

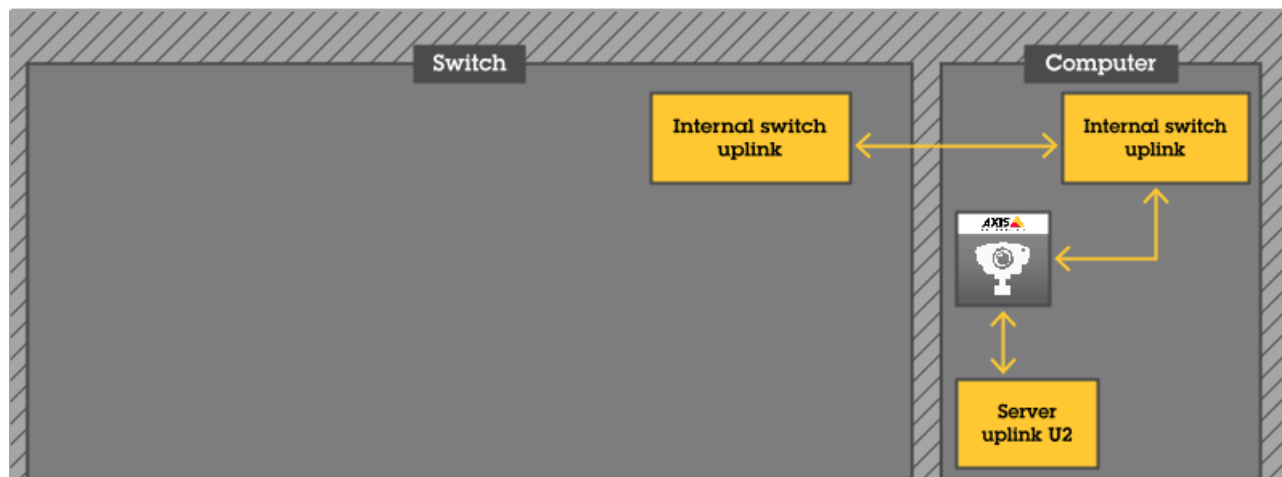
AXIS Camera Station S2108 Appliance

Despre dispozitivul dvs.

AXIS Camera Station S2108 Appliance este o soluție de înregistrare all-in-one cu switch PoE integrat, concepută să ofere supraveghere de înaltă definiție fiabilă, acceptând camere până la rezoluția 4K. Pentru o instalare rapidă și ușoară, dispozitivul este preconfigurat și preîncărcat cu ACS - sistem de video management, inclusiv licențele și toate software-urile de sistem necesare. AXIS Camera Station oferă o interfață pentru utilizator intuitivă care permite utilizatorilor să profite la maximum de gama largă de camere de supraveghere video și de alte produse IP de la Axis. Având sistemul de operare stocat pe o unitate SSD (solid-state drive) și o garanție de 5 ani pentru componentele hardware, acest dispozitiv oferă o soluție fiabilă de supraveghere.

AXIS Camera Station S2108 Appliance este alcătuit din două părți:

- **Switch (Comutator):** Switch integrat cu alimentare prin Power over Ethernet (PoE).
- **Computer:** Preîncărcat cu toate programele necesare pentru a crea o soluție de supraveghere, inclusiv sistemul de video management AXIS Camera Station.

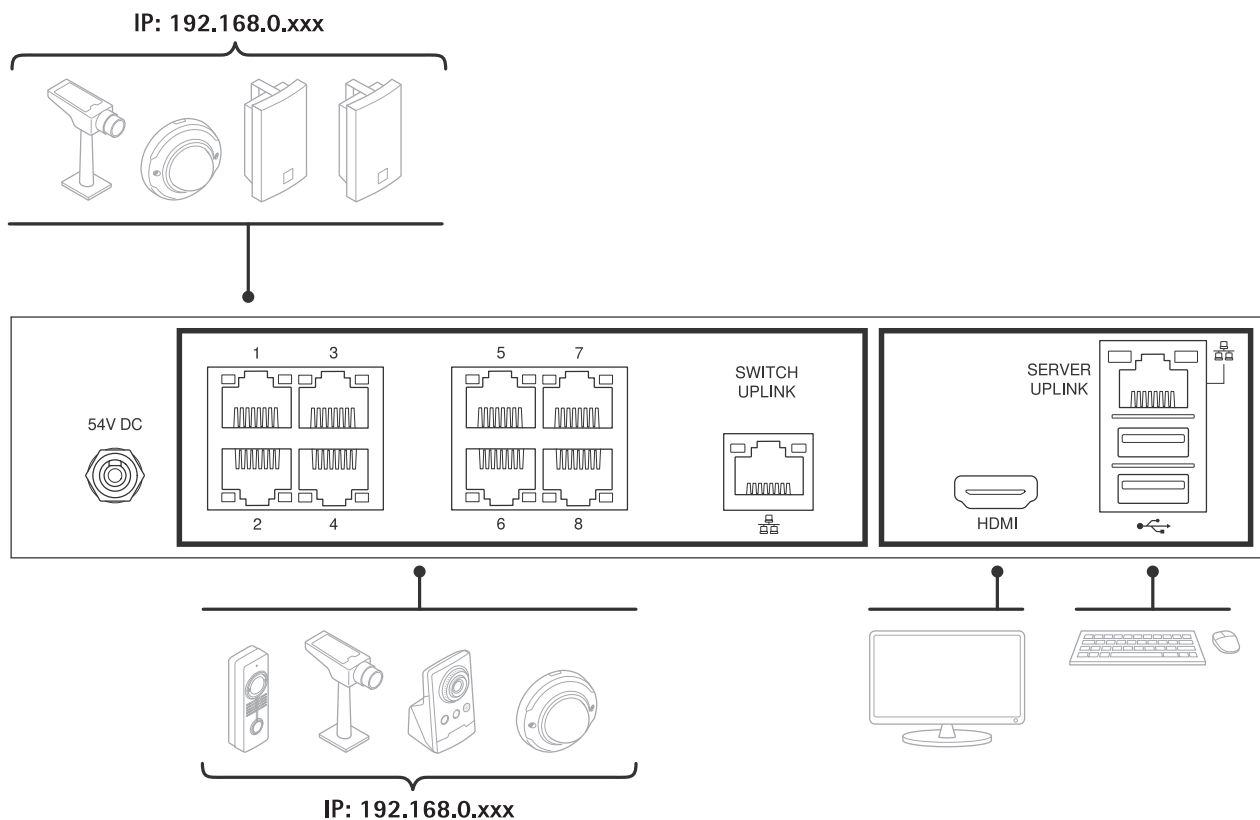


- Switch-ul și computerul sunt două componente separate.
- Switch-ul și computerul comunică prin intermediul conectorilor uplink interni: unul se află pe placa de circuit de alimentare a switch-ului, iar celălalt pe placa de bază a computerului.
- Uplink-ul serverului este o interfață de rețea externă care se poate conecta la o rețea existentă.
- Dispozitivele conectate la uplink-ul serverului nu pot comunica direct cu dispozitivele conectate la switch.
- Dispozitivele conectate la uplink-ul serverului pot comunica cu dispozitivele conectate la switch prin intermediul AXIS Camera Station.

Exemple de configurare

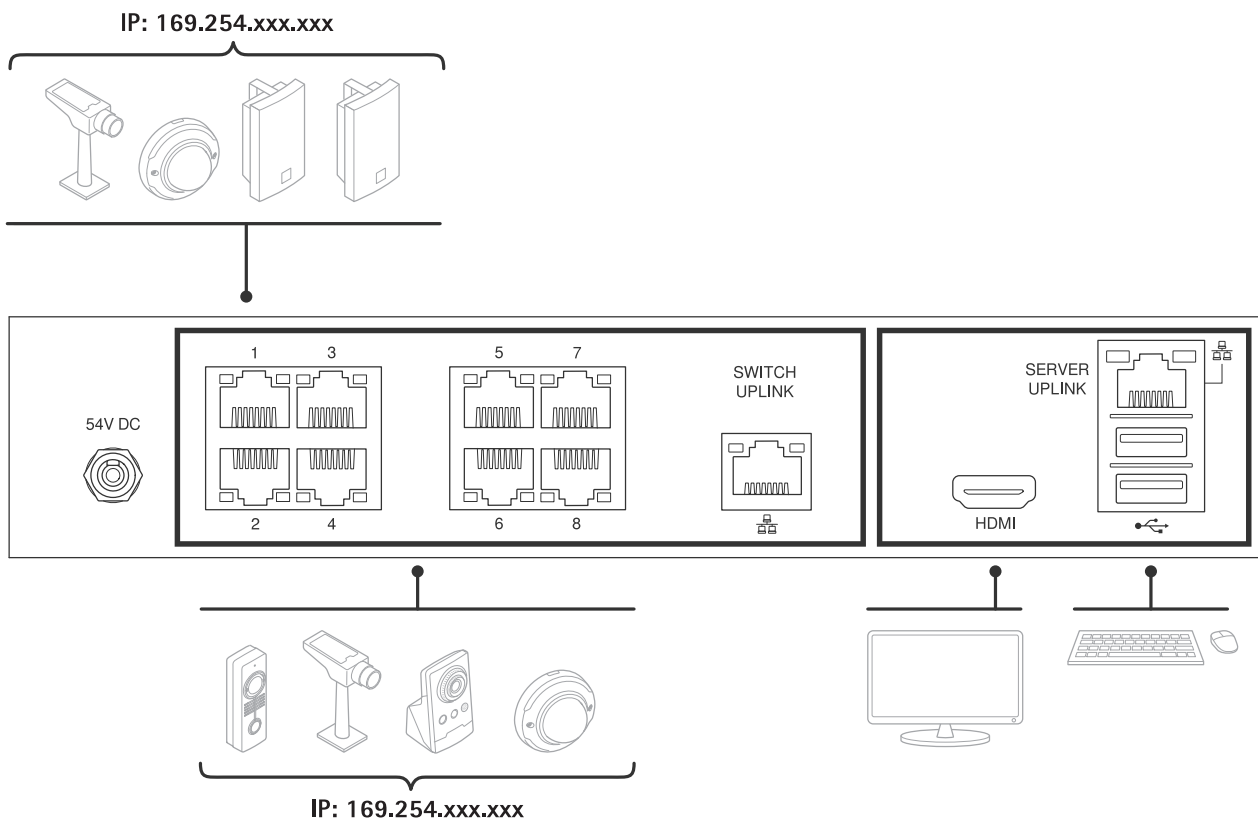
Atribuiți o adresă statică fiecărui dispozitiv

Puteți crea o rețea independentă prin atribuirea unei adrese IP statice fiecărui dispozitiv și dispozitivului AXIS S2108. Această rețea nu va avea nicio interconectivitate cu o altă rețea externă, cu excepția cazului în care parametrii celor două rețele coincid. Computerul poate beneficia în continuare de conexiune la internet prin portul de uplink al serverului. Imediat ce dispozitivele sunt conectate la porturile PoE alimentate, acestea vor prelua adresa link-local și vor avea nevoie de o adresă IP fixă, care să corespundă cu cea a dispozitivului AXIS S2108.



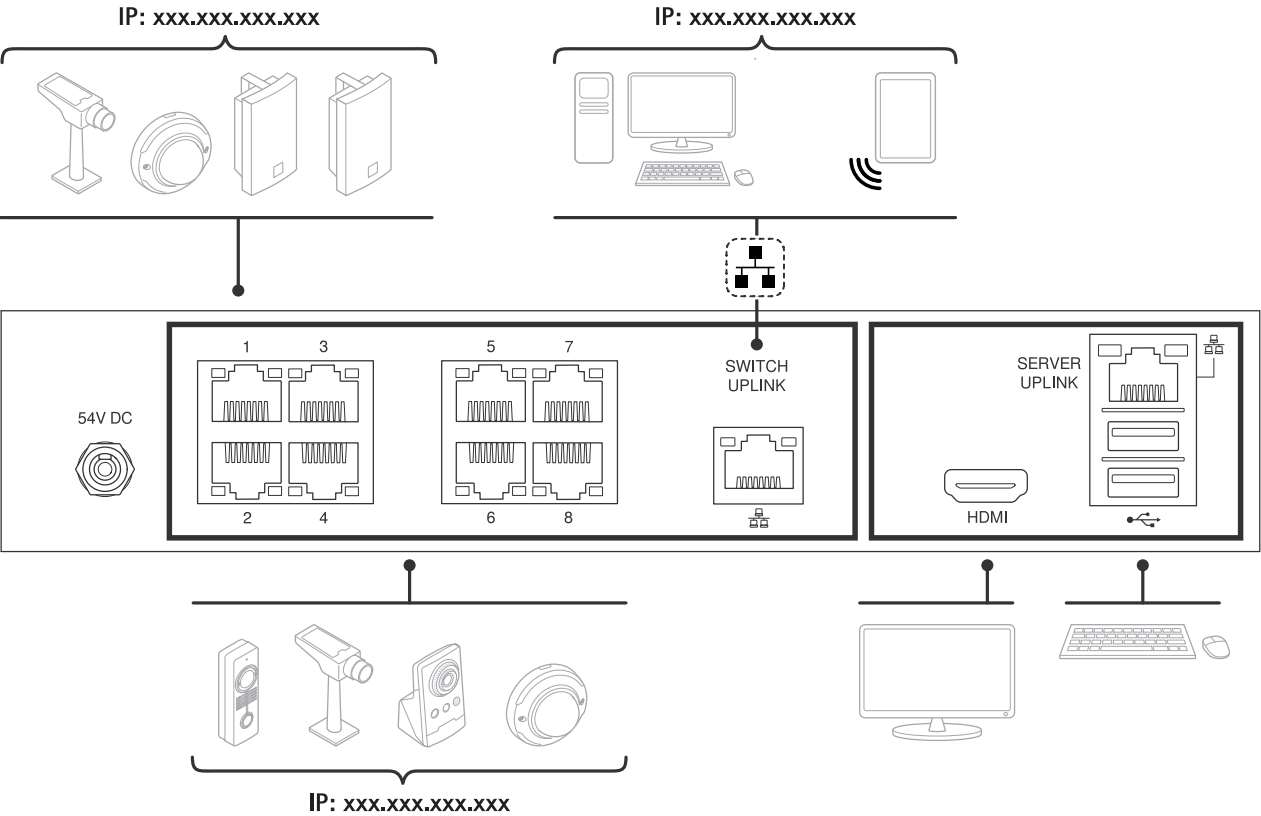
Utilizați adresa locală

Puteți crea o rețea independentă prin utilizarea adresei link-local la fiecare dispozitiv și la dispozitivul AXIS S2108. Această rețea nu va avea nicio interconectivitate cu o altă rețea externă. Computerul poate beneficia în continuare de conexiune la internet prin portul de uplink al serverului. Imediat ce dispozitivele sunt conectate la porturile PoE alimentate, acestea vor prelua adresa link-local și pot fi găsite de AXIS Camera Station pe dispozitivul AXIS S2108.



Utilizați un server DHCP dintr-o altă rețea

Vă puteți conecta la dispozitivul AXIS S2108 și la dispozitivele conectate la acesta dacă dispuneți de o rețea existentă și de un server DHCP conectat la uplink-ul switch-ului. Astfel toate dispozitivele conectate vor avea o adresă IP din intervalul alocat de serverul DHCP. Dacă în rețeaua respectivă este disponibilă conexiunea la internet, aceasta va fi disponibilă și pentru dispozitivul AXIS S2108. În caz contrar, computerul poate beneficia în continuare în mod independent de conexiune la internet prin portul de uplink al serverului. Atunci când dispozitivele sunt conectate la porturile PoE alimentate, ele vor primi o adresă DHCP dacă serverul DHCP este activ.



Începere

Fluxul de lucru standard pentru configurarea unui server de înregistrare AXIS Camera Station 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 secțiunea *Configurarea inițială a înregistratorului Axis, on page 15*.
4. Configurarea Windows®. Vă recomandăm să:
 - Actualizați Windows® la cea mai recentă versiune. Consultați secțiunea .
 - Creați un cont de utilizator standard. Consultați secțiunea *Crearea unui cont de utilizator, on page 21*.
5. Actualizați AXIS Camera Station la cea mai recentă versiune.
 - Dacă sistemul dvs. este online: deschideți aplicația AXIS Recorder Toolbox și faceți clic pe **Update AXIS Camera Station (Actualizați AXIS Camera Station)**.
 - Dacă sistemul dvs. este offline: accesați *axis.com* și descărcați cea mai recentă versiune.
6. Porniți AXIS Camera Station client.
7. *Connect to AXIS Camera Station server (Conectare la serverul AXIS Camera Station)*
8. *Configurarea AXIS Camera Station, on page 16*

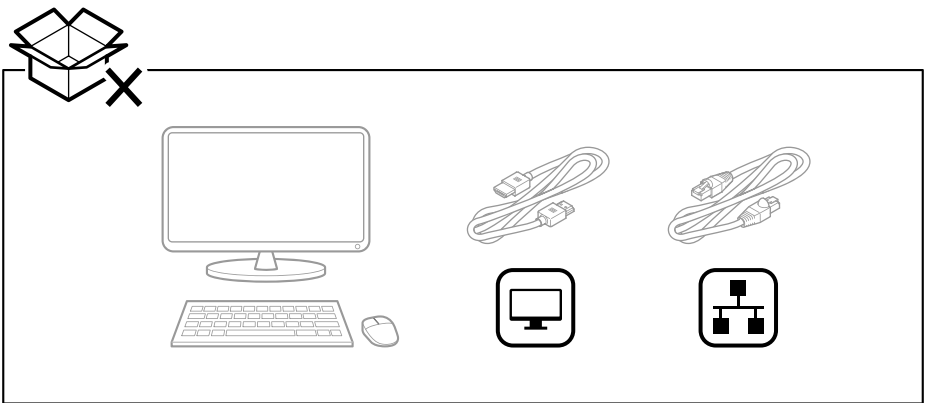
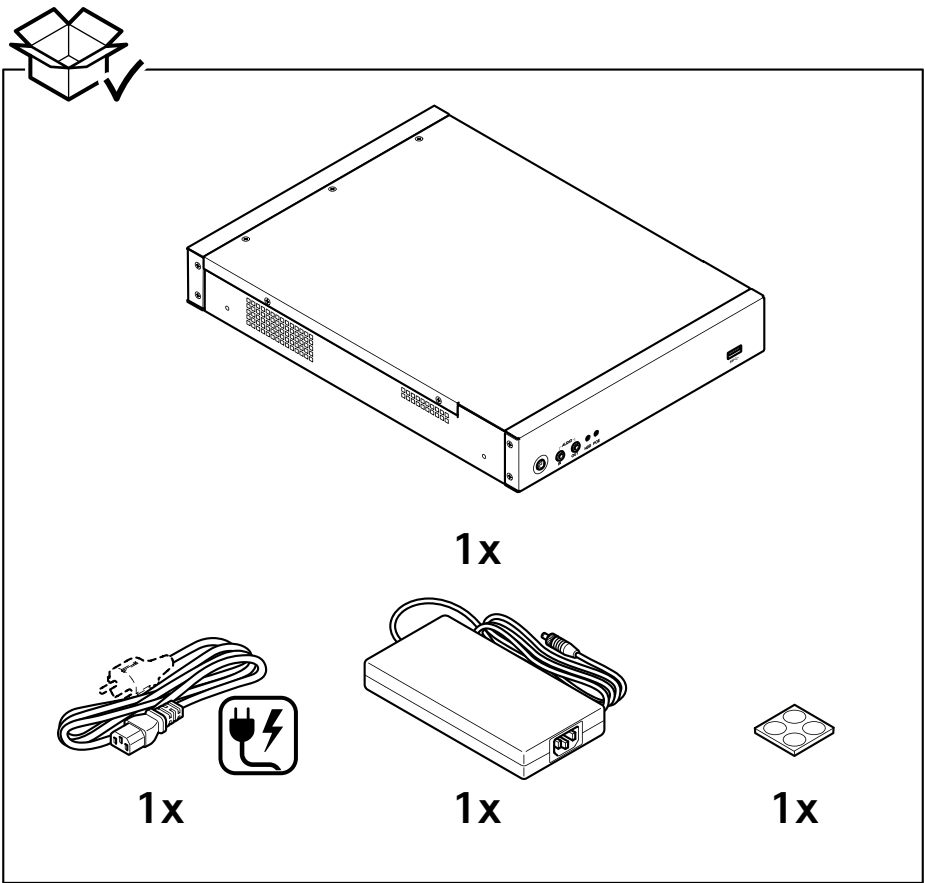
Instalarea dispozitivului dvs.

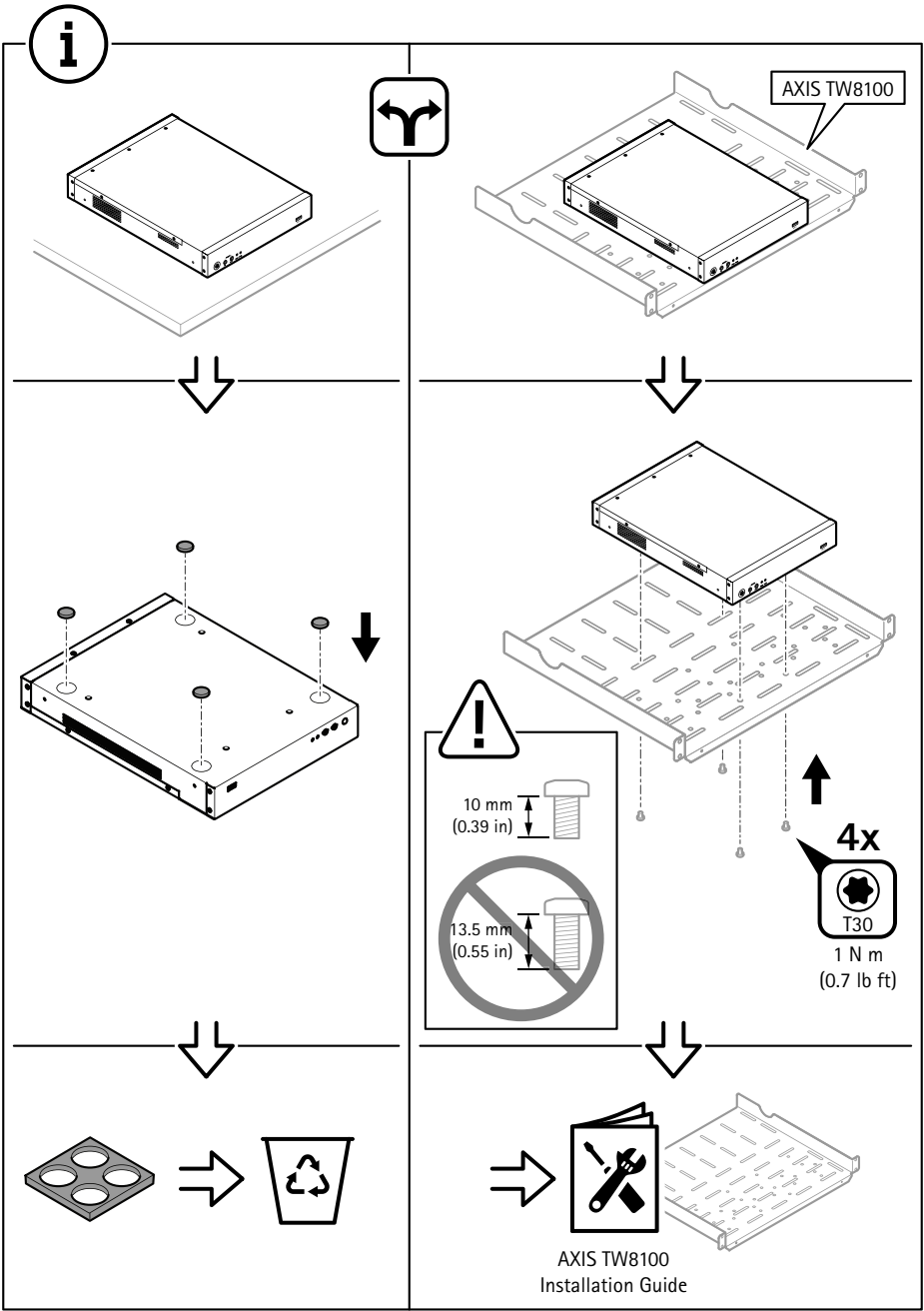
Înainte de instalare

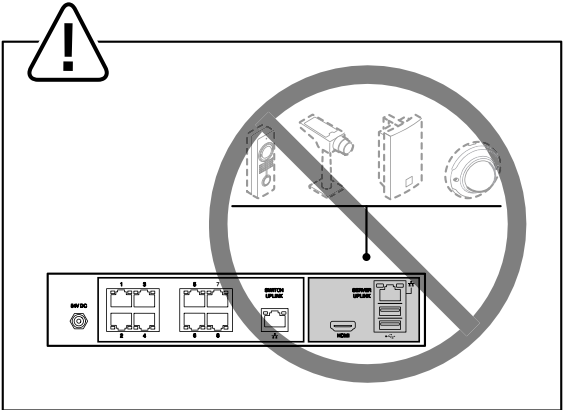
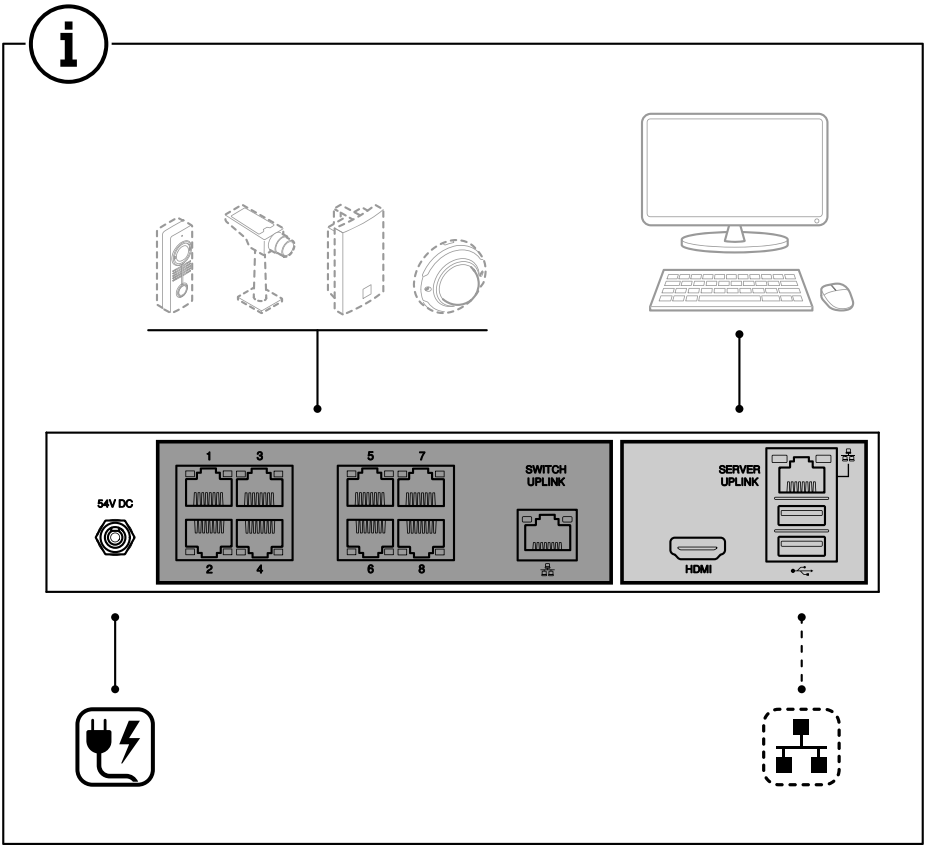
- Pregătiți accesoriile suplimentare utilizate pentru instalare: monitor, mouse, tastatură și cablu de rețea.
- Înțelegeți utilizarea diferitelor conturi de utilizator.

Tabelul următor enumeră conturile de utilizator care pot fi utilizate pentru instalarea, configurarea și operarea sistemului dvs. Axis.

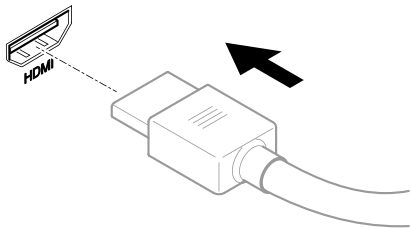
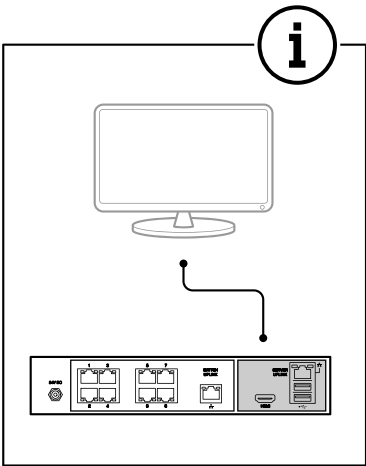
Cont de utilizator	Description (Descriere)	Notă
MyAxis	Utilizat pentru descărcarea celui mai recent software, accesarea sistemului de licențe, Axis Secure Remote Access (Acces de la distanță securizat Axis) și System Health Monitoring (Monitorizarea stării sistemului).	Înregistrat de pe <i>my.axis.com</i> .
Windows®		
Administrator Windows®	Privilegii de administrator în Windows®. Vă recomandăm să nu-l utilizați ca administrator AXIS Camera Station.	Creat în timpul configurării inițiale a Windows®.
Utilizator Windows® cu privilegii de administrator AXIS Camera Station	Un utilizator Windows® cu privilegii de administrator în AXIS Camera Station, pentru a fi utilizat de integratorul de sistem sau de administratorul de sistem pentru configurare sau depanare.	Creat în setările Windows®.
Utilizator Windows® cu privilegii de operator sau vizualizator AXIS Camera Station	Un utilizator Windows® căruia i s-au acordat privilegii de operator sau vizualizator în AXIS Camera Station.	Creat în setările Windows®.
Dispozitiv		
Administrator de dispozitiv	Utilizat de administrator pentru a accesa camera din sistemul de video management sau din pagina web a dispozitivului.	Creat de pe pagina web a dispozitivului sau când adăugați dispozitivul la AXIS Camera Station.



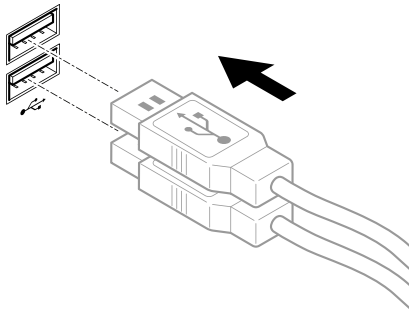
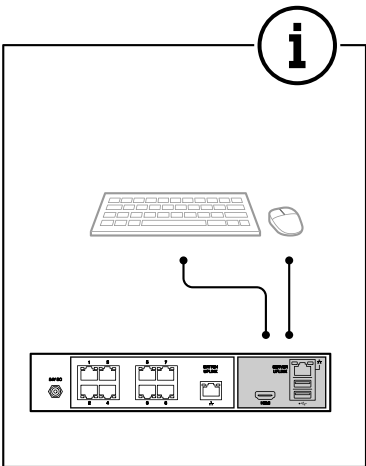




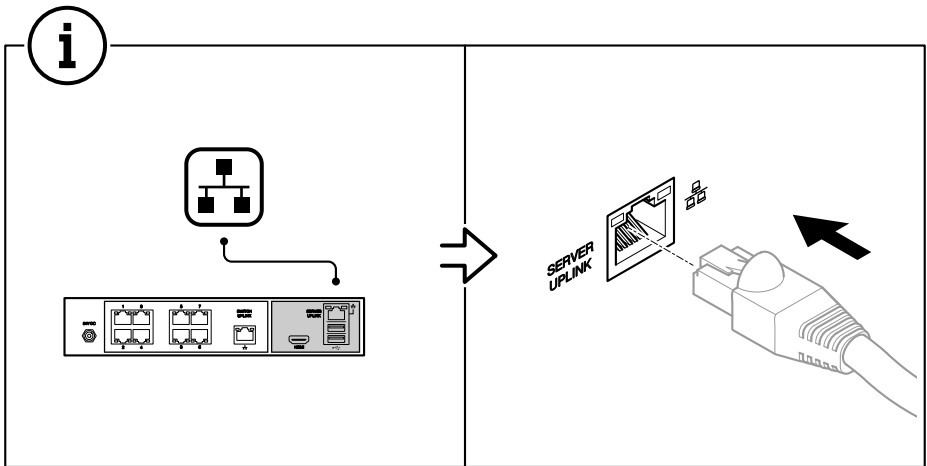
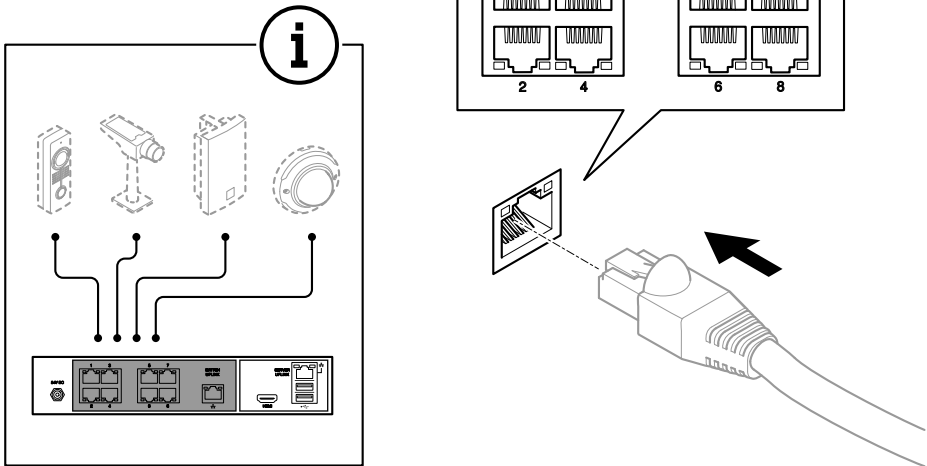
1.1



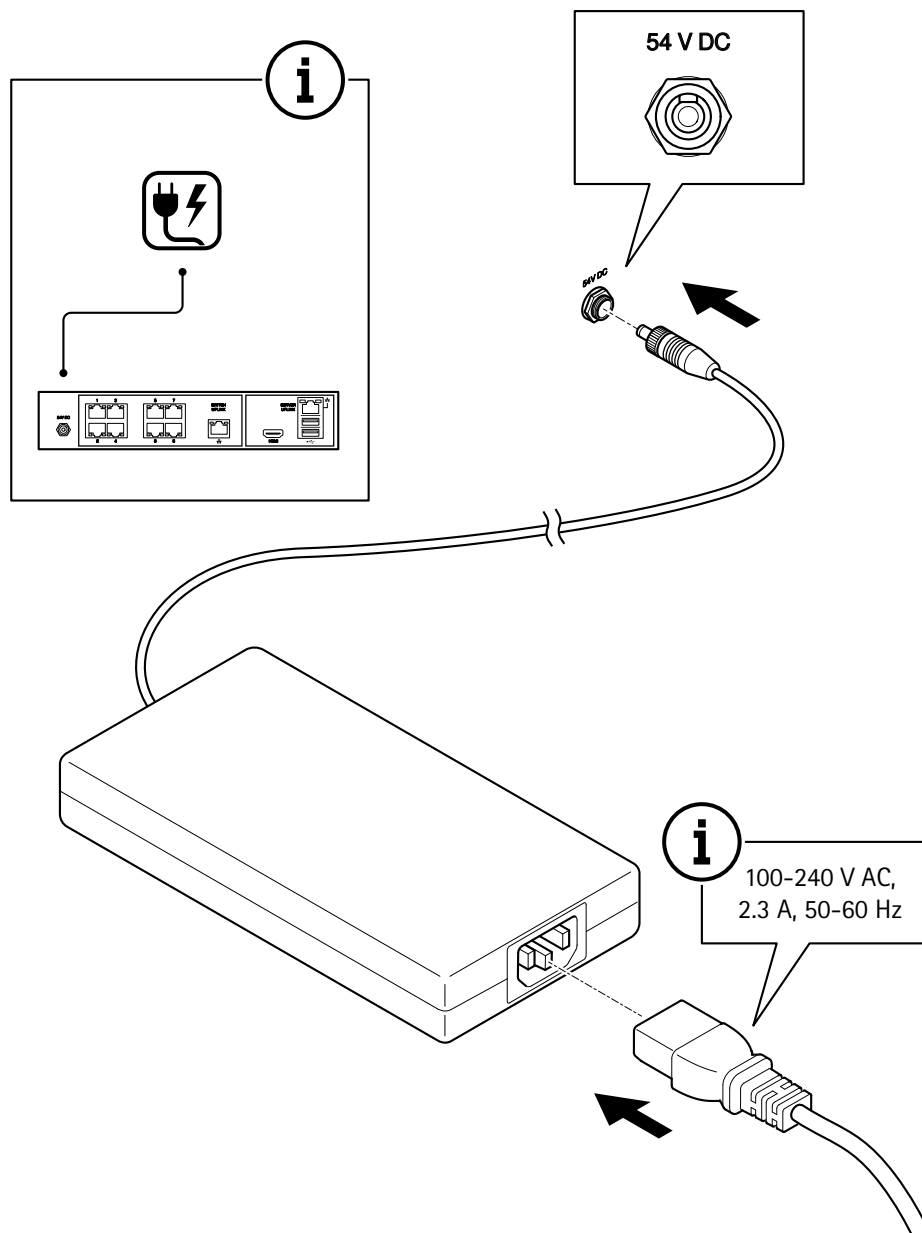
1.2



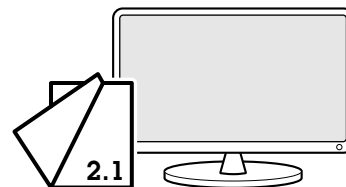
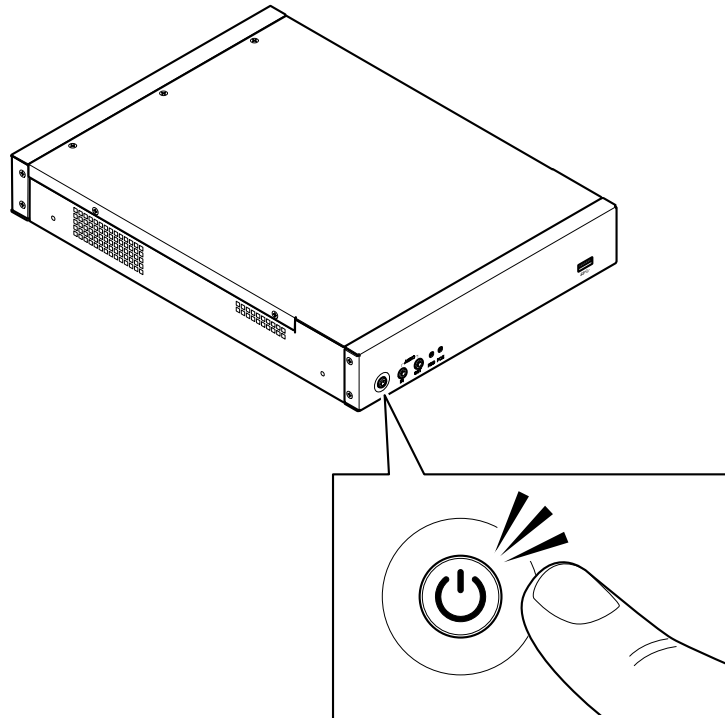
1.3



1.4



1.5



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.

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.

Conectarea la server

Folosind clientul AXIS Camera Station, vă puteți conecta la mai multe servere sau la un singur server instalat pe computerul local sau în altă parte în rețea. Vă puteți conecta la serverele AXIS Camera Station în diferite 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 secțiunea *Conectare la un server de la distanță, on page 16*.

AXIS Secure Remote Access – Consultați secțiunea *Conectarea la AXIS Secure Remote Access, on page 16*.

note

Când încercați să vă conectați la un server pentru prima dată, clientul verifică ID-ul certificatului serverului. Pentru a vă asigura că vă conectați la serverul corect, verificați manual ID-ul certificatului comparându-l cu cel afișat în control serviciu AXIS Camera Station.

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 ale tuturor serverelor conectate, faceți clic pe Delete saved passwords (Ștergere parole salvate) .
Change client proxy settings (Modificarea setărilor serverului intermediar (proxy) al clientului)	Poate fi necesar să modificați setările serverului intermediar (proxy) al clientului pentru a vă conecta la un server; faceți clic pe Change client proxy settings (Modificarea setărilor 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 derulantă **Remote server (Server la distanță)** sau introduceți adresa IP sau DNS. Dacă serverul nu este enumerat, faceți clic pe  pentru a reîmprospăta lista tuturor serverelor 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 opțiuni:
 - 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 serviciul **Axis Secure Remote Access (v1)** la **Axis Secure Remote Access v2**. Vom renunța la versiunea actuală în 1 decembrie 2025 și vă recomandăm cu tărie să faceți o actualizare la versiunea **Axis Secure Remote Access v2** înainte de această dată.

Ce înseamnă acest lucru pentru sistemul dumneavoastră **AXIS Camera Station S2108 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 serviciul **Axis Secure Remote Access v2**, trebuie să actualizați sistemul la **AXIS Camera Station Pro** versiunea 6.8. În prezent, această actualizare este gratuită pentru toți utilizatorii aplicației **AXIS Camera Station 5** până la data de 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 **AXIS Camera Station S2108 Appliance**, trebuie să configurați setările intermediarului (proxy) în Windows la serverul **AXIS Camera Station S2108 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**

Acest tutorial vă va îndruma prin pașii de bază pentru configurarea și funcționarea sistemului dvs.

Înainte de a începe:

- Configurați-vă rețeaua în funcție de instalația dvs. Consultați secțiunea *Configurarea rețelei, on page 18*.

- Configurați porturile serverului, dacă este necesar. Consultați secțiunea *Configurația portului serverului, on page 19*.
- Luați în considerare problemele de securitate. Consultați secțiunea *Considerații privind securitatea*.

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

1. *Porniți sistemul de video management, on page 17*
2. *Adăugarea dispozitivelor, on page 17*
3. *Configurați metoda de înregistrare, on page 17*
4. *Vizualizarea în direct a imaginilor video, on page 17*
5. *Vezi înregistrările, on page 17*
6. *Adăugați marcaje, on page 17*
7. *Export recordings (Export înregistrări), on page 18*
8. *Redarea și verificarea înregistrărilor în AXIS File Player, on page 18*

Porniți sistemul de video management

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

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

Adăugarea dispozitivelor

Pagina Add devices (Adăugare dispozitive) se deschide prima dată când porniți AXIS Camera Station. AXIS Camera Station caută în rețea dispozitive conectate și afișează o listă a dispozitivelor găsite.

1. Selectați camerele pe care doriți să le adăugați din listă. Dacă nu vă găsiți camera, faceți clic pe **Manual search (Căutare manuală)**.
2. Faceți clic pe **Add (Adăugare)**.
3. Selectați **Quick configuration (Configurație rapidă)** sau **Site Designer configuration (Configurare site designer)**. Faceți clic pe **Next (Mai departe)**.
4. Utilizați setările implicite și asigurați-vă că metoda de înregistrare este **None (Niciuna)**. Faceți clic pe **Install (Instalare)**.

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 marcatului.

5. Selectați **Prevent recording deletion (Prevenirea ștergerii înregistrării)** pentru a bloca înregistrarea.

note

Pentru a debloca înregistrarea, debifați **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 (Verificare)** pentru a vedea rezultatele verificării.

note

- O semnătură digitală este diferită de signed video (video-ul semnat). Un video semnat vă permite să monitorizați camera de la care provine înregistrarea, astfel încât să puteți verifica dacă 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 intermediare sau firewall înainte de a utiliza AXIS Camera Station dacă clientul AXIS Camera Station, serverul AXIS Camera Station și dispozitivele de rețea conectate se află pe rețele diferite.

Setări server intermediar (proxy) client

Atunci când un server intermediar (proxy) separă clientul și serverul, configurați setările serverului intermediar (proxy) al clientului.

1. Deschideți clientul AXIS Camera Station.
2. Faceți clic pe **Change client proxy settings (Modificați setările serverului intermediar (proxy) al clientului)**.
3. Modificați setările serverului intermediar (proxy) al clientului.
4. Faceți clic pe **OK**.

Setări server intermediar (proxy)

Atunci când un server intermediar (proxy) separă dispozitivele de rețea și serverul, configurați setările serverului intermediar (proxy).

1. Deschideți **AXIS Camera Station Service Control**.
2. Selectați **Modify settings (Modificare setări)**.

3. În secțiunea „Proxy settings (Setări server intermediar)”, utilizați **System account internet option (Opțiune de Internet cont sistem)** sau selectați **Use manual proxy settings (Utilizare setări manuale server intermediar)**.
4. Faceți clic pe **Save (Salvare)**.

NAT și firewall

Atunci când un NAT, un firewall sau ceva similar separă clientul și serverul, configurați NAT sau firewall-ul pentru a vă asigura că portul HTTP, portul TCP și portul de redare în flux specificate în AXIS Camera Station Service Control pot trece prin firewall sau NAT. Contactați administratorul de rețea pentru instrucțiuni privind configurarea NAT sau a firewall-ului.

Configurația portului serverului

Serverul AXIS Camera Station 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 AXIS Camera Station S2108 Appliance, camerele, codorii de imagine video și dispozitivele auxiliare pe o rețea securizată, separată de rețeaua biroului. Puteți instala clientul AXIS Camera Station S2108 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

Atât clientul AXIS Camera Station, cât și serverul trebuie să aibă conexiune la internet.

1. Accesați **Configuration (Configurație) > Licenses (Licențe) > Management (Gestionare)**.
2. Asigurați-vă că **Manage licenses online (Gestionați licențele online)** se activează.
3. Conectați-vă cu contul dvs. My Axis.
4. Cheia de licență se generează automat și apare la **License keys (Chei de licență)**.
5. Dacă ați achiziționat chei de licență în mod separat, introduceți cheia dvs. de licență la **Add license key (Adăugați cheia de licență)**.
6. Faceți clic pe **Add (Adăugare)**.
7. În clientul AXIS Camera Station, asigurați-vă că cheile dvs. de licență apar la **Configuration (Configurație) > Licenses (Licențe) > Keys (Chei)**.

Licențierea unui sistem offline

1. Accesați **Configuration (Configurație) > Licenses (Licențe) > Management (Gestionare)**.
2. Dezactivați **Manage licenses online (Gestionați licențele online)**.
3. Faceți clic pe **Export system file (Exportați fișierul de sistem)**.
4. Salvați fișierul dvs. de sistem pe un USB flash drive.
5. Conectați-vă cu contul dvs. My Axis.
6. Faceți clic pe **Upload system file (Încărcați fișierul de sistem)** pentru a încărca fișierul de sistem de pe USB flash drive.
7. Cheia de licență se generează automat și este afișată la **License keys (Chei de licență)**.
8. Dacă ați achiziționat chei de licență în mod separat, introduceți cheia dvs. de licență la **Add license key (Adăugați cheia de licență)**.
9. Faceți clic pe **Add (Adăugare)**.
10. La **License keys (Chei de licență)**, faceți clic pe **Download license file (Descărcați fișierul de licență)** și salvați fișierul pe un USB flash drive.

11. În clientul AXIS Camera Station, accesați **Configuration (Configurație) > Licenses (Licențe) > Management (Gestionare)**.
12. Faceți clic pe **Import license file (Importați fișierul de licență)** și selectați fișierul de licență de pe USB flash drive.
13. Asigurați-vă că cheile dvs. de licență apar la **Configuration (Configurație) > Licenses (Licențe) > Keys (Chei)**.

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 people (Alte persoane) > Add someone else to this PC (Adăugați o altă persoană la acest computer)**.
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

Permiuni utilizator

Accesați **Configuration (Configurație) > Security (Securitate) > User permissions (Permiuni utilizatori)** pentru a vedea utilizatorii și grupurile din AXIS Camera Station S2108 Appliance.

note

Administratorii computerului care rulează serverul AXIS Camera Station S2108 Appliance primesc automat privilegiile de administrator în AXIS Camera Station S2108 Appliance. Nu puteți modifica sau elimina privilegiile grupului Administratori.

Înainte de a adăuga un utilizator sau un grup, asigurați-vă că acestea sunt înregistrate 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 permiuni atribuit fie lui personal, fie grupului. De exemplu, un utilizator care are acces la camera X și care face parte și 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.
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 AXIS Camera Station S2108 Appliance. Pentru a adăuga un utilizator la AXIS Camera Station S2108 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 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 debifați **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 (Permiuni 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.
Domeniu	Selectați pentru a căuta utilizatori sau grupuri Active Directory.
Selected server (Server selectat)	Când sunteți conectat(ă) la mai multe servere AXIS Camera Station S2108 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 secțiunea *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 unui 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 videoclipuri în direct și înregistrate. Un operator are acces deplin la toate funcționalitățile AXIS Camera Station S2108 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 AXIS Camera Station S2108 Appliance.
Editare	Permite editarea vederilor în AXIS Camera Station S2108 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 (Alarmer 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) .

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.
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 noile certificate din 2023. Pentru a asigura securitatea înregistratorului, instalați certificatele din 2023 înainte de acea dată.

Instalarea certificatelor din 2023 necesită 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. De la acesta puteți afla dacă puteți realiza upgrade la o versiune LTSC înainte de a actualiza BIOS-ul sau de a modifica vreun certificat.

note

După iunie 2026, dispozitivele care nu dispun de certificatele din 2023 vor continua să funcționeze în mod 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 bootloader 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 certificatul din 2023 este instalat.

 (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)

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 la zi, pe card apare: „Secure Boot is on and all required certificate updates have been applied (Boot securizat este activat și toate actualizările necesare ale certificatului 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

Funcția Securitate Windows 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 schimb.

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 Windows Update.

important

Dacă doar instalați certificatele prin Windows Update 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 reseta 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 Windows Update

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

important

Certificatele instalate în acest mod sunt stocate în baza de date curentă a funcției boot securizat, nu în firmware. Dacă resetați cheile boot securizat din BIOS la valorile implicite din fabrică, veți pierde certificatele, iar dispozitivul s-ar putea să nu mai poată porni cu funcția boot securizat activată. Instalați o actualizare a BIOS-ului imediat ce 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 pe 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 de registru **UEFICA2023Status**. Dacă dispozitivul dvs. nu este eligibil pentru actualizarea automată, actualizați BIOS-ul 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-ul

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 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**.

Gestionarea puterii

Switch-ul are un buget de putere total de 105 W. Aceasta este puterea maximă furnizată tuturor dispozitivelor conectate.

În majoritatea cazurilor, dispozitivele conectate consumă mai puțină energie decât cea solicitată. Pentru a optimiza consumul de energie, controlerul PoE permite dispozitivelor conectate să solicite până la 125 W și, în același timp, limitează consumul efectiv de energie la 105 W.

De exemplu, switch-ul poate alimenta 8 dispozitive PoE de clasa 3.

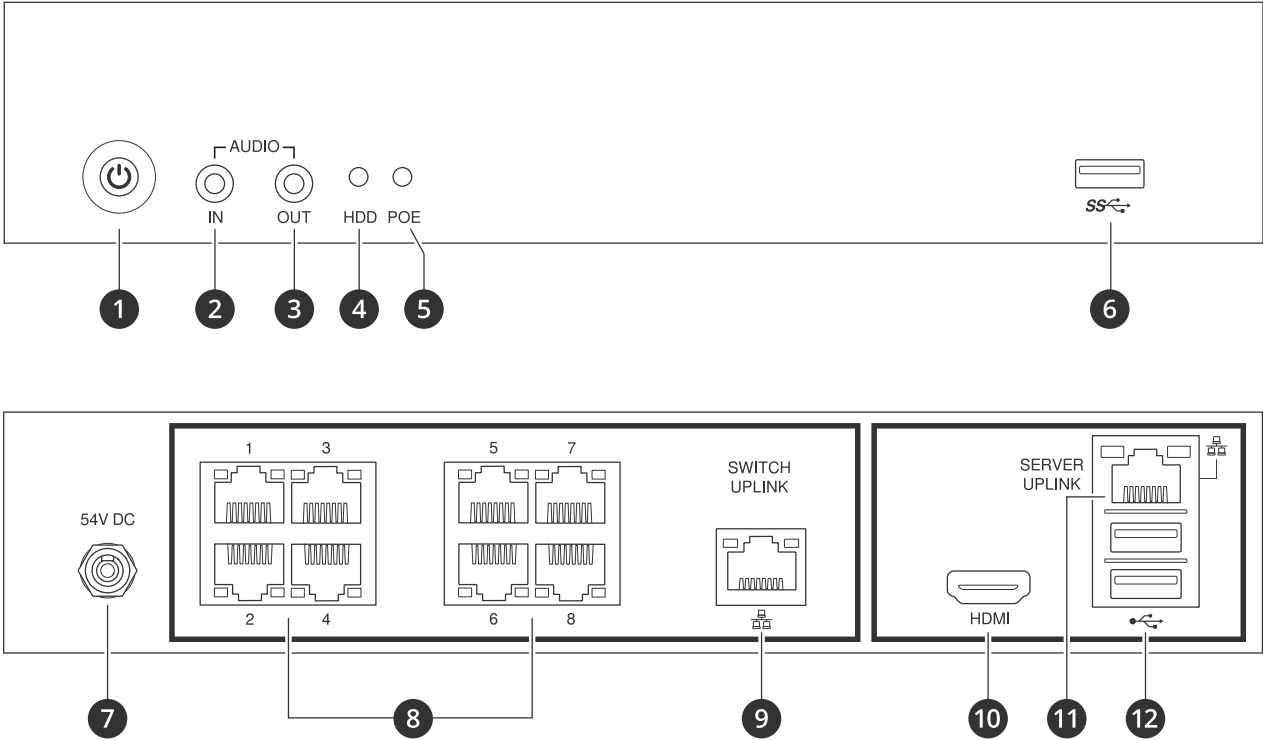
- 1 dispozitiv de clasa PoE 3 necesită o putere de 15,4 W.
- 8 dispozitive de clasa PoE 3 necesită o putere de $(8 \times 15,4) = 123,2$ W. Această valoare se încadrează în limita de 125 W permisă de controlerul PoE.
- 1 dispozitiv de clasa PoE 3 consumă, de obicei, între 10 și 12 W.
- 8 dispozitive de clasa PoE 3 consumă, de obicei, între 80 și 96 W. Aceasta se încadrează în limita de 105 W a bugetului total de putere.

⚠ warning

- Atunci când dispozitivele conectate solicită o putere mai mare de 125 W:
 - Ultimul dispozitiv conectat nu va porni.

- LED-ul de suprasarcină PoE va rămâne aprins cu lumină roșie continuă până când veți deconecta ultimul dispozitiv conectat sau veți elibera suficientă putere PoE prin scoaterea altor dispozitive.
- Atunci când dispozitivele conectate consumă de fapt o putere mai mare de 105 W:
 - Ultimul dispozitiv pornit se va opri și va încerca să repornească.
 - LED-ul de suprasarcină PoE nu se va aprinde.

Prezentare generală a produsului
 Părțile laterale din față și din spate



- 1 Buton de pornire/LED de pornire
- 2 Intrare audio
- 3 ieșire audio
- 4 LED de activitate a hard disk-ului
- 5 LED-ul de stare al porturilor PoE
- 6 Port USB 3.0
- 7 Conector de alimentare
- 8 Porturi PoE
- 9 Portul uplink-ului switch-ului RJ45
- 10 Port HDMI
- 11 Portul uplink-ului serverului RJ45
- 12 Porturi USB 2.0

Specificații
 LED-uri frontale

Indicator cu LED	Color (Culoare)	Indicație
Putere	Verde	Serverul este pornit
Unitate hard disk	Iluminează intermitent în culoarea chihlimbarie	Activitatea hard disk-ului
	Clipește în roșu	Posibilă defecțiune a hard disk-ului
Suprasarcină PoE	Roșu	Depășirea bugetului PoE
	Off (Oprit)	OK

LED-uri spate

Viteza și activitatea rețelei	Color (Culoare)	Indicație
LED-ul dreapta	Chihlimbariu	10/100 Mbit/s
	Verde ¹	1000 Mbit/s
LED-ul stânga	Iluminează intermitent în culoarea verde	Activitatea rețelei

1. Această setare este valabilă doar pentru uplink-ul Switch-ului și pentru uplink-ul serverului.

Depanare

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 înainte de a descărca kitul de recuperare și selectați varianta corespunzătoare. 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.

Dacă pe dispozitivul dvs. este 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 a fost revocat, va funcționa doar sb23.

Pentru a recrea sistemul:

1. Descărcați kitul de recuperare AXIS Network Video Recorder și instrumentul AXIS Network Video Recorder Recovery: ISO pe 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 instrumentul AXIS Network Video Recorder Recovery: 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 ce instrumentul AXIS Network Video Recorder Recovery: ISO pe USB a fost finalizat, luați USB drive și conectați-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

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

Aveți nevoie de mai mult ajutor?

Linkuri utile

- *Manual de utilizare AXIS Camera Station*
- *Conectarea la AXIS Secure Remote Access*
- *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.

T10181903_ro

2026-07 (M7.2)

© 2022 – 2026 Axis Communications AB