AXIS Camera Station Pro Secure Entry

Uživatelská příručka

Informace o

Secure Entry je součástí systému AXIS Camera Station Pro. Použijte jej k přidávání zařízení a správě rozvrhů. Pro více informací si přečtěte *návod pro uživatele softwaru AXIS Camera Station Pro*.

Konfigurace řízení přístupu

Pokud jste do systému přidali síťový ovladač dveří Axis, můžete v systému AXIS Camera Station verze 6.x nebo novější hardware řízení přístupu nakonfigurovat.

Úplný pracovní postup pro nastavení síťového ovladače dveří Axis v systému AXIS Camera Station Pro Secure Entry naleznete v článku *Nastavení síťového ovladače dveří Axis*.

Poznámka

Než začnete, proveďte následující úkony:

- Upgradujte verzi systému AXIS OS ovladače v rámci nabídky **Configuration > Devices > Management** (Nastavení > Zařízení > Správa).
- Nastavte datum a čas ovladače v části **Configuration > Devices > Management (Konfigurace > Zařízení > Správa)**.
- Zapněte protokol HTTPS na ovladači v části **Configuration > Devices > Management** (Konfigurace > Zařízení > Správa).

Pracovní postup pro konfiguraci řízení přístupu

1. Chcete-li upravit předdefinované identifikační profily nebo vytvořit nový identifikační profil, přečtěte si *Identifikační profily, on page 22*.
2. Chcete-li použít vlastní nastavení pro formáty karet a délku kódu PIN, přečtěte si *Formáty karet a kód PIN, on page 24*.
3. Přidejte dveře a aplikujte na ně identifikační profil. Viz část *Přidání dveří, on page 7*.
4. Nakonfigurujte dané dveře.
   - *Přidání monitoru dveří, on page 13*
   - *Přidat nouzový vstup, on page 15*
   - *Přidání čtečky, on page 16*
   - *Přidání zařízení REX, on page 19*
5. Přidejte zónu a přidejte dveře do této zóny. Viz část *Přidání zóny, on page 19*.

Kompatibilita softwaru zařízení pro ovladače dveří

Důležité

Při upgradu systému AXIS OS na ovladači dveří mějte na paměti následující informace:

- **Podporované verze operačního systému AXIS OS:** Níže uvedené podporované verze systému AXIS OS platí pouze při upgradu z jejich původní doporučené verze AXIS Camera Station Pro a pokud má systém dveře. Pokud systém tyto podmínky nesplňuje, je nutné provést upgrade na verzi operačního systému AXIS OS doporučenou pro konkrétní verzi AXIS Camera Station Pro.
- **Minimální podporovaná verze systému AXIS OS:** Nejstarší nainstalovaná verze operačního systému AXIS OS v systému určuje minimální podporovanou verzi systému AXIS OS, s omezením na dvě předchozí verze. Předpokládejme, že používáte AXIS Camera Station Pro verze 6.5 a upgradujete všechna zařízení na doporučenou verzi AXIS OS 12.0.86.2. Pak se verze AXIS OS 12.0.86.2 stane minimální podporovanou verzí pro váš systém pro další použití.
- **Upgradování nad rámec doporučené verze systému AXIS OS:** Předpokládejme, že provedete upgrade na verzi operačního systému AXIS OS vyšší než je doporučená verze pro konkrétní verzi AXIS Camera Station Pro. Pak můžete vždy bez problémů downgradovat zpět na doporučenou verzi operačního systému AXIS OS, pokud se vejde do limitů podpory nastavených pro verzi AXIS Camera Station Pro.
- **Budoucí doporučení pro operační systém AXIS OS:** Pro zajištění stability systému a plné kompatibility se vždy řiďte doporučenou verzí operačního systému AXIS OS pro příslušnou verzi AXIS Camera Station Pro.
- **Sledování změn:** Přechod mezi verzemi firmwaru 10.12.xx a 11.0.xx nebo vyššími vyžaduje obnovení na výchozí nastavení.

Níže uvedená tabulka uvádí minimální a doporučenou verzi operačního systému AXIS OS pro jednotlivé verze AXIS Camera Station Pro:

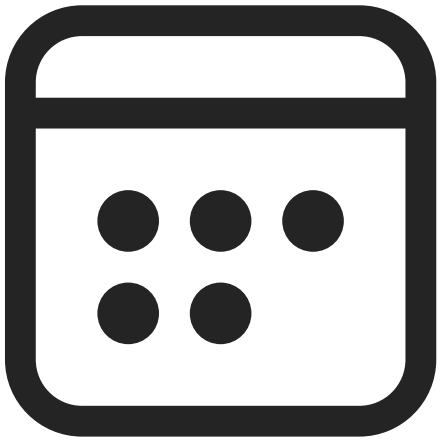
Verze AXIS Camera Station	Minimální verze operačního systému AXIS OS	Doporučená verze operačního systému AXIS OS
Pro 6.15	12.5.68.1	12.8.55.1
Pro 6.14	12.5.68.1	12.8.55.1
Pro 6.13	12.5.68.1	12.6.102.1

Níže uvedená tabulka uvádí minimální a doporučenou verzi operačního systému AXIS OS pro jednotlivé verze AXIS Camera Station 5:

Verze AXIS Camera Station	Doporučená verze operačního systému AXIS OS
5.59	12.4.68.1
5.58	12.4.68.1
5.57	11.8.20.2

Dveře a zóny

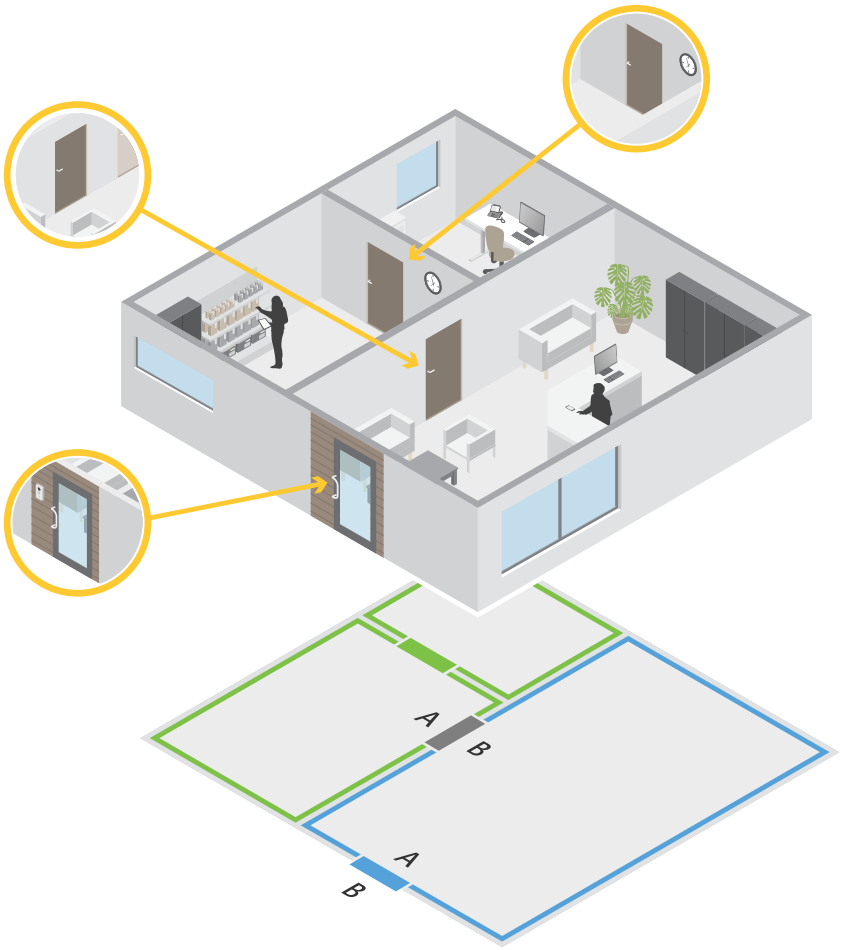
Chcete-li zobrazit přehled a konfigurovat dveře a zóny, přejděte do části **Configuration > Access control > Doors and zones** (Konfigurace > Řízení přístupu > Dveře a zóny).

 **Manuální akce**	Manuálně nastavte stav dveří. Vyberte si z následujících možností: **Reset** (Resetovat) (dodržovat systémová pravidla), **Grant access** (Udělit přístup) (odemknout dveře na 7 sekund), **Unlock** (Odemknout) (nechat dveře odemčené), **Lock** (Zamknout) (nechat dveře zamčené) nebo **Lockdown** (Uzamknout) (nikdo nesmí dovnitř ani ven).
 **Odemknout rozvrhy**	Nastavte rozvrh pro automatické odemykání dveří v určitých časech. V ostatních případech zůstávají dveře zamčené. Chcete-li nastavit, aby první osoba musela dveře odemknout manuálně před spuštěním rozvrhu, zapněte funkci **First person in** (První vstupující osoba).
Identifikační profil	Změňte identifikační profil na dveřích.
Připnout graf	Zobrazení pinového schématu ovladače přidruženého ke dveřím. Chcete-li pinové schéma vytisknout, klikněte na tlačítko **Print** (Tisk).
Zabezpečený kanál	Zapnutí nebo vypnutí zabezpečeného kanálu OSDP pro konkrétní čtečku.

Dveře	
Jméno	Název dveří.
Typ	Typ nastavení dveří.
Zařízení	Zařízení připojené ke dveřím.

IP adresa	IP adresa ovladače dveří připojeného ke dveřím.
Strana A	Zóna, ve které je strana A dveří.
Strana B	Zóna, ve které je strana B dveří.
Identifikační profil	Identifikační profil použitý na dveře.
Baterie	Stav baterie ovladače dveří.
Stav	Stav dveří. • **Online:** Dveře jsou online a pracují správně. • **Čtečka je offline:** Čtečka v konfiguraci dveří je offline. • **Chyba čtečky:** Čtečka v konfiguraci dveří nepodporuje zabezpečený kanál nebo zabezpečený kanál je pro čtečku vypnutý. • **Starý firmware:** Zařízení používá zastaralou verzi firmwaru. Aktualizujte firmware, abyste zajistili optimální výkon a bezpečnost.
Zóny	
Jméno	Název zóny.
Počet dveří	Počet dveří zahrnutých v zóně.
Úroveň zabezpečení	Úroveň zabezpečení použitá pro danou zónu.

Příklad dveří a zón



- Existují dvě zóny: zelená a modrá.
- Jsou zde troje dveře: zelené, modré a hnědé.
- Zelené dveře jsou vnitřní dveře v zelené zóně.
- Modré dveře jsou dveře v perimetru pouze pro modrou zónu.
- Hnědé dveře jsou dveře v perimetru pro zelenou i modrou zónu.

Přidání dveří

Poznámka

- Ovladač dveří můžete nakonfigurovat s jedněmi dveřmi se dvěma zámky nebo se dvěma dveřmi s jedním zámkem na každých dveřích. Multiovladače podporují další nastavení zámků.
- Pokud ovladač dveří nemá žádné dveře a používáte novou verzi systému AXIS Camera Station Pro Secure Entry se starším firmwarem ovladače dveří, systém vám neumožní přidat dveře. Systém však umožní instalaci nových dveří na systémových ovladačích se starším firmwarem, pokud již nějaké dveře existují.

Chcete-li přidat dveře, vytvořte novou konfiguraci dveří:

1. Přejděte do části **Configuration > Access control > Doors and zones** (Konfigurace > Řízení přístupu > Dveře a zóny).
2. Klikněte na + **Add door** (Přidat dveře) a vyberte typ dveří z rozevíracího seznamu.

Typy dveří	
Dveře	Běžné dveře s monitorem, které podporují zámky a čtečky. Vyžaduje ovladač dveří.
Bezdrátové dveře	Dveře, které můžete nastavit pomocí bezdrátových zámků a komunikačních rozbočovačů ASSA ABLOY Aperio®. Další informace naleznete v části *Přidejte bezdrátový zámek, on page 12*.
Monitorování dveří	Dveře, které mohou signalizovat, zda jsou otevřené nebo zavřené. Další informace naleznete v části *Přidání monitorovacích dveří, on page 14*.
Vybavené dveře	Dveře, které můžete přidat do systému jako zástupný symbol, aniž byste museli vybírat příslušný hardware.
Podlaží	Typ dveří pro ovládání výtahu, který ověřuje přístup na podlaží výtahu pomocí čteček karet. Další informace naleznete v části *Přidání podlaží pro ovládání výtahu BETA, on page 15*.

3. Zadejte název dveří a v rozbalovacím menu **Device** (Zařízení) vyberte ovladač dveří, který chcete s dveřmi spojit. Ovladač se zobrazí šedě, když nelze přidat další dveře, když je v režimu offline nebo když není aktivní protokol HTTPS.
4. Klepnutím na tlačítko **Next (Další)** přejděte na stránku konfigurace dveří.
5. V rozbalovacím menu **Primary lock** (Primární zámek) přidejte přenosový port.
6. Chcete-li na dveřích nakonfigurovat dva zámky, vyberte přenosový port z rozbalovacího menu **Secondary lock** (Sekundární zámek).
7. Vyberte identifikační profil. Viz část *Identifikační profily, on page 22*.
8. Nakonfigurujte nastavení dveří. Viz *Nastavení dveří, on page 9*.
9. *Přidání monitoru dveří, on page 13*
10. *Přidat nouzový vstup, on page 15*
11. *Přidání čtečky, on page 16*
12. *Přidání zařízení REX, on page 19*
13. Nakonfigurujte úroveň zabezpečení. Viz část *Úroveň zabezpečení dveří, on page 10*.
14. Klikněte na **Save** (Uložit).

Kopírování konfigurace dveří:

1. Přejděte do části **Configuration > Access control > Doors and zones** (Konfigurace > Řízení přístupu > Dveře a zóny).
2. Klikněte na + **Add door** (Přidat dveře).
3. Zadejte název dveří a v rozbalovacím menu **Device** (Zařízení) vyberte ovladač dveří, který chcete s dveřmi spojit.
4. Klikněte na tlačítko **Další**.
5. V rozbalovacím menu **Copy configuration** (Kopírovat konfiguraci) vyberte existující konfiguraci dveří. Zobrazí se připojené dveře a ovladač se zobrazí šedě, pokud byl nakonfigurován se dvěma dveřmi nebo s jedněmi dveřmi se dvěma zámky.
6. Pokud chcete, můžete toto nastavení změnit.
7. Klikněte na **Save** (Uložit).

Odebrání dveří:

1. Přejděte do části **Configuration > Access control > Doors and zones > Doors (Konfigurace > Řízení přístupu > Dveře a zóny > Dveře)**.
2. V seznamu vyberte dveře.
3. Klikněte na tlačítko **Remove** (Odebrat) a poté potvrďte.

Přidání a konfigurace dveří a zón

Nastavení dveří

Úprava dveří:

1. Přejděte do části **Configuration > Access control > Door and Zones** (Konfigurace > Řízení přístupu > Dveře a zóny).
2. Vyberte dveře, které chcete upravit.
3. Klikněte na **Edit** (Upravit).
4. Změňte nastavení a klikněte na tlačítko **Save (Uložit)**.

Přístupový čas (s)	Nastavte počet sekund, po který mají dveře po udělení přístupu zůstat odemčené. Dveře zůstanou odemčené, dokud je někdo neotevře nebo dokud neuplyne nastavená doba. Dveře se zamknou při zavření bez ohledu na to, zda doba přístupu vypršela.
Open-too-long time (sec) (Doba příliš dlouhého otevření (s))	Platí pouze v případě, že jste nakonfigurovali monitor dveří. Nastavte počet sekund, po který zůstanou dveře otevřené. Pokud jsou dveře po uplynutí nastaveného času otevřené, spustí se poplach příliš dlouhého otevření. Nastavením pravidla akcí nakonfigurujte, kterou akci událost příliš dlouhého otevření spustí.
Dlouhá doba přístupu (s)	Nastavte počet sekund, po který mají dveře po udělení přístupu zůstat odemčené. Dlouhá doba přístupu bude mít u držitelů karet, u kterých je toto nastavení zapnuto, vyšší prioritu než nastavená doba přístupu.
Long open-too-long time (sec) (Dlouhá doba příliš dlouhého otevření (s))	Platí pouze v případě, že jste nakonfigurovali monitor dveří. Nastavte počet sekund, po který zůstanou dveře otevřené. Pokud jsou dveře po uplynutí nastaveného času otevřené, spustí se událost příliš dlouhého otevření. Dlouhá doba příliš dlouhého otevření bude mít u držitelů karet vyšší prioritu než již nastavená doba příliš dlouhého otevření, pokud je zapnuto nastavení **Long access time (Dlouhá doba přístupu)**.
Doba zpoždění opětovného zamčení (ms)	Nastavte čas (v milisekundách), po který zůstanou dveře po otevření nebo zavření odemčeny.

Znovu zamknout	• **After opening (Po otevření):** Platí pouze v případě, že jste přidali monitor dveří. • **After closing (Po zavření):** Platí pouze v případě, že jste přidali monitor dveří.
Dveře otevřeny násilím	Zvolte, zda má systém nastavit spouštěč systémového poplachu při násilném otevření dveří. Vyžaduje senzor polohy dveří (DPS).
Dveře otevřeny příliš dlouho	Zvolte, zda má systém nastavit spouštěč systémového poplachu při příliš dlouhém otevření dveří.

Manuální akce

U dveří a zón můžete provádět následující manuální akce:

Obnovit – Vrátí se ke konfigurovaným systémovým pravidlům.

Udělit přístup – Odemkne dveře nebo zónu na 7 sekund a poté je opět zamkne.

Odemknout – Dveře zůstanou odemčené, dokud je neresetujete.

Zámek – Dveře zůstávají zamčené, dokud systém nepovolí přístup držiteli karty.

Uzamčení – Nikdo se nedostane dovnitř ani ven, dokud neprovedete reset nebo odemčení.

Provedení manuální akce:

1. Přejděte do části **Configuration** > **Access control** > **Doors and zones** (Konfigurace > Řízení přístupu > Dveře a zóny).
2. Vyberte dveře nebo zónu, u kterých chcete provést manuální akci.
3. Klikněte na některou z manuálních akcí.

Úroveň zabezpečení dveří

Ke dveřím můžete přidat následující funkce zabezpečení:

Pravidlo dvou osob – Pravidlo dvou osob vyžaduje, aby pro získání přístupu použily platné přihlašovací údaje dvě osoby.

Dvojité protáhnutí – Dvojité protáhnutí umožňuje držiteli karty přepsat aktuální stav dveří. Mohou jím například zamknout nebo odemknout dveře mimo pravidelný rozvrh, čímž odpadá nutnost vstupu do systému za účelem odemknutí dveří. Dvojité protáhnutí nemá vliv na existující rozvrh. Pokud je například naplánováno, že se dveře uzamknou při zavírací době, a zaměstnanec odejde na polední přestávku, dveře se podle rozvrhu stále zamknou.

Úroveň zabezpečení můžete nakonfigurovat při přidávání nových dveří, nebo ji můžete nakonfigurovat pro existující dveře.

Chcete-li k existujícím dveřím přidat **Two-person rule** (Pravidlo dvou osob):

1. Přejděte do části **Configuration** > **Access control** > **Doors and zones** (Konfigurace > Řízení přístupu > Dveře a zóny).
2. Vyberte dveře, pro které chcete nakonfigurovat úroveň zabezpečení.
3. Klikněte na **Edit (Upravit)**.
4. Klikněte **Security level** (Úroveň zabezpečení).
5. Zapněte možnost **Two-person rule** (Pravidlo dvou osob).
6. Klikněte na **Použít**.

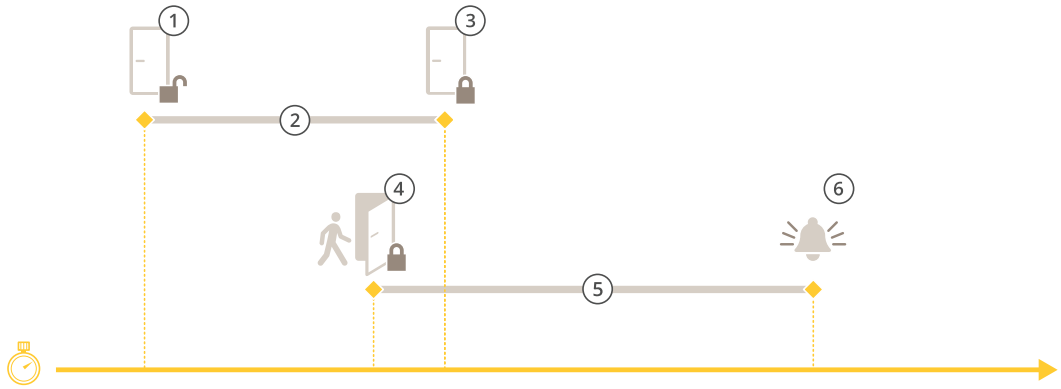
Pravidlo dvou osob	
Side A (Strana A) a **Side B (Strana B)**	Vyberte, na které strany dveří se má pravidlo použít.
Harmonogramy	Vyberte, kdy bude pravidlo aktivní.
Časový limit (v sekundách)	Časový limit je maximální povolená doba mezi jednotlivými úkony protáhnutí karty nebo jiných platných přihlašovacích údajů.

Chcete-li přidat **Double-swipe** (Dvojité protáhnutí) k existujícím dveřím:

1. Přejděte do části **Configuration** > **Access control** > **Doors and zones** (Konfigurace > Řízení přístupu > Dveře a zóny).
2. Vyberte dveře, pro které chcete nakonfigurovat úroveň zabezpečení.
3. Klikněte na **Edit (Upravit)**.
4. Klikněte **Security level** (Úroveň zabezpečení).
5. Zapněte možnost **Double-swipe** (Dvojité protáhnutí).
6. Klikněte na **Použít**.
7. Aplikujte na držitele karty **Double-swipe** (Dvojité protáhnutí).
   7.1. Otevřete kartu **Access Management** (Správa přístupu).
   7.2. Klikněte ⋮ na držitele karty, kterého chcete upravit, a klikněte na **Edit** (Upravit).
   7.3. Klikněte na **More** (Více).
   7.4. Vyberte možnost **Allow double-swipe** (Povolit dvojité protáhnutí).
   7.5. Klikněte na **Použít**.

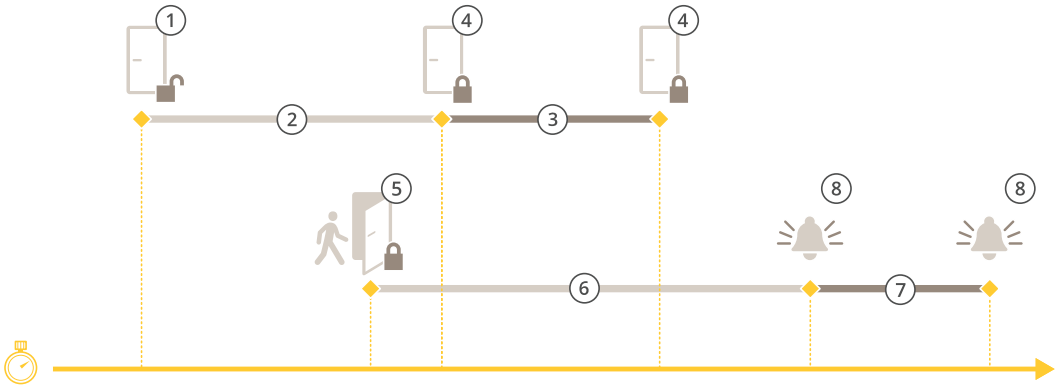
Dvojité protáhnutí	
Časový limit (v sekundách)	Časový limit je maximální povolená doba mezi jednotlivými úkony protáhnutí karty nebo jiných platných přihlašovacích údajů.

Časové možnosti



1 Přístup udělen – zámek se odemkne
2 Doba přístupu
3 Nebyla provedena žádná akce – zámek se zamkne
4 Byla provedena akce (otevření dveří) – zámek se zamkne nebo zůstane odemčený, dokud se dveře nezavřou

5 Doba příliš dlouhého otevření
6 Spustí se poplach příliš dlouhého otevření



1 Přístup udělen – zámek se odemkne
2 Doba přístupu
3 2+3: Dlouhá doba přístupu
4 Nebyla provedena žádná akce – zámek se zamkne
5 Byla provedena akce (otevření dveří) – zámek se zamkne nebo zůstane odemčený, dokud se dveře nezavřou
6 Doba příliš dlouhého otevření
7 6+7: Dlouhá doba příliš dlouhého otevření
8 Spustí se poplach příliš dlouhého otevření

Přidejte bezdrátový zámek

AXIS Camera Station Pro Secure Entry podporuje bezdrátové zámky a komunikační rozbočovače ASSA ABLOY Aperio®. Bezdrátový zámek se k systému připojuje prostřednictvím komunikačního rozbočovače Aperio připojeného ke konektoru RS485 ovladače dveří. K jednomu ovladači dveří můžete připojit až 16 bezdrátových zámků.

Chcete-li přehrát toto video, přejděte na webovou verzi tohoto dokumentu.

Poznámka

- Nastavení vyžaduje ovladač dveří Axis s operačním systémem AXIS OS verze 11.6.16.1 nebo novější.
- Nastavení vyžaduje platnou licenci na rozšíření ovladače dveří AXIS.
- Čas na ovladači dveří Axis musí být synchronizován s časem na serveru AXIS Camera Station Pro Secure Entry.
- Než začnete, spárujte zámky Aperio s rozbočovačem Aperio pomocí nástroje pro programování Aperio společnosti ASSA ABLOY.
- Na jeden konektor RS485 lze připojit pouze jeden komunikační hub Aperio. Funkce Multi-drop není podporována.
- Bezdrátové zámky nebudou v režimu offline dodržovat rozvrhy odemykání.

1. Přístup k ovladači dveří.
   1.1. Přejděte do nabídky **Nastavení > Zařízení > Další zařízení**.
   1.2. Otevřete webové rozhraní ovladače dveří připojeného ke komunikačnímu rozbočovači Aperio.

2. Zapněte Rozšíření ovladače dveří AXIS.
   2.1. Ve webovém rozhraní ovladače dveří přejděte na **Apps**.
   2.2. Zapněte kontextovou nabídku Rozšíření ovladače dveří AXIS .
   2.3. Klikněte na **Activate license (Přidat licenční klíč) klávesou** a zvolte licenční klíč.
   2.4. Zapněte **Rozšíření ovladače dveří AXIS**.
3. Připojte bezdrátový zámek k ovladači dveří pomocí komunikačního rozbočovače.
   3.1. Ve webovém interface ovladače dveří přejděte na **Access control > Wireless locks (Řízení přístupu > Bezdrátové zámky)**.
   3.2. Klikněte na **Connect communication hub (Připojit komunikační rozbočovač)**.
   3.3. Zadejte název rozbočovače a klikněte na **Connect (Připojit)**.
   3.4. Klikněte na **Connect wireless lock (Připojte bezdrátový zámek)**.
   3.5. Vyberte adresu zámku a možnosti zámku, který chcete přidat, a klikněte na **Save (Uložit)**.
4. Přidejte a nakonfigurujte dveře s bezdrátovým zámkem.
   4.1. V systému AXIS Camera Station Pro Secure Entry přejděte do části **Configuration > Access control > Doors and zones** (Konfigurace > Řízení přístupu > Dveře a zóny).
   4.2. Klikněte na **Add door** (Přidat dveře).
   4.3. Zvolte ovladač dveří připojený ke komunikačnímu rozbočovači Aperio, zvolte **Wireless door** (Bezdrátové dveře) jako **Door type** (Typ dveří).
   4.4. Klikněte na tlačítko **Další**.
   4.5. Zvolte **Wireless lock (Bezdrátový zámek)**.
   4.6. Definujte strany dveří A a B a přidejte snímače. Další informace naleznete v kapitole *Dveře a zóny, on page 4*.
   4.7. Klikněte na **Save** (Uložit).

Po připojení bezdrátového zámku můžete v přehledu dveří sledovat stav a úroveň nabití baterie.

Úroveň nabití baterie	Akce
Dobré	Žádné
Nízká	Zámek funguje, jak má, ale měli byste baterii vyměnit dříve, než se její stav stane kritickým.
Kritický	Vyměňte baterii Zámek nemusí fungovat tak, jak má.

Stav zámku	Akce
Online	Žádné
Zaseknutí zámku	Vyřešte případné mechanické problémy se zámkem.

Přidání monitoru dveří

Monitor dveří je přepínač polohy dveří, který sleduje fyzický stav dveří. Monitor dveří můžete přidat ke dveřím a nakonfigurovat způsob připojení monitoru dveří.

1. Přejděte na stránku konfigurace dveří. Viz část *Přidání dveří, on page 7*.
2. V části **Sensors** (Snímače) klikněte na **Add** (Přidat).
3. Vyberte možnost **Door monitor sensor** (Snímač monitoru dveří).

4. Zvolte V/V port, ke kterému chcete monitor dveří připojit.
5. V části **Door open if (Dveře otevřené, pokud)** vyberte způsob připojení okruhů monitoru dveří.
6. Pro ignorování změn stavu digitálního vstupu před přechodem do nového stabilního stavu nastavte **Debounce time (Čas vrácení)**.
7. Chcete-li spustit událost, jakmile dojde k přerušení spojení mezi ovladačem dveří a monitorem dveří, zapněte možnost **Supervised input** (Hlídaný vstup). Viz část *Hlídané vstupy, on page 21*.

Dveře otevřené, pokud	
Okruh je otevřený	Zvolte, jestliže je okruh monitoru dveří normálně zavřen. Monitor dveří odešle dveřím signál otevření, když je okruh otevřen. Monitor dveří odešle dveřím signál zavření, když je okruh uzavřen.
Okruh je uzavřený	Zvolte, jestliže je okruh monitoru dveří normálně otevřen. Monitor dveří odešle dveřím signál otevření, když je okruh zavřen. Monitor dveří odešle dveřím signál zavření, když je okruh otevřen.

Přidání monitorovacích dveří

Monitorovací dveře jsou typem dveří, který vám může ukázat, zda jsou otevřené nebo zavřené. Toto můžete využít například u protipožárních bezpečnostních dveří, které nevyžadují zámek, ale potřebujete u nich vědět, zda jsou otevřené.

Monitorovací dveře se liší od běžných dveří s monitorem dveří. Běžné dveře s monitorem dveří podporují zámky a čtečky, ale vyžadují ovladač dveří. Monitorovací dveře podporují jeden snímač polohy dveří, ale vyžadují pouze síťový V/V reléový modul připojený k ovladači dveří. K jednomu síťovému V/V reléovému modulu můžete připojit až pět snímačů polohy dveří.

Poznámka

Monitorovací dveře vyžadují reléový modul AXIS A9210 Network I/O Relay Module s nejnovějším firmwarem včetně aplikace AXIS Monitoring Door ACAP.

Nastavení monitorovacích dveří:

1. Nainstalujte AXIS A9210 a upgradujte jej na nejnovější verzi systému AXIS OS.
2. Namontujte snímače polohy dveří.
3. V kamerové stanici AXIS Camera Station Pro přejděte na **Configuration (Konfigurace)** > **Access control (Řízení přístupu)** > **Doors and zones (Dveře a zóny)**.
4. Klikněte na **Add door (Přidat dveře)**.
5. Zadejte jméno.
6. V části **Type (Typ)** vyberte možnost **Monitoring door (Monitorovací dveře)**.
7. V části **Device (Zařízení)** vyberte síťový V/V reléový modul.
8. Klikněte na tlačítko **Další**.
9. V části **Sensors (Snímače)** klikněte na tlačítko **+ Add (Přidat)** a vyberte položku **Door position sensor (Snímač polohy dveří)**.
10. Vyberte V/V, které je připojeno ke snímači polohy dveří.
11. Klikněte na **Přidat**.

Přidání podlaží pro ovládání výtahu BETA

Podlaží je typ dveří, který slouží k řízení přístupu k podlažím výtahu. Když přidáte podlaží, vytvoříte zdroj výtahu, který seskupuje všechna podlaží pro daný výtah. Každé podlaží používá čtečku karet uvnitř výtahové kabiny k ověření uživatelů před povolením přístupu na dané podlaží.

Než začneme, může být třeba:

- Podporovaný síťový ovladač dveří přidaný do vašeho systému, například *A1610*, *A1710-B* nebo *A1810-B*.
- *A9910 V/V Relay Expansion Module* pro další relé. Instrukce k přidání modulu do ovladače naleznete v části .

Poznámka

Tato funkce je ve fázi beta a v současné době pouze podporuje až 16 podlaží a čteček karet.

Nastavení podlaží:

1. Přejděte do části **Configuration > Access control > Doors and zones** (Konfigurace > Řízení přístupu > Dveře a zóny).
2. Klikněte na **Add** (Přidat) a vyberte možnost **Floor** BETA (Podlaží).
3. Zadejte název podlaží.
4. Vyberte svůj ovladač.
5. V rámci možnosti **Elevator** (Výtah) vyberte existující výtah a klikněte na **Create new elevator** (Vytvořit nový výtah), abyste přidali nový, a poté zadejte název.
6. V rámci možnosti **Side A** (Strana A) vyberte **Card reader** (Čtečka karet) a nakonfigurujte svou čtečku. Možnost **Side B** (Strana B) nelze z bezpečnostních důvodů nastavit.
7. Klikněte na **Save and add new** (Uložit a přidat nové), abyste přidali další podlaží ke stejnému výtahu. Nastavení výtahu a čtečky zůstává vyplněno pro další podlaží. Upozorňujeme, že tato možnost je k dispozici pouze v případě, že váš ovladač disponuje relé.
8. Po přidání podlaží klikněte na **Save** (Uložit). Podlaží se zobrazují podle konvence pojmenování „Název výtahu – Název podlaží“. Například: „Západní strana – Podlaží 1“

Poznámka

- Čtečky používané na více podlažích lze upravovat pouze na prvním podlaží, na kterém byly přidány.
- Výtahy se automaticky smažou, když se smažou všechna související podlaží.

Přidat nouzový vstup

Můžete přidat a nakonfigurovat nouzový vstup pro spuštění akce, která zamkne nebo odemkne dveře. Můžete také nakonfigurovat způsob připojení okruhu.

1. Přejděte na stránku konfigurace dveří. Viz část *Přidání dveří, on page 7*.
2. V části **Sensors** (Snímače) klikněte na **Add** (Přidat).
3. Vyberte možnost **Emergency input** (Nouzový vstup).
4. V části **Emergency state** (Nouzový stav) vyberte připojení okruhů.
5. Pro ignorování změn stavu digitálního vstupu před přechodem do nového stabilního stavu nastavte **Debounce time (ms) (Čas vrácení (ms))**.
6. Zvolte akci **Emergency action** (Nouzová akce), která se spustí, jakmile dveře přijmou signál nouzového stavu.

Nouzový stav	
Okruh je otevřený	Zvolte, jestliže je okruh nouzového vstupu normálně zavřen. Nouzový vstup odešle signál nouzového stavu v případě, že je okruh otevřen.
Okruh je uzavřený	Tuto možnost zvolte, jestliže je okruh nouzového vstupu normálně otevřen. Nouzový vstup odešle signál nouzového stavu v případě, že je okruh zavřen.

Nouzové opatření	
Odemknout dveře	Dveře se odemknou, jakmile obdrží signál nouzového stavu.
Zamknout dveře	Dveře se zamknou, jakmile obdrží signál nouzového stavu.

Přidat IP čtečku

Jako čtečku můžete použít síťový interkom Axis nebo jiné zařízení umožňující IP protokol. Než budete moci zařízení přiřadit ke dveřím, musíte jej přidat do aplikace AXIS Camera Station Pro.

Poznámka

Než začnete, ujistěte se, že je IP čtečka zapnutá a připojená ke stejné síti jako aplikace AXIS Camera Station Pro.

1. Přejděte do nabídky **Configuration > Devices > Add devices** (Nastavení > Zařízení > Přidat zařízení).
2. Vyberte svou IP čtečku ze seznamu nalezených zařízení a klikněte na **Add** (Přidat).
3. Po zobrazení výzvy zadejte přihlašovací údaje zařízení.

Jakmile je zařízení přidáno, můžete jej přiřadit ke dveřím. Viz *Přidání čtečky, on page 16*.

Přidání čtečky

Ovladač dveří můžete nakonfigurovat tak, aby podporoval několik kabelových čteček. Můžete přidat čtečku na jednu stranu nebo na obě strany dveří.

Použijete-li na čtečku vlastní nastavení formátů karet nebo délky kódu PIN, zobrazí se ve sloupci **Card formats** (Formáty karet) v části **Configuration > Access control > Doors and zones** (Konfigurace > Řízení přístupu > Dveře a zóny). Viz část *Dveře a zóny, on page 4*.

Poznámka

- K jednomu ovladači dveří můžete také přidat až 16 čteček Bluetooth. Další informace naleznete v části *Přidání čtečky Bluetooth, on page 17*.
- Pokud používáte síťový interkom Axis jako IP čtečku, systém použije konfiguraci kódu PIN nastavenou na webové stránce zařízení.

1. Přejděte na stránku konfigurace dveří. Viz část *Přidání dveří, on page 7*.
2. Pod jednou stranou dveří klikněte na **Add** (Přidat).
3. Zvolte **Card reader (Čtečka karet)**.
4. Zvolte **Reader type** (Typ čtečky).
5. Chcete-li použít vlastní nastavení délky kódu PIN pro tuto čtečku:
   5.1. Klikněte na **Pokročilý**.
   5.2. Zapněte možnost **Custom PIN length (Vlastní délka PIN kódu)**.

5.3. Nastavte **Min PIN length (Minimální délka kódu PIN)**, **Max PIN length (Maximální délka kódu PIN)** a **End of PIN character (Konec znaku PIN)**.

6. Použití vlastního nastavení formátu karet pro tuto čtečku:
   6.1. Klikněte na **Pokročilý**.
   6.2. Zapněte možnost **Custom card formats (Vlastní formáty karet)**.
   6.3. Vyberte formáty karet, které chcete pro čtečku použít. Je-li již formát karty se stejnou bitovou délkou používán, je třeba jej nejprve deaktivovat. Pokud se nastavení formátu karty liší od nakonfigurovaného nastavení systému, zobrazí se v klientovi výstražná ikona.
7. Klikněte na **Přidat**.
8. Chcete-li přidat čtečku na druhou stranu dveří, zopakujte tento postup.

Informace o instalaci čtečky AXIS Barcode Reader najdete v části *Instalace čtečky čárových kódů AXIS, on page 27*.

Typ čtečky	
OSDP RS485, poloviční duplex	Pro čtečky RS485 zvolte možnost **OSDP RS485 half duplex (OSDP RS485 poloduplexní)** a port čtečky.
Wiegand	U čteček, které používají protokoly Wiegand, vyberte možnost **Wiegand** a port čtečky.
IP čtečka	U čteček IP vyberte položku **IP reader** (Čtečka IP) a z rozbalovacího menu vyberte zařízení. Síťové interkomy Axis lze použít jako IP čtečku.

Wiegand	
Řízení LED	Vyberte možnost **Single wire** (Jeden vodič) nebo **Dual wire (R/G)** (Dvojitý vodič (R/G)). Čtečky s dvojitým řízením LED používají pro červenou a zelenou LED různé vodiče.
Upozornění na neoprávněnou manipulaci	Zvolte, kdy je vstup neoprávněného zásahu čtečky aktivní. • **Open circuit (Otevřený okruh)**: Čtečka dveřím odešle signál o neoprávněném zásahu v případě, že je okruh otevřený. • **Closed circuit (Uzavřený okruh)**: Čtečka dveřím odešle signál o neoprávněném zásahu v případě, že je okruh uzavřený.
Tamper debounce time (Čas vrácení neoprávněné manipulace)	Pro ignorování změn stavu vstupu neoprávněných zásahů čtečky před přechodem do nového stabilního stavu nastavte **Tamper debounce time (Čas vrácení neoprávněné manipulace)**.
Hlídaný vstup	Zapněte, chcete-li spustit událost při přerušení spojení mezi ovladačem dveří a čtečkou. Viz část *Hlídané vstupy, on page 21*.

Přidání čtečky Bluetooth

Čtečku AXIS A4612 Network Bluetooth Reader můžete použít k rozšíření limitů kabelem připojených dveří u dveřních ovladačů Axis, které umožňují přiřadit až 16 těchto čteček k vlastním dveřím. Každá čtečka může spravovat zámek dveří, požadavek na odchod (REX) a přepnutí polohy dveří (DPS).

Přidání a používání těchto čteček nevyžaduje žádné další licence.

Přidání čtečky AXIS A4612 Network Bluetooth Reader ke dveřím:

1. Ujistěte se, že jste spárovali čtečku AXIS A4612 s ovladačem dveří. Viz *Použití aplikace AXIS Mobile Credential jako přihlašovací údaj Bluetooth, on page 18*.
2. Přejděte na stránku konfigurace dveří. Viz část *Přidání dveří, on page 7*.
3. Pod jednou stranou dveří klikněte na **Add (Přidat)** a poté **Card reader (Čtečka karet)**.
4. Vyberte možnost **IP reader (IP čtečka)** a z rozbalovacího menu vyberte spárovanou čtečku AXIS A4612. Pokud bude tato čtečka použita pro párování přihlašovacích údajů, označte ji pro párování. Klikněte na **Přidat**.
5. Na kartě **Overview (Přehled)** změňte profil identifikace. Pokud máte čtečku AXIS A4612 připojenou pouze na jedné straně dveří a na druhé straně používáte zařízení REX, můžete použít profily **Tap in app (Poklepat v aplikaci)** nebo **Touch reader (Dotyková čtečka)**.

Použití aplikace AXIS Mobile Credential jako přihlašovací údaj Bluetooth

Tento příklad ukazuje, jak do systému přidat čtečku AXIS A4612 Bluetooth Reader, která držitelům karet umožní odemykat dveře pomocí mobilní aplikace AXIS Mobile Credential.

1. Nainstalujte čtečku Bluetooth a připojte ji k ovladači dveří.
2. Přidejte čtečku Bluetooth ve webovém interface ovladače dveří.
   2.1. Získejte přístup do ovladače dveří a přejděte na **Peripherals (Periferní zařízení)** > **Readers (Čtečky)**.
   2.2. Klikněte na **Add reader (Přidat čtečku)**.
   2.3. Zadejte požadované informace v dialogovém okně **Add Bluetooth reader (Přidat čtečku Bluetooth)**.
   2.4. Klikněte na **Přidat**.
3. Přidejte čtečku Bluetooth ke dveřím v AXIS Camera Station Pro.
   3.1. Přejděte do části **Configuration** > **Access control** > **Doors and zones** (Konfigurace > Řízení přístupu > Dveře a zóny).
   3.2. Vyberte dveře, ke kterým chcete přidat čtečku Bluetooth, a klikněte na **Edit (Upravit)**.
   3.3. Klikněte na **+ Add (Přidat)** na straně dveří, kde je umístěna čtečka Bluetooth.
   3.4. Zvolte **Card reader (Čtečka karet)**.
   3.5. V části **Add IP reader (Přidat čtečku IP)** vyberte možnost **IP reader (Čtečka IP)**.
   3.6. V části **Select IP reader (Vybrat čtečku IP)** vyberte čtečku Bluetooth.
   3.7. Klikněte na **Přidat**.
4. Vyberte čtečku Bluetooth pro spárování. Toto je třeba udělat pro alespoň jednu čtečku Bluetooth ve vašem systému.
   4.1. Vyberte čtečku Bluetooth, kterou jste právě přidali.
   4.2. Klikněte na **Edit (Upravit)**.
   4.3. V části **Edit bluetooth reader (Upravit čtečku bluetooth)** vyberte možnost **Use this reader for pairing (Použít tuto čtečku pro spárování)**.
   4.4. Klikněte na **Použít**.
5. Vyberte identifikační profil**Tap in app (Klepnutí v aplikaci)** nebo **Touch reader (Dotyková čtečka)**. Další informace naleznete zde: *Identifikační profily, on page 22*.
6. Přidejte mobilní přihlašovací údaj k držiteli karty. Viz část *Přidání přihlašovacích údajů, on page 33*.
7. Spárujte mobilní přihlašovací údaj s párovanou čtečkou.
   7.1. Přiložte mobilní telefon držitele karty ke čtečce Bluetooth s povoleným párováním.

7.2. Postupujte podle pokynů uvedených v e-mailu zaslaném držiteli karty.

Přidání zařízení REX

Můžete zvolit, zda se zařízení umožňující požádání o opuštění oblasti (REX) má přidat na jednu stranu nebo na obě strany dveří. Zařízením REX může být snímač PIR, tlačítko REX nebo tlačná hrazda.

1. Přejděte na stránku konfigurace dveří. Viz část *Přidání dveří, on page 7*.
2. Pod jednou stranou dveří klikněte na **Add** (Přidat).
3. Vyberte **REX device** (Zařízení REX).
4. Zvolte V/V port, ke kterému chcete zařízení REX připojit. Jestliže je k dispozici pouze jeden port, bude automaticky vybrán.
5. Vyberte možnost **Action** (Akce), která se má spustit, jakmile dveře přijmou signál REX.
6. V části **REX active** (REX aktivní) vyberte připojení okruhů monitoru dveří.
7. Pro ignorování změn stavu digitálního vstupu před přechodem do nového stabilního stavu nastavte **Debounce time (ms) (Čas vrácení (ms))**.
8. Chcete-li spustit událost při přerušení spojení mezi ovladačem dveří a zařízením REX, zapněte možnost **Supervised input** (Hlídaný vstup). Viz část *Hlídané vstupy, on page 21*.

Akce	
Odemknout dveře	Tuto možnost zvolte, jestliže se dveře mají odemknout při přijetí signálu REX.
Žádné	Tuto možnost zvolte, jestliže nechcete, aby se při přijetí signálu REX dveřmi spustila jakákoli akce.

REX aktivní	
Okruh je otevřený	Tuto možnost zvolte, pokud je okruh REX normálně zavřený. Zařízení REX odešle signál, když je okruh otevřený.
Okruh je uzavřený	Tuto možnost zvolte, pokud je okruh REX normálně otevřený. Zařízení REX odešle signál, když je okruh uzavřený.

Přidání zóny

Zóna je konkrétní fyzická oblast se skupinou dveří. Zóny můžete vytvářet a přidávat do nich dveře. Existují dva typy dveří:

- **Perimeter door (Dveře v perimetru):** Držitelé karet do zóny vstupují nebo ji opouštějí skrze tyto dveře.
- **Internal door (Vnitřní dveře):** Vnitřní dveře uvnitř zóny.

Poznámka

Dveře v perimetru mohou patřit ke dvěma zónám. Vnitřní dveře mohou patřit pouze k jedné zóně. Přehled naleznete v části *Příklad dveří a zón, on page 7*.

1. Přejděte do části **Configuration > Access control > Doors and zones > Zones (Konfigurace > Řízení přístupu > Dveře a zóny > Zóny)**.
2. Klikněte na + **Add zone** (Přidat zónu).
3. Zadejte název zóny.
4. Klikněte na **Add door (Přidat dveře)**.

5. Vyberte dveře, které chcete přidat do zóny, a klikněte na **Add** (Přidat).
6. Ve výchozím nastavení jsou dveře nastaveny jako dveře v perimetru. Chcete-li nastavení změnit, zvolte v rozbalovacím menu **Internal door (Vnitřní dveře)**.
7. Dveře v perimetru ve výchozím nastavení pro vstup do zóny používají stranu dveří A. Chcete-li nastavení změnit, zvolte v rozbalovacím menu možnost **Leave (Opustit)**.
8. Jestliže chcete odstranit dveře ze zóny, vyberte je a klikněte na **Remove (Odstranit)**.
9. Klikněte na **Save** (Uložit).

Úprava zóny:

1. Přejděte do části **Configuration > Access control > Doors and zones > Zones (Konfigurace > Řízení přístupu > Dveře a zóny > Zóny)**.
2. V seznamu vyberte zónu.
3. Klikněte na **Edit** (Upravit).
4. Změňte nastavení a klikněte na tlačítko **Save (Uložit)**.

Odstranění zóny:

1. Přejděte do části **Configuration > Access control > Doors and zones > Zones (Konfigurace > Řízení přístupu > Dveře a zóny > Zóny)**.
2. V seznamu vyberte zónu.
3. Klepněte na **Remove** (Odstranit).
4. Klikněte na **Yes (Ano)**.

Úroveň zabezpečení zóny

Do zóny můžete přidat následující funkci zabezpečení:

Anti-passback – Zabraňuje lidem používat stejné přihlašovací údaje jako někdo, kdo vstoupil do oblasti před nimi. Vynucuje, že osoba musí nejprve opustit prostor, než může znovu použít své přihlašovací údaje.

Poznámka

- U funkce anti-passback musí být všechny dveře v zóně vybaveny snímači polohy dveří, aby systém mohl zaregistrovat, že uživatel po protažení karty dveře otevřel.
- Pokud dojde k výpadku ovladače dveří, funkce anti-passback funguje, pokud všechny dveře v zóně patří ke stejnému ovladači dveří. Pokud však dveře v zóně patří různým ovladačům dveří, které jsou v režimu offline, funkce anti-passback přestane fungovat.

Úroveň zabezpečení můžete nakonfigurovat při přidávání nové zóny, nebo ji můžete nakonfigurovat pro existující zónu. Chcete-li přidat úroveň zabezpečení pro existující zónu:

1. Přejděte do části **Configuration** > **Access control** > **Doors and zones** (Konfigurace > Řízení přístupu > Dveře a zóny).
2. Vyberte zónu, pro kterou chcete nakonfigurovat úroveň zabezpečení.
3. Klikněte na **Edit (Upravit)**.
4. Klikněte **Security level** (Úroveň zabezpečení).
5. Zapněte bezpečnostní prvky, které chcete ke dveřím přidat.
6. Klikněte na **Použít**.

Anti-passback	
Pouze porušení protokolu (softwarový)	Tuto možnost použijte, pokud chcete umožnit druhé osobě vstoupit do dveří pomocí stejných

	přihlašovacích údajů jako první osoba. Výsledkem této možnosti je pouze poplach systému.
Odepřít přístup (hardwarový)	Tuto možnost použijte, pokud chcete zabránit druhému uživateli ve vstupu do dveří, pokud použije tytéž přihlašovací údaje jako první osoba. Výsledkem této možnosti je též poplach systému.
Časový limit (v sekundách)	Doba, po kterou systém umožní uživateli znovu vstoupit. Zadejte 0, pokud nechcete časový limit, což znamená, že zóna má anti-passback, dokud uživatel neopustí zónu. Používejte **0** časový limit s funkcí **Odepřít přístup (hardwarový)** jen za předpokladu, že všechny dveře v zóně mají čtečky na obou stranách.

Hlídané vstupy

Hlídané vstupy mohou spustit událost, při přerušení spojení s ovladačem dveří.

- Spojení mezi ovladačem dveří a monitorem dveří. Viz část *Přidání monitoru dveří, on page 13*.
- Spojení mezi ovladačem dveří a čtečkou, která používá protokoly Wiegand. Viz část *Přidání čtečky, on page 16*.
- Spojení mezi ovladačem dveří a zařízením REX. Viz část *Přidání zařízení REX, on page 19*.

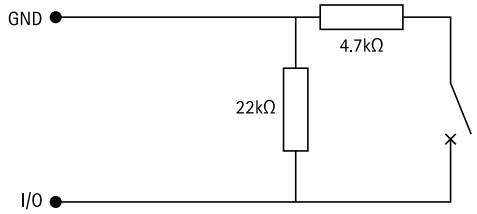
Používání hlídaných vstupů:

1. Podle diagramu připojení nainstalujte koncovou řadu odporů co nejblíže periferním zařízení.
2. Přejděte na stránku konfigurace čtečky, monitoru dveří nebo zařízení REX a zapněte **Supervised input** (Hlídaný vstup).
3. Jestliže jste postupovali podle diagramu upřednostňujícího paralelní připojení, vyberte možnost **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor** (Upřednostňované paralelní připojení s paralelním odporem 22 kΩ a sériovým odporem 4,7 kΩ).
4. Jestliže jste postupovali podle diagramu upřednostňujícího sériové připojení, vyberte možnost **Serial first connection** (Upřednostňované sériové připojení) a vyberte hodnotu rezistoru z rozbalovacího menu **Resistor values** (Hodnoty rezistoru).

Diagramy připojení

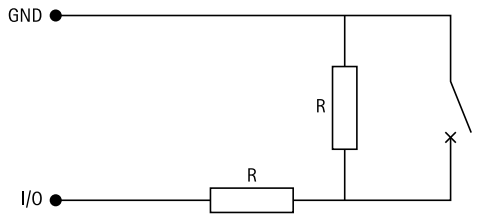
Parallel first connection (Upřednostňované paralelní připojení)

Hodnoty rezistoru musí být 4,7 kΩ a 22 kΩ.



Upřednostňované sériové připojení

Hodnoty rezistoru musí být stejné a v rozsahu 1–10 kΩ.



Identifikační profily

Identifikační profil je kombinací typů identifikace a rozvrhů. Identifikační profil můžete použít na jedny nebo více dveří, abyste určili, jak a kdy může držitel karty získat přístup ke dveřím.

Poznámka

Dynamický QR musí být použit spolu s kódem PIN.

Chcete-li vytvořit, editovat nebo odebrat identifikační profily, přejděte do části **Configuration > Access control > Identification profiles (Konfigurace > Řízení přístupu > Identifikační profily)**.

Dostupné identifikační profily:

Karta – Držitelé karty musí protáhnout kartu, aby získali přístup ke dveřím.

Karta a PIN – Držitelé karty musí protáhnout kartu a zadat kód PIN, aby získali přístup ke dveřím.

PIN – Držitelé karty musí zadat kód PIN, aby získali přístup ke dveřím.

Karta nebo PIN – Držitelé karty musí protáhnout kartu nebo zadat kód PIN, aby získali přístup ke dveřím.

QR – Držitelé karet musí na kameru ukázat QR kód®, aby získali přístup ke dveřím. Identifikační profil QR můžete použít pro statický i dynamický QR.

Registrační značka – Držitelé karet musí přijet ke kameře ve vozidle se schválenou registrační značkou.

Klepnutí v aplikaci – Držitelé karet musí přiložit přihlašovací údaje v mobilní aplikaci AXIS Camera Station a přitom stát v dosahu čtečky Bluetooth.

Dotyková čtečka – Držitelé karet se musí dotknout čtečky Bluetooth, když mají u sebe mobilní telefon s mobilními přihlašovacími údaji.

*QR Code je registrovaná ochranná známka společnosti Denso Wave Incorporated v Japonsku a dalších zemích.

Vytvoření identifikačního profilu

1. Přejděte na část **Configuration > Access control > Identification profiles (Konfigurace > Řízení přístupu > Identifikační profily)**.
2. Klikněte na **Create identification profile (Vytvořit identifikační profil)**.
3. Zadejte název identifikačního profilu.
4. Vyberte možnost **Include facility code for card validation (Zahrnout kód zařízení pro ověření karty)**, pokud chcete, aby byl kód zařízení použit jako jedno z polí k ověřování přihlašovacích údajů. Toto pole je k dispozici pouze v případě, že je zapnut **Facility code (Kód zařízení)** v části **Access management > Settings (Správa přístupu > Nastavení)**.
5. Pro stranu A klikněte na **+ Add** (Přidat), vyberte typ identifikace a rozvrh.
   - Chcete-li od držitelů karet vyžadovat použití více než jednoho typu identifikace, vyberte více typů v jednom řádku.
   - Chcete-li držitelům karet umožnit používat oba typy, klikněte opět na **+ Add** (Přidat) a přidejte další řádek.
6. Pro stranu B klikněte na **+ Add** (Přidat), vyberte typ identifikace a rozvrh.
7. Klikněte na tlačítko **OK**.

Nastavení identifikačních profilů

Úprava identifikačního profilu

1. Přejděte na část **Configuration > Access control > Identification profiles (Konfigurace > Řízení přístupu > Identifikační profily)**.
2. Zvolte identifikační profil a klikněte na tlačítko .
3. Chcete-li změnit název identifikačního profilu, zadejte nový název.
4. Proveďte úpravy na straně dveří.
5. Pro úpravu identifikačního profilu na druhé straně dveří zopakujte předchozí kroky.
6. Klikněte na tlačítko **OK**.

Upravit identifikační profil	
×	Slouží k odebrání typu identifikace a souvisejícího rozvrhu.
Typ identifikace	Chcete-li změnit typ identifikace, zvolte jeden nebo více typů v rozbalovacím menu **Identification type (Typ identifikace)**.
Harmonogram	Chcete-li změnit rozvrh, vyberte jeden nebo více rozvrhů v rozbalovacím menu **Schedule (Rozvrh)**.
+ **Přidat**	Jestliže chcete přidat typ identifikace a související rozvrh, klikněte na **Add** (Přidat) a nastavte typy identifikace a rozvrhy.

Odstranění identifikačního profilu

1. Přejděte na část **Configuration > Access control > Identification profiles (Konfigurace > Řízení přístupu > Identifikační profily)**.
2. Zvolte identifikační profil a klikněte na tlačítko .
3. Jestliže byl daný identifikační profil použit na nějaké dveře, zvolte pro tyto dveře jiný identifikační profil.
4. Klikněte na tlačítko **OK**.

Obnovení předem definovaného formátu karty

1. Přejděte do části **Configuration > Access Control > Card formats and PIN (Konfigurace > Řízení přístupu > Formáty karet a kód PIN)**.
2. Kliknutím na tlačítko resetujete formát karty na výchozí mapu pole.

Formáty karet a kód PIN

Formát karty určuje, jak čtečka karet interpretuje data z karty. K dispozici jsou předem definované formáty karet, které můžete použít nebo upravit, a můžete si také vytvořit vlastní formáty karet

Přejděte do nabídky **Configuration > Access Control > Card formats and PIN** (Konfigurace > Řízení přístupu > Formáty karet a kód PIN), chcete-li vytvářet, editovat nebo aktivovat formáty karet. Také můžete nakonfigurovat kód PIN.

Vlastní formáty karet mohou obsahovat následující datová pole používaná k ověřování přihlašovacích údajů.

Číslo karty – Podmnožina binárních dat přihlašovacích údajů, která jsou zakódována jako desítková nebo hexadecimální čísla. Pomocí čísla karty můžete identifikovat konkrétní karty nebo držitele karty.

Kód zařízení – Podmnožina binárních dat přihlašovacích údajů, která jsou zakódována jako desítková nebo hexadecimální čísla. Pomocí kódu zařízení můžete identifikovat konkrétního koncového zákazníka nebo pracoviště.

Konfigurace kódu PIN

1. Přejděte do části **Configuration > Access Control > Card formats and PIN (Konfigurace > Řízení přístupu > Formáty karet a kód PIN)**.
2. V části **PIN configuration** (Konfigurace kódu PIN) klikněte na položku .
3. Zadejte **Min PIN length (Minimální délka kódu PIN)**, **Max PIN length (Maximální délka kódu PIN)** a **End of PIN character (Konec znaku PIN)**.
4. Klikněte na tlačítko **OK**.

Vytvoření formátu karty

1. Přejděte do části **Configuration > Access Control > Card formats and PIN (Konfigurace > Řízení přístupu > Formáty karet a kód PIN)**.
2. Klikněte na **Add card format** (Přidat formát karty).
3. Zadejte název formátu karty.
4. Do pole **Bit length (Bitová délka)** zadejte bitovou délku od 1 do 256.
5. Chcete-li převrátit pořadí bitů dat obdržených od čtečky karet, zvolte možnost **Invert bit order (Převrátit pořadí bitů)**.
6. Chcete-li převrátit pořadí bajtů dat obdržených od čtečky karet, zvolte možnost **Invert byte order (Převrátit pořadí bajtů)**. Tato možnost je k dispozici pouze v případě, že zadáte bitovou délku, která je dělitelná osmi.
7. Zvolte a nakonfigurujte datová pole, která budou ve formátu karty aktivní. Ve formátu karty musí být aktivní buď **Card number (Číslo karty)** nebo **Facility code (Kód zařízení)**.
8. Klikněte na tlačítko **OK**.
9. Pokud chcete formát karty aktivovat, vyberte zaškrtávací políčko před názvem formátu karty.

Poznámka

- Dva formáty karet se stejnou bitovou délkou nemohou být aktivní současně. Máte-li například definovány dva 32bitové formáty karet, může být aktivní pouze jeden. Chcete-li aktivovat druhý formát karty, deaktivujte nejprve ten první.
- Formáty karet můžete aktivovat a deaktivovat pouze v případě, že ovladač dveří byl nakonfigurován s aspoň jednou čtečkou.
- Předem definované formáty karet lze upravovat, ale nelze je smazat. Chcete-li zrušit jakékoli změny předem definovaného formátu, klikněte na ikonu obnovení a obnovte jeho výchozí nastavení. Vytvořené formáty karet lze smazat.

ⓘ	Kliknutím na ⓘ zobrazíte příklad výstupu po převrácení pořadí bitů.
Rozsah	Nastavte bitový rozsah dat pro datové pole. Rozsah musí spadat do stejných hodnot, jaké jste nastavili pro **Bitovou délku**.
Formát výstupu	Zvolte výstupní formát dat pro datové pole. **Decimal (Desetinný)**: Známý také jako poziční číselný systém base-10, sestává z čísel 0 až 9. **Šestnáctková soustava**: známá také jako poziční číselná soustava na 16kové bázi se skládá z 16 jedinečných symbolů: čísel 0–9 a písmen a–f.
Bitové pořadí podrozsahu	Zvolte bitové pořadí. **Little endian**: První bit je nejmenší (nejméně významný). **Big endian**: První bit je největší (nejvýznamnější).

Nastavení formátů karet

Úprava formátu karty

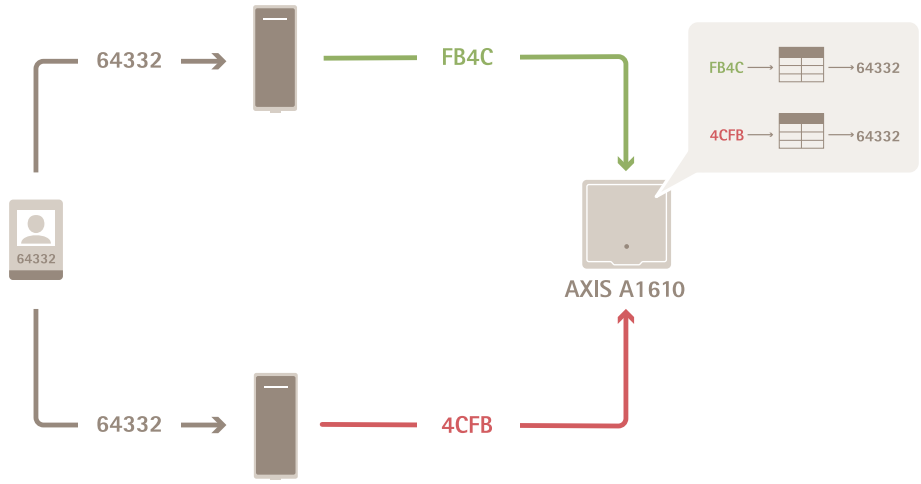
1. Přejděte do části **Configuration > Access Control > Card formats and PIN (Konfigurace > Řízení přístupu > Formáty karet a kód PIN)**.
2. Vyberte formát karty a klikněte na tlačítko .
3. Pokud upravujete předem definovaný formát karty, můžete upravit pouze **Invert bit order (Převrátit pořadí bitů)** a **Invert byte order (Převrátit pořadí bajtů)**.
4. Klikněte na tlačítko **OK**.

Odstranit lze pouze vlastní formáty karet. Odstranění vlastního formátu karty:

1. Přejděte do části **Configuration > Access Control > Card formats and PIN (Konfigurace > Řízení přístupu > Formáty karet a kód PIN)**.
2. Vyberte vlastní formát karty a klikněte na tlačítko a poté na **Yes** (Ano).

Nastavení formátu karty

Celkový přehled



- Číslo karty v desítkové soustavě je `64332`.
- Jedna čtečka převádí číslo karty na hexadecimální číslo `FB4C`. Druhá čtečka ho převádí na hexadecimální číslo `4CFB`.
- Ovladač dveří AXIS A1610 Network Door Controller přijme `FB4C` a převede ho na desítkové číslo `64332` podle nastavení formátu karty u čtečky.
- Ovladač dveří AXIS A1610 Network Door Controller přijme `4CFB` a přehozením pořadí bajtů ho převede na `FB4C` a dále na desítkové číslo `64332` podle nastavení formátu karty u čtečky.

Převrátit pořadí bitů

Po převrácení pořadí bitů jsou data karty získaná ze čtečky čtena po bitech zprava doleva.

Převrátit pořadí bajtů

Bajt je skupina osmi bitů. Po převrácení pořadí bajtů jsou data karty získaná ze čtečky čtena po bajtech zprava doleva.

26bitový standardní formát karty Wiegand

1 *Počáteční parita*
2 *Kód zařízení*
3 *Číslo karty*
4 *Koncová parita*

Šifrovaná komunikace

Zabezpečený kanál OSDP

Systém AXIS Camera Station Secure Entry podporuje zabezpečený kanál OSDP (Open Supervised Device Protocol – Otevřený protokol zařízení pod dohledem), který umožňuje šifrování propojení mezi ovladačem a čtečkami AXIS.

Zapnutí zabezpečeného kanálu OSDP pro celý systém:

1. přejdete do nabídky **Configuration > Access control > Encrypted communication (Konfigurace > Řízení přístupu > Šifrovaná komunikace)**.
2. Zadejte hlavní šifrovací klíč a klikněte na **OK**.
3. Zapněte **zabezpečený kanál OSDP**. Tato možnost je k dispozici pouze po nastavení hlavního šifrovacího klíče.
4. Ve výchozím nastavení je klíč zabezpečeného kanálu OSDP generován hlavním šifrovacím klíčem. Chcete-li klíč zabezpečeného kanálu OSDP nastavit ručně:
   4.1. V nabídce **OSDP Secure Channel** (Zabezpečený kanál OSDP) klikněte na .
   4.2. Zrušte volbu **Use main encryption key to generate OSDP Secure Channel key (Vygenerovat klíč zabezpečeného kanálu OSDP pomocí hlavního šifrovacího klíče)**.
   4.3. Zadejte klíč zabezpečeného kanálu OSDP a klikněte na **OK**.

Chcete-li zapnout nebo vypnout zabezpečený kanál OSDP pro konkrétní čtečku, viz *Doors and zones (Dveře a zóny)*.

Poznámka

Pokud jednotka kontroly přístupu, hostitelský počítač nebo ovládací panel podporují zabezpečený kanál OSDP, doporučujeme jej nastavit na zařízení, aby se zvýšila bezpečnost komunikace. Chcete-li zajistit zabezpečený kanál, nastavte DIP č. 6 na zařízení čtečky.

Šifrovací klíč se při počátečním nastavení přenáší v otevřené podobě, proto by během tohoto procesu mělo být veškeré zapojení sběrnice RS485 a všechna zařízení pod dohledem.

Čtečka čárových kódů AXIS

Čtečka čárových kódů AXIS je aplikace, kterou lze nainstalovat na kamery Axis. Ovladač dveří Axis využívá externí ověřovací klíč k udělení přístupu a ověření čtečky AXIS Barcode Reader a aplikace AXIS License Plate Verifier. Celý postup nastavení nástroje AXIS License Plate Verifier v systému AXIS Camera Station Pro naleznete v tématu .

Instalace čtečky čárových kódů AXIS

1. Stáhněte si instalační soubor aplikace z *axis.com*.
2. Přejděte na webovou stránku interkomu nebo kamery Axis.
3. Nainstalujte aplikaci.
4. Aktivujte licenci.
5. Spuštění aplikace.
6. Doporučujeme změnit následující nastavení kamery pro lepší přesnost QR.
   6.1. Přejděte do nastavení kamery.
   6.2. V části **Image > Exposure (Obrázek > Expozice)** přesuňte posuvník **Blur-noise trade-off (Vyvážení rozmazání–šumu)** doprostřed.

Konfigurace čtečky čárových kódů AXIS

1. Chcete-li změnit profil identifikace QR, přejděte na **Configuration > Access control > Identification profiles (Konfigurace > Řízení přístupu > Identifikační profily)** a klikněte na . Viz *Identifikační profily*.
2. Přidejte dveře. Viz část *Přidání dveří*.
3. Jako identifikační profil pro tato dveře zvolte **QR**. Viz *Nastavení dveří*.
4. Přidání čtečky čárových kódů. Viz *Přidání čtečky*.
   4.1. Pod jednou stranou dveří klikněte na **Add reader (Přidat čtečku)**.
   4.2. Z rozevíracího seznamu **Reader type (Typ čtečky)** vyberte **AXIS Barcode Reader**. Zadejte název a klikněte na tlačítko **OK**.

1. Chcete-li změnit profil identifikace QR, přejděte na **Configuration > Access control > Identification profiles (Konfigurace > Řízení přístupu > Identifikační profily)** a klikněte na . Viz *Identifikační profily*.
2. Přidejte dveře. Viz část *Přidání dveří*.
3. Jako identifikační profil pro tato dveře zvolte **QR**. Viz *Nastavení dveří*.
4. Přidání čtečky čárových kódů. Viz *Přidání čtečky*.
   4.1. Pod jednou stranou dveří klikněte na **Add reader (Přidat čtečku)**.
   4.2. Z rozevíracího seznamu **Reader type (Typ čtečky)** vyberte **AXIS Barcode Reader**. Zadejte název a klikněte na tlačítko **OK**.

1. Chcete-li změnit profil identifikace QR, přejděte na **Configuration > Access control > Identification profiles (Konfigurace > Řízení přístupu > Identifikační profily)** a klikněte na . Viz *Identifikační profily*.
2. Přidejte dveře. Viz část *Přidání dveří*.
3. Jako identifikační profil pro tato dveře zvolte **QR**. Viz *Nastavení dveří*.
4. Přidání čtečky čárových kódů. Viz *Přidání čtečky*.
   4.1. Pod jednou stranou dveří klikněte na **Add reader (Přidat čtečku)**.
   4.2. Z rozevíracího seznamu **Reader type (Typ čtečky)** vyberte **AXIS Barcode Reader**. Zadejte název a klikněte na tlačítko **OK**.

Vytvoření připojení pomocí ovladače dveří

1. V AXIS Camera Station Pro Secure Entry:
   1.1. přejdete do nabídky **Configuration > Access control > Encrypted communication (Konfigurace > Řízení přístupu > Šifrovaná komunikace)**.
   1.2. V části **External Peripheral Authentication Key (Externí periferní ověřovací klíč)** klikněte na možnost **Show authentication key (Zobrazit ověřovací klíč)** a na **Copy key (Zkopírovat klíč)**.
2. Ve webovém rozhraní zařízení, kde je spuštěna čtečka čárových kódů AXIS:
   2.1. Otevřete aplikaci čtečky čárových kódů AXIS.
   2.2. Jestliže serverový certifikát nebyl v AXIS Camera Station Pro Secure Entry nakonfigurován, zapněte možnost **Ignore server certificate validation (Ignorovat ověření certifikátu serveru)**. Více informací najdete v části *Certifikáty*.
   2.3. Jestliže serverový certifikát nebyl v AXIS Camera Station Pro Secure Entry nakonfigurován, zapněte možnost **Ignore server certificate validation (Ignorovat ověření certifikátu serveru)**. Více informací najdete v části *Certifikáty*.

2.4. Jestliže serverový certifikát nebyl v AXIS Camera Station Pro Secure Entry nakonfigurován, zapněte možnost **Ignore server certificate validation (Ignorovat ověření certifikátu serveru)**. Více informací najdete v části *Certifikáty*.

2.5. Zapněte **AXIS Camera Station Secure Entry**.

2.6. Klikněte na **Add (Přidat)** a zadejte IP adresu ovladače dveří a vložte ověřovací klíč.

2.7. Z rozbalovacího menu dveří vyberte čtečku, která čte čárové kódy.

Více serverů BETA

Připojené sub servery mohou, s více servery, používat globální držitele karet a skupiny držitelů karet z hlavního serveru.

Poznámka

- Jeden systém může podporovat až 64 dílčích serverů.
- Tato možnost vyžaduje AXIS Camera Station 5.47 nebo novější.
- Vyžaduje, aby hlavní server a sub servery byly umístěny ve stejné síti.
- Na hlavním serveru a sub serverech ověřte, že je brána Windows Firewall nakonfigurována tak, aby umožňovala příchozí připojení TCP na portu Secure Entry. Výchozí port je 55767. Pro informace o přizpůsobené konfiguraci portů viz .
- Připojením podřízeného serveru k hlavnímu serveru dojde k nahrazení jeho čtecího klíče, čímž se stávající přístupové údaje pro Bluetooth stanou neplatnými. Chcete-li tomu zabránit, vytvořte přístupové údaje pro Bluetooth na hlavním serveru namísto na podřízeném serveru.

Pracovní postup

1. Nakonfigurujte server jako sub server a vytvořte konfigurační soubor. Viz část *Vygenerování konfiguračního souboru ze sub serveru, on page 29*.
2. Nakonfigurujte server jako hlavní server a importujte konfigurační soubor sub serverů. Viz část *Importování konfiguračního souboru do hlavního serveru, on page 29*.
3. Nakonfigurujte globální držitele karet a skupiny držitelů karet na hlavním serveru. Viz *Přidání držitele karty, on page 32* a *Přidání skupiny, on page 36*.
4. Zobrazte a monitorujte globální držitele karet a skupiny držitelů karet na sub serveru. Viz část *Správa přístupu, on page 32*.

Vygenerování konfiguračního souboru ze sub serveru

1. Ze sub serveru přejděte do části **Configuration > Access control > Multi server (Konfigurace > Řízení přístupu > Více serverů)**.
2. Klikněte na možnost **Sub server**.
3. Klikněte na **Generate (Vygenerovat)**. Vygeneruje konfigurační soubor ve formátu .json.
4. Klikněte na možnost **Download (Stáhnout)** a zvolte umístění pro uložení souboru.

Importování konfiguračního souboru do hlavního serveru

1. Z hlavního serveru přejděte do části **Configuration > Access control > Multi server (Konfigurace > Řízení přístupu > Více serverů)**.
2. Klikněte na možnost **Main server (Hlavní server)**.
3. Klikněte na + **Add** (Přidat) a přejděte na konfigurační soubor, který jste vygenerovali ze sub serveru.
4. Zadejte název serveru, IP adresu a číslo portu sub serveru.
5. Přidejte sub server kliknutím na **Import**.

6. Stav sub serveru se zobrazí jako `Connected`.

Zrušení sub serveru

Sub server můžete zrušit pouze před importováním jeho konfiguračního souboru do hlavního serveru.

1. Z hlavního serveru přejděte do části **Configuration > Access control > Multi server (Konfigurace > Řízení přístupu > Více serverů)**.
2. Klikněte na možnost **Sub server**a poté klikněte na možnost **Revoke server (Zrušit server)**.
   Nyní můžete tento server nakonfigurovat jako hlavní server nebo jako sub server.

Odebrání sub serveru

Po importování konfiguračního souboru sub serveru se sub server připojí k hlavnímu serveru.

Odebrání sub serveru:

1. Z hlavního serveru:
   1.1. Přejděte do části **Access management > Dashboard (Správa přístupu > Řídicí panel)**.
   1.2. Změňte globální držitele karet a skupiny na místní držitele karet a skupiny.
   1.3. Přejděte do části **Configuration > Access control > Multi server** (Konfigurace > Řízení přístupu > Více serverů).
   1.4. Kliknutím na **Main server** (Hlavní server) zobrazíte seznam sub serverů.
   1.5. Zvolte sub server a klikněte na možnost **Delete (Odstranit)**.
2. Ze sub serveru:
   – Přejděte do části **Configuration > Access control > Multi server** (Konfigurace > Řízení přístupu > Více serverů).
   – Klikněte na možnost **Sub server** a poté klikněte na možnost **Revoke server** (Zrušit server).

Nastavení služby Active Directory[BETA]

Poznámka

K systému AXIS Camera Station Pro Secure Entry mají přístup uživatelské účty ze systému Microsoft Windows a uživatelé a skupiny Active Directory. Způsob přidávání uživatelů v systému Windows se liší v závislosti na verzi systému. Další informace naleznete na *support.microsoft.com*. Pokud používáte síť s doménou Active Directory, obraťte se na správce sítě.

Při prvním otevření stránky nastavení služby Active Directory můžete importovat uživatele služby Microsoft Active Directory do držitelů karet v aplikaci AXIS Camera Station Pro Secure Entry. Viz část *Importování uživatelů služby Active Directory, on page 30*.

Po počáteční konfiguraci se na stránce nastavení služby Active Directory zobrazí následující možnosti.

- Vytváření a správa skupin držitelů karet na základě skupin v Active Directory.
- Nastavení plánované synchronizace mezi službou Active Directory a systémem správy přístupu.
- Ruční synchronizací aktualizujte všechny držitele karet importované ze služby Active Directory.
- Správa mapování dat mezi údaji uživatele ze služby Active Directory a vlastnostmi držitele karty.

Importování uživatelů služby Active Directory

Chcete-li importovat uživatele služby Active Directory do držitelů karet v AXIS Camera Station Pro Secure Entry:

1. Přejděte do části **Configuration** > **Access control** > **Active directory settings**[BETA] (Konfigurace > Řízení přístupu > Nastavení Active directory).
2. Klikněte na **Set up import** (Nastavit import).

3. Tyto tři hlavní kroky proveďte podle instrukcí na obrazovce:
   3.1. Vyberte uživatele ze služby Active Directory, kterého chcete použít jako šablonu pro mapování dat.
   3.2. Mapujte uživatelská data z databáze Active Directory na vlastnosti držitelů karet.
   3.3. Vytvořte novou skupinu držitelů karet v systému správy přístupu a vyberte, které skupiny ze služby Active Directory chcete importovat.

Nemůžete měnit žádné z importovaných uživatelských údajů, ale můžete přidat přihlašovací údaje k importovanému držiteli karty, viz *Přidání přihlašovacích údajů, on page 33*.

Důležité

Pokud v Active Directory deaktivujete uživatele, aplikace AXIS Camera Station Pro trvale odstraní držitele karty i veškerá související data, včetně jeho historie. Toto nelze vzít zpět. Chcete-li zablokovat přístup držiteli karty, aniž byste přišli o jeho data, pozastavte mu přístup v aplikaci AXIS Camera Station Pro namísto toho, abyste mu zrušili oprávnění v Active Directory.

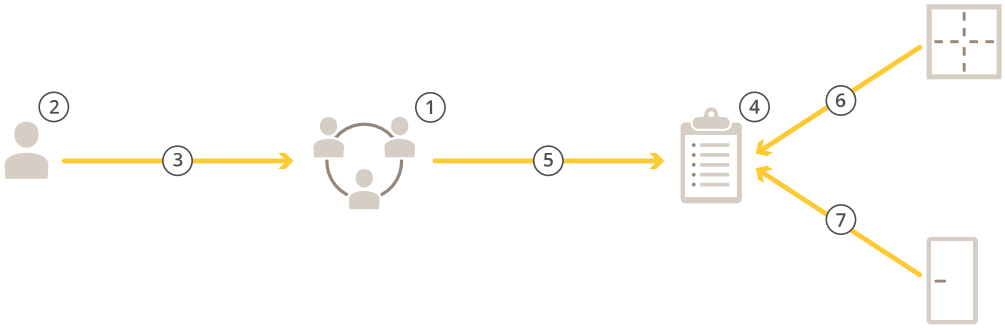
Správa přístupu

Karta správy přístupu umožňuje konfigurovat a spravovat držitele karet, skupiny a pravidla přístupu systému.

Úplný pracovní postup pro nastavení síťového ovladače dveří Axis v systému AXIS Camera Station Pro Secure Entry naleznete v článku *Nastavení síťového ovladače dveří Axis*.

Pracovní postup správy přístupu

Struktura správy přístupu je flexibilní, což umožňuje vyvinout pracovní postup podle vašich potřeb. Toto je příklad pracovního postupu:



1. *Přidání skupiny, on page 36*.
2. *Přidání držitele karty, on page 32*.
3. Přidejte do skupin držitele karet.
4. *Přidání pravidla přístupu, on page 37*.
5. Použijte skupiny na pravidla přístupu.
6. Použijte zóny na pravidla přístupu.
7. Použijte dveře na pravidla přístupu.

Přidání držitele karty

Držitel karty je osoba s jedinečným identifikátorem registrovaným v systému. Nakonfigurujte držitele karty s přihlašovacími údaji, které identifikují osobu a kdy a jak jí udělit přístup ke dveřím.

Můžete také mapovat uživatele v databázi služby Active Directory jako držitele karet, viz část *Nastavení služby Active Directory*^{BETA}*, on page 30*.

1. Otevřete kartu Access Management (Správa přístupu).
2. Přejděte do nastavení **Cardholder management** > **Cardholders** (Správa držitelů karet > Držitelé karet) a klikněte na **+ Add** (+ přidat).
3. Zadejte jméno a příjmení držitele karty. Případně můžete do údajů o držiteli karty doplnit další informace:
   - V poli **Email** zadejte e-mailovou adresu držitele karty.
   - V části **Groups** (Skupiny) vyberte skupiny, do kterých chcete držitele karty přidat.
   - V části **Access rules** (Pravidla přístupu) vyberte pravidla přístupu, která chcete na držitele karty uplatnit.
4. Chcete-li přidat fotografii, klikněte na **Cardholder picture** (Obrázek držitele karty) a vyberte:
   - **Upload** (Nahrát) pro přidání obrázku ze svého zařízení.
   - **Capture** (Pořídit snímek) pro pořízení fotografie přímo pomocí kamery.

Poznámka

Obrázek musí být ve formátu JPG, PNG nebo GIF. Obrázky se automaticky zmenší na maximální rozměry 700 × 700 pixelů a převedou do formátu JPG.

5. Klikněte na **Advanced** (Další nastavení), abyste provedli nastavení dalších možností.
6. Přidejte přihlašovací údaje k držiteli karty. Viz část *Přidání přihlašovacích údajů, on page 33*.
7. Klikněte na **Save** (Uložit).
8. Chcete-li vytisknout průkazy pro jednoho nebo více držitelů karet, vyberte držitele karet a klikněte na **Print Badge**[BETA] (Vytisknou průkaz). Další informace najdete v části *Vytisknutí průkazu [BETA], on page 42*.

Pomocí vyhledávacího pole můžete vyhledat držitele karty podle jména nebo příjmení. Chcete-li filtrovat podle zdroje, klikněte na možnost **Filter** (Filtr) a vyberte položku **Local**, **Global**, **AD** nebo **Center** (Zdroje, Místní, Globální, AD nebo Centrum).

Pokročilé	
Dlouhá doba přístupu	Vyberte, pokud chcete, aby držitel karty měl dlouhou dobu přístupu a dlouhou dobu příliš dlouhého otevření, když je nainstalován monitor dveří.
Pozastavit držitele karty	Umožňuje pozastavit držitele karty. Tento úkon dočasně odebere držiteli karty veškerý přístup.
Povolení dvojitého protáhnutí	Vyberte, chcete-li držiteli karty povolit přepsání aktuálního stavu dveří. Mohou jím například odemknout dveře mimo běžný rozvrh.
Výjimka z lockdownu	Vyberte, pokud chcete, aby měl držitel karty přístup během lockdownu.
Exempt from anti-passback (Výjimka z ochrany proti zpětnému vstupu)	Vyberte, pokud chcete držiteli karty udělit výjimku z pravidla anti-passback. Funkce Anti-passback zabraňuje lidem používat stejné přihlašovací údaje jako někdo, kdo vstoupil do oblasti před nimi. První osoba musí nejprve opustit prostor, než bude možné její přihlašovací údaje znovu použít.
Globální držitel karty	Tuto možnost vyberte, abyste umožnili zobrazení a monitorování držitele karet na sub serverech. Tato možnost je k dispozici pouze pro držitele karet, kteří byli vytvořeni na hlavním serveru. Viz část *Více serverů [BETA], on page 29*.

Přidání držitelů karet a skupin

Přidání přihlašovacích údajů

K držiteli karty můžete přidat následující typy přihlašovacích údajů:

- *Přístupový údaj pomocí QR kódu, on page 34*
- *Ověření kódem PIN, on page 34*

- *Mobilní přístupové údaje, on page 35*
- *Ověření kartou, on page 35*
- *Ověření registrační značkou, on page 35*

Datum vypršení platnosti	
Platí od	Nastavte datum a čas, ke kterému má být přihlašovací údaj platný.
Platí do	Z rozbalovacího menu vyberte možnost.

Platí do	
Žádné datum ukončení	Platnost přihlašovacího údaje nikdy nevyprší.
Datum	Nastavte datum a čas, kdy platnost přihlašovacího údaje vyprší.
Od prvního použití	Zvolte dobu, po kterou bude přihlašovací údaj platit po prvním použití. Může se jednat o počet dnů, měsíců nebo let nebo o počet použití po prvním použití.
Od posledního použití	Zvolte dobu, po kterou bude přihlašovací údaj platit po posledním použití. Může se jednat o počet dnů, měsíců nebo let po posledním použití.

Přístupový údaj pomocí QR kódu

Poznámka

Použití QR kódů jako přístupových údajů vyžaduje, aby byl synchronizován čas na systémovém ovladači a na kameře se čtečkou AXIS Barcode Reader. Pro dokonalou synchronizaci času doporučujeme pro obě zařízení použít stejný zdroj času.

Přidání přístupového údaje pomocí QR kódu k držiteli karty:

1. V rámci možnosti **Credentials** (Přihlašovací údaje) klikněte na **+ Add** (+ přidat) a zvolte **QR-code** (QR kód).
2. Zadejte název přihlašovacího údaje.
3. Možnost **Dynamic QR** (Dynamický QR) je ve výchozím nastavení zapnutá. Dynamický QR musí být použit spolu s kódem PIN.
4. Nastavte počáteční a koncové datum přihlašovacího údaje.
5. Chcete-li QR kód automaticky odeslat e-mailem po uložení držitele karty, vyberte možnost **Send QR code to cardholder when credential is saved (Odeslat QR kód držiteli karty při uložení přístupového údaje)**.
6. Klikněte na **Přidat**.

Ověření kódem PIN

Přidání přihlašovacích údajů PIN k držiteli karty:

1. V rámci možnosti **Credentials** (Přihlašovací údaje) klikněte na **+ Add** (+ přidat) a zvolte **PIN**.
2. Zadejte kód PIN.
3. Chcete-li spustit tichý poplach pomocí samostatného kódu PIN, zapněte možnost **Duress PIN (Tísňový kód PIN)** a zadejte tísňový kód PIN.
4. Nastavte pro dané přístupové údaje data **Valid from** (Platné od) a **Valid to** (Platné do).
5. Klikněte na **Přidat**.

Mobilní přístupové údaje

Poznámka

Držitel karty musí mít e-mailovou adresu, aby mohl obdržet mobilní přístupové údaje.

Přidání přihlašovacích údajů k držiteli karty:

1. V rámci možnosti **Credentials** (Přihlašovací údaje) klikněte na **+ Add** (+ přidat) a zvolte **Mobile credential** (Mobilní přihlašovací údaj).
2. Zadejte název přihlašovacího údaje.
3. Nastavte počáteční a koncové datum přihlašovacího údaje.
4. Vyberte možnost **Send the mobile credential to the cardholder after saving (Po uložení odeslat mobilní přihlašovací údaj držiteli karty)**. Držitel karty obdrží e-mail s pokyny pro spárování.
5. Klikněte na **Přidat**.

Viz příklad v části *Použití aplikace AXIS Mobile Credential jako přihlašovací údaj Bluetooth, on page 18*.

Ověření kartou

Přidání přihlašovacích údajů karty k držiteli karty:

1. V rámci možnosti **Credentials** (Přihlašovací údaje) klikněte na **+ Add** (+ přidat) a zvolte **Card** (Karta).
2. Jestliže chcete údaje karty zadat ručně, zadejte název karty, číslo karty a bitovou délku.

Poznámka

Bitová délka je konfigurovatelná, pouze když vytvoříte formát karty s určitou bitovou délkou, která se nenachází v systému.

3. Jestliže chcete automaticky načíst údaje poslední protáhnuté karty:
   3.1. Z rozbalovacího menu **Select reader** (Vyberte čtečku) vyberte dveře.
   3.2. Protáhněte kartu čtečkou připojenou k daným dveřím.
   3.3. Klikněte na možnost **Get last swiped card data from the door's reader(s)** (Získat data poslední karty ze čteček dveří).

Poznámka

K získání dat karty můžete použít desktopovou USB čtečku karet 2N. Další informace naleznete v tématu *Nastavení desktopové USB čtečky karet 2N*.

4. Zadejte kód zařízení. Toto pole je k dispozici pouze v případě, že je povolen **Facility code (Kód zařízení)** v části **Access management > Settings (Správa přístupu > Nastavení)**.
5. Nastavte počáteční a koncové datum přihlašovacího údaje.
6. Klikněte na **Přidat**.

Ověření registrační značkou

Přidání přihlašovacích údajů registrační značky k držiteli karty:

1. V rámci možnosti **Credentials** (Přihlašovací údaje) klikněte na **+ Add** (+ přidat) a zvolte **License plate** (Registrační značka).
2. Zadejte název přihlašovacího údaje popisující vozidlo.
3. Zadejte číslo registrační značky vozidla.
4. Nastavte počáteční a koncové datum přihlašovacího údaje.
5. Klikněte na **Přidat**.

Použití registrační značky jako přihlašovacího údaje

Tento příklad ukazuje, jak použít ovladač dveří, kameru s funkcí AXIS License Plate Verifier a registrační značku vozidla jako přihlašovací údaj pro udělení přístupu.

1. Přidejte ovladač dveří a kameru do AXIS Camera Station Pro Secure Entry. Viz část .
2. Upgradujte firmware na nových zařízeních na nejnovější dostupnou verzi. Viz část .
3. Přidejte nové dveře připojené k vašemu ovladači dveří. Viz část *Přidání dveří, on page 7*.
   3.1. Přidejte čtečku v části **Side A (Strana A)**. Viz *Přidání čtečky, on page 16*.
   3.2. V části **Door settings (Nastavení dveří)** vyberte možnost **AXIS License Plate Verifier** jako **Reader type (Typ čtečky)** a zadejte název čtečky.
   3.3. Volitelně můžete přidat čtečku nebo zařízení REX v části **Side B (Strana B)**.
   3.4. Klikněte na **Ok**.
4. Nainstalujte na svou kameru nástroj AXIS License Plate Verifier a aktivujte ho. Viz uživatelská příručka pro *AXIS License Plate Verifier*.
5. Spusťte AXIS License Plate Verifier.
6. Nakonfigurujte AXIS License Plate Verifier.
   6.1. přejdete do nabídky **Configuration > Access control > Encrypted communication (Konfigurace > Řízení přístupu > Šifrovaná komunikace)**.
   6.2. V části **External Peripheral Authentication Key (Externí periferní ověřovací klíč)** klikněte na možnost **Show authentication key (Zobrazit ověřovací klíč)** a na **Copy key (Zkopírovat klíč)**.
   6.3. Otevřete AXIS License Plate Verifier z webového interface kamery.
   6.4. Nekonfigurujte nastavení.
   6.5. Přejděte do nabídky **Settings (Nastavení)**.
   6.6. V části **Access control (Řízení přístupu)** vyberte možnost **Secure Entry** jako **Type (Typ)**.
   6.7. V části **IP address (IP adresa)** zadejte IP adresu ovladače dveří.
   6.8. Do části **Authentication key (Ověřovací klíč)** vložte ověřovací klíč, který jste dříve zkopírovali.
   6.9. Klepněte na **Connect (Připojit)**.
   6.10. Pod položkou **Door controller name (Název ovladače dveří)** vyberte svůj ovladač dveří.
   6.11. Pod položkou **Reader name (Název čtečky)** vyberte čtečku, kterou jste přidali dříve.
   6.12. Zapněte integraci.
7. Přidejte držitele karty, kterému chcete udělit přístup. Viz část *Přidání držitele karty, on page 32*
8. Přidejte přihlašovací údaje registrační značky k novému držiteli karty. Viz část *Přidání přihlašovacích údajů, on page 33*
9. Přidejte pravidlo přístupu. Viz část *Přidání pravidla přístupu, on page 37*.
   9.1. Přidejte rozvrh.
   9.2. Přidejte držitele karty, kterému chcete udělit přístup registrační značky.
   9.3. Přidejte dveře pomocí čtečky AXIS License Plate Verifier.

Přidání skupiny

Skupiny vám umožňují hromadně a efektivně spravovat držitele karet a jejich pravidla přístupu.

1. Otevřete kartu Access Management (Správa přístupu).
2. Přejděte do nastavení **Cardholder management** > **Groups** (Správa držitelů karet > Skupiny) a klikněte na **+ Add** (+ přidat).
3. Zadejte název a případně iniciály skupiny.
4. Vyberte možnost **Global group (Globální skupina)**, abyste umožnili zobrazení a monitorování držitele karet na sub serverech. Tato možnost je k dispozici pouze pro držitele karet, kteří byli vytvořeni na hlavním serveru. Viz část *Více serverů BETA, on page 29*.

5. Jestliže chcete do skupiny přidat držitele karet:
   5.1. Klikněte na **+ Add** (+ přidat).
   5.2. Vyberte držitele karet, které chcete přidat, a klikněte na **Add** (Přidat).
6. Klikněte na **Save** (Uložit).
7. Chcete-li vytisknout průkazy pro všechny držitele karet ve skupině, vyberte skupinu a klikněte na **Print Badge**[BETA] (Vytisknout průkaz). Další informace najdete v části *Vytisknutí průkazu [BETA], on page 42*.

Přidání pravidla přístupu

Pravidlo přístupu definuje podmínky, které musí být splněny pro udělení přístupu.

Pravidlo přístupu se skládá z následujících částí:

Držitelé karet a skupiny držitelů karet – komu má být přístup udělen.

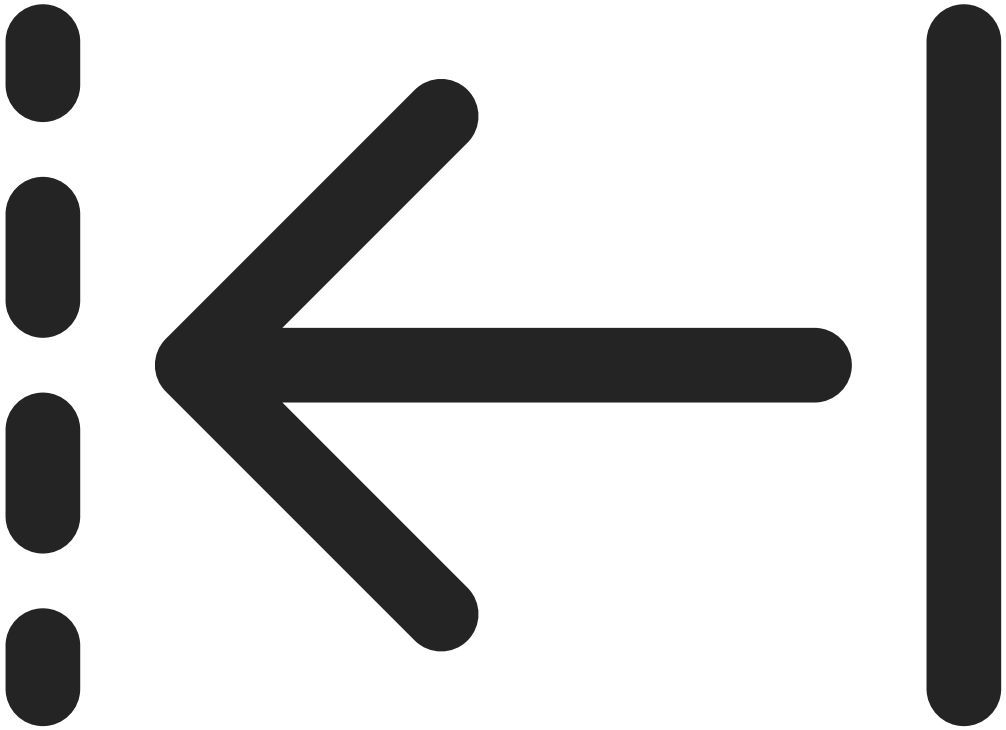
Dveře a zóny – na co se přístup vztahuje.

Harmonogramy – čas pro udělení přístupu.

Jestliže chcete přidat pravidlo přístupu:

1. Otevřete kartu Access Management (Správa přístupu).
2. Přejděte do nabídky **Cardholder Management** (Správa držitelů karet).

3. V části **Access rules** (Pravidla přístupu)



klikněte na položku **+ Add** (+ přidat).

4. Zadejte název pravidla přístupu a klikněte na tlačítko **Next** (Další).
5. Konfigurace držitelů karet a skupin:
   5.1. V části **Cardholders** (Držitelé karet) nebo **Groups** (Skupiny) klikněte na položku **+ Add** (+ přidat).
   5.2. Zvolte držitele karet nebo skupiny a klikněte na **Add** (Přidat).
   5.3. Držitele karty nebo skupinu můžete také přetáhnout přímo na pravidlo přístupu a tím jej na ně aplikovat. Při přetahování jsou zvýrazněna pravidla přístupu, na která lze přetahované položky umístit. Pokud přetáhnete více držitelů karet nebo skupin najednou, zobrazí se počet, kolik jich přesouváte.
6. Konfigurace dveří a zón:
   6.1. V části **Doors** (Dveře) nebo **Zones** (Zóny) klikněte na položku **+ Add** (+ přidat).
   6.2. Zvolte dveře nebo zóny a klikněte na **Add** (Přidat).
7. Konfigurace rozvrhů:
   7.1. V části **Schedules** (Rozvrhy) klikněte na **+ Add** (+ přidat).
   7.2. Zvolte jeden nebo více rozvrhů a klikněte na **Add** (Přidat).
8. Klikněte na **Save** (Uložit).

Pravidlo přístupu, kterému chybí jedna nebo více výše popsaných součástí, je neúplné. Všechna neúplná pravidla přístupu můžete zobrazit na kartě **Incomplete** (Neúplné).

Export zpráv o konfiguraci systému

Můžete exportovat zprávy, které obsahují různé typy informací o systému. AXIS Camera Station Pro Secure Entry exportuje zprávu jako soubor CSV (hodnoty oddělené čárkou) a uloží ji do výchozí složky pro stahování. Jestliže chcete exportovat zprávu:

1. Otevřete kartu Access Management (Správa přístupu).
2. Přejděte do nabídky **Reports** > **System configurations** (Zprávy > Konfigurace systému).
3. Vyberte zprávy, které chcete exportovat, a klikněte na **Download** (Stáhnout).

Zpráva o podrobnostech držitelů karet	Obsahuje informace o držitelích karet, přihlašovacích údajích, ověření karty a poslední transakci.
Zpráva o přístupu držitelů karet	Obsahuje informace o držitelích karet a informace o skupinách držitelů karet, pravidlech přístupu, dveřích a zónách souvisejících s držitelem karty souvisí.
Zpráva o přístupu skupiny držitelů karet	Obsahuje název skupiny držitelů karet a informace o držitelích karet, pravidlech přístupu, dveřích a zónách souvisejících se skupinou držitelů karet.
Zpráva o pravidlech přístupu	Obsahuje název pravidla přístupu a informace o držitelích karet, skupinách držitelů karet, dveřích a zónách souvisejících s pravidlem přístupu.
Zpráva o dveřním přístupu	Obsahuje název dveří a informace o držitelích karet, skupinách držitelů karet, pravidlech přístupu a zónách souvisejících s dveřmi.
Zpráva o zónovém přístupu	Obsahuje název zóny a informace o držitelích karet, skupinách držitelů karet, pravidlech přístupu a dveřích souvisejících se zónou.

Vytvářejte zprávy o aktivitách držitelů karet

Zpráva o nástupu obsahuje seznam držitelů karet v určité zóně a pomáhá určit, kdo je v danou chvíli přítomen.

Zpráva o shromažďování obsahuje seznam držitelů karet v určité zóně a pomáhá určit, kdo je v bezpečí a kdo je pohřešovaný během mimořádných událostí. Pomáhá správcům budov při hledání zaměstnanců a návštěvníků po evakuaci. Shromažďovací místo je určená čtečka, kde se personál hlásí při mimořádných událostech a kde se vytváří zpráva o osobách na místě i mimo něj. Systém označuje držitele karet jako nezvěstné, dokud se nepřihlásí na shromažďovacím místě nebo dokud je někdo ručně neoznačí jako v bezpečí.

Jak zpráva o nástupu tak zpráva o shromáždění vyžadují, aby zóny sledovaly držitele karet.

Vytvoření a spuštění zprávy o nástupu nebo shromáždění:

1. Otevřete kartu Access Management (Správa přístupu).

2. Přejděte do nabídky **Reports** > **Cardholder activity** (Přehledy > Aktivity držitelů karet).
3. Klikněte na **+ Add** (+ přidat) a vyberte **Roll call / Mustering** (Nástup / shromáždění).
4. Zadejte název zprávy.
5. Vyberte, které zóny mají být zahrnuty do zprávy.
6. Vyberte všechny skupiny, které chcete do zprávy zahrnout.
7. Pokud chcete zprávu o shromažďování, vyberte **Mustering point** (Místo shromažďování) a čtečku pro místo shromažďování.
8. Vyberte časový rámec pro zprávu.
9. Klikněte na **Save** (Uložit).
10. Vyberte zprávu a klikněte na **Run** (Spustit).

Stav zprávy o nástupu	Popis
Současnost	Držitel karty vstoupil do zadané zóny a neodešel před spuštěním zprávy.
Není přítomen	Držitel karty opustil zadanou zónu a nevstoupil do ní opět před spuštěním zprávy.

Stav zprávy o shromažďování	Popis
V bezpečí	Držitel karty přejel kartou na místě shromažďování.
Chybí	Držitel karty nepřejel kartou na místě shromažďování.

Import a export

Importovat držitele karet

Tato možnost importuje držitele karty, skupiny držitelů karty, přihlašovací údaje a fotografie držitelů karty ze souboru CSV. Chcete-li importovat fotografie držitelů karet, zkontrolujte, že server má k fotografiím přístup.

Při importování držitelů karet systém pro správu přístupu automaticky uloží konfiguraci systému včetně veškeré konfigurace hardwaru a odstraní jakoukoli dříve uloženou.

Můžete také mapovat uživatele v databázi služby Active Directory jako držitele karet, viz část *Nastavení služby Active Directory[BETA], on page 30*.

Možnosti importu	
Novinka	Tato možnost odebere stávající držitele karty a přidá nové držitele karty.
Aktualizovat	Tato možnost aktualizuje stávající držitele karty a přidá nové držitele karty.
Přidat	Tato možnost zachová stávající držitele karty a přidá nové držitele karty. Čísla karet a ID držitelů karet jsou jedinečná a lze je použít pouze jednou.

1. Na kartě **Access management** (Správa přístupu) klikněte na možnost **Import and export** (Import a export).
2. Klikněte na **Import cardholders** (Importovat držitele karet).
3. Zvolte možnost **New** (Nový), **Update** (Aktualizovat) nebo **Add** (Přidat).

4. Klikněte na tlačítko **Další**.
5. Klikněte na **Choose a file** (Vybrat soubor) a přejděte na soubor CSV. Klikněte na **Open** (Otevřít).
6. Zadejte oddělovač sloupců a vyberte jedinečný identifikátor a klikněte na **Next** (Další).
7. Přiřaďte každému sloupci nadpis.
8. Klikněte na **Import**.

Nastavení importu	
První řádek je záhlaví	Zvolte, jestliže soubor CSV obsahuje záhlaví se sloupci.
Oddělovač sloupců	Zadejte formát oddělovače sloupců pro soubor CSV.
Jedinečný identifikátor	Systém ve výchozím nastavení používá položku **Cardholder ID (ID držitele karty)** k identifikaci držitele karty. Můžete také použít křestní jméno a příjmení nebo e-mailovou adresu. Jedinečný identifikátor zabraňuje importu duplicitních záznamů o zaměstnancích.
Formát čísla karty	Ve výchozím nastavení je vybrána možnost **Allow both hexadecimal and number (Povolit hexadecimální i číselné)**.

Exportovat držitele karet

Tato možnost exportuje data držitelů karet v systému do souboru CSV.

1. Na kartě **Access management** (Správa přístupu) klikněte na možnost **Import and export** (Import a export).
2. Klikněte na **Export cardholders** (Exportovat držitele karet).
3. Vyberte umístění pro stahování a klikněte na **Save** (Uložit).

AXIS Camera Station Pro Secure Entry aktualizuje fotografie držitelů karet na adrese `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos` při každé změně nastavení.

Zrušit import

Při importování držitelů karet systém automaticky uloží svou konfiguraci. Možnost **Undo import** (Zrušit import) obnoví data držitelů karet a všechny hardwarové konfigurace do stavu, ve kterém byly před posledním importem držitelů karet.

1. Na kartě **Access management** (Správa přístupu) klikněte na možnost **Import and export** (Import a export).
2. Klikněte na **Undo import** (Zrušit import).
3. Klikněte na **Yes (Ano)**.

Nastavení správy přístupu

Přizpůsobení polí držitelů karet používaných v řídicím panelu pro správu přístupu:

1. Na kartě **Access management** (Správa přístupu) klikněte na tlačítko **Settings** > **Custom cardholder fields** (Nastavení > Vlastní pole držitele karty).
2. Klikněte na **+ Add** (+ přidat) a zadejte název. Můžete přidat až 6 vlastních polí.
3. Klikněte na **Přidat**.

Chcete-li k ověření vašeho systému řízení přístupu použít kód zařízení:

1. Na kartě **Access management** (Správa přístupu) klikněte na **Settings** > **Facility code** (Nastavení > Kód zařízení).
2. Vyberte možnost **Facility code on** (Kód zařízení zapnutý).

Poznámka

Při konfiguraci identifikačních profilů musíte také zvolit **Include facility code for card validation** (Zahrnout kód zařízení pro ověření karty). Viz část *Identifikační profily, on page 22*.

Úprava e-mailové šablony pro odeslání QR kódu nebo mobilních přihlašovacích údajů:

1. Na kartě **Access management** (Správa přístupu) klikněte na **Settings** > **Email templates** (Nastavení > Šablony e-mailů).
2. Upravte šablonu a klikněte na **Update** (Aktualizovat).

Šablony průkazů BETA

Šablony průkazů můžete přizpůsobit pomocí informací o držiteli karty, fotografií, log a vlastního brandingu. Vytvoření nové šablony:

1. Přejděte na **Access management > Settings > Badge templates** BETA (Správa přístupu > Nastavení > Šablony průkazů).
2. Klikněte na **Create new template** (Vytvořit novou šablonu).
3. Do pole **Template name** (Název šablony) zadejte název.
4. Chcete-li tuto šablonu nastavit jako výchozí, zvolte možnost **Use as default template for printing** (Použít jako výchozí šablonu pro tisk).
5. Přizpůsobení designu průkazu:
   - Vyberte až pět textových polí, která se mají zobrazit na přední straně, včetně všech vlastních polí, která jste vytvořili. Při tisku se na průkazu zobrazí pouze vyplněná pole.
   - Vyberte písmo a barvu textu.
   - Přidejte barvu nebo obrázek pozadí.
   - Nahrajte logo své organizace.
   - Na zadní stranu přidejte buď barvu pozadí, nebo obrázek.
6. Klikněte na **Save** (Uložit), abyste uložili změny, nebo na **Save as** (Uložit jako), abyste obsah uložili jako novou šablonu.

Poznámka

Jakmile je šablona vytvořena, nelze ji upravovat, pouze přejmenovat.

Vytisknutí průkazu BETA

Průkazy identifikace pro držitele karet můžete tisknout pomocí nastavených šablon průkazů. Upozorňujeme, že kódování karet není v současné době podporováno. Než začnete:

- Ujistěte se, že držitel karty má alespoň jednu kartu s přihlašovacími údaji. Bez přihlašovacích údajů nelze tisknout průkazy pro držitele karet.
- Potřebujete tiskárnu, která podporuje formát karet CR80 a kompatibilní tiskový materiál, jako je silný karton.
- Nastavte tiskové nastavení svého prohlížeče:
  1. Nastavte velikost stránky na CR80 nebo vlastní velikost odpovídající rozměrům vaší karty.
  2. Nastavte orientaci na výšku.
  3. Vypněte okraje nebo nastavte na minimum.

Důležité

Secure Entry funguje s tiskárnami, které mají ovladače pro Windows. Tiskárny řady HID Fargo jsou ověřeny jako funkční. Pokud potřebujete ovladač pro svou tiskárnu, obraťte se na dodavatele tiskárny.

Tisk průkazů:

1. Přejděte na **Access management > Cardholder management > Cardholders** (Správa přístupu > Správa držitelů karet > Držitelé karet).
2. Zvolte jednoho nebo více držitelů karet.
3. Klikněte na **Print badge** (Vytisknout průkaz) BETA.
4. Klikněte na **Select template** (Vybrat šablonu) a z rozevíracího seznamu **Template** (Šablona) vyberte šablonu průkazu, kterou chcete použít.
5. Pokud má držitel karty více údajů o kartě, vyberte jednu z rozevíracího seznamu **Card** (Karta).
6. Klikněte na **Print** (Tisk).

Poznámka

Pokud vaše tiskárna nepodporuje oboustranný tisk, vytiskněte nejprve všechny přední strany, poté otočte balíček karet a vložte je znovu do zásobníku, abyste mohli vytisknout zadní strany.

T10231644_cs

2026-04 (M7.2)