

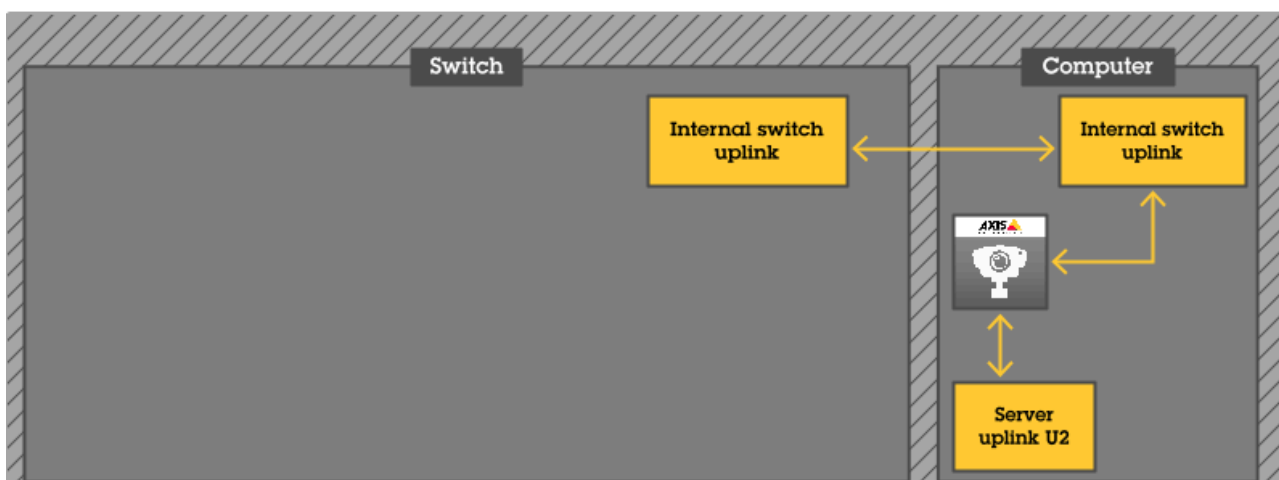
AXIS Camera Station S2108 Appliance

O zařízení

Zařízení AXIS Camera Station S2108 je univerzálním řešením záznamu s vestavěným přepínačem PoE. Účelem zařízení je zajištění spolehlivého dohledu s vysokým rozlišením a podporou kamer až do rozlišení 4K. Pro rychlou a snadnou instalaci je toto zařízení předkonfigurováno a předinstalováno se softwarem pro monitoring AXIS Camera Station včetně licencí a veškerého potřebného systémového softwaru. AXIS Camera Station nabízí intuitivní uživatelské rozhraní, které uživatelům umožňuje plně využívat širokou škálu kamer pro videodohled a dalších IP produktů společnosti Axis. Díky operačnímu systému uloženému na jednotce SSD (Solid-State Drive) a 3leté záruce na hardware poskytuje toto zařízení spolehlivé řešení dohledu.

Zařízení AXIS Camera Station S2108 se skládá ze dvou částí:

- **Přepínač:** Integrovaný přepínač Napájení přes ethernet (PoE).
- **Počítač:** Předinstalovaný veškerý potřebný software nutný k vytvoření řešení dohledu, včetně softwaru pro správu videa AXIS Camera Station.

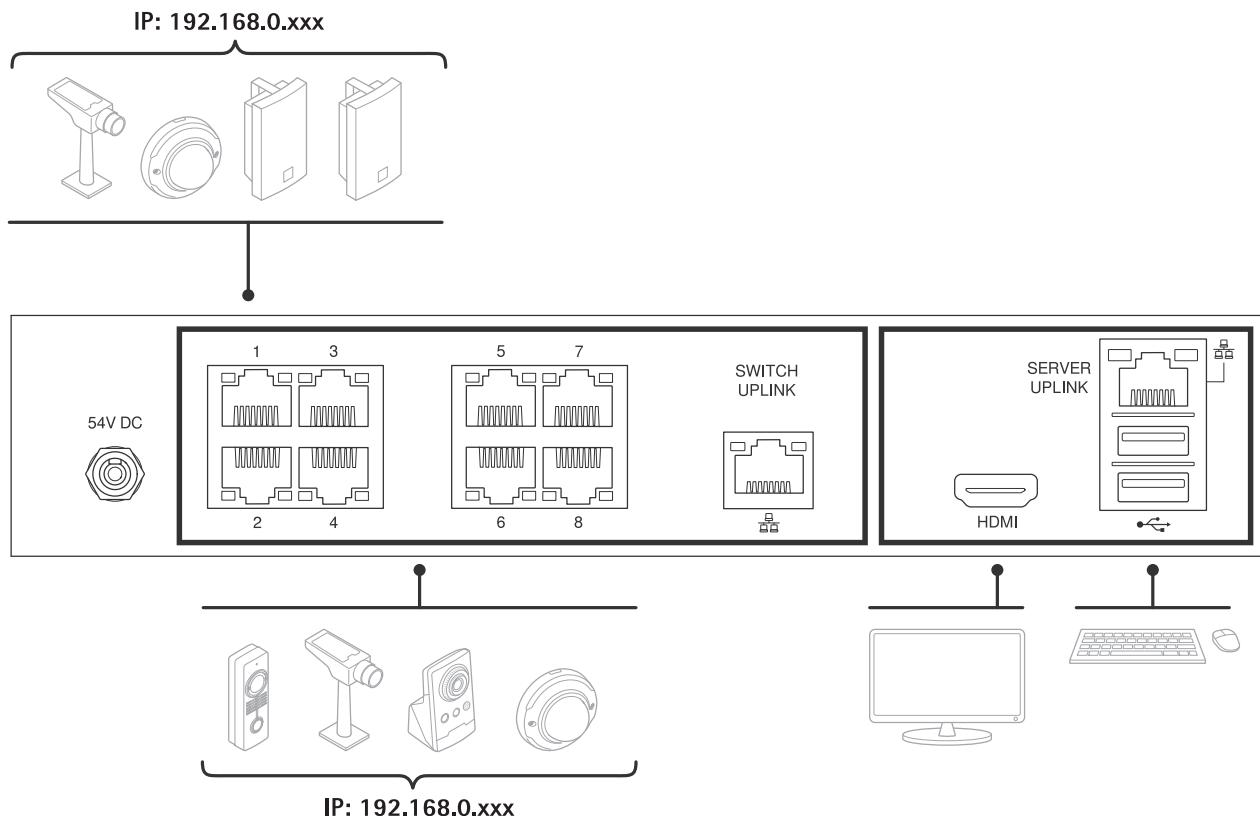


- Přepínač a počítač tvoří dvě samostatné části.
- Switch a počítač spolu komunikují prostřednictvím interních konektorů odchozí komunikace: jeden je umístěn na desce s napájecími obvody switchu a druhý na základní desce počítače.
- Odchozí připojení serveru je externí síťové rozhraní, které lze připojit k existující síti.
- Zařízení připojená k odchozímu připojení serveru nemohou komunikovat se zařízeními, která jsou připojena přímo k přepínači.
- Zařízení připojená k odchozímu připojení serveru mohou komunikovat se zařízeními, která jsou k přepínači připojena přes systém AXIS Camera Station.

Příklady nastavení

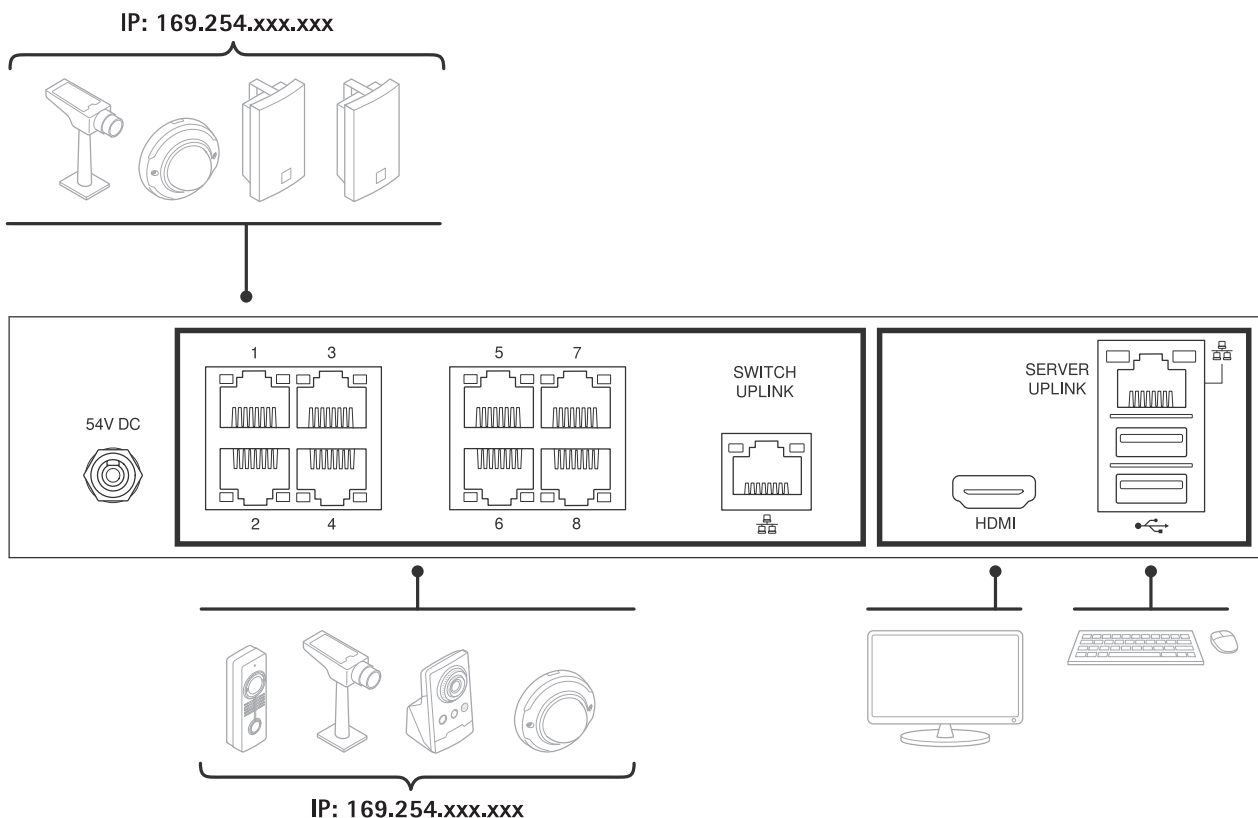
Přiřazení statické adresy každému zařízení

Můžete vytvořit samostatnou síť přidělením statické IP adresy každému zařízení a zařízení AXIS S2108. Tato síť nebude mít žádné propojení s jinou externí sítí, pokud se parametry mezi sítěmi neshodují. Počítač se stále může připojit k internetu přes port odchozího připojení serveru. Když jsou zařízení zapojena do napájených PoE portů, převezmou adresu link-local a budou potřebovat pevnou IP sadu, odpovídající zařízení AXIS S2108.



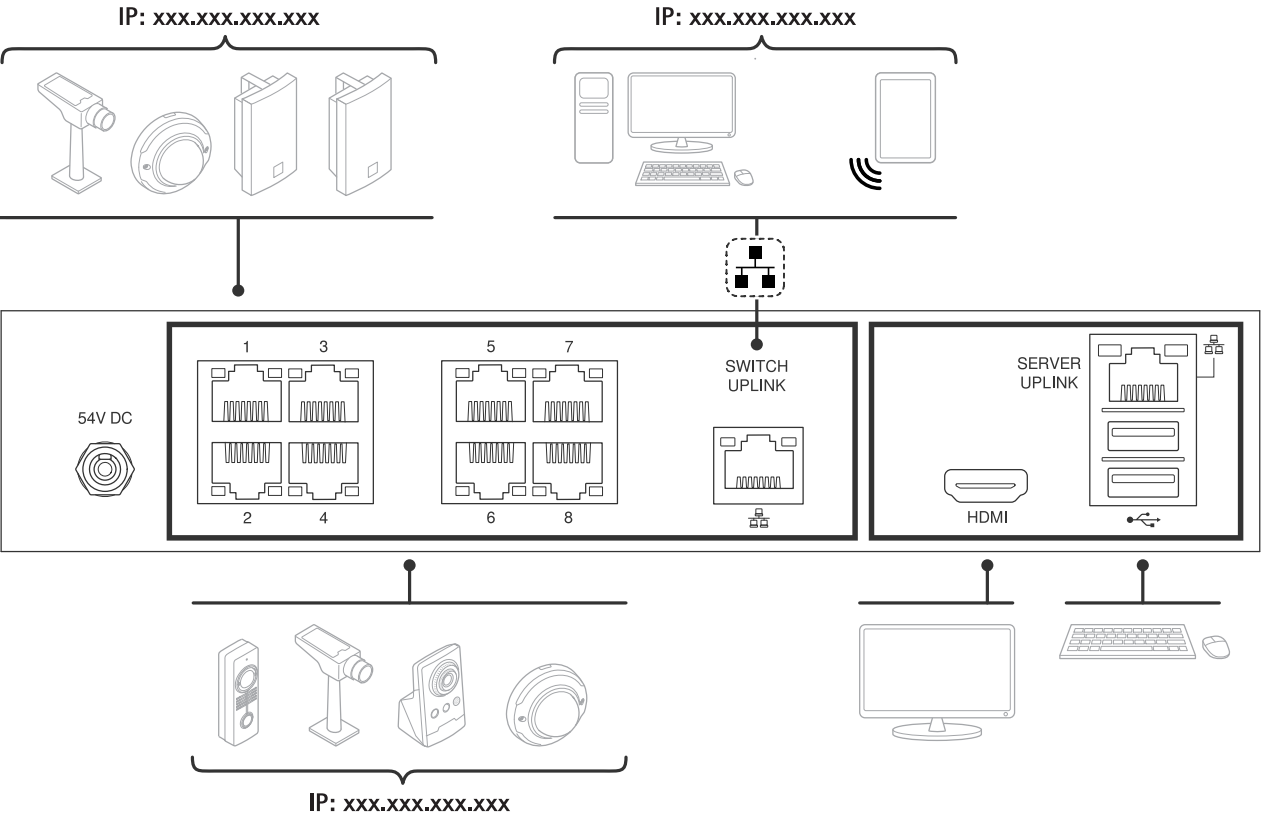
Použití místní adresy

Můžete vytvořit nezávislou síť pomocí adresy link-local pro připojení pro každé zařízení a zařízení AXIS S2108. Tato síť nebude mít žádné propojení s jinou externí sítí. Počítač se stále může připojit k internetu přes port odchozího připojení serveru. Když jsou zařízení zapojena do napájených PoE portů, převezmou adresu link-local a lze je vyhledat pomocí systému AXIS Camera Station na zařízení AXIS S2108.



Použití serveru DHCP z jiné sítě

K zařízení AXIS S2108 a připojeným zařízením se můžete připojit tak, že do odchozího připojení přepínače zapojíte stávající síť a server DHCP. Všechna připojená zařízení pak budou mít IP adresu z rozsahu serveru DHCP. Je-li v této síti k dispozici připojení k internetu, bude k dispozici i pro zařízení AXIS S2108. V opačném případě se počítač stále může připojit k internetu nezávisle přes port odchozího připojení serveru. Když jsou zařízení zapojena do napájených PoE portů, převezmou adresu DHCP, pokud je server DHCP aktivní.



Začněte

Standardní pracovní postup konfigurace záznamového serveru systému AXIS Camera Station je:

1. *Instalace zařízení*
2. Počáteční nastavení systému Windows®: Po instalaci zařízení budete provedeni několika kroky k nastavení oblasti, jazyka, rozložení klávesnice, účtu správce a hesla.
3. Počáteční nastavení rekordéru Axis: Po úvodním nastavení systému Windows se otevře aplikace AXIS Recorder Toolbox a budete provedeni několika kroky k nastavení základních a nezbytných nastavení, jako je název počítače, datum, čas a síť. Viz část *Počáteční nastavení rekordéru Axis, on page 15*.
4. Nastavení systému Windows®. Doporučujeme:
 - Aktualizovat systém Windows® na nejnovější verzi. Viz .
 - Vytvořte standardní uživatelský účet. Viz *Vytvoření uživatelského účtu, on page 21*.
5. Aktualizujte systém AXIS Camera Station na nejnovější verzi.
 - Pokud je váš systém online: otevřete aplikaci AXIS Recorder Toolbox a klikněte na **Update AXIS Camera Station** (Aktualizovat AXIS Camera Station).
 - Pokud je váš systém offline: přejděte na *axis.com* a stáhněte si nejnovější verzi.
6. Spusťte klienta AXIS Camera Station.
7. *Připojení k serveru AXIS Camera Station*
8. *Konfigurace kamerové stanice AXIS, on page 17*

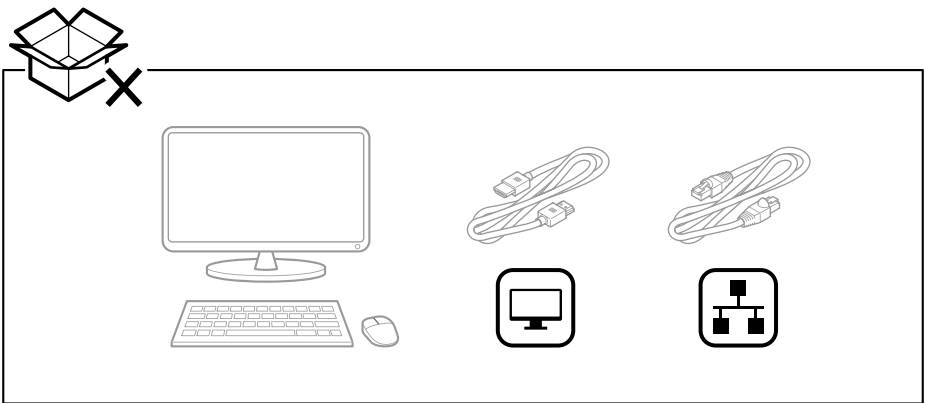
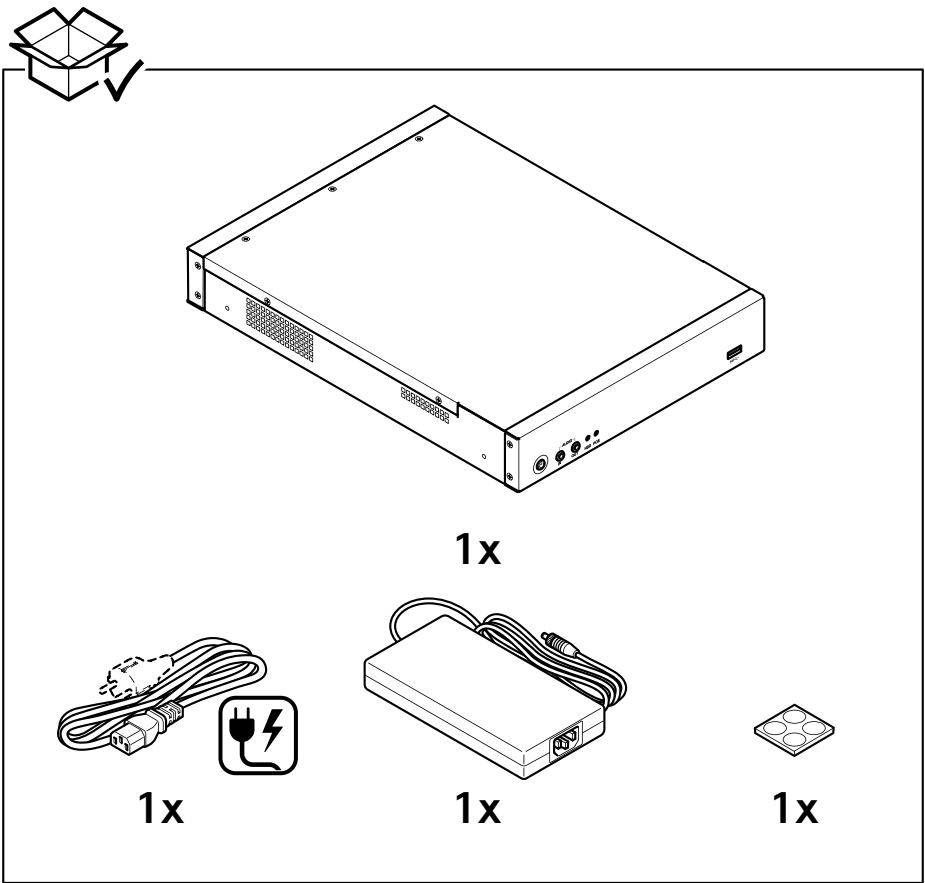
Instalace zařízení

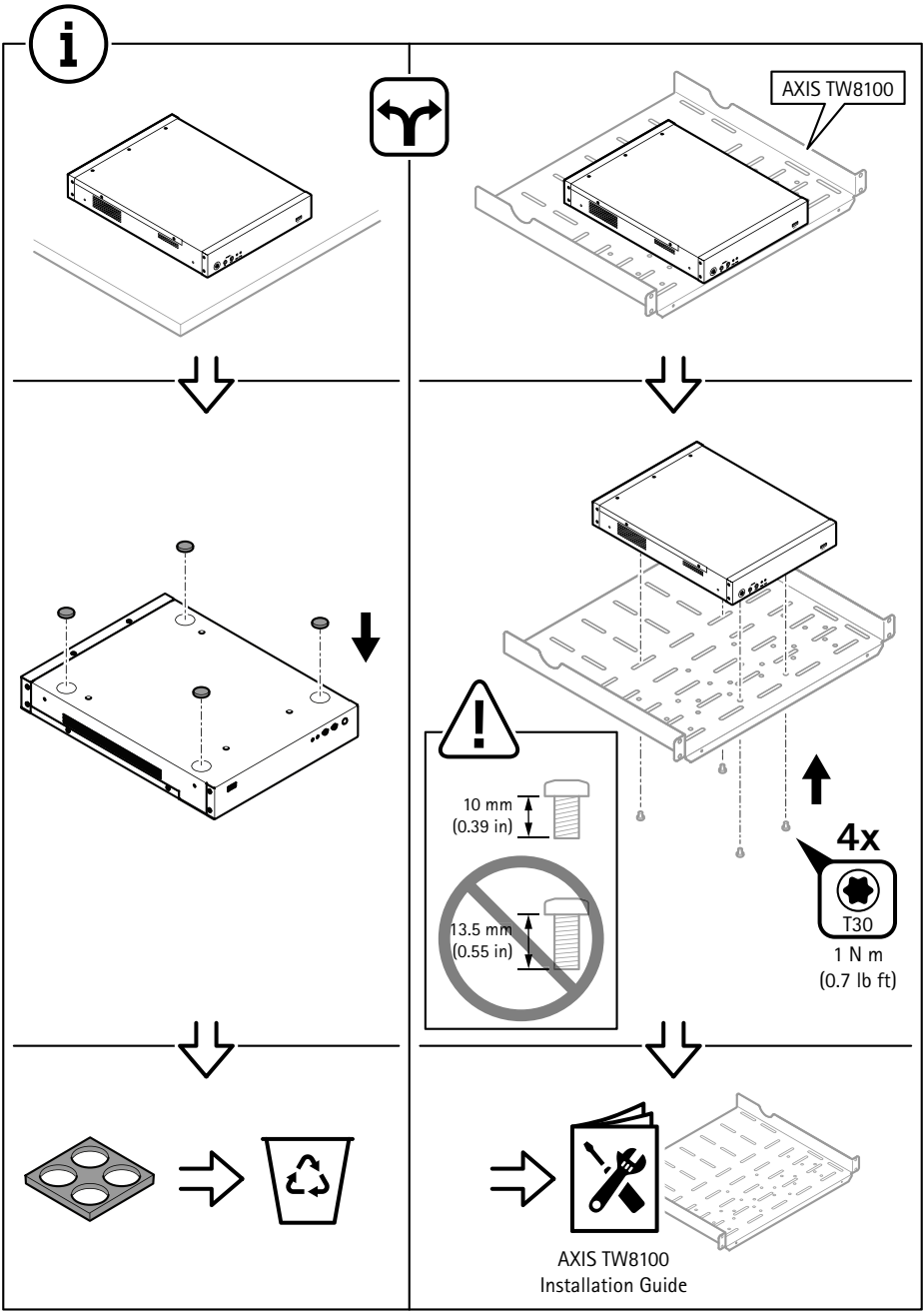
Před instalací

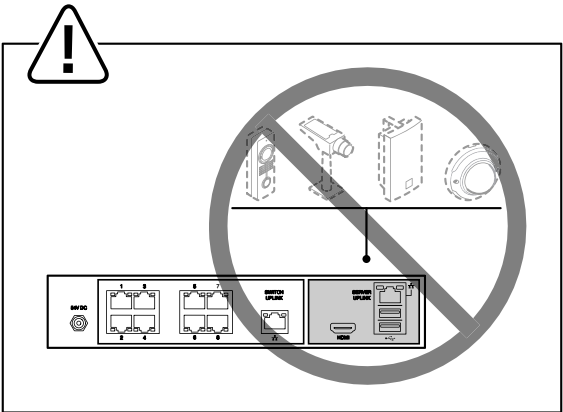
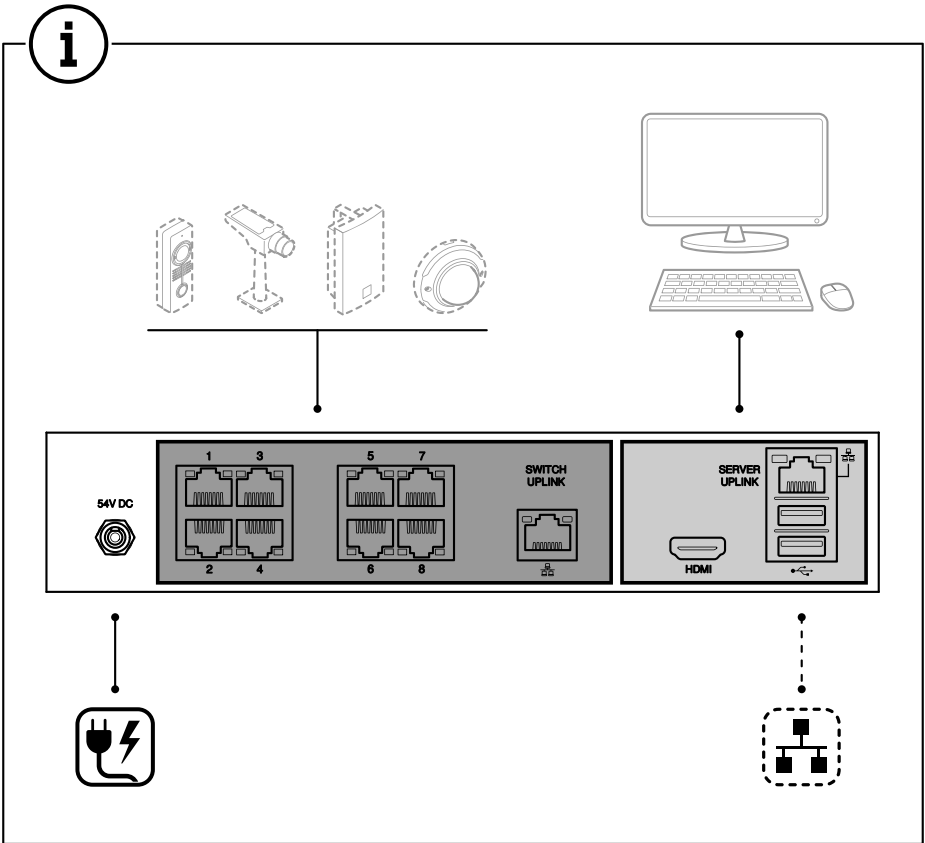
- Připravte si další příslušenství používané při instalaci: monitor, myš, klávesnici a síťový kabel.
- Seznamte se s používáním různých uživatelských účtů.

V následující tabulce jsou uvedeny uživatelské účty, které lze použít k instalaci, konfiguraci a provozu systému Axis.

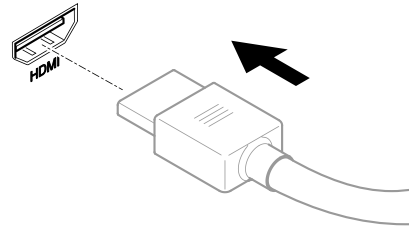
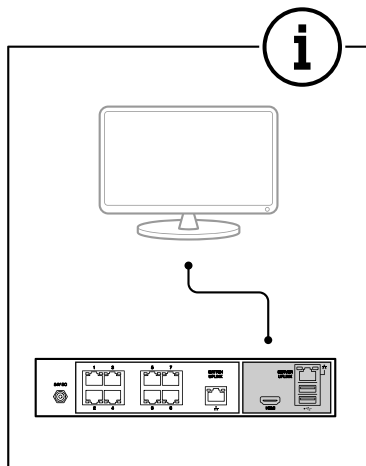
Uživatelský účet	Popis	Poznámka
MyAxis	Používá se ke stažení nejnovějšího softwaru, získání přístupu k licenčnímu systému, zabezpečenému vzdálenému přístupu Axis a ke sledování stavu systému.	Registrováno ze stránky <i>my.axis.com</i> .
Windows®		
Správce systému Windows®	Oprávnění správce v systému Windows®. Doporučujeme, abyste jej jako správce AXIS Camera Station nepoužívali.	Vytvořeno během úvodního nastavení systému Windows®.
Uživatel systému Windows® s oprávněními správce systému AXIS Camera Station	Uživatel systému Windows®, kterému byla v systému AXIS Camera Station udělena oprávnění správce, která má používat systémový integrátor nebo správce systému pro konfiguraci nebo řešení problémů.	Vytvořeno v nastaveních systému Windows®.
Uživatel systému Windows® s oprávněními operátora nebo diváka systému AXIS Camera Station	Uživatel systému Windows®, kterému bylo v systému AXIS Camera Station uděleno oprávnění operátora nebo diváka.	Vytvořeno v nastaveních systému Windows®.
Zařízení		
Správce zařízení	Používá správce pro přístup ke kameře ze systému správy videa nebo webové stránky zařízení.	Vytvořeno z webové stránky zařízení nebo přidáním zařízení do systému AXIS Camera Station.



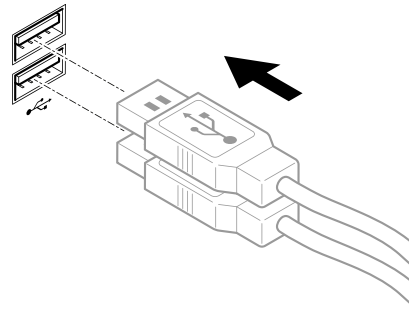
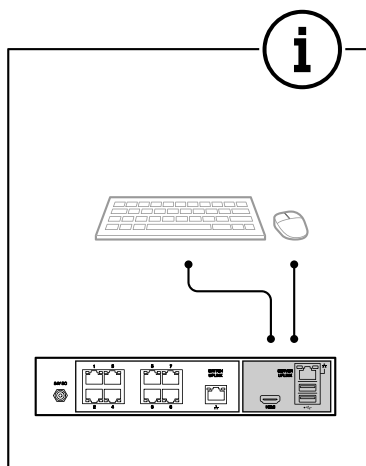




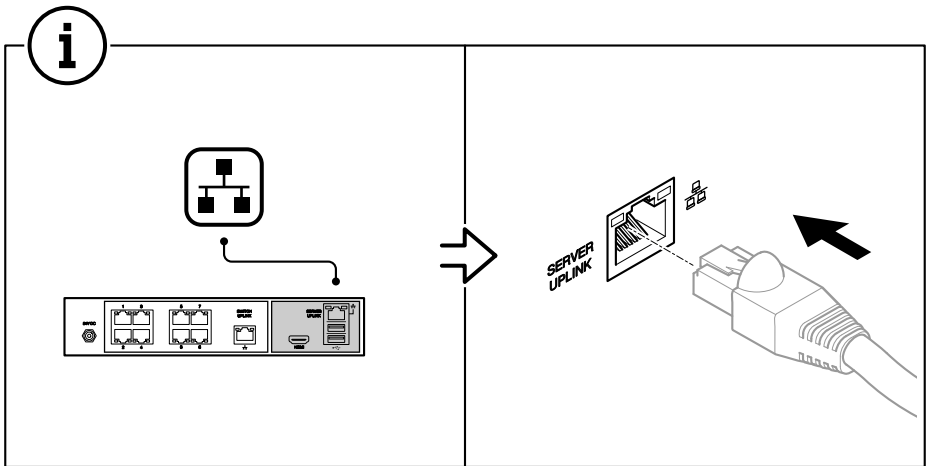
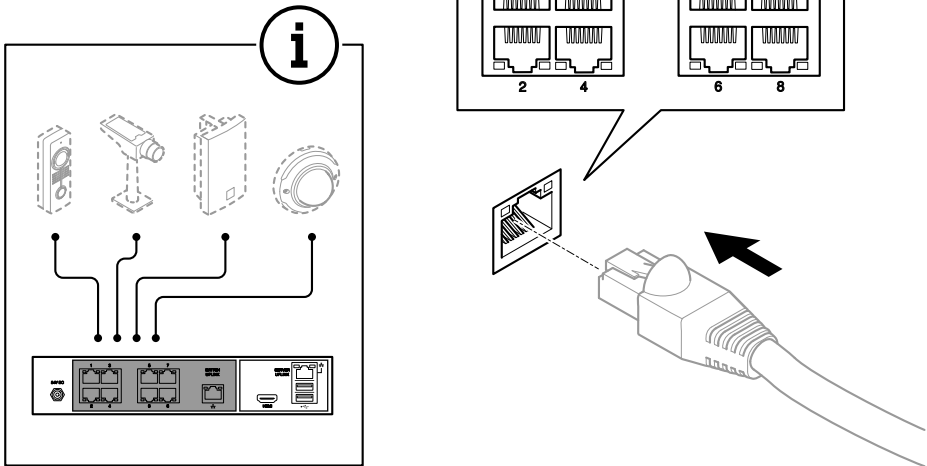
1.1



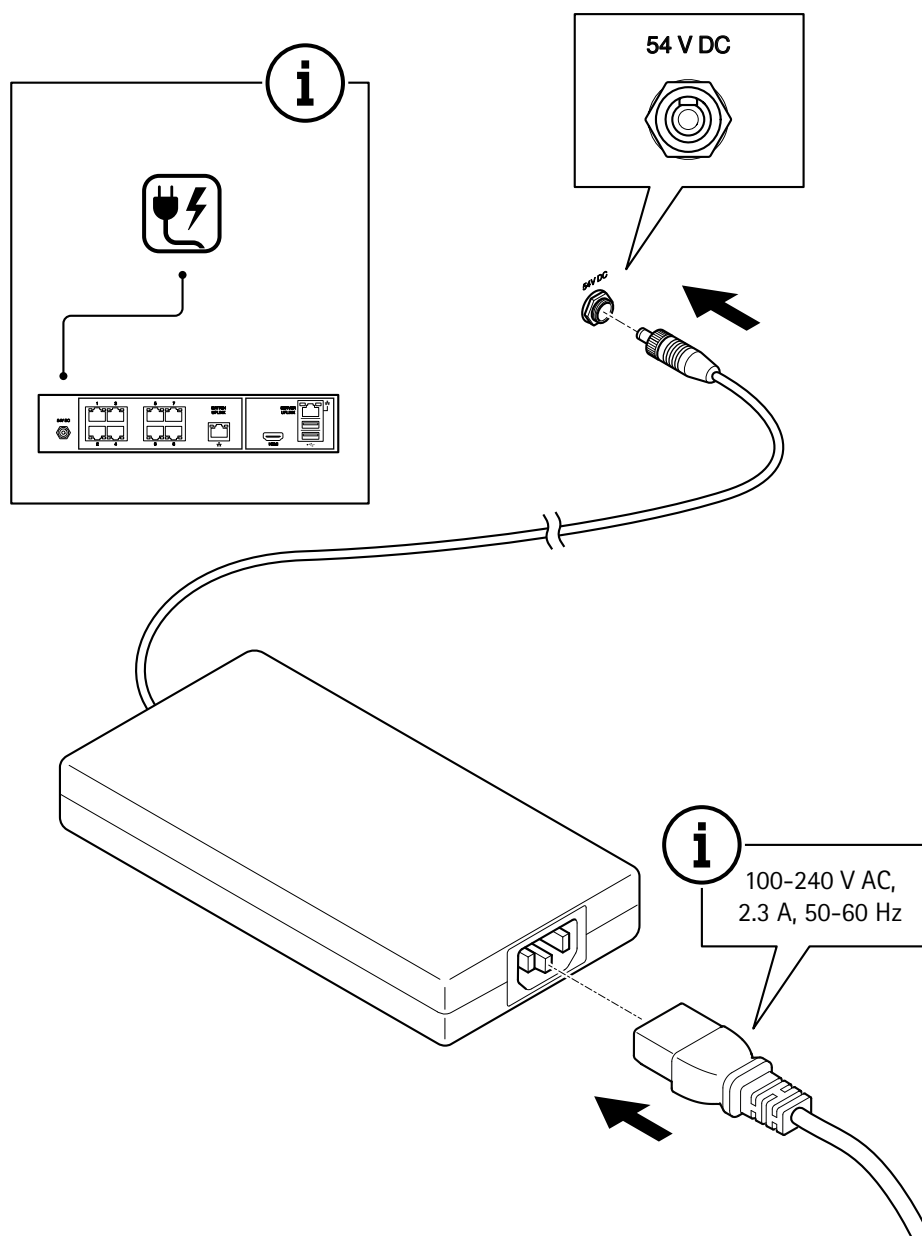
1.2



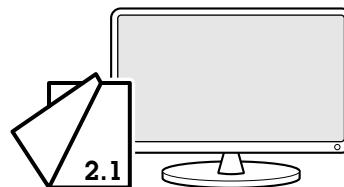
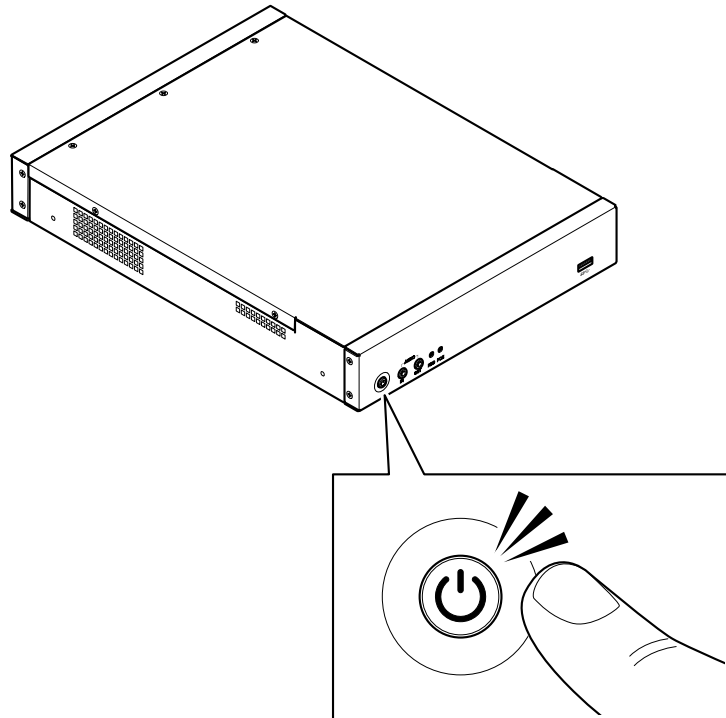
1.3



1.4



1.5



Konfigurace zařízení

Počáteční nastavení rekordéru Axis

Po konfiguraci systému Windows® se automaticky spustí aplikace AXIS Recorder Toolbox, která vás provede průvodcem prvním nastavením. V tomto průvodci nastavením můžete před správou zařízení v aplikaci AXIS Recorder Toolbox nakonfigurovat několik základních a nezbytných nastavení.

1. Vyberte **Light (světlý)** nebo **Dark (tmavý)** motiv a klikněte na tlačítko **Next (Další)** (pokud je k dispozici pro váš produkt).
2. Podle potřeby změňte název počítače a klikněte na tlačítko **Next (Další)**.
3. V části **Date and time (Datum a čas)** nakonfigurujte následující nastavení a klikněte na tlačítko **Next (Další)**.
 - Zvolte časové pásmo.
 - Chcete-li nastavit NTP server, vyberte možnost **NTP server** a zadejte adresu NTP serveru.
 - Chcete-li nastavit ručně, vyberte možnost **Manual (Manuální)** a vyberte datum a čas.
4. V části **Network settings (Nastavení sítě)** nakonfigurujte následující nastavení a klikněte na tlačítko **Next (Další)**.
 - Ve výchozím nastavení jsou zapnuty možnosti **Use automatic IP settings (DHCP) (Použít automatické nastavení IP (DHCP))** a **Use automatic DNS settings (Použít automatické nastavení DNS)**.
 - Pokud je zařízení připojeno k síti se serverem DHCP, automaticky se zobrazí přidělená IP adresa, maska podsítě, brána a preferovaný server DNS.
 - Pokud zařízení není připojeno k síti nebo není k dispozici server DHCP, zadejte IP adresu, masku podsítě, bránu a preferovaný server DNS manuálně v závislosti na požadavcích sítě.
5. Klikněte na možnost **Dokončit**. Pokud jste změnili název počítače, aplikace AXIS Recorder Toolbox vás vyzve k restartování zařízení.

Přihlášení k serveru

Pomocí klienta AXIS Camera Station se můžete připojit k více serverům nebo k jedinému serveru nainstalovanému v místním počítači nebo jinde v síti. K serverům AXIS Camera Station se můžete připojit různými způsoby:

Poslední použité servery – Připojení k serverům použitým v předchozí relaci.

Tento počítač – Připojení k serveru nainstalovanému na stejném počítači jako klient.

Vzdálený server – Viz část *Připojení ke vzdálenému serveru, on page 16*.

Zabezpečený vzdálený přístup AXIS – Viz část *Přihlásit se k zabezpečenému vzdálenému přístupu AXIS, on page 16*.

Poznámka

Při prvním pokusu o připojení k serveru klient kontroluje ID certifikátu serveru. Chcete-li se ujistit, že se připojujete ke správnému serveru, ověřte ručně ID certifikátu s ID zobrazeným v nástroji AXIS Camera Station Service Control.

Seznam serverů	Chcete-li se připojit k serverům ze seznamu serverů, vyberte některý z rozbalovacího menu Seznam severů . Klikněte na ikonu  , jestliže chcete vytvořit nebo editovat seznamy serverů.
Importovat seznam serverů	Pokud chcete importovat soubor seznamu serverů, který byl exportován ze systému AXIS Camera Station,

	klikněte na možnost Importovat seznam serverů vyhledejte soubor .msl.
Vymazat uložená hesla	Jestliže chcete odstranit uložená uživatelská jména a hesla všech připojených serverů, klikněte na možnost Odstranit uložená hesla .
Změnit nastavení proxy serveru klienta	Pro připojení k serveru bude možná nutné změnit nastavení proxy serveru klienta, klikněte tedy na tlačítko Změnit nastavení proxy serveru klienta .

Připojení ke vzdálenému serveru

1. Vyberte možnost **Vzdálený server**.
2. Zvolte server z rozvinovacího seznamu **Remote server (Vzdálený server)** nebo do pole zadejte IP nebo DNS adresu. Pokud server na seznamu není, kliknutím na ikonu ↺ obnovte seznam všech dostupných vzdálených serverů. Jestliže je server konfigurován tak, aby přijímal klienty na jiném portu než na výchozím portu číslo 55754, zadejte IP adresu, za kterou bude následovat číslo portu, například 192.168.0.5:46001.
3. Proveďte jedno z těchto řešení:
 - Vyberte možnost **Log in as current user (Přihlásit se jako aktuální uživatel)** pro přihlášení jako aktuální uživatel Windows®.
 - Zrušte výběr možnosti **Log in as current user (Přihlásit se jako aktuální uživatel)** a klikněte na možnost **Log in (Přihlásit)**. Vyberte možnost **Other user (Jiný uživatel)** a zadejte jiné uživatelské jméno a heslo, pokud se chcete přihlásit pomocí jiných přihlašovacích údajů.

Přihlásit se k zabezpečenému vzdálenému přístupu AXIS

Důležité

V zájmu zlepšení zabezpečení a funkčnosti aktualizujeme **Zabezpečený vzdálený přístup Axis (v1)** na **Zabezpečený vzdálený přístup Axis v2**. Stávající verzi přestaneme používat od 1. prosince 2025 a důrazně doporučujeme, abyste na Zabezpečený vzdálený přístup Axis v2 přešli ještě předtím.

Co to znamená pro váš systém AXIS Camera Station S2108 Appliance?

- Po 1. prosinci 2025 již nebude možné vzdáleně přistupovat k systému pomocí **Zabezpečeného vzdáleného přístupu Axis (v1)**.
- Chcete-li používat **Zabezpečený vzdálený přístup Axis v2**, musíte provést upgrade na AXIS Camera Station Pro verze 6.8. Tento upgrade je v současné době zdarma pro všechny uživatele AXIS Camera Station 5 do 1. března 2026.

Poznámka

- Při pokusu o připojení k serveru pomocí Axis Secure Remote Access nemůže server automaticky aktualizovat klienta.
 - Pokud je proxy server umístěn mezi síťovým zařízením a serverem AXIS Camera Station S2108 Appliance, je třeba nakonfigurovat nastavení proxy serveru v systému Windows na serveru AXIS Camera Station S2108 Appliance, aby bylo možné k serveru přistupovat pomocí zabezpečeného vzdáleného přístupu AXIS.
1. Klikněte na odkaz **Přihlásit k zabezpečenému vzdálenému přístupu AXIS**.
 2. Zadejte přihlašovací údaje k účtu My Axis.
 3. Klikněte na **Přihlášení**.
 4. Klikněte na **Grant (Povolit)**.

Konfigurace kamerové stanice AXIS

Tento tutoriál vám pomůže se základními kroky při uvádění systému do provozu.

Než začnete:

- Provést nastavení sítě v závislosti na instalaci. Viz *Konfigurace sítě, on page 19*.
- Provést nastavení portů serveru, je-li to třeba. Viz *Nastavení portu serveru, on page 19*.
- Zvážit otázky zabezpečení. Viz část *Bezpečnostní aspekty*.

Po provedení potřebných nastavení můžete se systémem AXIS Camera Station začít pracovat:

1. *Spustíte systém pro správu videa, on page 17*
2. *Přidat zařízení, on page 17*
3. *Nastavení metody záznamu, on page 17*
4. *Video se živým zobrazením, on page 17*
5. *Prohlížení záznamů, on page 18*
6. *Přidávání záložek, on page 18*
7. *Exportovat záznamy, on page 18*
8. *Přehrávání a ověřování záznamů v přehrávači AXIS File Player, on page 18*

Spustíte systém pro správu videa

Dvakrát klikněte na ikonu klienta AXIS Camera Station, čímž klienta spustíte. Po prvním spuštění se klient pokusí přihlásit k serveru AXIS Camera Station, který je nainstalovaný na stejném počítači jako klient.

Můžete se připojit k více serverům AXIS Camera Station a různými způsoby.

Přidat zařízení

Při prvním spuštění systému AXIS Camera Station se otevře stránka Add devices (Přidat zařízení). AXIS Camera Station vyhledá v síti připojená zařízení a zobrazí seznam nalezených zařízení.

1. Ze seznamu vyberte kamery, které chcete přidat. Nemůžete-li kameru nalézt, klikněte na možnost **Ruční vyhledávání**.
2. Klikněte na **Přidat**.
3. Vyberte možnost **Rychlé nastavení** nebo **Nastavení nástroje Site Designer**. Klikněte na tlačítko **Další**.
4. Použijte výchozí nastavení a zkontrolujte, že je u položky **Metoda záznamu** vybrána možnost **Žádná**. Klikněte na tlačítko **Instalovat**.

Nastavení metody záznamu

1. Přejděte do nabídky **Nastavení > Záznam a události > Metoda záznamu**.
2. Vyberte kameru.
3. Zapněte **Detekce pohybu**, nebo **Nepřetržitě**, nebo obojí.
4. Klikněte na **Použít**.

Video se živým zobrazením

1. Otevřete kartu **Živé zobrazení**.
2. Výběrem kamery zobrazíte její živé zobrazení.

Prohlížení záznamů

1. Otevřete záložku **Záznamy**.
2. Vyberte kameru, ze které chcete prohlížet záznamy.

Přidávání záložek

1. Přejděte na záznam.
2. Na časové ose přibližujte a oddalujte obraz a pohybujte časovou osou tak, aby se značka umístila na požadované místo.
3. Klikněte na .
4. Zadejte název a popis záložky. Použijte klíčová slova, aby se záložka dala snadno najít.
5. Uzamkněte záznam volbou položky **Zabránit ve vymazání záznamu**.

Poznámka

Jestliže chcete záznam odemknout, zrušte možnost **Prevent recording deletion** (Zabránit smazání záznamu) nebo odstraňte záložku.

6. Záložku uložte kliknutím na **OK**.

Exportovat záznamy

1. Otevřete záložku **Záznamy**.
2. Vyberte kameru, ze které chcete záznamy exportovat.
3. Kliknutím na  můžete zobrazit značky volby.
4. Přetažením značek volby můžete zahrnout záznamy, které chcete exportovat.
5. Kliknutím na  otevřete kartu **Export**.
6. Klikněte na **Export...**

Přehrávání a ověřování záznamů v přehrávači AXIS File Player

1. Přejděte do složky s exportovanými záznamy.
2. Klikněte dvakrát na přehrávač AXIS File Player.
3. Kliknutím na  zobrazíte poznámky k záznamu.
4. Postup ověření digitálního podpisu:
 - 4.1. Přejděte do nabídky **Nástroje > Ověřit digitální podpis**.
 - 4.2. Vyberte možnost **Validate with password (Ověřit pomocí hesla)** a zadejte heslo.
 - 4.3. Klikněte na **Verify (Ověřit)** si zkontrolujte výsledky ověření.

Poznámka

- Digitální podpis se liší od podepsaného videa. Podepsané video umožňuje vysledovat, z které kamery záznam pochází, takže můžete ověřit, že s ním nikdo nemanipuloval. Další informace najdete na kartě *Signed video (Podepsané video)* a v uživatelské příručce kamery.
- Pokud uložené soubory nemají žádné spojení s databází AXIS Camera Station (neindexované soubory), je třeba je převést, aby je bylo možné přehrávat v nástroji AXIS File Player. Pro pomoc s převodem souborů se obraťte na technickou podporu společnosti Axis.

Konfigurace sítě

Pokud se klient AXIS Camera Station, server AXIS Camera Station a připojená síťová zařízení nacházejí v různých sítích, může být nutné před použitím aplikace AXIS Camera Station provést nastavení proxy serveru nebo firewallu.

Zástupná nastavení klienta

Když mezi klientem a serverem stojí proxy server, je třeba provést nastavení proxy u klienta.

1. Otevřít klient AXIS Camera Station.
2. Klikněte na možnost **Změnit nastavení proxy u klienta**.
3. Změňte nastavení proxy u klienta.
4. Klikněte na tlačítko **OK**.

Nastavení proxy u serveru

Když mezi síťovými zařízeními a serverem stojí proxy server, je třeba provést nastavení proxy u serveru.

1. Otevřete nástroj AXIS Camera Station Service Control.
2. Vyberte možnost **Upravit nastavení**.
3. V části **Nastavení proxy** použijte výchozí **Možnost internetu systémového účtu** nebo vyberte možnost **Použít manuální nastavení proxy**.
4. Klikněte na **Save (Uložit)**.

NAT a firewall

Když stojí mezi klientem a serverem NAT, firewall apod., je třeba nastavit NAT nebo firewall tak, aby bylo zajištěno, že porty HTTP, TCP a streamovací port zadané v nástroji AXIS Camera Station Service Control mohou procházet přes firewall a/nebo NAT. Pokyny ohledně nastavení NAT nebo firewallu vám poskytne váš správce sítě.

Nastavení portu serveru

Server AXIS Camera Station používá pro komunikaci mezi serverem a klientem porty 55752 (HTTP), 55754 (TCP), 55756 (mobilní komunikace) a 55757 (mobilní streamování). V případě potřeby můžete porty změnit v nástroji AXIS Camera Station Service Control.

Bezpečnostní aspekty

Aby se zabránilo neoprávněnému přístupu k kamerám a záznamům:

- Používejte silná hesla pro všechna síťová zařízení (kamery, videokodéry a pomocná zařízení).
- Nainstalujte server AXIS Camera Station S2108 Appliance, kamery, videokodéry a pomocná zařízení v zabezpečené síti oddělené od kancelářské sítě. Klienta AXIS Camera Station S2108 Appliance můžete nainstalovat do počítače v jiné síti, například v síti s přístupem k internetu.
- Ujistěte se, že všichni uživatelé používají silná hesla.

Licence pro systém online

Klient AXIS Camera Station i server musejí mít připojení k internetu.

1. Přejděte do nabídky **Nastavení > Licence > Správa**.
2. Zkontrolujte, zda se zapne funkce **Manage licenses online (Spravovat licence online)**.
3. Přihlaste se s pomocí účtu My Axis.
4. Licenční klíč se vygeneruje automaticky a objeví v části **License keys (Licenční klíče)**.

5. Pokud jste zakoupili licenční klíč samostatně, zadejte svůj licenční klíč v části **Add license key (Přidat licenční klíč)**.
6. Klikněte na **Přidat**.
7. V klientu AXIS Camera Station zajistěte, aby vaše licenční klíče byly uvedeny v nabídce **Configuration > Licenses > Keys (Nastavení > Licence > Klíče)**.

Licence pro systém offline

1. Přejděte do nabídky **Nastavení > Licence > Správa**.
2. Vypněte **Manage licenses online (Spravovat licence online)**.
3. Klikněte na možnost **Exportovat soubor systému**.
4. Uložte soubor systému na jednotku USB flash.
5. Přihlaste se s pomocí účtu My Axis.
6. Klikněte na možnost **Upload system file (Nahrát systémový soubor)** pro nahrání systémového souboru, jenž jste exportovali na jednotku USB flash.
7. Licenční klíč se vygeneruje automaticky a zobrazí v části **License keys (Licenční klíče)**.
8. Pokud jste zakoupili licenční klíč samostatně, zadejte svůj licenční klíč v části **Add license key (Přidat licenční klíč)**.
9. Klikněte na **Přidat**.
10. V nabídce **License keys (Licenční klíče)** klikněte na možnost **Download license file (Stáhnout licenční soubor)** a uložte soubor na jednotku USB flash.
11. Z klienta AXIS Camera Station přejděte do části **Configuration > Switch > Management (Konfigurace > Přepínač > Správa)**.
12. Klikněte na možnost **Import license file (Importovat licenční soubor)** a zvolte licenční soubor uložený na jednotce USB flash.
13. Ujistěte se, zda je váš licenční klíč uveden v nabídce **Configuration > Licenses > Keys (Konfigurace > Licence > Klíče)**.

Správa lokálních uživatelských účtů systému Windows®

Vytvoření uživatelského účtu

Pro lepší zabezpečení osobních dat a informací doporučujeme ke každému místnímu účtu přidat heslo.

Důležité

Jakmile vytvoříte heslo pro místní účet, nezapomeňte ho. Ztracené heslo pro místní účty nelze žádným způsobem obnovit.

1. Přejděte do **Settings > Accounts > Other people > Add someone else to this PC** (Nastavení > Účty > Ostatní lidé > Přidat někoho dalšího do tohoto počítače).
2. Klikněte na položku **I don't have this person's sign-in information** (Nemám přihlašovací údaje této osoby).
3. Klikněte na položku **Add a user without a Microsoft account** (Přidat uživatele bez účtu Microsoft).
4. Zadejte uživatelské jméno, heslo a nápovědu pro heslo.
5. Klikněte na **Next** (Další) a postupujte podle pokynů.

Vytvoření účtu správce

1. Přejděte do sekce **Settings > Accounts > Other people** (Nastavení > Účty > Ostatní lidé).
2. Přejděte na účet, který chcete změnit, a klikněte na možnost **Change account type** (Změnit typ účtu).
3. Přejděte do sekce **Account type** (Typ účtu) a vyberte možnost **Administrator** (Správce).
4. Klikněte na tlačítko **OK**.
5. Restartujte zařízení a přihlaste se pomocí nového účtu správce.

Vytvoření místní skupiny uživatelů

1. Přejděte do nabídky **Computer Management** (Správa počítače).
2. Přejděte do části **Local Users and Groups > Group** (Místní uživatelé a skupiny > Skupina).
3. Klikněte pravým tlačítkem na možnost **Group** (Skupina) a vyberte **New Group** (Nová skupina).
4. Zadejte název a popis skupiny.
5. Přidání členů skupiny:
 - 5.1. Klikněte na **Přidat**.
 - 5.2. Klikněte na **Pokročilý**.
 - 5.3. Najděte uživatelské účty, které chcete přidat do skupiny, a klikněte na tlačítko **OK**.
 - 5.4. Znovu klikněte na tlačítko **OK**.
6. Klikněte na možnost **Create** (Vytvořit).

Odstranění uživatelského účtu

Důležité

Při odstranění účtu odeberete uživatelský účet z přihlašovací obrazovky. Odeberete také všechny soubory, nastavení a programová data uložená v uživatelském účtu.

1. Přejděte do sekce **Settings > Accounts > Other people** (Nastavení > Účty > Ostatní lidé).
2. Přejděte na účet, který chcete odebrat, a klikněte na **Remove** (Odebrat).

Změna hesla uživatelského účtu

1. Přihlaste se pomocí účtu správce.

2. Přejděte do sekce **User Accounts > User Accounts > Manage another account in sequence** (Uživatelské účty > Uživatelské účty > Spravovat jiný účet v sekvenci). Zobrazí se seznam se všemi uživatelskými účty v zařízení.
3. Vyberte uživatelský účet, jehož heslo chcete změnit.
4. Klikněte na možnost **Change the password** (Změnit heslo).
5. Zadejte nové heslo a klikněte na **Change password** (Změnit heslo).

Vytvoření disku pro obnovení hesla uživatelského účtu

Doporučujeme vytvořit disk pro obnovení hesla na jednotce USB flash. Pomocí něj můžete heslo obnovit. Bez disku pro obnovení hesla nelze heslo obnovit.

Poznámka

Používáte-li systém Windows® 10 nebo novější, můžete k místnímu účtu přidat bezpečnostní otázky pro případ, že zapomenete heslo, takže nemusíte vytvářet disk pro obnovení hesla. Chcete-li tak učinit, otevřete nabídku **Start** a klikněte na **Settings > Sign-in options > Update your security questions** (Nastavení > Možnosti přihlášení > Aktualizovat bezpečnostní otázky).

1. Přihlaste se k zařízení pomocí místního uživatelského účtu. Pro připojený účet nelze vytvořit disk pro obnovení hesla.
2. Připojte prázdnou jednotku USB flash do zařízení.
3. Z vyhledávacího pole systému Windows® přejděte do sekce **Create a password reset disk** (Vytvořit disk pro obnovení hesla).
4. V průvodci nastavením **Forgotten Password** (Zapomenuté heslo) klikněte na **Next** (Další).
5. Vyberte svou jednotku USB flash a klikněte na možnost **Next** (Další).
6. Zadejte své současné heslo a klikněte na možnost **Next** (Další).
7. Postupujte dle pokynů na obrazovce.
8. Vyjměte jednotku USB flash a uložte ji na bezpečném místě. Když změníte heslo (i opakovaně), nemusíte vždy vytvářet nový disk.

Správa uživatelských účtů systému AXIS Camera Station

Uživatelská oprávnění

Přejděte do nabídky **Configuration > Security > User permissions** (Konfigurace > Zabezpečení > Uživatelská oprávnění) pro zobrazení uživatelů a skupin v AXIS Camera Station S2108 Appliance.

Poznámka

Správčům počítače, na kterém je spuštěn server AXIS Camera Station S2108 Appliance, jsou automaticky udělena oprávnění správce v AXIS Camera Station S2108 Appliance. Oprávnění skupiny Administrators nelze změnit ani odebrat.

Než budete moci přidat uživatele nebo skupinu, ujistěte se, že jsou zaregistrováni na místním počítači nebo že mají uživatelský účet ve službě Windows® Active Directory. Jestliže chcete přidat uživatele nebo skupiny, viz *Přidání uživatelů nebo skupin*.

Pokud uživatel patří do nějaké skupiny, získává oprávnění s nejvyšší úrovní role, která mu byla přiřazena buď individuálně, nebo v rámci dané skupiny. Například uživatel, který má přístup ke kameře X a zároveň patří do skupiny s přístupem ke kamerám Y a Z, má přístup ke všem třem kamerám.

	Označuje, že zadání je jeden uživatel.
	Označuje, že zadání je skupina.
Jméno	Uživatelské jméno tak, jak je zobrazeno na místním počítači nebo ve službě Active Directory.
Doména	Doména, do které uživatel nebo skupina patří.
Role	Role přístupu přiřazená uživateli nebo skupině. Možné hodnoty: Správce, Operátor a Pozorovatel.
Detaily	Podrobné údaje o uživateli tak, jak jsou uvedeny na místním počítači nebo ve službě Active Directory.
Server	Server, ke kterému uživatel nebo skupina patří.

Přidání uživatelů nebo skupin

Uživatelé a skupiny Microsoft Windows® a Active Directory mohou přistupovat do systému AXIS Camera Station S2108 Appliance. Pokud chcete přidat uživatele do systému AXIS Camera Station S2108 Appliance, musíte přidat uživatele nebo skupinu v systému Windows®.

Přidání uživatele v systému Windows® 10 a 11:

- Stiskněte klávesy Windows + X a vyberte **Computer Management** (Správa počítače).
- V okně **Computer Management** (Správa) počítače přejděte na **Local Users and Groups > Users** (Místní uživatelé a skupiny > Uživatelé).
- Klikněte pravým tlačítkem na **Users** (Uživatelé) a vyberte možnost **New User** (Nový uživatel).
- Ve vyskakovacím okně zadejte údaje nového uživatele a zrušte zaškrtnutí políčka **User must change password at next login** (Uživatel musí při příštím přihlášení změnit heslo).
- Klikněte na možnost **Create** (Vytvořit).

Pokud používáte doménu Active Directory, obraťte se na správce sítě.

Přidání uživatelů nebo skupin

1. Přejděte do nabídky **Configuration > Security > User permissions** (Nastavení > Zabezpečení > Uživatelská oprávnění).

2. Klikněte na **Přidat**. V seznamu se zobrazí dostupní uživatelé a skupiny.
3. V části **Scope (Prostor)** vyberte, kde chcete vyhledávat uživatele a skupiny.
4. V části **Show (Zobrazit)** vyberte, zda chcete zobrazit uživatele nebo skupiny. Výsledky vyhledávání se nemusí zobrazit, pokud je počet uživatelů nebo skupin příliš vysoký. Pomocí filtru můžete výsledky zúžit.
5. Zvolte uživatele nebo skupiny a klikněte na **Přidat**.

Prostor	
Server	Vyberte, chcete-li vyhledat uživatele nebo skupiny v místním počítači.
Doména	Vyberte, zda chcete vyhledat uživatele nebo skupiny služby Active Directory.
Zvolený server	Pokud jste připojeni k více serverům AXIS Camera Station S2108 Appliance, vyberte server, na kterém chcete vyhledávat uživatele nebo skupiny.

Nastavení uživatele nebo skupiny

1. V seznamu vyberte uživatele nebo skupinu.
2. V části **Role** zvolte možnost **Administrator (Správce)**, **Operator (Operátor)** nebo **Viewer (Prohlížeč)**.
3. Pokud jste zvolili možnost **Operator (Operátor)** nebo **Viewer (Prohlížeč)**, můžete nakonfigurovat oprávnění uživatele nebo skupiny. Viz část *Oprávnění uživatele nebo skupiny*.
4. Klikněte na **Save (Uložit)**.

Odebrání uživatele nebo skupiny

1. Vyberte uživatele nebo skupinu.
2. Klepněte na **Remove (Odstranit)**.
3. Kliknutím na možnost **OK** ve vyskakovacím okně uživatele nebo skupinu odstraníte.

Oprávnění uživatele nebo skupiny

Uživatelé nebo skupině můžete přiřadit tři role. Informace o tom, jak definovat roli pro uživatele nebo skupinu, naleznete v části *Přidání uživatelů nebo skupin*.

Správce – Plný přístup k celému systému, včetně přístupu k živým a nahraným videím všech kamer, všem vstupním/výstupním portům a pohledům. Tato role je nutná pro přístup ke nastavení systému.

Operátor – Výběrem kamer, zobrazení a portů vstupů/výstupů získáte přístup k živému vysílání a videozáznamům. Obsluha má plný přístup ke všem funkcím systému AXIS Camera Station S2108 Appliance s výjimkou konfigurace systému.

Divák – Přístup k živým videím vybraných kamer, vstupním/výstupním portům a pohledům. Pozorovatel nemá přístup k nahraným videím nebo ke konfiguraci systému.

Kamery

Pro uživatele s rolí **Operátor (Operátor)** nebo **Pozorovatel (Viewer)** jsou k dispozici následující oprávnění přístupu.

Přístup	Povolit přístup ke kameře a všem funkcím kamery.
Video	Povolit přístup k živému videu z kamery.
Poslech zvuku	Povolit přístup k poslechu zvuku z kamery.
Reproduktory	Povolte přístup k hovoru prostřednictvím kamery.

Manuální nahrávání	Povolit manuální spouštění a zastavování záznamů.
Mechanický systém PTZ	Povolit přístup k mechanickému ovládání PTZ. K dispozici pouze pro kamery s mechanickým ovládáním PTZ.
Priorita PTZ	Nastavte prioritu PTZ. Nižší hodnota znamená vyšší prioritu. Není nastavena žádná přidělená priorita pro 0. Správce má nejvyšší prioritu. Bude-li kameru PTZ ovládat uživatel v roli s vyšší prioritou, nemohou ve výchozím nastavení ostatní uživatelé ovládat příslušnou kameru po dobu 10 sekund. K dispozici pouze pro kamery s mechanickým PTZ, které mají vybranou možnost Mechanical PTZ (Mechanický systém PTZ).

Pohledy

Pro uživatele s rolí **Operátor (Operátor)** nebo **Pozorovatel (Viewer)** jsou k dispozici následující oprávnění přístupu. Můžete vybrat více pohledů a nastavit přístupová privilegia.

Přístup	Umožňuje povolit přístup k pohledům v systému AXIS Camera Station S2108 Appliance.
Upravit	Umožňuje úpravy záběrů v AXIS Camera Station S2108 Appliance.

I/O

Pro uživatele s rolí **Operátor (Operátor)** nebo **Pozorovatel (Viewer)** jsou k dispozici následující oprávnění přístupu.

Přístup	Povolit plný přístup ke vstupnímu/výstupnímu portu.
Číst	Umožňuje zobrazit stav V/V portu, aniž by došlo k jeho změně.
Zápis	Umožňuje změnit stav V/V portu.

Systém

V seznamu nelze nastavit šedě označená přístupová práva. Zaškrtnutí znamená, že uživatel nebo skupina má toto oprávnění ve výchozím nastavení.

Pro uživatele nebo skupiny s rolí **Operator (Operátor)** jsou k dispozici následující oprávnění přístupu. **Take snapshots (Pořídit snímek)** je také dostupný pro roli **Pozorovatel (Viewer)**.

Pořídit snímky	Umožňuje pořizovat snímky v režimu živého zobrazení i v režimu záznamu.
Exportovat záznamy	Povolit export záznamů.
Vytvořit zprávu o incidentech	Umožnit generování sestav incidentů.
Zabránit v přístupu k záznamům starším než	Zabránění v přístupu k záznamům starším než stanovený počet minut. Uživatelé tyto záznamy při vyhledávání nenajdou.

Poplachy, úkoly a protokoly přístupu:	Získávání upozornění na poplachy a umožnění přístupu na lištu Alarms and tasks (Poplachy a úlohy) a záložku Logs (Záznamy) .
Vyhledávání dat o přístupu	Umožňuje vyhledávat data za účelem sledování toho, co se stalo v době události.
Přidat kategorie k událostem	Povolte přidávání kategorií k událostem na kartě Recordings (Záznamy) .
Odebrat kategorie z události	Povolte odebrání kategorií z událostí na kartě Recordings (Záznamy) .

Kontrola přístupu

Pro uživatele nebo skupiny s rolí **Operator (Operátor)** jsou k dispozici následující oprávnění přístupu. **Access Management (Řízení přístupu)** je také dostupný pro roli **Pozorovatel (Viewer)**.

Konfigurace řízení přístupu	Umožnění konfigurace dveří a zón, profilů identifikace, formátů karet a kódů PIN, šifrované komunikace a více serverů.
Správa přístupu	Povolení správy přístupu a přístup k nastavení služby Active Directory.

Pro uživatele s rolí **Pozorovatel** jsou k dispozici následující oprávnění přístupu.

Sledování stavu systému

Pro uživatele nebo skupiny s rolí **Operator (Operátor)** jsou k dispozici následující oprávnění přístupu. **Access to system health monitoring (Přístup ke sledování stavu systému)** je také dostupný pro roli **Pozorovatel (Viewer)**.

Konfigurace sledování stavu systému	Umožňuje konfiguraci sledování stavu systému.
Přístup ke sledování stavu systému:	Umožňuje přístup ke sledování stavu systému.

Správa zařízení

Aktualizace certifikátů funkce Secure Boot

Společnost Microsoft v červnu 2026 ukončí platnost certifikátů funkce Secure Boot z roku 2011 a nahradí je novými certifikáty z roku 2023. Aby byl váš rekordér v bezpečí, proveďte instalaci certifikátů z roku 2023 ještě před tímto datem.

Instalaci certifikátů z roku 2023 vyžaduje systém Windows 10 LTSC (Long-Term Servicing Channel) nebo Windows 11 LTSC. Pokud je vaše zařízení v záruční lhůtě, ale místo verze LTSC na něm běží systém Windows 10 SAC (Semi-Annual Channel), obraťte se na technickou podporu společnosti Axis. Mohou vám sdělit, zda je možné provést upgrade na verzi LTSC ještě před aktualizací systému BIOS nebo změnou jakýchkoli certifikátů.

Poznámka

Po červnu 2026 budou zařízení bez certifikátů z roku 2023 fungovat jako dosud, nebudou však dostávat nové bezpečnostní aktualizace pro počáteční fázi spouštění systému, včetně aktualizací nástroje Windows Boot Manager a seznamů odvolaných certifikátů souvisejících s novými slabými místy.

Zkontrolujte stav svého certifikátu

Chcete-li ověřit, zda je instalována verze certifikátů pro rok 2023 a zda byl aktualizován zavaděč systému Windows, použijte jeden z následujících postupů:

Metoda 1:

1. Otevřete Editor registru.
2. Přejděte na HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing.
3. Zkontrolujte hodnotu UEFICA2023Status. Pokud hodnota uvádí **Updated** (Aktualizováno), je provedena instalace certifikátu z roku 2023.

 (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. Otevřete nastavení Windows Security (Zabezpečení systému Windows).
2. Přejděte na možnost Device security (Zabezpečení zařízení).
3. V části Secure boot (Zabezpečené spouštění) zkontrolujte stavovou zprávu. Je-li certifikát aktuální, na kartě se zobrazí: „Secure Boot is on and all required certificate updates have been applied. (Funkce Secure Boot je zapnutá a byly provedeny všechny požadované aktualizace certifikátu.) No further certificate changes are needed. (Žádné další změny certifikátu nejsou nutné.)“



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

Poznámka

Aplikace Zabezpečení systému Windows zobrazuje stav certifikátu pouze v případě, že máte na zařízení dokončenou instalaci kumulativní aktualizace ze dne 14. dubna 2026 nebo novější. Pokud se nezobrazí

zpráva o stavu certifikátu, proveďte instalaci nejnovější aktualizace systému Windows nebo místo toho použijte metodu 1.

Doporučené akce

Aktualizace systému BIOS trvale uloží certifikáty z roku 2023 do firmwaru. Toto je nejspolehlivější způsob a doporučujeme jej i v případě, že jste si certifikáty již instalovali prostřednictvím služby Windows Update.

Důležité

Pokud certifikáty nainstalujete pouze prostřednictvím služby Windows Update a poté resetujete klíče funkce Secure Boot v systému BIOS na výchozí nastavení, dojde ke ztrátě certifikátů a zařízení se při zapnutí funkce Secure Boot nespustí. Před resetováním klíčů funkce Secure Boot proveďte aktualizaci systému BIOS, aby se certifikáty staly trvalými.

Aktualizace certifikátu prostřednictvím systému BIOS

Pro instalaci použijte verzi systému BIOS uvedenou pro váš model nebo novější verzi. Tyto soubory si můžete stáhnout ze stránky produktu na webu Axis.com:

Model	Minimální verze systému BIOS
AXIS S2208	Bude upřesněno
AXIS S2212	Bude upřesněno
AXIS S2216	Bude upřesněno
AXIS S2224	Bude upřesněno
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

Aktualizace certifikátu prostřednictvím služby Windows Update

Pokud pro váš model zatím není k dispozici aktualizace systému BIOS, můžete si certifikáty pro rok 2023 stáhnout místo toho prostřednictvím služby Windows Update.

Důležité

Certifikáty nainstalované tímto způsobem se ukládají do aktuální databáze funkce Secure Boot, nikoli do firmwaru. Pokud resetujete klíče funkce Secure Boot v systému BIOS na výchozí nastavení, ztratíte certifikáty a zařízení se s aktivovanou funkcí Secure Boot nemusí spustit. Jakmile bude pro váš model k dispozici aktualizace systému BIOS, proveďte její instalaci, i když jste tuto metodu již použili.

Chcete-li tuto cestu použít:

1. Ujistěte se, že na vašem zařízení běží systém Windows 10 LTSC nebo Windows 11 LTSC.
2. Nainstalujte všechny aktualizace systému Windows vydané 14. dubna 2026 nebo později.
3. Přejděte na nastavení **Windows Security > Device security > Secure Boot** (Zabezpečení systému Windows > Zabezpečení zařízení > Zabezpečené spouštění), kde si můžete zkontrolovat stav svého certifikátu.
4. Pokud se certifikát po instalaci nejnovějších aktualizací neaktualizuje, zkontrolujte hodnotu registru **UEFICA2023Status**. Pokud vaše zařízení stále nesplňuje podmínky pro automatickou aktualizaci, aktualizujte systém BIOS nebo se obraťte na technickou podporu společnosti Axis.

Důležité

Nerevokujte manuálně certifikát z roku 2011, dokud se neujistíte, že všechna média obnovení, spouštěcí prostředí a ovladače ve vašem prostředí jsou podepsány certifikátem z roku 2023. Pokud certifikát z roku 2011 revokujete příliš brzy, zařízení se při zapnutí funkce Secure Boot nebude moci spustit.

Kontrola aktuální verze systému BIOS

Kontrola aktuálního systému BIOS:

1. Zapněte zařízení a opakovaně tiskněte klávesu **DEL**, dokud se nezobrazí logo Axis.
2. Číslo verze je uvedeno jako první položka v části **Main** (Hlavní).

Aktualizujte systém BIOS

Postupujte podle pokynů uvedených v příručce k systému BIOS, která je k dispozici na stránce pro stažení souboru systému BIOS.

Aktualizace systému Windows®

Systém Windows® pravidelně kontroluje dostupné aktualizace. Pokud je k dispozici aktualizace, zařízení ji automaticky stáhne, ale musíte ji nainstalovat ručně.

Poznámka

Během plánovaného restartování systému bude přerušeno nahrávání.

Postup ručního vyhledání aktualizací:

1. Přejděte do nabídky **Settings > Windows Update** (Nastavení > Windows Update).
2. Klikněte na možnost **Check for updates** (Zkontrolovat aktualizace).

Úprava nastavení aktualizací systému Windows®

Je možné změnit, jak a kdy systém Windows® bude provádět aktualizace, aby to vyhovovalo vašim potřebám.

Poznámka

Během plánovaného restartování systému se všechny probíhající záznamy zastaví.

1. Otevřete aplikaci **Run** (Spustit).
 - Přejděte do části **Windows System > Run** (Systém Windows > Spustit), nebo
2. Zadejte `gpedit.msc` a klikněte na **OK**. Otevře se Editor místních zásad skupiny.
3. Přejděte do sekce **Computer Configuration > Administrative Templates > Windows Components > Windows Update** (Konfigurace počítače > Administrativní šablony > Součásti Windows > Aktualizace Windows).
4. Proveďte požadované nastavení, viz příklad.

Příklad:

Chcete-li automaticky stahovat a instalovat aktualizace bez zásahu uživatele a v případě nutnosti restartovat zařízení mimo pracovní dobu, použijte následující konfiguraci:

1. Otevřete možnost **Always automatically restart at the scheduled time** (Vždy automaticky restartovat v naplánovanou dobu) a vyberte:
 - 1.1. **Povoleno**
 - 1.2. **The restart timer will give users this much time to save their work (minutes)** (Časovač pro restartování poskytne uživatelům následující množství času k uložení jejich práce (minuty)): 15.
 - 1.3. Klikněte na tlačítko **OK**.
2. Otevřete možnost **Configure Automatic Updates** (Konfigurovat automatické aktualizace) a vyberte:
 - 2.1. **Povoleno**

- 2.2. **Configure Automatic updates** (Konfigurovat automatické aktualizace): Automatické stažení a naplánování instalace
- 2.3. **Schedule Install day** (Naplánovat den instalace): Každou neděli
- 2.4. **Schedule Install time** (Naplánovat čas instalace): 00:00
- 2.5. Klikněte na tlačítko **OK**.
3. Otevřete možnost **Allow Automatic Updates immediate installation** (Povolit okamžitou instalaci automatických aktualizací) a vyberte:
 - 3.1. **Povoleno**
 - 3.2. Klikněte na tlačítko **OK**.

Správa napájení

Přepínač má celkové vyhrazené napájení 105 W. Toto je maximální výstupní výkon všech připojených zařízení.

Ve většině případů spotřebovávají připojená zařízení méně energie, než je požadováno. Pro optimalizaci spotřeby energie umožňuje řadič PoE připojeným zařízením požadovat až 125 W a současně omezuje skutečnou spotřebu energie na 105 W.

Přepínač může například napájet 8 zařízení PoE třídy 3.

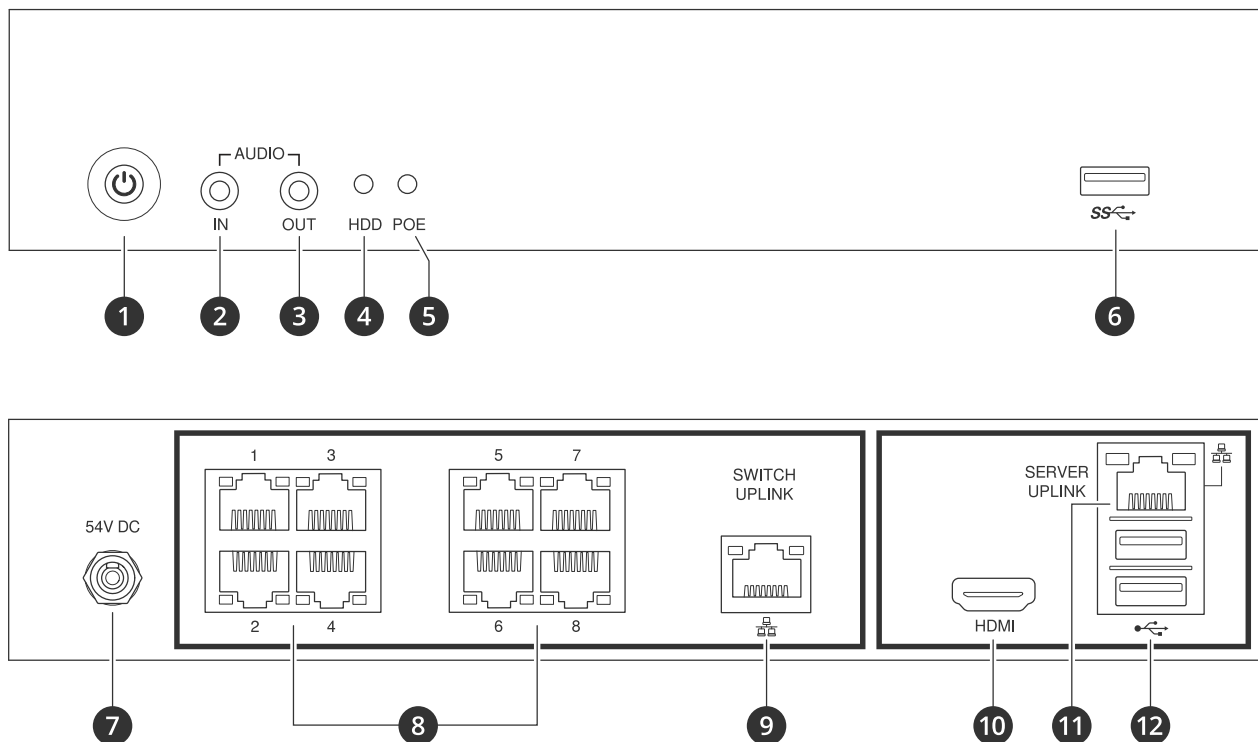
- 1 zařízení PoE třídy 3 vyžaduje výkon 15,4 W.
- 8 zařízení PoE třídy 3 vyžaduje výkon $(8 \times 15,4) = 123,2$ W. To je v rámci limitu 125 W povoleného řadičem PoE.
- 1 zařízení PoE třídy 3 obvykle spotřebovává 10 až 12 W.
- 8 zařízení PoE třídy 3 obvykle spotřebovává 80 až 96 W. To je v rámci limitu 105 W celkového vyhrazeného napájení.

▲ VAROVÁNÍ

- Když připojená zařízení požadují výkon vyšší než 125 W:
 - Poslední připojené zařízení se nespustí.
 - LED dioda přetížení PoE bude svítit červeně, dokud neodpojíte poslední připojené zařízení nebo neuvolníte dostatečnou kapacitu PoE odebráním jiných zařízení.
- Když připojená zařízení skutečně spotřebovávají více než 105 W:
 - Poslední zapnuté zařízení se vypne a pokusí se o restart.
 - LED dioda přetížení PoE se nezapne.

Přehled produktů

Přední a zadní strana



- 1 Tlačítko napájení / LED dioda napájení
- 2 Zvukový vstup
- 3 Zvukový výstup
- 4 LED dioda aktivity pevného disku
- 5 Stavové LED diody portů PoE
- 6 Port USB 3.0
- 7 Konektor napájení
- 8 Porty PoE
- 9 Port odchozího připojení přepínače RJ45
- 10 HDMI port
- 11 Port odchozího připojení serveru RJ45
- 12 USB 2.0 porty

Specifikace

Přední LED

LED indikátor	Barva	Indikace
Napájení	Zelená	Server zapnutý
Pevný disk	Bliká žlutě	Aktivita pevného disku
	Bliká červeně	Možné selhání pevného disku
Přetížení PoE	Červená	Překročena kapacita PoE
	Vypnuto	OK

Zadní LED

Rychlost a aktivita sítě	Barva	Indikace
Pravá LED	Žlutá	10/100 Mbit/s
	Zelená ¹	1000 Mbit/s
Levá LED	Bliká zeleně	Síťová aktivita

1. Toto platí pouze pro odchozí připojení přepínače a odchozí připojení serveru.

Odstraňování potíží

Obnovení systému

Pokud by u zařízení došlo k úplnému selhání systému, musíte znovu vytvořit systém Windows® pomocí bitové kopie pro obnovení. Chcete-li stáhnout sadu AXIS pro obnovení síťového videorekordéru, kontaktujte technickou podporu společnosti AXIS a sdělte jí výrobní číslo svého zařízení.

Poznámka

Sada AXIS Network Video Recorder Recovery Kit se dodává ve dvou variantách:

- **sb11** – pro zařízení, která stále používají certifikát z roku 2011.
- **sb23** – pro zařízení, která přešla na certifikát z roku 2023.

Než si stáhnete sadu pro obnovení, zkontrolujte stav svého certifikátu a vyberte odpovídající variantu. Pokud vyberete nesprávnou variantu, instalace nevytvoří spustitelný výsledek a budete muset začít znovu se správným obrazem. Tím se vaše zařízení nepoškodí.

Pokud máte ve svém zařízení již nainstalovaný certifikát z roku 2023, lze variantu sb11 nadále bezpečně používat, pokud nebyl certifikát z roku 2011 manuálně zrušen. Jakmile bude revokován, bude fungovat pouze sb23.

Opětovné vytvoření systému:

1. Stáhněte si sadu AXIS pro obnovení síťového videorekordéru a nástroj AXIS ISO to USB pro obnovení síťového videorekordéru.
2. Vložte do svého počítače USB disk.
 - Použijte disk USB s minimálně 16 GB.
 - USB disk bude zformátován a všechna existující data na něm budou vymazána.
3. Spustěte nástroj AXIS ISO to USB pro obnovení síťového videorekordéru a postupujte podle pokynů na obrazovce.
Zápis dat na USB disk trvá přibližně 10 až 15 min. USB disk neodstraňujte, dokud nebude proces dokončen.
4. Až nástroj AXIS ISO to USB pro obnovení síťového videorekordéru zápis dokončí, vytáhněte disk USB a zapojte ho do zařízení.
5. Spustěte zařízení.
6. Jakmile se zobrazí úvodní obrazovka Axis, stiskněte klávesu F12.
7. Klikněte na **UEFI: USB Drive** (UEFI: Jednotka USB).
8. Přejděte ke svému USB disku a stiskněte klávesu Enter. Systém se spustí do sady AXIS pro obnovení síťového videorekordéru.
9. Klikněte na možnost **Reinstall Operating System (Přinstalovat operační systém)**.
Obnovení trvá zhruba 10 až 15 minut. Ve stažených souborech sady pro obnovení naleznete podrobné pokyny.

Řešení problémů se systémem AXIS Camera Station

Informace o tom, jak řešit potíže se systémem AXIS Camera Station, naleznete v *návodu pro uživatele systému AXIS Camera Station*.

Potřebujete další pomoc?

Užitečné odkazy

- *Návod pro uživatele systému AXIS Camera Station*
- *Přihlásit se k zabezpečenému vzdálenému přístupu AXIS*
- *Co zahrnout do seznamu výjimek antivirových programů pro systém AXIS Camera Station*

Kontaktovat podporu

Pokud potřebujete další pomoc, přejděte na axis.com/support.

T10181903_cs

2026-07 (M7.2)

© 2022 – 2026 Axis Communications AB