

Dispozitiv AXIS Camera Station S2224 Mk II Appliance

content

Începere.....	4
Instalarea dispozitivului dvs.	5
.....	5
Exemple de configurare	5
Configurare într-o rețea de supraveghere independentă	5
Configurarea într-o rețea existentă	6
Conectarea comutatorului în mod direct la rețeaua corporativă.....	6
Configurarea dispozitivului	8
Configurarea inițială a înregistratorului Axis	8
Conectare la un server	8
Conectare la un server de la distanță	9
Conectarea la AXIS Secure Remote Access	9
Configurarea AXIS Camera Station Pro	9
Porniți sistemul de video management.....	10
Adăugarea dispozitivelor	10
Configurați metoda de înregistrare	10
Vizualizarea în direct a imaginilor video.....	10
Vezi înregistrările	10
Adăugați marcaje	10
Export recordings (Export înregistrări).....	11
Redarea și verificarea înregistrărilor în AXIS File Player.....	11
Configurarea rețelei.....	11
Configurația portului serverului	11
Considerații privind securitatea.....	12
Licențierea unui sistem online	12
Licența unui sistem care este offline	12
Gestionarea conturilor de utilizator Windows® locale	13
Crearea unui cont de utilizator	13
Crearea unui cont de administrator.....	13
Crearea unui grup local de utilizatori.....	13
Ștergerea unui cont de utilizator.....	13
Schimbarea parolei unui cont de utilizator.....	13
Crearea unui disc de resetare a parolei pentru un cont de utilizator.....	13
Gestionarea conturilor de utilizator AXIS Camera Station Pro	15
Permișiuni utilizator	15
Adăugarea utilizatorilor sau a grupurilor.....	15
Privilegii de utilizator sau de grup	16
Gestionarea dispozitivului.....	19
Actualizarea certificatelor boot securizat.....	19
Verificați starea certificatului dvs.....	19
Acțiuni recomandate.....	19
Actualizați certificatul prin BIOS.....	19
Actualizați certificatul prin actualizare Windows	20
Verificarea versiunii curente a BIOS.....	20
Actualizați BIOS.....	20
Actualizarea Windows®	20
Configurarea setărilor de actualizare Windows®	20
Adăugarea de spațiu de stocare suplimentar	21
Demontarea ramei.....	22
Instalarea hard disk-ului.....	22
Adăugarea unei stocări noi de înregistrare.....	22
Crearea volumului RAID	23
Inițierea volumului RAID în Microsoft Windows®.....	23

Gestionarea comutatorului încorporat.....	24
Despre comutatorul încorporat	24
Autentificarea la pagina de gestionare a comutatorului.....	24
Configurația curentă	24
Prezentare generală.....	24
Gestionarea puterii.....	25
Alocarea puterii.....	25
Activarea și dezactivarea PoE.....	26
Prezentarea generală a rețelei	27
Blocarea și deblocarea porturilor.....	27
Setări.....	28
Configurarea setărilor de rețea.....	28
Configurarea datei și orei	28
Configurarea serverului DHCP	28
Configurarea SNMP	28
Maintenance (Întreținere):	28
Actualizare firmware.....	28
Reinițializarea comutatorului.....	29
Efectuarea de backup la setările comutatorului.....	29
Restabilirea setărilor comutatorului.....	29
Gestionarea certificatelor.....	29
Schimbarea parolei	29
Configurarea setărilor web	29
Resetare la setările implicite din fabrică.....	30
Logs (Jurnale)	30
Crearea rapoartelor comutatorului	30
Specificații.....	31
Prezentare generală a produsului	31
Față și spate	31
Indicatori LED	31
Depanarea.....	33
Resetarea serverului dvs.....	33
Efectuarea unei recuperări a sistemului	33
.....	33
Depanarea AXIS Camera Station Pro.....	34
Aveți nevoie de mai mult ajutor?	35
Linkuri utile.....	35
Contact Asistență.....	35

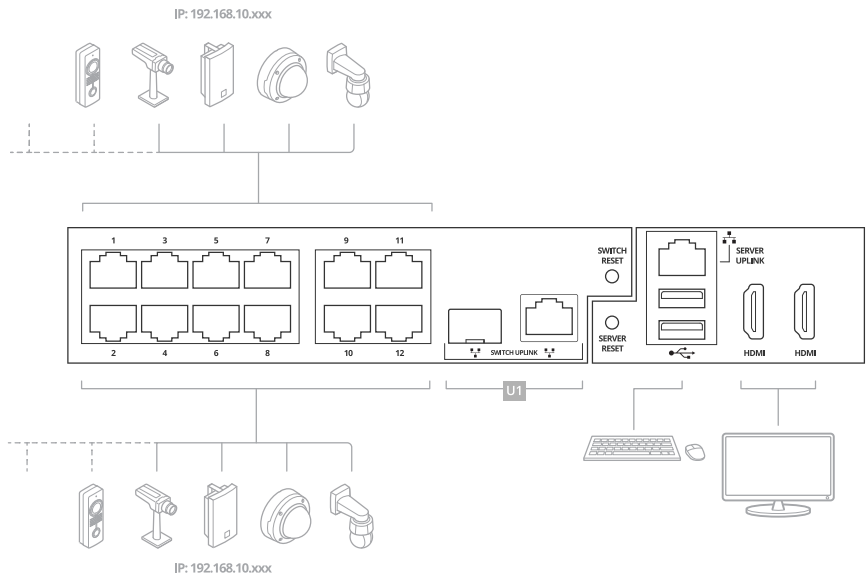
Începere

Fluxul de lucru standard pentru configurarea unui server de înregistrare AXIS Camera Station Pro este:

1. *Instalarea dispozitivului dvs..*
2. Configurarea inițială a Windows®: După instalarea dispozitivului, sunteți ghidat prin câțiva pași pentru a configura regiunea, limba, aspectul tastaturii, un cont de administrator și parola acestuia.
3. Configurarea inițială a înregistratorului Axis: După configurarea inițială a Windows®, se deschide AXIS Recorder Toolbox și sunteți ghidat prin câțiva pași pentru a configura setările de bază și setările necesare, de exemplu, numele computerului, data și ora și rețeaua. Consultați *Configurarea inițială a înregistratorului Axis, on page 8*.
4. Configurați Windows®. Vă recomandăm să:
 - Actualizați Windows® la cea mai recentă versiune. Consultați *Actualizarea Windows®, on page 20*.
 - Creați un cont de utilizator standard. Consultați *Crearea unui cont de utilizator, on page 13*.
5. Actualizați AXIS Camera Station Pro la cea mai recentă versiune.
 - Dacă sistemul dvs. este online: deschideți aplicația AXIS Recorder Toolbox și faceți clic pe **Update AXIS Camera Station Pro (Actualizați AXIS Camera Station Pro)**.
 - Dacă sistemul dvs. este offline: accesați site-ul *axis.com* și descărcați cea mai recentă versiune.
6. Porniți AXIS Camera Station Pro client.
7. *Connect to AXIS Camera Station Pro server (Conectare la serverul AXIS Camera Station Pro)*.
8. *Configurarea AXIS Camera Station Pro, on page 9*.

Instalarea dispozitivului dvs.
Pentru instrucțiuni privind modul de instalare a produsului, consultați ghidul de instalare inclus în cutie sau pe pagina de asistență a produsului de pe axis.com.

Exemple de configurare
Configurare într-o rețea de supraveghere independentă
Puteți crea o rețea de supraveghere independentă care nu are nicio interconectivitate cu nicio altă rețea externă. Această configurare este o instalare de bază de conectare și de redare. Serverul DHCP al comutatorului încorporat este activat în mod implicit. Imediat ce conectați camerele la porturile PoE, ele se vor porni și vor obține o adresă IP și vor fi accesibile prin intermediul AXIS Camera Station Pro.



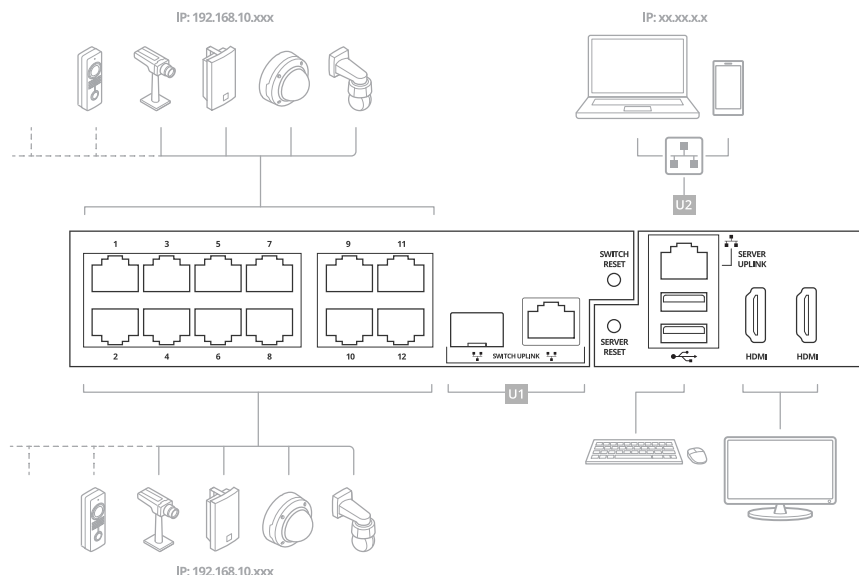
Nivelul de dificultate	Bază
Avantaje	Rețea de supraveghere dedicată, fără nicio interconectivitate cu nicio altă rețea externă Instalare de conectare și de redare
Limitări	Lățime de bandă Buget PoE Fără acces de la distanță
Acțiuni necesare	Schimbarea parolei implicite pentru comutatorul încorporat Înregistrarea licenței AXIS Camera Station Pro
Conectori utilizați	Porturi Ethernet PoE Porturi USB 2.0 (pentru tastatură și mouse) Port afișaj™ sau conector HDMI
Conectori NEUTILIZAȚI	Portul legăturii ascendente a comutatorului Portul legăturii ascendente a serverului Port USB 3.2 (partea frontală) Mufă audio universală (partea frontală)

Configurarea într-o rețea existentă

Puteți crea o rețea de supraveghere în cadrul unei rețele existente. Aceasta înseamnă că rețeaua de supraveghere este separată de rețeaua existentă.

note

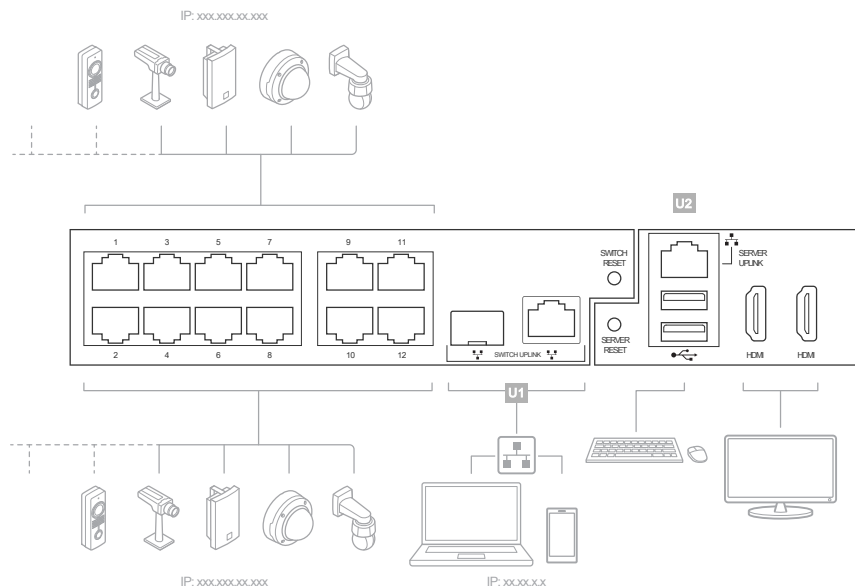
Când utilizați un înregistrator suplimentar, de exemplu înregistratoarele AXIS S30, dispozitivul nu redirecționează datele de rețea din rețeaua de supraveghere către rețeaua de servere pentru înregistrare. Asigurați-vă că înregistratoarele AXIS S30 sunt conectate la aceeași rețea ca și camerele.



Nivelul de dificultate	Advanced (Avansat)
Avantaje	Posibilitatea de a utiliza un client AXIS Camera Station Pro pentru conectarea la seria S22 prin rețea. Segregarea rețelei
Limitări	Poate fi necesar să respectați politicile rețelei corporative
Acțiuni necesare	Schimbarea parolei implicite pentru comutatorul încorporat Înregistrarea licenței AXIS Camera Station Pro
Conectori utilizați	Porturi Ethernet PoE Port Ethernet – Legătură ascendentă a serverului pentru conectarea la rețea (Opțional) Porturi USB 2.0 (pentru tastatură și mouse) (Opțional) Port afișaj™ sau conector HDMI
Conectori NEUTILIZAȚI	Portul legăturii ascendente a comutatorului Port USB 3.2 (partea frontală) Mufă audio universală (partea frontală)

Conectarea comutatorului în mod direct la rețeaua corporativă

Această configurație integrează sistemul direct în rețeaua corporativă existentă, permițând accesul la camere și monitorizarea lor de oriunde din rețea.



Nivelul de dificultate	Advanced (Avansat)
Avantaje	Camerele sunt accesibile din rețeaua corporativă și pot fi monitorizate cu ajutorul unui server SNMP.
Limitări	Poate fi necesar să respectați politicile rețelei corporative
Acțiuni necesare	Deconectarea DHCP la comutator Schimbarea adresei IP a comutatorului cu una statică din rețeaua corporativă Setarea plăcii de rețea interne a computerului (NIC) la DHCP sau la o adresă IP statică în rețeaua corporativă Schimbați parola implicită a comutatorului. Configurarea și înregistrarea AXIS Camera Station Pro
Conectori utilizați	Porturi Ethernet PoE Portul legăturii ascendente a comutatorului (U1) (Opțional) Porturi USB 2.0 (pentru tastatură și mouse) (Opțional) Port afișaj™ sau conector HDMI
Conectori NEUTILIZAȚI	Portul legăturii ascendente a computerului (U2) Port USB 3.2 (partea frontală) Mufă audio universală (partea frontală)

Configurarea dispozitivului

Configurarea inițială a înregistratorului Axis

După ce ați configurat Windows®, AXIS Recorder Toolbox este deschis automat și sunteți ghidat prin asistentul pentru prima configurare. În acest asistent de configurare, puteți configura mai multe setări de bază și setări necesare înainte de a vă gestiona dispozitivul în AXIS Recorder Toolbox.

note

Setările sunt pentru server. Pentru a modifica setările switch, mergeți la pagina de gestionare a switch. Consultați *Setări, on page 28*.

1. Selectați tema **Light (Luminos)** sau **Dark (Întunecat)** și faceți clic pe **Next (Mai departe)** (dacă este disponibilă pentru produsul dvs.).
2. Dacă doriți, schimbați numele computerului și faceți clic pe **Next (Mai departe)**.
3. La **Date and time (Data și ora)**, configurați următoarele setări și faceți clic pe **Next (Mai departe)**.
 - Selectați un fus orar.
 - Pentru a configura un server NTP, selectați **NTP server (Server NTP)** și introduceți adresa serverului NTP.
 - Pentru setarea manuală, selectați **Manual** și selectați o dată și o oră.
4. La **Network settings (Setări rețea)**, configurați următoarele setări și faceți clic pe **Next (Mai departe)**.
 - **Use automatic IP settings (DHCP) (Utilizarea setărilor IP automate (DHCP))** și **Use automatic DNS settings (Utilizarea setărilor DNS automate)** sunt activate implicit.
 - Dacă dispozitivul dvs. este conectat la o rețea cu un server DHCP, adresa IP atribuită, masca de subrețea, portalul și DNS-ul preferat sunt afișate automat.
 - Dacă dispozitivul dvs. nu este conectat la o rețea sau nu este disponibil niciun server DHCP, introduceți manual adresa IP, masca de subrețea, portalul și DNS-ul preferat, în funcție de cerințele rețelei.
5. Faceți clic pe **Finish (Încheiere)**. Dacă ați schimbat numele computerului, AXIS Recorder Toolbox vă va solicita să reporniți dispozitivul.

Conectare la un server

Clientul Dispozitiv AXIS Camera Station S2224 Mk II Appliance vă permite să vă conectați la un singur server sau la mai multe servere în diverse moduri:

Ultimele servere utilizate – Conectare la serverele utilizate în sesiunea anterioară.

Acest computer – Conectare la serverul instalat pe același computer ca și clientul.

Server la distanță – Consultați *Conectare la un server de la distanță, on page 9*.

note

- La prima conectare la un server, clientul verifică ID-ul certificatului serverului. Pentru a vă asigura că vă conectați la serverul corect, comparați ID-ul certificatului cu cel afișat în Service Control (Controlul serviciilor) Dispozitiv AXIS Camera Station S2224 Mk II Appliance.

Listă de servere	Pentru a vă conecta la servere dintr-o listă de servere, selectați un server din meniul vertical Server list (Listă de servere). Faceți clic pe  pentru a crea sau a edita listele de servere.
Import listă de servere	Pentru a importa un fișier de listă de servere exportat din AXIS Camera Station, faceți clic pe Import server list (Import listă de servere) și căutați un fișier .msl.

Ștergere parole salvate	Pentru a șterge numele de utilizator și parolele salvate pentru toate serverele conectate, faceți clic pe Delete saved passwords (Ștergere parole salvate) .
Change client proxy settings (Modificarea setărilor serverului intermediar (proxy) al clientului)	Dacă nu reușiți să vă conectați la un server, s-ar putea să fie necesar să actualizați setările proxy (intermediare) ale clientului. Faceți clic pe Change client proxy settings (Modificați setările serverului intermediar (proxy) al clientului) .

Conectare la un server de la distanță

1. Selectați **Remote server (Server la distanță)**.
2. Selectați un server din lista verticală **Remote server (Server la distanță)** sau introduceți adresa IP sau DNS. Dacă serverul nu apare în listă, faceți clic pe  pentru a reîmprospăta lista tuturor serverelor de la distanță disponibile. Dacă serverul este configurat pentru a accepta clienți pe un port diferit de numărul portului implicit 55754, introduceți adresa IP urmată de numărul portului, de exemplu 192.168.0.5:46001.
3. Efectuați una dintre următoarele:
 - Selectați **Log in as current user (Autentificare ca utilizator curent)** pentru a vă autentifica ca utilizator Windows® curent.
 - Ștergeți **Log in as current user (Autentificare ca utilizator curent)** și faceți clic pe **Log in (Autentificare)**. Selectați **Other user (Alt utilizator)** și furnizați un alt nume de utilizator și altă parolă pentru a vă autentifica cu alte informații de conectare.

Conectarea la AXIS Secure Remote Access

important

Pentru a îmbunătăți securitatea și funcționalitatea, actualizăm Axis Secure Remote Access (Axis Secure Acces de la distanță) (v1) la Axis Secure Remote Access v2 (Axis Secure Acces de la distanță v2). Vom renunța la versiunea curentă în 1 decembrie 2025 și vă recomandăm cu insistență să faceți upgrade la Axis Secure Remote Access v2 înainte de această dată.

Ce înseamnă acest lucru pentru sistemul dumneavoastră Dispozitiv AXIS Camera Station S2224 Mk II Appliance?

- După 1 decembrie 2025, nu veți mai putea să vă accesați de la distanță sistemul utilizând **Axis Secure Remote Access (v1)**.
- Pentru a utiliza **Axis Secure Remote Access v2 (Axis Secure Acces de la distanță v2)**, trebuie să efectuați actualizarea la versiunea 6.8 a AXIS Camera Station Pro. Această actualizare este disponibilă gratuit pentru toți utilizatorii AXIS Camera Station 5 până la 1 martie 2026.

note

- Când încercați să vă autentificați la un server utilizând Axis Secure Remote Access, serverul nu poate face automat upgrade la client.
 - Dacă serverul intermediar (proxy) se află între dispozitivul de rețea și serverul Dispozitiv AXIS Camera Station S2224 Mk II Appliance, trebuie să configurați setările intermediarului (proxy) în Windows la serverul Dispozitiv AXIS Camera Station S2224 Mk II Appliance pentru a accesa serverul utilizând AXIS Secure Remote Access.
1. Faceți clic pe linkul **Conectare la AXIS Secure Remote Access**.
 2. Introduceți datele contului My Axis.
 3. Faceți clic pe **Sign in (Autentificare)**.
 4. Faceți clic pe **Grant (Acordare)**.

Configurarea AXIS Camera Station Pro

Înainte de a începe:

- Configurați-vă rețeaua în funcție de instalația dvs. Consultați *Configurarea rețelei*.
- Configurați porturile serverului, dacă este necesar. Consultați *Configurația portului serverului*.
- Luați în considerare problemele de securitate. Consultați *Considerații privind securitatea*.

După configurațiile necesare, puteți începe să lucrați cu AXIS Camera Station Pro:

1. Porniți sistemul de video management
2. Adăugarea dispozitivelor
3. Configurați metoda de înregistrare, on page 10
4. Vizualizarea în direct a imaginilor video, on page 10
5. Vezi înregistrările, on page 10
6. Adăugați marcaje, on page 10
7. Export recordings (Export înregistrări), on page 11
8. Redarea și verificarea înregistrărilor în AXIS File Player, on page 11

Porniți sistemul de video management

Faceți dublu clic pe pictograma clientului AXIS Camera Station Pro pentru a porni clientul. Când porniți clientul pentru prima dată, acesta încearcă să se conecteze la serverul AXIS Camera Station Pro instalat pe același computer ca și clientul.

Vă puteți conecta la mai multe servere AXIS Camera Station Pro în diferite moduri:

Adăugarea dispozitivelor

La prima pornire a Dispozitiv AXIS Camera Station S2224 Mk II Appliance, se deschide pagina **Add devices (Adăugare dispozitive)**, care caută în rețea dispozitivele de adăugat.

1. Selectați dispozitivele pe care doriți să le adăugați din listă. Dacă nu găsiți un dispozitiv, faceți clic pe **Manual search (Căutare manuală)** sau introduceți un text pentru filtrare.
2. Faceți clic pe **Add (Adăugare)**.
3. Faceți clic pe **Close (Închideți)** pentru a sări peste configurație și a continua mai târziu. Pentru a continua configurația acum:
 - 3.1. Alegeți **Quick configuration (Configurație rapidă)** sau **Site Designer configuration (Configurare site designer)**. Pentru mai multe informații, consultați .
 - 3.2. Selectați **Add image overlay for date, time, and text (Adăugare suprapunere imagine pentru dată, oră și text)** pentru a adăuga suprapuneri la orice cameră Axis care nu dispune încă de una.
 - 3.3. Faceți clic pe **Next (Mai departe)**.
 - 3.4. Selectați **Recording method (Metoda de înregistrare)** preferată.
 - 3.5. Faceți clic pe **Next (Mai departe)**.
 - 3.6. Alegeți **Retention time (Timpul de păstrare)** și **Recording storage (Spațiul de stocare pentru înregistrări)**, apoi faceți clic pe **Finish (Finalizare)** pentru a aplica configurația.

Configurați metoda de înregistrare

1. Accesați **Configuration (Configurație) > Recording and events (Înregistrare și evenimente) > Recording method (Metodă de înregistrare)**.
2. Selectați o cameră.
3. Activați **Motion detection (Detectarea mișcării)** sau **Continuous (Continuă)** sau ambele.
4. Faceți clic pe **Apply (Aplicare)**.

Vizualizarea în direct a imaginilor video

1. Deschideți o filă **Live view (Vizualizare în direct)**.
2. Selectați o cameră pentru a vizualiza în direct imaginile video ale acesteia.

Vezi înregistrările

1. Deschideți o filă **Recordings (Înregistrări)**.
2. Selectați camera de la care doriți să vizualizați înregistrările.

Adăugați marcaje

1. Accesați înregistrarea.
2. În cronologie, măriți, micșorați și mutați cronologia pentru a plasa markerul în poziția dorită.

3. Faceți clic pe .
4. Introduceți numele și descrierea semnului de carte. Folosiți cuvinte-cheie pentru a facilita găsirea marcajului.
5. Selectați **Prevent recording deletion (Prevenirea ștergerii înregistrării)** pentru a bloca înregistrarea.

note

Pentru a debloca înregistrarea, ștergeți **Prevent recording deletion (Prevenirea ștergerii înregistrării)** sau ștergeți marcajul.

6. Faceți clic pe **OK** pentru a salva marcajul.

Export recordings (Export înregistrări)

1. Deschideți o filă **Recordings (Înregistrări)**.
2. Selectați camera de la care doriți să exportați înregistrările.
3. Faceți clic pe  pentru a afișa marcajele de selecție.
4. Trageți marcajele pentru a include înregistrările pe care doriți să le exportați.
5. Faceți clic pe  pentru a deschide fila **Export**.
6. Faceți clic pe **Export...**

Redarea și verificarea înregistrărilor în AXIS File Player

1. Accesați folderul cu înregistrările exportate.
2. Faceți dublu clic pe **AXIS File Player**.
3. Faceți clic pe  pentru a afișa notele înregistrării.
4. Pentru a verifica semnătura digitală:
 - 4.1. Accesați **Tools (Instrumente) > Verify digital signature (Verificarea semnăturii digitale)**.
 - 4.2. Selectați **Validate with password (Validare cu parolă)** și introduceți parola.
 - 4.3. Faceți clic pe **Verify (Verificați)** pentru a vedea rezultatele verificării.

note

- O semnătură digitală este diferită de signed video (videoclipul semnat). Un videoclip semnat vă permite să identificați camera de la care provine înregistrarea, astfel încât să puteți verifica dacă aceasta nu a fost supusă unei modificări neautorizate. Pentru mai multe informații, consultați *Signed video (Semnat video)* și manualul utilizatorului camerei.
- Dacă fișierele stocate nu au nicio legătură cu o bază de date AXIS Camera Station (fișiere neindexate), trebuie să le convertiți pentru a le face redabile în AXIS File Player. Contactați asistența tehnică Axis pentru a vă ajuta să vă convertiți fișierele.

Configurarea rețelei

Configurați setările intermediar (proxy) sau firewall înainte de a utiliza Dispozitiv AXIS Camera Station S2224 Mk II Appliance dacă clientul, serverul și dispozitivele de rețea conectate se află în rețele diferite.

Setări server intermediar (proxy) client

Dacă un server intermediar (proxy) se află între client și server, configurați setările proxy în Windows, pe computerul client. Pentru mai multe informații, contactați serviciul de asistență Axis.

Setări server intermediar (proxy)

Dacă serverul intermediar (proxy) se află între dispozitivul de rețea și server, trebuie să configurați setările proxy în Windows pe server. Pentru mai multe informații, contactați serviciul de asistență Axis.

NAT și firewall

Atunci când un NAT sau un firewall separă clientul de server, configurați-l astfel încât să se asigure că portul HTTP, portul TCP și portul de streaming specificate în Controlul serviciului Dispozitiv AXIS Camera Station S2224 Mk II Appliance pot trece prin acesta. Pentru ajutor, contactați administratorul de rețea.

Configurația portului serverului

Dispozitiv AXIS Camera Station S2224 Mk II Appliance utilizează porturile 55752 (HTTP), 55754 (TCP), 55756 (comunicare mobilă) și 55757 (redare mobilă în flux) pentru comunicarea dintre server și client. Dacă este necesar, puteți modifica porturile în AXIS Camera Station Service Control.

Considerații privind securitatea

Pentru a preveni accesul neautorizat la camere și înregistrări:

- Utilizați parole puternice pentru toate dispozitivele de rețea (camere, codoare de imagine video și dispozitive auxiliare).
- Instalați serverul Dispozitiv AXIS Camera Station S2224 Mk II Appliance, camerele, codorii de imagine video și dispozitivele auxiliare într-o rețea securizată, separată de rețeaua biroului. Puteți instala clientul Dispozitiv AXIS Camera Station S2224 Mk II Appliance pe un computer dintr-o altă rețea, de exemplu, o rețea cu acces la internet.
- Asigurați-vă că toți utilizatorii au parole puternice.

Licențierea unui sistem online

Pentru a utiliza licențierea automată, trebuie să vă înregistrați sistemul și să îl conectați la o organizație.

1. Accesați **Configuration (Configurație) > Licenses (Licențe) > Management (Gestionare)**.
2. Asigurați-vă că **Automatic licensing (Licențiere automată)** este activată.
3. Faceți clic pe **Register... (Înregistrare...)**.
4. Autentificați-vă cu ajutorul contului My Axis și urmați instrucțiunile de pe ecran.
5. Faceți clic pe **Go to AXIS License Manager (Accesați AXIS License Manager)** pentru a vă gestiona licențele. Pentru mai multe informații, citiți *manualul de utilizare pentru My Systems de pe site-ul help.axis.com*.

Licența unui sistem care este offline

Pentru a vă licenția sistemul manual:

1. Accesați **Configuration (Configurație) > Licenses (Licențe) > Management (Gestionare)**.
2. Dezactivați **Automatic licensing (Licențiere automată)**.
3. Faceți clic pe **Export system file... (Exportați fișierul de sistem...)** și salvați fișierul pe computer.

note

Trebuie să aveți o conexiune la internet pentru a accesa AXIS License Manager. Dacă computerul clientului nu are internet, copiați fișierul de sistem pe un computer care are internet.

4. Deschideți *AXIS License Manager (Manager licențe AXIS)*.
5. În **AXIS License Manager**:
 - 5.1. Selectați organizația corectă sau creați una dacă nu ați făcut-o deja. Pentru mai multe informații, citiți *manualul de utilizare pentru My Systems de pe site-ul help.axis.com*.
 - 5.2. Accesați **System setup (Configurație sistem)**.
 - 5.3. Faceți clic pe **Upload system file (Încărcați fișierul de sistem)**.
 - 5.4. Faceți clic pe **Upload system file (Încărcați fișierul de sistem)** și selectați fișierul de sistem.
 - 5.5. Faceți clic pe **Upload system file (Încărcați fișierul de sistem)**.
 - 5.6. Faceți clic pe **Download license file (Descărcați fișierul de licență)**.
6. Reveniți la clientul Dispozitiv AXIS Camera Station S2224 Mk II Appliance.
7. Faceți clic pe **Import license file... (Importați fișierul de licență...)** și selectați fișierul de licență.
8. Faceți clic pe **Go to AXIS License Manager (Accesați AXIS License Manager)** pentru a vă gestiona licențele.

Gestionarea conturilor de utilizator Windows® locale

Crearea unui cont de utilizator

Pentru a vă păstra datele cu caracter personal și informațiile mai sigure, vă recomandăm să adăugați o parolă pentru fiecare cont local.

important

După ce ați creat o parolă pentru un cont local, nu o uitați. Nu există nicio modalitate de a recupera o parolă pierdută pentru conturile locale.

1. Accesați **Settings (Setări) > Accounts (Conturi) > Other users (Alți utilizatori) > Add other user (Adăugați alt utilizator)** și faceți clic pe **Add account (Adăugați cont)**.
2. Faceți clic pe **I don't have this person's sign-in information (Nu am informațiile de autentificare ale acestei persoane)**.
3. Faceți clic pe **Add a user without a Microsoft account (Adăugați un utilizator fără un cont Microsoft)**.
4. Introduceți un nume de utilizator, o parolă și un indiciu pentru parolă.
5. Faceți clic pe **Next (Mai departe)** și urmați instrucțiunile.

Crearea unui cont de administrator

1. Accesați **Settings (Setări) > Accounts (Conturi) > Other people (Alte persoane)**.
2. Accesați contul pe care doriți să îl modificați și faceți clic pe **Change account type (Schimbare tip cont)**.
3. Accesați **Account type (Tip cont)** și selectați **Administrator**.
4. Faceți clic pe **OK**.
5. Reporniți dispozitivul și autentificați-vă în noul cont de administrator.

Crearea unui grup local de utilizatori

1. Accesați **Computer Management (Management computer)**.
2. Accesați **Local Users and Groups (Utilizatori și grupuri locale) > Group (Grup)**.
3. Faceți clic dreapta pe **Group (Grup)** și selectați **New Group (Grup nou)**.
4. Introduceți un nume de grup și o descriere.
5. Adăugarea membrilor grupului:
 - 5.1. Faceți clic pe **Add (Adăugare)**.
 - 5.2. Faceți clic pe **Advanced (Avansat)**.
 - 5.3. Găsiți contul (conturile) de utilizator pe care doriți să îl (le) adăugați la grup și faceți clic pe **OK**.
 - 5.4. Faceți din nou clic pe **OK**.
6. Faceți clic pe **Create (Creare)**.

Ștergerea unui cont de utilizator

important

Când ștergeți un cont, ștergeți contul de utilizator de pe ecranul de autentificare. De asemenea, ștergeți toate fișierele, setările și datele programului memorate în contul de utilizator.

1. Accesați **Settings (Setări) > Accounts (Conturi) > Other people (Alte persoane)**.
2. Accesați contul pe care doriți să îl ștergeți și faceți clic pe **Remove (Ștergere)**.

Schimbarea parolei unui cont de utilizator

1. Autentificați-vă cu un cont de administrator.
2. Accesați **User Accounts (Conturi utilizator) > User Accounts (Conturi utilizator) > Manage another account in sequence (Gestionați un alt cont în secvență)**.
Veți vedea o listă cu toate conturile de utilizator de pe dispozitiv.
3. Selectați contul de utilizator a cărui parolă doriți să o schimbați.
4. Faceți clic pe **Change the password (Schimbarea parolei)**.
5. Introduceți noua parolă și faceți clic pe **Change password (Schimbarea parolei)**.

Crearea unui disc de resetare a parolei pentru un cont de utilizator

Vă recomandăm să creați un disc de resetare a parolei pe un USB flash drive. În felul acesta vă puteți reseta parola. Fără un disc de resetare a parolei, nu vă puteți reseta parola.

note

Dacă utilizați Windows® 10 sau o versiune ulterioară, puteți adăuga întrebări de securitate la contul dvs. local în cazul în care vă uitați parola, astfel încât să nu fie nevoie să creați un disc de resetare a parolei. Pentru a face acest lucru, accesați **Start** și faceți clic pe **Settings (Setări) > Sign-in options (Opțiuni de autentificare) > Update your security questions (Actualizați-vă întrebările de securitate)**.

1. Autentificați-vă la dispozitiv cu un cont de utilizator local. Nu puteți crea un disc de resetare a parolei pentru un cont conectat.
2. Conectați un USB flash drive gol la dispozitivul dvs.
3. Din câmpul de căutare Windows®, accesați **Create a password reset disk (Creați un disc de resetare a parolei)**.
4. În asistentul de configurare **Forgotten Password (Parolă uitată)**, faceți clic pe **Next (Mai departe)**.
5. Selectați USB flash drive și faceți clic pe **Next (Mai departe)**.
6. Introduceți parola dvs. curentă și faceți clic pe **Next (Mai departe)**.
7. Urmați instrucțiunile de pe ecran.
8. Scoateți USB flash drive și păstrați-l într-un loc sigur. Nu trebuie să creați un disc nou atunci când vă schimbați parola, chiar dacă o schimbați de mai multe ori.

Gestionarea conturilor de utilizator AXIS Camera Station Pro

Permisuni utilizator

Accesați **Configuration (Configurație) > Security (Securitate) > User permissions (Permisuni utilizatori)** pentru a vedea utilizatorii și grupurile din Dispozitiv AXIS Camera Station S2224 Mk II Appliance.

note

Administratorilor computerului care rulează serverul Dispozitiv AXIS Camera Station S2224 Mk II Appliance li se acordă automat privilegii de administrator în Dispozitiv AXIS Camera Station S2224 Mk II Appliance. Nu puteți modifica sau elimina privilegiile grupului Administratori.

Înainte de a putea adăuga un utilizator sau un grup, asigurați-vă că aceștia sunt înregistrați pe computerul local sau că dețin un cont de utilizator Windows® Active Directory. Pentru a adăuga utilizatori sau grupuri, consultați *Adăugarea utilizatorilor sau a grupurilor*.

Atunci când un utilizator face parte dintr-un grup, el beneficiază de cel mai înalt nivel de permisiuni pentru rol, atribuit fie lui personal, fie grupului. De exemplu, un utilizator care are acces la camera X și care face parte, de asemenea, dintr-un grup cu acces la camerele Y și Z, are acces la toate cele trei camere.

	Indică faptul că intrarea este pentru un singur utilizator.
	Indică faptul că intrarea este pentru un grup.
Name (Nume)	Numele de utilizator așa cum apare în computerul local sau în Active Directory.
Domain (Domeniu)	Domeniul din care face parte utilizatorul sau grupul.
Role (Rol)	Rolul de acces atribuit utilizatorului sau grupului. Valori posibile: Administrator, Operator și Viewer (Supraveghetor).
Details (Detalii)	Informații detaliate referitoare la utilizator așa cum apar pe computerul local sau în Active Directory.
Server	Serverul din care face parte utilizatorul sau grupul.

Adăugarea utilizatorilor sau a grupurilor

Utilizatorii și grupurile Microsoft Windows® și Active Directory pot accesa Dispozitiv AXIS Camera Station S2224 Mk II Appliance. Pentru a adăuga un utilizator la Dispozitiv AXIS Camera Station S2224 Mk II Appliance, trebuie să adăugați utilizatori sau un grup la Windows®.

Pentru a adăuga un utilizator în Windows® 10 și 11:

- Apăsați tasta Windows + X și selectați **Computer Management (Gestionare computer)**.
- În fereastra **Computer Management (Gestionare computer)**, navigați la **Local Users and Groups (Utilizatori locali și grupuri locale) > Users (Utilizatori)**.
- Faceți clic dreapta pe **Users (Utilizatori)** și selectați **New User (Utilizator nou)**.
- În fereastra de dialog, introduceți detaliile noului utilizator și ștergeți **User must change password at next login (Utilizatorul trebuie să schimbe parola la următoarea autentificare)**.
- Faceți clic pe **Create (Creare)**.

Dacă utilizați un domeniu Active Directory, consultați administratorul de rețea.

Adăugarea utilizatorilor sau a grupurilor

1. Accesați **Configuration (Configurație) > Security (Securitate) > User permissions (Permisuni utilizatori)**.
2. Faceți clic pe **Add (Adăugare)**. Utilizatorii și grupurile disponibile apar în listă.
3. La **Scope (Domeniu de aplicare)**, selectați locul în care urmează să fie căutați utilizatorii și grupurile.
4. La **Show (Afișare)**, selectați pentru a afișa utilizatorii sau grupurile. Este posibil ca rezultatele căutării să nu apară dacă există prea mulți utilizatori sau prea multe grupuri. Folosiți filtrul pentru a restrânge rezultatele.
5. Selectați utilizatorii sau grupurile și faceți clic pe **Add (Adăugare)**.

Domeniul de aplicare	
Server	Selectați pentru a căuta utilizatori sau grupuri pe computerul local.
Domain (Domeniu)	Selectați pentru a căuta utilizatori sau grupuri Active Directory.
Selected server (Server selectat)	Când sunteți conectat(ă) la mai multe servere Dispozitiv AXIS Camera Station S2224 Mk II Appliance, selectați un server pentru a căuta utilizatori sau grupuri pe acel server.

Configurarea unui utilizator sau grup

1. Selectați un utilizator sau un grup din listă.
2. La Role (Rol), selectați Administrator, Operator, sau Viewer (Supraveghetor).
3. Dacă ați selectat Operator sau Viewer (Supraveghetor), puteți configura privilegiile utilizatorului sau ale grupului. Consultați *Privilegii de utilizator sau de grup*.
4. Faceți clic pe Save (Salvare).

Eliminarea unui utilizator sau grup

1. Selectați utilizatorul sau grupul.
2. Faceți clic pe Remove (Eliminare).
3. În fereastra de dialog pop-up, faceți clic pe OK pentru a elimina utilizatorul sau grupul.

Privilegii de utilizator sau de grup

Există trei roluri pe care le puteți atribui unui utilizator sau grup. Pentru a afla cum se definește rolul unui utilizator sau al unui grup, consultați *Adăugarea utilizatorilor sau a grupurilor*.

Administrator – Acces complet la întregul sistem, inclusiv acces la imaginile video în direct și înregistrate ale tuturor camerelor, la toate porturile I/O și la vizualizări. Acest rol este necesar pentru a accesa configurația sistemului.

Operator – Selectați camere, vizualizări și porturi I/O pentru a obține acces la video-uri în direct și înregistrate. Un operator are acces deplin la toate funcționalitățile Dispozitiv AXIS Camera Station S2224 Mk II Appliance, cu excepția configurării sistemului.

Viewer (Supraveghetor): – Acces la imaginile video în direct ale camerelor selectate, la porturile I/O și la vizualizări. Un supraveghetor nu are acces la înregistrările video sau la configurarea sistemului.

Camere

Următoarele privilegii de acces sunt disponibile pentru utilizatorii sau grupurile cu rolul Operator sau Viewer (Supraveghetor).

Access (Acces)	Permite accesul la cameră și la toate funcțiile acesteia.
Video	Permite accesul la imagini video în direct de la cameră.
Audio listen (Ascultare audio)	Permite accesul la ascultare de la cameră.
Audio speak (Comunicare audio)	Permite accesul pentru a vorbi la cameră.
Manual Recording (Înregistrare manuală)	Permite pornirea și oprirea manuală a înregistrărilor.

Mechanical PTZ (PTZ mecanic)	Permite accesul la comenzile PTZ mecanice. Disponibil numai pentru camerele cu PTZ mecanic.
PTZ priority (Prioritate PTZ)	Setează prioritatea PTZ. Un număr mai mic înseamnă o prioritate mai mare. Nicio prioritate atribuită nu este setată la 0. Un administrator are cea mai mare prioritate. În mod implicit, atunci când un rol cu prioritate mai mare operează o cameră PTZ, celelalte roluri nu pot opera aceeași cameră timp de 10 secunde. Disponibil numai pentru camerele cu PTZ mecanic care au selectat Mechanical PTZ (PTZ mecanic) .

Vizualizări

Următoarele privilegii de acces sunt disponibile pentru utilizatorii sau grupurile cu rolul **Operator** sau **Viewer (Supraveghetor)**. Puteți selecta mai multe vizualizări și puteți seta privilegiile de acces.

Access (Acces)	Permite accesul la vizualizări în Dispozitiv AXIS Camera Station S2224 Mk II Appliance.
Edit (Editare)	Permite editarea vederilor în Dispozitiv AXIS Camera Station S2224 Mk II Appliance.

I/O

Următoarele privilegii de acces sunt disponibile pentru utilizatorii sau grupurile cu rolul **Operator** sau **Viewer (Supraveghetor)**.

Access (Acces)	Permite accesul complet la portul I/O.
Read (Citire)	Permite vizualizarea stării portului I/O fără a o modifica.
Write (Scriere)	Permite modificarea stării portului I/O.

System (Sistem)

Nu puteți configura privilegiile de acces din listă evidențiate cu gri. O bifă înseamnă că utilizatorul sau grupul are acest privilegiu în mod implicit.

Următoarele privilegii de acces sunt disponibile pentru utilizatorii sau grupurile cu rolul **Operator**. **Take snapshots (Realizare instantanee)** este disponibil și pentru rolul **Viewer (Supraveghetor)**.

Take snapshots (Realizare instantanee)	Permite realizarea de instantanee în modul de vizualizare în direct și în modul de înregistrare.
Export recordings (Export înregistrări)	Permiteți exportarea înregistrărilor.
Generate incident report (Generare raport de incident)	Permiteți generarea rapoartelor de incident.
Prevent access to recordings older than (Prevenire acces la înregistrările mai vechi de)	Împiedică accesul la înregistrările mai vechi decât numărul de minute specificat. Utilizatorii nu găsesc aceste înregistrări atunci când efectuează o căutare.
Access alarms, tasks, and logs (Acces jurnale de alarmă, sarcini și registre)	Se primesc notificări de alarmă și se permite accesul la bara Alarms and tasks (Alarme și sarcini) și la fila Logs (Jurnale) .

Access data search (Acces căutare de date)	Permite căutarea de date pentru a urmări ce s-a întâmplat la momentul unui eveniment.
Adăugați categorii la evenimente	Permiteți adăugarea de categorii la evenimente în fila Recordings (Înregistrări) .
Eliminați categorii de la eveniment	Permiteți eliminarea de categorii de la evenimente în fila Recordings (Înregistrări) .

Access control (Control de acces)

Următoarele privilegii de acces sunt disponibile pentru utilizatorii sau grupurile cu rolul **Operator**. **Access Management (Gestionare acces)** este disponibil și pentru rolul **Viewer (Supraveghetor)**.

Access control configuration (Configurare control de acces)	Permite configurarea pentru uși și zone, profiluri de identificare, formatele de carduri și coduri PIN, comunicație criptată și multi-server.
Access management (Gestionare acces)	Permite gestionarea accesului și accesul la setările Active Directory.

Următoarele privilegii de acces sunt disponibile pentru utilizatorii sau grupurile cu rolul **Viewer (Supraveghetor)**.

Monitorizarea stării sistemului

Următoarele privilegii de acces sunt disponibile pentru utilizatorii sau grupurile cu rolul **Operator**. **Access to system health monitoring (Acces la monitorizarea stării sistemului)** este disponibil și pentru rolul **Viewer (Supraveghetor)**.

Configuration of system health monitoring (Configurare monitorizare stare sistem)	Permite configurarea monitorizării stării sistemului.
Access to system health monitoring (Acces la monitorizarea stării sistemului)	Permite accesul la monitorizarea stării sistemului.

Gestionarea dispozitivului

Actualizarea certificatelor boot securizat

Microsoft va retrage certificatele boot securizat din 2011 în iunie 2026 și le va înlocui cu noi certificate din 2023. Pentru a vă asigura că înregistratorul dvs. funcționează în condiții de siguranță, instalați certificatele din 2023 înainte de acea dată.

Pentru instalarea certificatelor din 2023 este necesar Windows 10 LTSC (Long-Term Servicing Channel) sau Windows 11 LTSC. Dacă dispozitivul dvs. se află încă în perioada de garanție, dar are sistemul de operare Windows 10 SAC (Semi-Annual Channel) în loc de o versiune LTSC, contactați serviciul de asistență tehnică Axis. Ei vă pot spune dacă puteți trece la o versiune LTSC înainte de a actualiza BIOS-ul sau de a modifica orice certificat.

note

După iunie 2026, dispozitivele care nu dețin certificatele din 2023 vor continua să funcționeze normal, dar nu vor mai primi noi măsuri de securitate pentru procesul de boot inițial, inclusiv actualizări ale Windows Boot Manager și liste de revocare pentru noile vulnerabilități.

Verificați starea certificatului dvs.

Pentru a verifica dacă certificatele din 2023 sunt instalate și dacă programul de pornire Windows a fost actualizat, utilizați una dintre următoarele metode:

Metoda 1:

1. Deschideți Registry Editor (Editorul de registru).
2. Accesați HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing.
3. Verificați valoarea UEFICA2023Status. Dacă valoarea indică Updated (Actualizat), înseamnă că este instalat certificatul din 2023.

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

Metoda 2:

1. Deschideți Windows Security (Securitate Windows).
2. Accesați Device security (Securitate dispozitiv).
3. La Secure boot (Boot securizat), verificați mesajul de stare. Dacă certificatul este actualizat, pe card se afișează: „Funcția boot securizat este activată și toate actualizările necesare ale certificatelor au fost aplicate. No further certificate changes are needed.” (Nu sunt necesare alte modificări ale certificatului.)

Secure boot

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

note

Windows Security afișează starea certificatului numai dacă pe dispozitivul dvs. este instalată actualizarea cumulativă din 14 aprilie 2026 sau o versiune ulterioară. Dacă nu apare niciun mesaj privind starea certificatului, instalați cea mai recentă actualizare Windows sau folosiți Metoda 1 în loc de aceasta.

Acțiuni recomandate

O actualizare a BIOS-ului stochează definitiv certificatele din 2023 în firmware. Aceasta este cea mai fiabilă metodă și o recomandăm chiar și în cazul în care ați instalat deja certificatele prin Actualizare Windows.

important

Dacă instalați certificatele doar prin Actualizare Windows și apoi reseați cheile boot securizat din BIOS la valorile implicite din fabrică, certificatele se vor pierde, iar dispozitivul nu va mai porni cu funcția boot securizat activată. Actualizați BIOS-ul pentru a face certificatele permanente înainte de a resea cheile boot securizat.

Actualizați certificatul prin BIOS

Instalați versiunea BIOS enumerată pentru modelul dvs. sau o versiune ulterioară. Le puteți descărca de pe pagina produsului de pe Axis.com:

Model	Versiunea minimă a BIOS-ului
AXIS S2208	TBC
AXIS S2212	TBC
AXIS S2216	TBC
AXIS S2224	TBC
AXIS S2108	Z218-004
AXIS S2208 Mk II	Z670-005
AXIS S2212 Mk II	Z671-005
AXIS S2216 Mk II	Z672-005
AXIS S2224 Mk II	Z673-005

Actualizați certificatul prin actualizare Windows

Dacă încă nu este disponibilă o actualizare BIOS pentru modelul dvs., puteți obține certificatele din 2023 prin actualizarea Windows.

important

Certificatele instalate în acest mod sunt stocate în baza de date curentă a boot securizat, nu în firmware. Dacă reșetați cheile boot securizat din BIOS la valorile implicite din fabrică, veți pierde certificatele, și este posibil ca dispozitivul să nu mai poată porni cu boot securizat activat. Instalați o actualizare BIOS imediat este disponibilă una pentru modelul dvs., chiar dacă ați folosit deja această metodă.

Pentru a utiliza această cale:

1. Asigurați-vă că dispozitivul dvs. are sistemul de operare Windows 10 LTSC sau Windows 11 LTSC.
2. Instalați toate actualizările Windows lansate în 14 aprilie 2026 sau ulterior.
3. Accesați **Windows Security (Securitatea Windows) > Device security (Securitatea dispozitivului) > Secure Boot (Boot securizat)** pentru a verifica starea certificatului dvs.
4. Dacă certificatul nu se actualizează după instalarea celor mai recente actualizări, verificați valoarea în registrul **UEFICA2023Status**. Dacă dispozitivul dvs. nu este eligibil pentru actualizarea automată, actualizați BIOS sau contactați serviciul de asistență tehnică Axis.

important

Nu revocați manual certificatul din 2011 până când nu vă asigurați că toate suporturile de recuperare, mediile de boot și driverele din mediul dvs. sunt semnate cu certificatul din 2023. Dacă revocați certificatul din 2011 prea devreme, dispozitivul dvs. nu va mai putea porni cu funcția boot securizat activată.

Verificarea versiunii curente a BIOS

Pentru a verifica BIOS-ul curent:

1. Porniți dispozitivul și apăsați în mod repetat **DEL** până când apare logo-ul Axis.
2. Numărul versiunii este afișat ca prima intrare la **Main (Principal)**.

Actualizați BIOS

Urmați instrucțiunile incluse în ghidul BIOS, disponibil pe pagina de descărcare a fișierului BIOS.

Actualizarea Windows®

Windows® verifică periodic dacă există actualizări. Atunci când este disponibilă o actualizare, dispozitivul descarcă automat actualizarea, însă trebuie să o instalați manual.

note

Înregistrarea va fi întreruptă în timpul unei reporniri programate a sistemului.

Pentru a verifica manual dacă există actualizări:

1. Accesați **Settings (Setări) > Windows Update (Actualizare Windows)**.
2. Faceți clic pe **Check for updates (Verificați dacă există actualizări)**.

Configurarea setărilor de actualizare Windows®

Este posibil să modificați modul și momentul în care Windows® își face actualizările, în funcție de nevoile dvs.

note

Toate înregistrările în curs de derulare se opresc în timpul unei reporniri programate a sistemului.

1. Deschideți aplicația Run (Rulare).
 - Accesați **Windows System (Sistem Windows) > Run (Rulare)** sau
2. Tastați `gpedit.msc` și faceți clic pe **OK**. Se deschide Local Group Policy Editor (Editorul de politici de grup locale).
3. Accesați **Computer Configuration (Configurarea computerului) > Administrative Templates (Modele administrative) > Windows Components (Componente Windows) > Windows Update (Actualizare Windows)**.
4. Configurați setările după cum este necesar, vezi exemplul.

example:

Pentru a descărca și a instala automat actualizările fără nicio interacțiune a utilizatorului și pentru a reporni dispozitivul, dacă este necesar, în afara orelor programului de muncă, utilizați următoarea configurație:

1. Deschideți **Always automatically restart at the scheduled time (Reporniți întotdeauna automat la ora programată)** și selectați:
 - 1.1. **Activat**
 - 1.2. **The restart timer will give users this much time to save their work (minutes) (Temporizatorul de repornire va oferi utilizatorilor acest timp pentru a-și salva munca (minute))**: 15.
 - 1.3. Faceți clic pe **OK**.
2. Deschideți **Configure Automatic Updates (Configurarea actualizărilor automate)** și selectați:
 - 2.1. **Activat**
 - 2.2. **Configure Automatic updates (Configurarea actualizărilor automate)**: Descărcare automată și programarea instalării
 - 2.3. **Programarea zilei de instalare**: În fiecare duminică
 - 2.4. **Programarea orei de instalare**: 00:00
 - 2.5. Faceți clic pe **OK**.
3. Deschideți **Allow Automatic Updates immediate installation (Permiteți instalarea imediată a actualizărilor automate)** și selectați:
 - 3.1. **Activat**
 - 3.2. Faceți clic pe **OK**.

Adăugarea de spațiu de stocare suplimentar

Condițiile impuse stocării pot fi diferite. Timpul de păstrare a datelor stocate sau pentru stocarea înregistrărilor de înaltă rezoluție duce adesea la necesitatea de a instala mai mult spațiu de stocare. Această secțiune explică modul de instalare a unui hard disk suplimentar în produsul dvs. din seria AXIS S22.

note

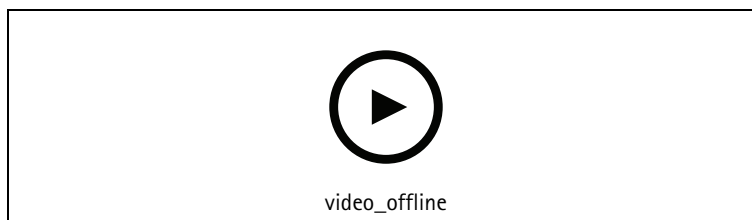
Urmați instrucțiunile de mai jos pentru a adăuga spațiu de stocare suplimentar la produsele AXIS S22 aplicabile. Aceste instrucțiuni sunt date ca atare, iar Axis Communications AB nu își asumă nicio responsabilitate pentru pierderea de date sau configurarea greșită în timpul acestor pași. Trebuie luate măsurile de precauție standard pentru a face copii de rezervă ale datelor care sunt esențiale pentru afacere. Următoarea procedură de extindere a spațiului de stocare nu va fi asistată de Asistența tehnică Axis.

note

Pentru a evita descărcările electrostatice, vă recomandăm să utilizați întotdeauna un covoraș antistatic și o curea antistatică atunci când lucrați la componentele interne ale sistemului.

Garanție

Informații detaliate referitoare la garanție sunt disponibile pe: www.axis.com/support/warranty.



Demontarea ramei

1. Slăbiți cele două șuruburi cu cap rotund situate pe fiecare parte a ramei.
2. Demontarea ramei.

Instalarea hard disk-ului

caution

- Utilizați numai hard disk-urile care au fost testate și aprobate pentru utilizarea cu seria AXIS S22.
 - Când instalați un hard disk, asigurați-vă că suportul hard disk-ului este împins până la capăt în interior. Veți auzi un clic atunci când suportul disk-ului este blocat.
 - Înainte de a instala un hard disk, asigurați-vă că cablul de alimentare este deconectat.
1. Deconectați sistemul și asigurați-vă că alimentarea este oprită.
 2. Deconectați cablul de alimentare.
 3. Apăsăți butonul de deblocare de pe partea frontală a suportului hard disk-ului și deschideți mânerul suportului hard disk-ului.
 4. Scoateți suportul hard disk-ului folosind mânerul.
 5. Introduceți un hard disk în suportul hard disk-ului.
 6. Fixați hard disk-ul de suportul pentru hard disk cu patru șuruburi.
 7. Introduceți suportul hard disk-ului în slotul hard disk-ului până când suportul se conectează la placa de bază.
 8. Închideți mânerul suportului hard disk-ului pentru a bloca hard disk-ul în poziție.
 9. Reatașați rama frontală.
 10. Porniți sistemul.

Adăugarea unei stocări noi de înregistrare

1. Creați și formatați o nouă partiție a hard disk-ului în Windows:
 - 1.1. Faceți clic dreapta pe **Start menu (meniul Start)** și selectați **Disk Management (Management disc)**.
 - 1.2. Faceți clic pe **OK** dacă apare fereastra pop-up **Initialize Disk (Inițializare disk)**. Dacă nu apare, faceți clic dreapta pe noul hard drive și selectați **Initialize Disk (Inițializare disk)**.
 - 1.3. Faceți clic dreapta pe o regiune nealocată de pe disk-ul nou inițializat și selectați **New Simple Volume (Volum simplu nou)**.
 - 1.4. Urmați instrucțiunile expertului pentru a seta dimensiunea volumului, a atribui o literă de unitate și a formata partiția.
 - 1.5. Finalizați expertul pentru a crea noul volum simplu.
2. Adăugați un nou spațiu de stocare pentru înregistrări în AXIS Camera Station Pro:
 - 2.1. Deschideți **AXIS Camera Station Pro**.
 - 2.2. Accesați **Storage (Stocare) > Management (Gestionare)**.
 - 2.3. Faceți clic pe **Add... (Adăugare...)**
 - 2.4. Selectați unitatea drive nou adăugată și faceți clic pe **OK**.
 - 2.5. Accesați **Storage (Stocare) > Selection (Selectare)**.
 - 2.6. Selectați dispozitivele pe care doriți să transferați datele înregistrate pe noua unitate drive.

- 2.7. În lista derulantă **Store to (Stocare pe)**, selectați noua unitate drive și faceți clic pe **Apply (Aplicare)**.

Pentru mai multe informații despre gestionarea stocării, consultați *AXIS Camera Station Pro – User manual (Manual de utilizare)*.

Crearea volumului RAID

1. Asigurați-vă că discurile care vor fi utilizate în volumul RAID sunt detectate.
 - 1.1. Porniți dispozitivul și apăsați imediat F12 până când apare logoul Axis.
 - 1.2. În meniul de bootare UEFI, selectați **Device Configuration (Configurație dispozitiv)** și apăsați Enter.
 - 1.3. În meniul Intel® Rapid Storage Technology, asigurați-vă că discurile sunt afișate corect la **Non-RAID Physical Disks (Discuri fizice non-RAID)**.

note

Numai RAID 0 și RAID 1 sunt disponibile pe dispozitivele care au spațiu fizic pentru doar o singură unitate suplimentară.

2. În meniul Intel Rapid Storage Technology, selectați **Create RAID Volume (Creare volum RAID)** și apăsați Enter.
3. Introduceți un nume pentru volum.
4. Alegeți nivelul RAID.
 - 4.1. Selectați **RAID Level (Nivel RAID)** și apăsați Enter.
 - 4.2. În fereastra pop-up, selectați nivelul RAID pe care doriți să îl utilizați și apăsați Enter.
5. Includeți discurile care vor fi utilizate în volum.
 - 5.1. Selectați un disc și apăsați Enter.
 - 5.2. Selectați **X** pentru a include acest disc în volum.
 - 5.3. Repetați până când ați selectat toate discurile pe care doriți să le utilizați.
6. Lăsați **Stripe Size (Dimensiunea dungii)** și **Capacity (Capacitate)** la valorile implicite, dacă nu se specifică altfel.
7. Selectați **Create Volume (Creare volum)** și apăsați Enter.
8. În meniul Intel Rapid Storage Technology, volumul RAID nou creat apare la **RAID Volumes (Volume RAID)**.
9. Apăsați **Esc** și apoi **Y (Da)** pentru a salva și a ieși din meniul UEFI.
10. Apăsați **CTRL + ALT + DELETE** pentru a reporni dispozitivul.

Inițierea volumului RAID în Microsoft Windows®

Pentru a configura un volum nou:

1. Faceți clic dreapta pe **Start menu (meniul Start)** și selectați **Disk Management (Management disc)**.
2. În fereastra pop-up „**Initialize Disk (Inițializare disc)**”, selectați **GPT** și faceți clic pe **OK**.
3. Faceți clic dreapta pe discul nealocat și selectați **New Simple Volume (Volum simplu nou)**.
 - Urmați instrucțiunile din asistentul de configurare.
4. Când asistentul de configurare a fost finalizat, **Disk Management (Management disc)** afișează noul volum. Închideți **Disk Management (Management disc)** pentru ca sistemul să utilizeze noul volum.

Gestionarea comutatorului încorporat

Despre comutatorul încorporat

Seria dispozitivului AXIS Camera Station S22 Mk II Appliance este livrat cu un comutator de pornire prin Ethernet (PoE) integrat. Puteți configura și gestiona comutatorul încorporat.

Scopul comutatorului este de a segrega traficul din rețea, astfel încât camerele de securitate și traficul asociat gestionat de comutator (PoE și porturile legăturii ascendente a comutatorului) să nu fie partajate cu alte rețele.

Gestionarea puterii comutatorului respectă următoarele reguli:

- Fiecare port poate rezerva putere în funcție de clasa PoE a dispozitivului alimentat conectat. De asemenea, puteți alocă manual putere la un port.
- Dacă consumul real de putere pentru un anumit port depășește puterea rezervată pentru acel port, acesta se va deconecta.
- Porturile se vor deconecta atunci când consumul real de putere pentru toate porturile depășește cantitatea totală de putere pe care o poate alimenta sursa de alimentare. Porturile sunt apoi deconectate în funcție de prioritatea porturilor, unde un număr de port mai mic înseamnă o prioritate mai mare.

Autentificarea la pagina de gestionare a comutatorului

1. Accesați bara de meniu.
 - Din browserul web, introduceți adresa IP a comutatorului. În mod implicit: 192.168.10.1
 - Din AXIS Recorder Toolbox, accesați **Switch (Comutator) > Open the switch configuration (Deschideți configurația comutatorului)**.
2. Autentificați-vă cu numele de utilizator și parola.
 - Numele dvs. de utilizator este `admin`
 - Parola dvs. se află pe un autocolant lipit pe partea superioară a unității sau este inclusă în conținutul cutiei sub formă de autocolant.

Deconectați-vă din bara de meniu pentru a ieși de pe pagina de gestionare a comutatorului.

Configurația curentă

Configurația curentă este setul de setări care sunt active și operaționale în prezent pe dispozitivul dvs. de rețea. Ea reflectă starea curentă a dispozitivului dvs. și modul în care funcționează în timp real. Însă aceste modificări nu sunt salvate dacă dispozitivul dvs. se reinițializează.

Spre deosebire de aceasta, configurația de pornire este setul de setări care sunt salvate în memoria nevolatilă a dispozitivului. Această configurație este încărcată și aplicată la pornirea sau repornirea dispozitivului.

Când efectuați modificări în interfața web și faceți clic pe **Save (Salvare)**, aceste modificări sunt aplicate configurației curente.

Pentru a salva setările dvs. în configurația de pornire, utilizați pictograma Save (Salvare) din colțul din dreapta sus al interfeței web.

Dacă există modificări nesalvate în configurația curentă, pictograma va clipi în culoarea galbenă.

Prezentare generală

În bara de meniu, faceți clic pe **Overview (Prezentare generală)**.

Informații generale

Category (Categorie)	Articolul	Description (Descriere)
Rezumatul porturilor	Porturi active	Numărul de porturi în uz.
	Porturi care utilizează PoE	Numărul de porturi activate PoE în uz.
	Porturi blocate	Numărul de porturi blocate.

Consum de putere	Utilizarea actuală a PoE	Puterea PoE în wați consumată de dispozitive și procentul de putere PoE consumată din puterea PoE totală dedicată.
	Putere solicitată	Puterea totală în wați și procentul alocat dispozitivelor.
Starea portului	Activ	Portul este în uz.
	Inactiv	Portul este gata de utilizare.
	Blocat	Portul este blocat.

note

Puteți face clic pe un port pentru a vedea mai multe informații despre acesta.

Gestionarea puterii

În bara de meniu, faceți clic pe **Power management (Gestionarea puterii)**.

Lista porturilor

Articolul	Description (Descriere)
Port	Numărul portului la care este conectat dispozitivul.
PoE	Starea PoE. Puteți face clic pe pictogramă pentru a activa sau a dezactiva PoE la port.
PoE class (Clasa PoE)	Clasa PoE a dispozitivului conectat.
Prioritate	Prioritatea alocării puterii la dispozitivul conectat. În mod implicit prioritatea este numărul portului.
Putere consumată (W)	Puterea în wați consumată de dispozitivul conectat la port.
Putere solicitată (W)	Puterea în wați solicitată de dispozitivul conectat la port.
Putere alocată (W)	Ajustați manual puterea alocată portului. Disponibil numai când selectați Manual ca metodă de alocare a puterii.

Alocarea puterii

Puterea PoE poate fi alocată dispozitivelor conectate în următoarele moduri:

- **PoE class (Clasa PoE):** Comutatorul alocă puterea PoE în funcție de clasa PoE a dispozitivului conectat.
- **Manual:** Puteți ajusta manual puterea PoE alocată dispozitivului conectat.
- **LLDP-MED:** Comutatorul comunică cu dispozitivul conectat și alocă dinamic puterea PoE în funcție de necesități.

note

Metoda de alocare a puterii LLDP-MED funcționează numai pentru camerele cu sistemul de operare AXIS OS 9.20 sau o versiune ulterioară.

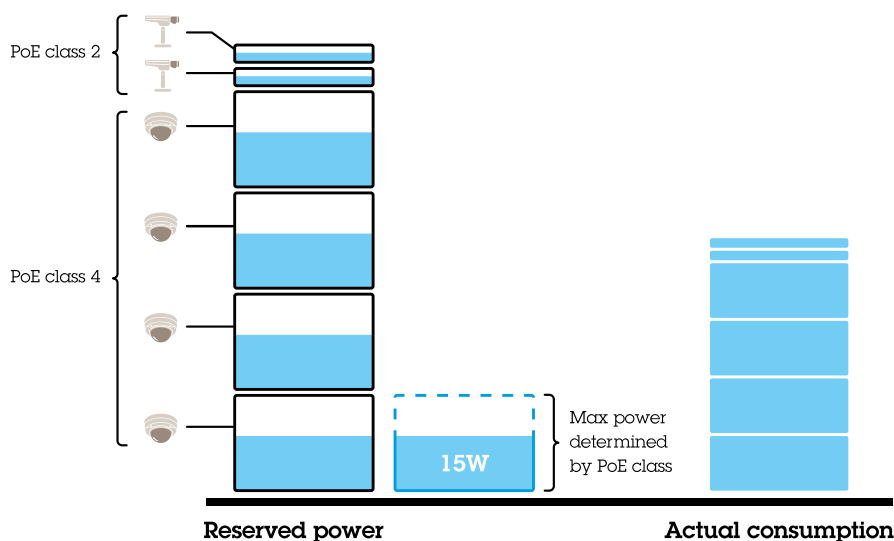
Pentru a modifica metoda de alocare a puterii:

1. Pe pagina de gestionare a puterii comutatorului, accesați **Power management (Gestionarea puterii)**.
2. Selectați **PoE class (Clasa PoE)**, **Manual** sau **LLDP-MED** la **Allocate power (Alocarea puterii)**
3. Dacă ați selectat **Manual**, puteți modifica puterea alocată dispozitivului conectat în coloana **Power allocated (Putere alocată)**.
4. Dacă doriți să modificați prioritatea dispozitivului conectat, selectați o prioritate pentru acel dispozitiv. Prioritatea celorlalte dispozitive se va modifica automat.

example:

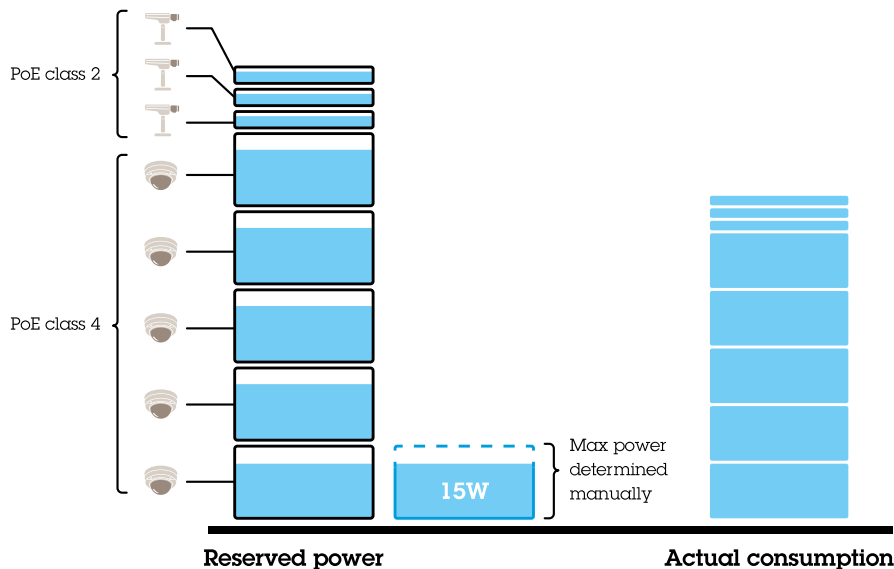
În acest exemplu, comutatorul are un buget de putere totală de 135 W. Un dispozitiv clasa PoE 4 solicită o putere de 30 W, dar consumă doar 15 W. Un dispozitiv clasa PoE 2 solicită o putere de 7 W, dar consumă doar 5 W.

Alocarea puterii în funcție de clasa PoE



Puterea solicitată de fiecare dispozitiv este determinată de clasa PoE. Comutatorul poate alimenta 4 dispozitive clasa PoE 4 și 2 dispozitive clasa PoE 2. Puterea totală solicitată este $(4 \times 30) + (2 \times 7) = 134$ W. Puterea reală consumată este $(4 \times 15) + (2 \times 5) = 70$ W. În acest fel, toate dispozitivele conectate au garantată suficientă putere, iar prioritatea este mai puțin importantă.

Alocarea puterii în mod manual



Puterea solicitată este ajustată manual la 20 W pentru dispozitivele clasa PoE 4. Comutatorul poate alimenta 5 dispozitive clasa PoE 4 și 3 dispozitive clasa PoE 2. Puterea totală solicitată este $(5 \times 20) + (3 \times 7) = 121$ W. Puterea reală consumată este $(5 \times 15) + (3 \times 5) = 90$ W. În acest fel, toate dispozitivele conectate au garantată suficientă putere, iar prioritatea este mai puțin importantă.

Activarea și dezactivarea PoE

Activarea PoE într-un port

1. În bara de meniu, faceți clic pe **Overview (Prezentare generală)**.
2. În coloana PoE, faceți clic pe ☐ pentru a activa PoE în portul specific.

Dezactivarea PoE de la un port

1. În bara de meniu, faceți clic pe **Overview (Prezentare generală)**.
2. În coloana PoE, faceți clic pe  pentru a dezactiva PoE în portul specific.

Activarea și dezactivarea PoE în toate porturile

1. În bara de meniu, faceți clic pe **Power management (Gestionarea puterii)**.
2. Pentru a dezactiva PoE din toate porturile, accesați meniul derulant **PoE ports state (Starea porturilor PoE)** și selectați **Turn off all (Dezactivare toate)**.
3. Pentru a activa PoE în toate porturile, accesați meniul derulant **PoE ports state (Starea porturilor PoE)** și selectați **Turn on all (Activare toate)**.

Prezentarea generală a rețelei

Prezentarea generală a rețelei oferă informații detaliate despre starea traficului de rețea a fiecărui port.

Porturi PoE

Articolul	Description (Descriere)
Port	Numărul portului la care este conectat dispozitivul.
Dispozitiv	Numele dispozitivului conectat la port.
Adresa IP	Adresa IP a dispozitivului conectat la port.
MAC address (Adresa MAC)	Adresa MAC a dispozitivului conectat la port.
Primire	Rata actuală de transfer a datelor în megabiți pe secundă pentru datele primite pe port.
Transmitere	Rata actuală de transfer a datelor în megabiți pe secundă pentru datele trimise pe port.
Pachet trimis	Numărul de pachete de date pe care comutatorul le-a transmis către rețea.
Pachet primit	Numărul de pachete de date pe care comutatorul le-a primit de la rețea.
Pachet pierdut	Numărul și procentul de pachete de date care nu au ajuns la destinație din cauza problemelor de rețea.
Lock (Blocare)	Afișează dacă portul este blocat. Puteți face clic pe pictogramă pentru a bloca sau a debloca portul.

Blocarea și deblocarea porturilor

Puteți bloca o adresă MAC la un port, astfel încât să treacă numai traficul provenit de la acea adresă MAC. Acest lucru îmbunătățește securitatea și împiedică utilizatorii neautorizați să conecteze un laptop sau alte dispozitive la rețeaua de securitate.

Blocarea unei adrese MAC la un port

1. În bara de meniu, faceți clic pe **Network overview (Prezentarea generală a rețelei)**.
2. În coloana **Lock (Blocare)** faceți clic pe  pentru a bloca portul specific.

Deblocarea unei adrese MAC de la un port

1. În bara de meniu, faceți clic pe **Network overview (Prezentarea generală a rețelei)**.
2. În coloana **Lock (Blocare)** faceți clic pe  pentru a debloca portul specific.

Blocarea sau deblocarea tuturor porturilor

1. În bara de meniu, faceți clic pe **Network overview (Prezentarea generală a rețelei)**.
2. Pentru a bloca toate porturile, accesați meniul derulant **Lock ports (Blocare porturi)** și selectați **Lock all (Blocare toate)**.
3. Pentru a debloca toate porturile, accesați meniul derulant **Lock ports (Blocare porturi)** și selectați **Unlock all (Deblocare toate)**.

Setări

Configurarea setărilor de rețea

Puteți modifica adresa IP a comutatorului. Însă pentru majoritatea instalațiilor de camere, recomandăm utilizarea setărilor implicite. Motivul este că o rețea de supraveghere este, de obicei, izolată de alte rețele, cum ar fi, de exemplu, o rețea LAN corporativă. În acest caz, ați folosi rețeaua de supraveghere doar pentru a gestiona și a colecta dispozitivele de supraveghere și datele din sistemul de video management instalat pe server.

1. În bara de meniu, accesați **Settings (Setări) > Network settings (Setări de rețea)**.
2. Introduceți tipul conexiunii, adresa IP, masca de subrețea, gateway-ul, DNS-ul principal, DNS-ul secundar și numele gazdei.

note

Setările implicite din fabrică sunt: o conexiune IP statică cu adresa 192.168.10.1 și o mască de subrețea cu adresa 255.255.255.0.

3. Faceți clic pe **Save (Salvare)**.

Configurarea datei și orei

1. În bara de meniu, accesați **Settings (Setări) > Date and time (Data și ora)**.
2. Selectați țara și fusul orar.
3. Pentru a seta ora manual, selectați **Manual** și ajustați manual ora.
4. Pentru a configura un server NTP, selectați **NTP server (Server NTP)** și introduceți adresa serverului NTP.

note

NTP funcționează numai când comutatorul este conectat la o rețea și configurat cu acces la Internet.

5. Faceți clic pe **Save (Salvare)**.

Configurarea serverului DHCP

Puteți configura comutatorul pentru a-i utiliza serverul DHCP intern pentru atribuirea adreselor IP dispozitivelor conectate. Când utilizați conexiunea legăturii ascendente a comutatorului pentru a permite dispozitivelor să acceseze sau să fie accesate de aplicații externe, trebuie să specificați gateway-ul și adresele DNS.

1. În bara de meniu, accesați **Settings (Setări) > DHCP server (Serverul DHCP)**.
2. Selectați **Enable DHCP server (Activați serverul DHCP)**.
3. Introduceți adresa IP de început, adresa IP de sfârșit, masca de subrețea, gateway-ul, DNS-ul principal, DNS-ul secundar, durata de închiriere și numele domeniului.
4. Faceți clic pe **Save (Salvare)**.

Configurarea SNMP

1. În bara de meniu, accesați **Settings (Setări) > SNMP**.
2. Introduceți numele serverului, datele de contact și locația utilizate pentru conexiunea SNMP.
3. Dacă doriți să utilizați SNMPV1 sau SNMPV2c, selectați **SNMPV1 / SNMPV2c** și introduceți comunitatea de citire.
4. Dacă doriți să utilizați SNMPV3, selectați **SNMPV3 (MD5)** și introduceți numele de utilizator și parola.

note

În prezent acceptăm doar autentificarea MD5 utilizată pentru SNMP.

5. Faceți clic pe **Save (Salvare)**.

Maintenance (Întreținere):

Actualizare firmware

1. În bara de meniu, accesați **Maintenance (Întreținere) > Update firmware (Actualizare firmware)**.

2. Trageți și plasați fișierul de firmware sau faceți clic pe **Browse (Navigare)** și navigați până la fișierul de firmware.
3. Faceți clic pe **Upload (Încărcare)**.
4. După actualizarea firmware-ului, reinițializați comutatorul.

Reinițializarea comutatorului

important

În timp ce comutatorul se reinițializează, toate dispozitivele conectate vor pierde temporar conexiunea cu comutatorul, inclusiv PoE.

1. În bara de meniu, accesați **Maintenance (Întreținere) > Reboot switch (Reinițializarea comutatorului)**.
2. Faceți clic pe **Reboot (Reinițializare)** și pe **Yes (Da)**.
3. Când comutatorul se reinițializează după câteva minute, introduceți numele de utilizator și parola pentru a vă autentifica.

Efectuarea de backup la setările comutatorului

note

Numele de utilizator și parola sunt incluse în fișierul de backup.

1. În bara de meniu, accesați **Maintenance (Întreținere) > Backup and restore (Backup și restabilire)**.
2. Faceți clic pe **Create a backup file (Creați un fișier de backup)**. Aceasta creează un fișier de backup în format .bin și îl salvează în folderul dvs. **Downloads (Descărcări)**.

Restabilirea setărilor comutatorului

note

Pentru a restabili setările comutatorului, trebuie să fi creat anterior un fișier de backup.

1. În bara de meniu, accesați **Maintenance (Întreținere) > Backup and restore (Backup și restabilire)**.
2. Trageți și plasați fișierul de backup sau faceți clic pe **Browse (Navigare)** și navigați până la fișierul de backup.
3. Faceți clic pe **Upload (Încărcare)**.

Restabilirea comutatorului din fișierul de backup poate dura câteva minute. După ce setările au fost restabilite, comutatorul se va reinițializa automat și va trebui să vă autentificați din nou.

Gestionarea certificatelor

1. În bara de meniu, accesați **Maintenance (Întreținere) > Manage certificates (Gestionați certificatele)**.
2. Faceți clic pe  și navigați până la fișierul cu cheia dvs. privată.
3. Faceți clic pe  și navigați până la fișierul dvs. cu certificatul.
4. Faceți clic pe  și navigați până la fișierul CA bundle (pachet CA).
5. Faceți clic pe **Save (Salvare)**.
6. Reinițializarea comutatorului.

Schimbarea parolei

Puteți schimba parola implicită a comutatorului cu o parolă aleasă de dvs.

important

Asigurați-vă că alegeți o parolă pe care o puteți reține. Dacă uitați noua parolă, consultați *Resetare la setările implicite din fabrică, on page 30* pentru a restabili parola implicită din fabrică.

1. În bara de meniu, accesați **Maintenance (Întreținere) > Change password (Schimbați parola)**.
2. Introduceți parola actuală și noua dvs. parolă, conform solicitării.
3. Faceți clic pe **Save (Salvare)**.

Configurarea setărilor web

1. În bara de meniu, accesați **Maintenance (Întreținere) > Web settings (Setări web)**.
2. Introduceți numărul portului.

note

- Dacă decideți să schimbați numărul portului, asigurați-vă că vă notați noul număr al portului. Dacă uitați noul număr de port, consultați *Resetare la setările implicite din fabrică, on page 30* pentru a restabili numărul de port implicit din fabrică.
- Vă recomandăm să țineți HTTPS activat.

Resetare la setările implicite din fabrică

Țineți apăsat butonul de resetare timp de cinci secunde pentru a reseta comutatorul la setările sale implicite din fabrică.

De asemenea, puteți reseta comutatorul și prin intermediul interfeței web:

1. În bara de meniu, accesați **Maintenance (Întreținere) > Reset to factory default settings (Resetare la setările implicite din fabrică)**.
2. Faceți clic pe **Reset (Resetare)** și pe **Yes (Da)**.

După resetare, comutatorul se va reinițializa automat.

Logs (Jurnale)

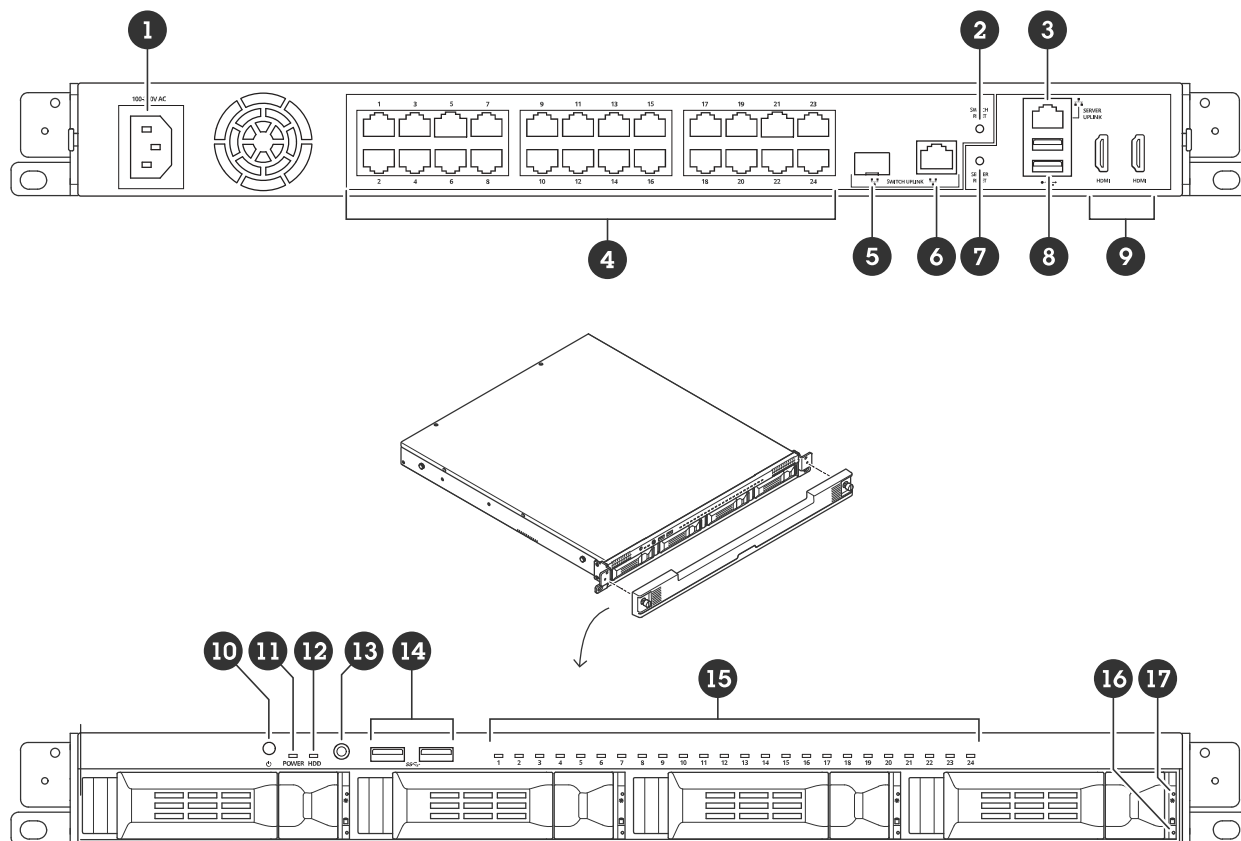
În bara de meniu, faceți clic pe **Logs (Jurnale)** pentru a vedea o listă a jurnalelor. Faceți clic pe titlul coloanei pentru a le sorta în ordine alfabetică.

Articolul	Description (Descriere)
Time (Oră)	Data și ora la care a avut loc evenimentul înregistrat în jurnal.
Nivel	Nivelul de gravitate afișat sub formă de pictograme de avertizare.
User (Utilizator)	Utilizatorul care a inițiat evenimentul de jurnal.
Adresa IP	Adresa IP a utilizatorului care a inițiat evenimentul de jurnal.
Serviciu	Serviciul la care se referă evenimentul jurnalului. Valorile posibile sunt desktop, rețele, rețea, sistem, ntpd, stocare, DHCP etc.
Eveniment	O descriere a evenimentului din jurnal.

Crearea rapoartelor comutatorului

Pe pagina jurnalului, faceți clic pe **Export (Exportare)** pentru a crea un fișier text cu informații despre comutator, inclusiv intrările în jurnal de pe pagina jurnalului.

Specificații Prezentare generală a produsului Față și spate



- 1 Conector de alimentare
- 2 Buton de resetare a comutatorului
- 3 Port Ethernet de 1 GbE – Legătură ascendentă a serverului
- 4 Porturi Ethernet PoE de 1 GbE
- 5 Port Ethernet de 1 GbE – Legătură ascendentă a comutatorului (SFP)
- 6 Port Ethernet de 1 GbE – Legătură ascendentă a comutatorului (RJ45)
- 7 Buton de resetare a serverului
- 8 Porturi USB 2.0
- 9 Porturi HDMI
- 10 Buton de pornire
- 11 LED de alimentare
- 12 LED de activitate a hard disk-ului
- 13 Jack audio universal
- 14 Porturi USB 3.2
- 15 LED de stare pentru porturile Ethernet PoE
- 16 LED de activitate a hard disk-ului
- 17 LED de stare a hard disk-ului

Indicatori LED LED-uri frontale

Buton de pornire	LED de alimentare	Indicație
Nu este apăsat	Off (Oprit)	Computerul și comutatorul sunt deconectate
	Chihlimburiu	Computerul este conectat și comutatorul este deconectat

	Iluminează intermitent în culoarea chihlimbarie	Computerul este conectat și comutatorul se inițializează
	Verde	Computerul este conectat și comutatorul a terminat inițializarea
Apăsat	Până la 0 secunde	Pornește atât comutatorul, cât și computerul dacă sunt deconectate
	Până când luminează intermitent în culoarea chihlimbarie (3 secunde)	Comutatorul inițiază deconectarea controlată
	Până când luminează intermitent în culoarea roșie (6 secunde)	Computerul și comutatorul inițiază deconectarea controlată
	Până când se aprinde continuu în culoarea roșie (9 secunde)	Comutatorul inițiază deconectarea necontrolată, comutatorul inițiază deconectarea controlată

Indicator cu LED	Color (Culoare)	Indicație
Hard disk (HDD)	Iluminează intermitent în culoarea verde	Activitatea hard disk-ului
	Roșu	Posibilă defecțiune a hard disk-ului
Starea portului Ethernet PoE	Verde	Starea legăturii
	Chihlimburiu	Dispozitiv alimentat, nicio stare a legăturii
	Roșu	Bugetul PoE depășit
Starea hard disk-ului	Verde	Hard disk prezent
	Roșu	Posibilă defecțiune a hard disk-ului

LED-uri spate

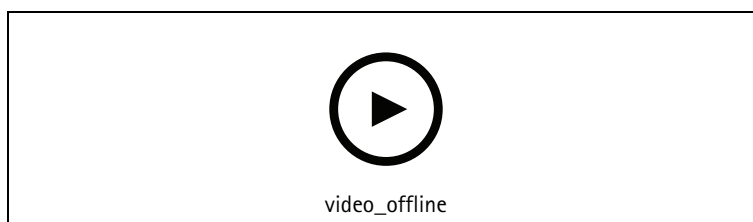
Viteza și activitatea rețelei	Color (Culoare)	Indicație
LED-ul dreapta	Chihlimburiu	10/100 Mbit/s
	Verde	1000 Mbit/s
LED-ul stânga	Verde	Conexiunea PoE OK
	Roșu	Bugetul PoE depășit

Depanarea

Resetarea serverului dvs.

Puteți utiliza butonul de resetare a serverului pentru a vă reseta serverul. Resetarea serverului va dura mai mult de o oră.

1. Deconectați dispozitivul.
2. Apăsați butonul de resetare a serverului și țineți-l apăsat timp de 5 secunde. Windows® RE va fi pornit.
3. Selectați Troubleshoot (Depanare).
4. Selectați Reset your PC (Resetați-vă computerul).
5. Selectați Keep my files (Păstrează fișierele mele) sau Remove everything (Ștergeți tot). Dacă selectați Keep my files (Păstrează fișierele mele), trebuie să furnizați datele de autentificare ale administratorului.
6. Urmați instrucțiunile de pe ecran.
7. Serverul se reinițializează și începe procedura de restabilire a Windows® la setările implicite din fabrică.



Resetarea serverului dvs. la setările implicite din fabrică

Efectuarea unei recuperări a sistemului

Dacă dispozitivul a suferit o defecțiune completă a sistemului, trebuie să utilizați o imagine de recuperare pentru a recrea sistemul Windows®. Pentru a descărca kitul de recuperare AXIS Network Video Recorder (înregistrator video de rețea), contactați asistența tehnică Axis și furnizați numărul de serie al dispozitivului dvs.

note

Kitul de recuperare pentru înregistratorul video de rețea AXIS este disponibil în două variante:

- **sb11** — pentru dispozitivele care încă utilizează certificatul din 2011.
- **sb23** — pentru dispozitivele care au trecut la certificatul din 2023.

Verificați starea certificatului dvs. înainte de a descărca kitul de recuperare și selectați varianta potrivită. Dacă selectați varianta greșită, instalarea nu va genera un rezultat bootabil și va trebui să o luați de la capăt cu imaginea corectă. Acest lucru nu va defecta dispozitivul dvs.

Dacă dispozitivul dvs. are deja instalat certificatul din 2023, varianta sb11 poate fi utilizată în continuare în condiții de siguranță, atâta timp cât certificatul din 2011 nu a fost revocat manual. După ce va fi revocat, va funcționa doar sb23.

Pentru a recrea sistemul:

1. Descărcați kitul de recuperare AXIS Network Video Recorder și AXIS Network Video Recorder Recovery: Instrument de conversie ISO în USB.
2. Introduceți un USB drive în computer.
 - Utilizați un USB drive cu o capacitate minimă de 16 GB.
 - USB drive va fi formatat și toate datele existente vor fi șterse.
3. Rulați procedura de recuperare a înregistratorului video de rețea AXIS: Rulați instrumentul ISO pe USB și urmați instrucțiunile de pe ecran.
Scrierea datelor pe USB drive durează aproximativ 10-15 minute. Nu scoateți USB drive până când procesul nu a fost finalizat.
4. După recuperarea înregistratorului video de rețea AXIS: După ce instrumentul ISO pe USB Tool a fost finalizat, scoateți USB drive și introduceți-l în dispozitivul dvs.
5. Porniți dispozitivul dvs.
6. Când vedeți ecranul de întâmpinare Axis, apăsați F12.
7. Faceți clic pe **UEFI: USB Drive** (UEFI: Unitate USB Drive).

8. Navigați la USB drive și apăsați Enter. Sistemul se inițializează în kitul de recuperare AXIS Network Video Recorder.
9. Faceți clic pe **Reinstall Operating System (Reinstalați sistemul de operare)**. Recuperarea durează aproximativ 10 până la 15 minute. Veți găsi instrucțiuni detaliate în descărcarea pentru kitul de recuperare.

Depanarea AXIS Camera Station Pro

Pentru informații cu privire la modul de depanare a AXIS Camera Station Pro, accesați *AXIS Camera Station Pro user manual (manualul de utilizare AXIS Camera Station Pro)*.

Aveți nevoie de mai mult ajutor?

Linkuri utile

- *AXIS Camera Station Pro user manual (manualul de utilizare AXIS Camera Station Pro)*
- *Conectarea la AXIS Secure Remote Access*
- *Conectarea la AXIS Secure Remote Access v2*
- *Ce trebuie inclus într-o listă de permisiuni antivirus pentru AXIS Camera Station*

Contact Asistență

Dacă aveți nevoie de ajutor suplimentar, accesați axis.com/support.

T10207039_ro

2026-09 (M5.2)

© 2024 – 2026 Axis Communications AB