistema.

Trusted Platform Module (TPM)

Il TPM è un componente che fornisce funzionalità di crittografia per proteggere le informazioni da accessi non autorizzati. È attiva per impostazione predefinita e non consigliamo la sua disattivazione.

Per maggiori informazioni relativamente alle funzioni di cybersecurity nei dispositivi Axis, vai su axis.com/learning/white-papers e cerca cybersecurity.

Servizio di notifica di sicurezza Axis

Axis fornisce un servizio di notifica con informazioni sulla vulnerabilità e altre questioni relative alla sicurezza per i dispositivi Axis. Per ricevere le notifiche, è possibile iscriversi a axis.com/security-notification-service.

Gestione delle vulnerabilità

Per ridurre al minimo il rischio di esposizione dei clienti, Axis, in qualità di **autorità per la numerazione delle Vulnerabilità ed Esposizioni (CNA, Common Vulnerability and Exposures)**, segue gli standard di settore per gestire e rispondere alle vulnerabilità rilevate nei nostri dispositivi, software e servizi. Per ulteriori informazioni sui criteri di gestione delle vulnerabilità di Axis, sulla modalità di segnalazione delle vulnerabilità, sulle vulnerabilità già sfruttate e sui corrispondenti avvisi di sicurezza, consultare axis.com/vulnerability-management.

Funzionamento sicuro dei dispositivi Axis

I dispositivi Axis con impostazioni predefinite di fabbrica sono preconfigurati con meccanismi di protezione predefiniti sicuri. Si consiglia di utilizzare più configurazione di sicurezza quando si installa il dispositivo. Per saperne di più sull'approccio di Axis alla cybersecurity, comprese le pratiche migliori, le risorse e le linee guida per la protezione dei dispositivi, consultare axis.com/about-axis/cybersecurity.

Risoluzione dei problemi

Esecuzione della diagnostica

L'esecuzione della diagnostica consente di identificare la causa di un problema di sistema. La diagnostica testa l'hardware del sistema senza richiedere apparecchiature aggiuntive o rischiare la perdita di dati.

1. Durante l'avvio del sistema, premere F10 per accedere a Lifecycle Controller.
2. Andare a **Hardware Diagnostics (Diagnostica hardware)** e fare clic su **Run Hardware Diagnostics (Esegui diagnostica hardware)**.
3. Annotare il codice di errore e contattare il supporto tecnico Axis.

Eseguire un ripristino del sistema

Ripristino interno

Se avviene un guasto di sistema nel dispositivo, esegui un ripristino interno al fine di ripristinare il sistema.

1. Apri **Windows Settings (Impostazioni Windows)**.
2. Selezionare **System (Sistema)**.
3. Nel menu, seleziona **Recovery (Ripristino)**.
4. In **Recovery options (Opzioni di ripristino)** selezionare **Reset this PC (Ripristina questo PC)**.
5. Selezionare **Keep my files (Conserva i miei file)** o **Remove everything (Rimuovi tutto)**.
 - La funzione **Conserva i miei file** conserverà tutti i file personali e i dati degli utenti, nonché tutti i software Axis installati.
 - La rimozione completa eliminerà tutti i file personali e i dati utente, ma manterrà tutto il software Axis installato (impostazione predefinita in fabbrica).
6. Seguire le istruzioni visualizzate.

Nota

Prima di selezionare **Reset (Ripristino)**, puoi visualizzare una lista di app che saranno rimosse nel processo. Le app Axis verranno recuperate dopo il ripristino, ma se sono state installate altre app, queste non verranno ripristinate.

Importante

Dopo un ripristino avvenuto correttamente, è importante eseguire l'accesso a Windows con un account amministratore per la finalizzazione del processo di ripristino.

Ripristino esterno

Se si è verificato un guasto totale del sistema, è necessario utilizzare un'immagine di ripristino per ricreare il sistema Windows®. Per scaricare il kit di ripristino del video di rete **AXIS Network Video Recovery Kit**, contattare il supporto tecnico *AXIS Technical Support* e fornire il numero di serie del dispositivo.

Nota

Il kit di ripristino per Registratori video di rete AXIS è disponibile in due versioni:

- **sb11** — per i dispositivi che utilizzano ancora il certificato del 2011.
- **sb23** — per i dispositivi che sono passati al certificato del 2023.

Controllare lo stato del certificato prima di scaricare il kit di ripristino e selezionare la variante corrispondente. Se si seleziona la variante sbagliata, l'installazione non produrrà un risultato con possibilità di avvio e dovrà ricominciare da capo con l'immagine corretta. Tutto questo non danneggerà il dispositivo.

Se sul dispositivo è già installato il certificato del 2023, la variante sb11 può essere utilizzata in tutta sicurezza, a condizione che il certificato del 2011 non sia stato revocato in modo manuale. Una volta revocato, funzionerà solo sb23.

1. Scarichi il kit di ripristino video di rete AXIS Network Video Recovery Kit e uno strumento di scrittura ISO su USB di sua scelta.
2. Inserire un'unità USB nel computer.
 - Utilizzare un'unità USB di minimo 16 GB.
 - L'unità USB verrà formattata e tutti i dati esistenti verranno cancellati.
3. Eseguire ISO sullo strumento di scrittura USB e seguire le istruzioni visualizzate sullo schermo.
 - La scrittura dei dati sul disco USB richiede circa 10-15 minuti. Non rimuovere l'unità USB fino al completamento del processo.
4. Dopo l'uso dello strumento da ISO a USB, rimuovere l'unità USB dal computer e collegarla al dispositivo.
5. Avviare il dispositivo. Quando viene visualizzata la schermata iniziale di Axis, premere il tasto F12 per accedere al menu di avvio.
6. Selezionare l'unità USB e premere **Enter** (Invio). Il sistema si avvia nel kit di ripristino del registratore di rete AXIS Network Video Recorder Recovery Kit.
7. Fare clic su **Start (Avvia)** e seguire le istruzioni visualizzate.
 - Il recupero richiede dai 10 ai 15 minuti.

Esportazione di una raccolta SupportAssist

È possibile esportare la raccolta SupportAssist in un'unità USB o in una condivisione di rete (CIFS/NFS). La raccolta include i seguenti dati:

- Hardware
- Registri del controller RAID

Per esportare la raccolta SupportAssist:

1. Durante il test di alimentazione (Power-on-self-test, POST), premere F10 per avviare il Lifecycle Controller.
2. Andare a **Hardware Diagnostics > Export SupportAssist collection (Diagnostica hardware > Esporta raccolta SupportAssist)**.
3. Leggere i termini e le condizioni e fare clic su **Next (Avanti)**.
È necessario accettare i termini e le condizioni per consentire al supporto tecnico di utilizzare i dati della raccolta SupportAssist.
4. Selezionare le opzioni relative ai dati che si desidera includere nella raccolta SupportAssist e fare clic su **Next (Avanti)**.
5. Immettere le informazioni necessarie per le impostazioni di esportazione e fare clic su **Next (Avanti)**.
 - Per esportare su un supporto USB: selezionare l'opzione relativa all'unità USB, quindi selezionare il nome dell'unità USB e immettere i dettagli del percorso del file in cui si devono spostare gli elementi.
 - Per esportare su NFS: selezionare l'opzione NFS e inserire le informazioni richieste.
 - Per esportare su CIFS: selezionare l'opzione CIFS e inserire le informazioni richieste. Fare clic su **Test Network Connection (Verifica collegamento di rete)** per verificare che Lifecycle Controller può connettersi all'indirizzo IP fornito. Per impostazione predefinita, viene eseguito il ping dell'IP del gateway, dell'IP del server DNS, dell'IP host e dell'IP proxy.
6. Verificare la selezione e fare clic su **Finish (Fine)**.
Lifecycle Controller recupera i dati della raccolta selezionata ed esegue l'esportazione nella posizione specificata. L'operazione può richiedere alcuni minuti.

Risoluzione dei problemi relativi all'unità di alimentazione

Nota

Dopo aver installato un'unità di alimentazione, attendere alcuni secondi che il sistema la riconosca e determini se funziona correttamente.

1. Assicurarsi che non vi siano collegamenti allentati, ad esempio i cavi di alimentazione.
2. Assicurarsi che il LED dell'handle dell'alimentatore indichi che l'alimentatore funziona correttamente.
3. Controllare lo stato dell'indicatore di alimentazione sull'unità di alimentazione. Vedere *Dati tecnici*, on page 31.
4. Se si dispone di una configurazione di alimentazione ridondante, assicurarsi che entrambe le unità di alimentazione siano dello stesso tipo e wattaggio.
5. Assicurarsi di utilizzare solo le unità di alimentazione con l'etichetta EPP (Extended Power Performance) sul retro.
6. Reimpostare l'unità di alimentazione.
7. Se il problema persiste, contattare il supporto tecnico di Axis.

Risoluzione dei problemi relativi agli errori di memoria

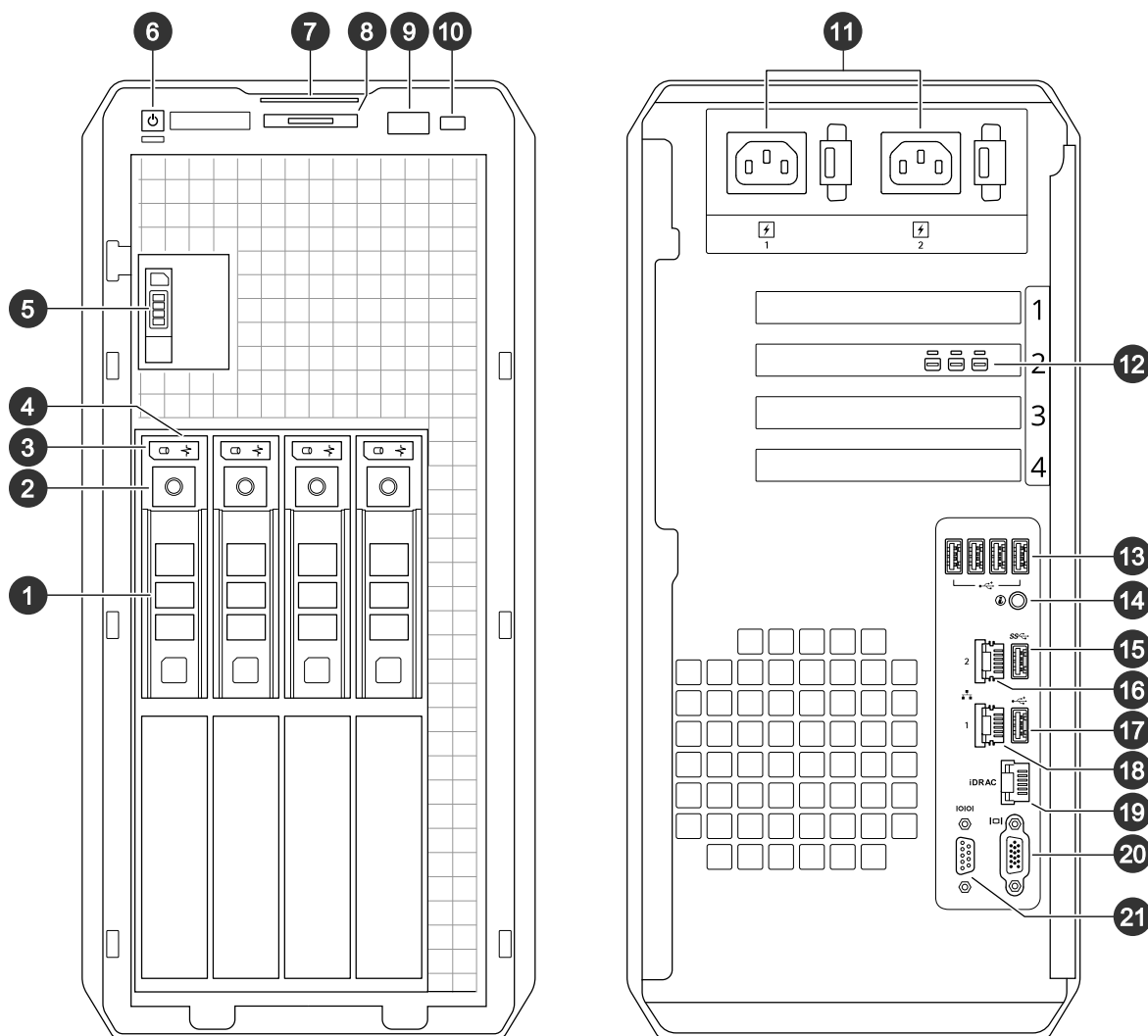
1. Aggiornare il BIOS alla versione più recente.
2. Se gli errori persistono, contattare il supporto tecnico Axis.

Risoluzione di problemi per AXIS Camera Station Pro

Per informazioni su come risolvere i problemi di AXIS Camera Station Pro, andare al *manuale utente di AXIS Camera Station Pro*.

Panoramica dei prodotti

Parte anteriore e posteriore



- 1 Vassoio del disco rigido
- 2 Pulsante di rilascio del vassoio del disco rigido
- 3 LED attività disco rigido
- 4 LED di stato del disco rigido
- 5 Vassoio unità SSD
- 6 Tasto di accensione/LED di accensione
- 7 Etichetta informazioni
- 8 Pulsante e indicatore di identificazione di sistema
- 9 Porta USB 3.0
- 10 Porta iDRAC direct
- 11 Unità di alimentazione
- 12 Connettori Mini DisplayPort
- 13 Porte USB 2.0
- 14 Pulsante e indicatore di identificazione di sistema
- 15 Porta USB 3.0
- 16 Porta Ethernet da 1 GbE 2
- 17 Porta USB 2.0
- 18 Porta Ethernet da 1 GbE 1
- 19 Porta Ethernet dedicata iDRAC
- 20 Connettore VGA (non utilizzare)
- 21 Porta seriale

Dati tecnici

Indicatori di integrità e ID del sistema

LED	Descrizione	Operazione
Blu fisso	Il sistema è acceso, integro e la modalità ID di sistema non è attiva.	Premere il pulsante relativo all'integrità del sistema e all'ID di sistema per passare alla modalità ID di sistema.
Blu lampeggiante	La modalità ID di sistema è attiva.	Premere il pulsante relativo all'integrità del sistema e all'ID di sistema per passare alla modalità di integrità del sistema.
Giallo fisso	Il sistema è in modalità sicurezza intrinseca.	
Giallo lampeggiante	Si è verificato un errore di sistema.	Controllare il registro degli eventi di sistema per il messaggio di errore specifico.

Indicatori LED iDRAC direct

LED	Descrizione
Verde fisso per due secondi	Il computer portatile o il tablet è collegato.
Verde lampeggiante (acceso per due secondi e spento per due secondi)	Il computer portatile o il tablet connesso viene riconosciuto.
Off	Il computer portatile o il tablet è scollegato.

Indicatori NIC

LED	Descrizione
Gli indicatori di collegamento e di attività sono disattivati	La scheda NIC non è collegata alla rete.
L'indicatore di collegamento è verde e l'indicatore di attività lampeggia di verde	La scheda NIC è collegata a una rete valida alla velocità massima della porta e i dati vengono inviati o ricevuti.
L'indicatore di collegamento è giallo e l'indicatore di attività lampeggia di verde	La scheda NIC è collegata a una rete valida a una velocità inferiore alla rispettiva velocità massima della porta e i dati vengono inviati o ricevuti.
L'indicatore di collegamento è verde e l'indicatore di attività è spento	La scheda NIC è collegata a una rete valida alla velocità massima della porta e i dati non vengono inviati o ricevuti.
L'indicatore di collegamento è giallo e l'indicatore di attività è spento	La scheda NIC è collegata a una rete valida a una velocità inferiore alla rispettiva velocità massima della porta e i dati non vengono inviati o ricevuti.

Indicatori dell'unità di alimentazione (PSU)

LED	Descrizione
Verde	Una sorgente di alimentazione valida è collegata alla PSU e la PSU è operativa.
Giallo lampeggiante	Si è verificato un problema con la PSU.
Non acceso	L'alimentazione non è collegata alla PSU.
Verde lampeggiante	È in corso l'aggiornamento del firmware della PSU. ▲ ATTENZIONE Non scollegare il cavo di alimentazione né scollegare l'alimentatore (PSU) durante l'aggiornamento del firmware. Interrompendo l'aggiornamento del firmware, gli alimentatori non funzioneranno.
Verde lampeggiante, quindi spento	Quando una PSU viene collegata a caldo, il LED verde lampeggia cinque volte alla velocità di 4 Hz e poi si spegne. Ciò indica una mancata corrispondenza di PSU in termini di efficienza, serie di funzioni, stato di integrità o tensione supportata. ▲ ATTENZIONE - Se sono installate due PSU, entrambe devono avere lo stesso tipo di etichetta. Ad esempio, l'etichetta EPP (Extended Power Performance). La combinazione di PSU di generazioni precedenti di server PowerEdge non è supportata, anche se le PSU hanno la stessa potenza nominale. Ciò comporta una condizione di mancata corrispondenza di PSU o la mancata accensione del sistema. - Se vengono utilizzate due PSU, queste devono essere dello stesso tipo e avere la stessa potenza massima di uscita. - Quando si corregge una mancata corrispondenza di PSU, sostituire la PSU con l'indicatore lampeggiante. Lo scambio della PSU per creare una coppia abbinata può causare una condizione di errore e un arresto imprevisto del sistema. Per passare da una configurazione a uscita elevata a una configurazione a uscita bassa o viceversa, è necessario spegnere il sistema.

Indicatori unità

LED	Descrizione
Lampeggia in verde due volte al secondo	Identificazione dell'unità o preparazione alla rimozione.
Off	L'unità disco è pronta per essere rimossa. Nota L'indicatore di stato dell'unità disco rimane spenta finché tutte le unità disco non vengono inizializzate dopo l'accensione del sistema.

	Durante questo periodo le unità disco non sono pronte per essere rimosse.
Lampeggia in verde, giallo e quindi si spegne	Errore imprevisto dell'unità.
Lampeggia in giallo quattro volte al secondo	L'unità è guasta.
Lampeggia in verde lentamente	L'unità è in fase di ripristino.
Verde fisso	L'unità è online.
Lampeggia in verde per tre secondi, in giallo per tre secondi, quindi si spegne dopo sei secondi	Il ripristino è stato interrotto.

Bisogno di assistenza?

Link utili

- *Manuale per l'utente di AXIS Camera Station Pro*
- *Accedi ad AXIS Secure Remote Access*
- *Accedere ad AXIS Secure Remote Access v2*
- *Elementi da includere nella lista consentiti di un antivirus per AXIS Camera Station*

Contattare l'assistenza

Se serve ulteriore assistenza, andare su axis.com/support.

T10177843_it

2026-07 (M6.2)

© 2022 – 2026 Axis Communications AB