



ATEAS Security

dokumentace

ATEAS CZ

Na Dlouhém lánu 508/41 | 160 00 Praha 6 | Česká republika

www.ateas.net | info@ateas.net

KAPITOLA 1 - INSTALACE	14
1.1. OBECNÉ PŘEDPOKLADY	14
1.2. SHODNÝ POSTUP INSTALACE	15
1.3. SPECIFIKA ADMINISTRAČNÍHO SERVERU	18
1.4. SPECIFIKA KAMEROVÉHO SERVERU	19
1.5. INSTALAČNÍ SLOŽKA	20
1.6. PO INSTALACI	20
1.7. KONFIGURAČNÍ POLOŽKY ADMINISTRAČNÍHO SERVERU	21
1.8. KONFIGURAČNÍ POLOŽKY KAMEROVÉHO SERVERU	22
1.9. KONFIGURAČNÍ POLOŽKY KAMEROVÉHO KLIENTA	24
1.10. AUTOMATICKÉ AKTUALIZACE	24
1.11. INSTALACE MOBILNÍHO KLIENTA	26
1.12. INSTALACE NEURONOVÝCH SÍTÍ	27
1.13. INSTALACE DOPLŇKU PRO WEBOVÝ OBSAH	28
1.14. INSTALACE DALŠÍCH DOPLŇKŮ – LPR, UIC	29
1.15. IPV6 KOMPATIBILITA	29
KAPITOLA 2 - PRVNÍ SPOUŠTĚNÍ	30
2.1. PRVNÍ PŘIHLÁŠENÍ A ZADÁNÍ LICENČNÍHO KLÍČE	30
2.2. VÍCEFAKTOROVÉ OVĚŘENÍ	36
2.3. IDENTIFIKÁTOR ATEAS ID VAŠÍ INSTALACE	37
2.4. CERTIFIKOVANÉ INSTALACE	37
2.5. PRŮVODCE ZÁKLADNÍM NASTAVENÍM	39
2.6. VLASTNÍ NÁZVY PRO PŘIHLÁŠENÍ	41
2.7. INFORMACE O VERZI	42
2.8. INFORMACE O PMA	44
2.9. HLAVNÍ MENU APLIKACE	45
2.10. AUTOMATICKÉ STARTOVÁNÍ APLIKACÍ	46
2.11. VYHLEDÁVÁNÍ, FILTROVÁNÍ A ŘAZENÍ	46
2.12. PŘEJMENOVÁVÁNÍ POLOŽEK	47
2.13. KLIENTSKÝ TERMINÁLOVÝ PŘÍSTUP	48

2.14. PROTOKOLY	48
KAPITOLA 3 - POMOC	50
3.1. DOKUMENTACE A NÁPOVĚDA	50
KAPITOLA 4 - DOHLED	51
4.1. POHLEDY	51
4.1.1. SPRÁVA POHLEDŮ	51
4.1.2. VYHLEDÁVÁNÍ KAMER PODLE NÁZVU	62
4.1.3. ZOBRAZENÍ WEBOVÉHO OBSAHU	63
4.1.4. EDITOR ROZVRŽENÍ POHLEDŮ	64
4.1.5. ORGANIZACE POHLEDŮ	68
4.1.6. AUTOMATY	70
4.1.7. TÚRY	72
4.1.8. OTEVŘENÍ DALŠÍCH OKEN	75
4.2. UDÁLOSTI A POPLACHOVÝ POHLED	75
4.2.1. PŘÍJEM UDÁLOSTI	75
4.2.2. PŘÍJEM AKCÍ	78
4.2.3. PŘEPÍNÁNÍ UDÁLOSTÍ	79
4.2.4. ROZDĚLENÍ OKNA	79
4.2.5. SAMOSTATNÉ UDÁLOSTNÍ OKNO	79
4.2.6. ŘEŠENÍ POPLACHŮ	80
4.2.7. UDÁLOSTNÍ POZICE V DOHLEDOVÉM OKNĚ	82
4.3. ZÁZNAM POHLEDU	83
4.3.1. PŘEHRÁVÁNÍ POHLEDU	83
4.3.2. AUTOMATICKÉ PŘEHRÁVÁNÍ	88
4.3.3. STAŽENÍ ZÁZNAMU	88
4.3.4. VKLÁDÁNÍ ZÁLOŽEK	91
4.3.5. INTELIGENTNÍ VYHLEDÁVÁNÍ	92
4.3.6. VYHLEDÁVÁNÍ DLE PODOBNOSTI	95
4.3.7. OMEZENÍ PŘÍSTUPU K ZÁZNAMU	97
4.4. FUNKCE VYBRANÉ KAMERY	98
4.4.1. VÝBĚR KAMERY	98
4.4.2. ZOBRAZENÍ DETAILU	100

4.4.3. UKLÁDÁNÍ SNÍMKŮ	101
4.4.4. OVLÁDÁNÍ OTOČNÉ KAMERY	101
4.4.5. PTZ ZÁMKY	105
4.4.6. SPECIÁLNÍ PTZ FUNKCE	106
4.4.7. PREPOZIČNÍ BODY	107
4.4.8. AKTIVACE VÝSTUPŮ	108
4.4.9. PŘÍJEM ZVUKU	109
4.4.10. STISKNI A MLUV	110
4.4.11. DIGITÁLNÍ PŘIBLÍŽENÍ	112
4.4.12. RUČNÍ NAHRÁVÁNÍ	114
4.4.13. KOREKCE OBRAZU TYPU RYBÍ OKO	116
4.4.14. ZOBRAZENÍ METADAT	117
4.4.15. KONFIGURACE DETEKCE POHYBU A ANALÝZY UŽIVATELEM	119
4.5. PRÁCE S TRANSAKČNÍMI DATY	120
4.5.1. ŽIVÝ NÁHLED	120
4.5.2. PŘEHRÁVÁNÍ TRANSAKČÍ	120
4.5.3. ULOŽENÍ TRANSAKCE	121
4.6. SPOLUPRÁCE S MAPOVÝM OKNEM	122
4.6.1. SYNCHRONIZACE PŘI VÝBĚRU KAMER ČI PRVKŮ	122
4.6.2. SYNCHRONIZACE PŘI UDÁLOSTI	123
4.6.3. VÝBĚRY Z MAPY	124
4.7. PRÁCE S VIDEO STĚNOU	125
4.7.1. PŘEPÍNÁNÍ KAMER	125
4.7.2. ZOBRAZENÍ METADAT	127
4.7.3. PŘEPÍNÁNÍ URL	127
4.7.4. ZOBRAZENÍ DETAILU	128
4.7.5. POHLEDY VIDEO STĚNY	129
4.7.6. AUTOMATICKÝ REŽIM	130
4.8. PRÁCE S ČÍTAČI	133
4.8.1. ZÓNOVÉ ČÍTAČE	134
4.8.2. KOMPLEXNÍ ČÍTAČE	134
4.8.3. ZOBRAZENÍ HODNOTY ČÍTAČE	134
4.8.4. RUČNÍ RESET HODNOTY ČÍTAČE	135

4.8.5. UDÁLOSTNÍ RESET HODNOTY ČÍTAČE	136
4.8.6. ZÓNOVÉ ČÍTAČE V MAPĚ	136
4.8.7. HODNOTA ČÍTAČE VE WEBOVÉ STRÁNCE	137
4.9. PRÁCE S DATABÁZÍ OBLIČEJŮ	137
4.9.1. NÁHLED OBLIČEJŮ	137
4.9.2. DATABÁZE OBLIČEJŮ	138
4.9.3. VKLÁDÁNÍ OBRÁZKŮ	139
4.10. INFORMACE O VIDEU	140
KAPITOLA 5 - PRÁCE SE ZÁZNAMEM	141
5.1. VYHLEDÁVÁNÍ ZÁZNAMU	141
5.1.1. PŘEHLED ZÁZNAMU	141
5.1.2. ZOBRAZENÍ VIDEO PŘEHLEDŮ	143
5.1.3. NÁHLED A ULOŽENÍ ZÁZNAMU	146
5.2. META VYHLEDÁVÁNÍ	146
5.2.1. ZADÁNÍ KRITÉRIÍ	147
5.2.2. ZOBRAZENÍ VÝSLEDKŮ	151
5.2.3. ROZŠÍŘENÉ TEXTOVÉ VYHLEDÁVÁNÍ	151
5.2.4. EXPORTNÍ FUNKCE	154
5.2.5. GRAFY	155
5.2.6. AUTOMATICKÝ REPORTING	160
5.3. DENÍK POPLACHŮ	163
5.3.1. PROHLÍŽENÍ DENÍKU POPLACHŮ	163
5.3.2. EXPORT A TISK DENÍKU	166
KAPITOLA 6 - PRÁCE S MANAŽEREM STAHOVÁNÍ	168
6.1. ZÁKLADNÍ POPIS	168
6.2. SPRÁVA ÚKOLŮ	169
6.2.1. AUTOMATICKÉ PŘIDÁVÁNÍ ÚKOLŮ	169
6.2.2. RUČNÍ PŘIDÁVÁNÍ ÚKOLŮ	170
6.2.3. ČASOSBĚRNÁ VIDEA	171
6.2.4. OVLÁDÁNÍ SEZNAMU ÚKOLŮ	173
6.3. NASTAVENÍ STAHOVÁNÍ	174
KAPITOLA 7 - PRÁCE SE SNÍMKY	176

7.1. SPRÁVA SNÍMKŮ	176
7.1.1. PŘEHLED SNÍMKŮ	176
7.1.2. DOPLNĚNÍ ÚDAJŮ	178
7.1.3. TISK SNÍMKŮ	178
7.1.4. VYTVOŘENÍ NÁHLEDU NA SERVERU	180
KAPITOLA 8 - LOKÁLNÍ NASTAVENí	181
8.1. ZÁKLADNí NASTAVENí	181
8.1.1. JAZYKOVÉ PROSTŘEDí	182
8.1.2. MONITORY A OBRAZOVKY	183
8.1.3. UDÁLOSTI	185
8.1.4. MAPA	186
8.1.5. ZOBRAZENí VIDEA	188
8.1.6. PRACOVNí PROSTOR	192
8.1.7. AUTOMATICKÉ STARTOVÁNí	194
8.1.8. HISTORIE PŘIHLÁŠENí	196
8.1.9. ZOBRAZENí TEXTŮ	196
8.1.10. KLÁVESNICE	197
8.1.11. ZPRÁVY	198
8.1.12. VLASTNí INDIKÁTORY	198
8.2. NASTAVENí JOYSTICKU	199
8.2.1. ZÁKLADNí NASTAVENí	199
8.2.2. FUNKCE TLAČÍTEK	201
KAPITOLA 9 - DALŠí NÁSTROJE	203
9.1. OSOBNí HLÍDAČ	203
9.2. UŽIVATELSKÁ TLAČÍTKA	204
9.3. SEZNAMY ZNAČEK	206
KAPITOLA 10 - WEBOVý PŘÍSTUP	207
10.1. SPUŠTĚNí A PŘIHLÁŠENí DO SYSTÉMU	207
10.2. ŽIVý DOHLED	208
10.3. FUNKCE VYBRANÉ KAMERY	210
10.4. PRÁCE SE ZÁZNAMEM	212
10.4.1. PŘEHRÁVÁNí ZÁZNAMU	212

10.4.2. EXPORT ZÁZNAMU	213
10.5. NASTAVENÍ KLIENTA	213
KAPITOLA 11 - ADMINISTRACE SYSTÉMU	214
11.1. VSTUP DO ADMINISTRACNÍ SEKCE	214
11.2. SPRÁVA KAMER	216
11.2.1. AUTOMATICKÉ VYHLEDÁNÍ KAMER NA SÍTI	216
11.2.2. PŘIDÁVÁNÍ A ODEBÍRÁNÍ KAMER V SYSTÉMU	218
11.2.3. PODPORA GRABOVACÍCH KARET	229
11.2.4. ZÁKLADNÍ NASTAVENÍ KAMERY	230
11.2.5. NASTAVENÍ VIDEO	251
11.2.6. HROMADNÉ NASTAVENÍ A ODEBÍRÁNÍ KAMER	258
11.2.7. ZMĚNA ADRESY A PŘIHLÁŠENÍ	259
11.2.8. DETEKCE POHYBU NA SERVERU	260
11.2.9. NASTAVENÍ ZDROJŮ VIDEO ANALÝZY	264
11.2.10. LOKALIZACE ZÓN V MAPĚ	278
11.2.11. ANONYMIZACE VIDEO	279
11.2.12. STATICKE MASKY TVOŘENÉ NA SERVERU	280
11.2.13. VAZBA ZDROJŮ ANALÝZY NA PREPOZICE	280
11.2.14. PODROBNÉ NASTAVENÍ	281
11.2.15. UDÁLOSTI A JEJICH MANAGEMENT	282
11.2.16. DYNAMICKÉ ZDROJE A ZDROJE UDÁLOSTÍ ONVIF	303
11.2.17. HROMADNÉ NASTAVENÍ UDÁLOSTÍ	307
11.2.18. DYNAMICKÉ PLÁNOVÁNÍ UDÁLOSTÍ	308
11.2.19. SLOŽENÉ ZDROJE UDÁLOSTÍ	310
11.2.20. UMÍSTĚNÍ KAMERY DO MAPY	316
11.2.21. EXPORT A IMPORT KAMER	319
11.3. VLASTNÍ UDÁLOSTI A TYPY OBJEKTŮ	320
11.3.1. VLASTNÍ UDÁLOSTI	320
11.3.2. SYSTÉMOVÉ NÁZVY VLASTNÍCH UDÁLOSTÍ	323
11.3.3. ŘÍZENÍ UDÁLOSTÍ	324
11.3.4. VLASTNÍ TYPY OBJEKTŮ	324
11.4. PLÁNOVANÉ UDÁLOSTI	325
11.4.1. ZÁKLADNÍ NASTAVENÍ	325

11.4.2. ŘÍZENÍ UDÁLOSTÍ	328
11.5. REŽIM ŘEŠENÍ POPLACHŮ	329
11.5.1. PRINCIP A AKTIVACE REŽIMU	329
11.6. SPRÁVA ZÁZNAMU	330
11.6.1. ZÁZNAMOVÉ OBLASTI	330
11.6.2. ZÁZNAMOVÉ PROFILY	344
11.6.3. ZÁLOHOVÁNÍ	351
11.7. SPRÁVA POHLEDŮ	355
11.7.1. SDÍLENÍ POHLEDŮ	355
11.7.2. SYSTÉMOVÉ SDÍLENÉ SKUPINY POHLEDŮ	356
11.7.3. VIDEO STĚNA	356
11.8. SPRÁVA MODULU DETEKCE RZ	361
11.8.1. VÝBĚR KAMER PRO DETEKCI	361
11.8.2. NASTAVENÍ MASKY	367
11.8.3. PRÁCE SE SEZNAMY RZ	368
11.8.4. NASTAVENÍ ROZPOZNÁVÁNÍ RZ	371
11.8.5. INTEGRACE DO SYSTÉMU ŘÍZENÍ UDÁLOSTÍ	372
11.9. SPRÁVA MODULU DETEKCE UIC	373
11.9.1. VÝBĚR KAMER PRO DETEKCI	373
11.9.2. INTEGRACE DO SYSTÉMU ŘÍZENÍ UDÁLOSTÍ	377
11.10. SPRÁVA UŽIVATELŮ A SERVERŮ	378
11.10.1. ZÁKLADNÍ SPRÁVA SERVERŮ	378
11.10.2. CLOUDOVÝ REŽIM PŘIPOJENÍ KAMEROVÉHO SERVERU	385
11.10.3. POUŽITÍ DOMÉNOVÉHO NÁZVU PRO KAMEROVÝ SERVER	387
11.10.4. GPU AKCELERACE VE SLUŽBĚ SERVERU	387
11.10.5. SPUŠTĚNÍ NEURONOVÉ SÍTĚ NA SERVERU	389
11.10.6. SPRÁVA CLUSTERŮ	394
11.10.7. SMTP ÚČTY	397
11.10.8. CERTIFIKACE ZAŘÍZENÍ	397
11.10.9. NOTIFIKACE	399
11.10.10. ZÁLOHA A OBNOVA KONFIGURACE	401
11.10.11. PODPORA DLNA VYSÍLÁNÍ	404
11.10.12. MIGRACE NA NOVÉ SERVERY	407

11.10.13. SPRÁVA UŽIVATELŮ	407
11.10.14. SPRÁVA SKUPIN	424
11.10.15. PRINCIP ČTYŘ OČÍ	425
11.10.16. UŽIVATELSKÁ POLITIKA	426
11.10.17. INTEGRACE UŽIVATELŮ S EXTERNÍMI ZDROJI	429
11.10.18. ZPŮSOBY AUTENTIZACE	433
11.10.19. FUNKCE ATEAS INTERLOGIN	435
11.10.20. TISKOVÉ SESTAVY	437
11.10.21. SYSTÉMOVÝ LOG	437
11.10.22. PODPORA STANDARDU SYSLOG	441
11.11. PROPOJENÍ	442
11.11.1. VIRTUÁLNÍ STRUKTURA OBJEKTŮ	442
11.11.2. VYTVÁŘENÍ UDÁLOSTNÍCH SCÉNÁŘŮ	446
11.11.3. UMÍSTĚNÍ PRVKU DO MAPY	448
11.11.4. KOMUNIKAČNÍ KANÁLY	448
11.11.5. SÍŤOVÝ KANÁL TCP A HTTP	449
11.11.6. SÍŤOVÝ KANÁL SNMP	451
11.11.7. WEBOVÁ SLUŽBA AKV	453
11.11.8. INTEGRAČNÍ KANÁL SIA	454
11.11.9. FILTROVÁNÍ IP ADRES	456
11.11.10. UŽIVATELSKÁ TLAČÍTKA	456
11.11.11. INTEGRACE DOKUMENTŮ	460
11.12. LICENCE A AKTIVACE	462
11.12.1. LICENČNÍ KLÍČE A JEJICH AKTIVACE	462
11.12.2. ROZŠIŘOVÁNÍ SYSTÉMU	465
11.12.3. AKTIVACE NOVÝCH VERZÍ	465
11.12.4. AUTOMATICKÁ REAKTIVACE LICENCÍ	466
KAPITOLA 12 - PŘEHRÁVAČ	468
12.1. SPUŠTĚNÍ PŘEHRÁVAČE	468
12.2. PŘEHRÁVÁNÍ VIDEA VE FORMÁTU ATS	469
12.2.1. OTEVŘENÍ SLOŽKY	469
12.2.2. SEZNAM SOUBORŮ	471
12.2.3. PŘEHRÁVÁNÍ SOUBORU	472

12.2.4. INDEXOVANÉ SLOŽKY	478
12.2.5. KOREKCE OBRAZU TYPU RYBÍ OKO	479
12.2.6. EXPORT VIDEA	480
12.2.7. EXPORT VIDEA DO AVI	481
12.2.8. EXPORT VIDEA DO MP4	484
12.3. DIGITÁLNÍ PODPIS	485
12.4. VLASTNOSTI SOUBORU	487
KAPITOLA 13 - MAPOVÉ OKNO	490
13.1. ZÁKLADY MAPOVÉHO OKNA	490
13.2. DISTRIBUCE MAPOVÝCH PODKLADŮ	492
13.3. ZÁKLADNÍ PRÁCE S MAPOU	493
13.3.1. POSUNY A ZOOMOVÁNÍ MAPY	493
13.3.2. PŘEPÍNÁNÍ ÚROVNÍ	495
13.3.3. VYHLEDÁVÁNÍ V MAPĚ	496
13.4. DALŠÍ MAPOVÉ FUNKCE	496
13.5. DYNAMICKÁ MAPOVÁ VRSTVA A NÁHLED VIDEA V MAPĚ	498
13.6. ZOBRAZENÍ MAPY PŘÍMO V DOHLEDOVÉM OKNĚ	502
13.7. GEOGRAFICKÉ PROPOJENÍ MAPOVÝCH ÚROVNÍ	504
KAPITOLA 14 - PŘÍSTUP ZE ZAŘÍZENÍ APPLE	506
14.1. PODPOROVANÉ FUNKCE	506
14.2. SPUŠTĚNÍ A PŘIHLÁŠENÍ	506
14.3. SEZNAM KAMER A ŽIVÉ VIDEO	509
14.4. POHLEDY VÍCE KAMER	511
14.5. PŘEHRÁVÁNÍ ZÁZNAMU	512
14.6. NASTAVENÍ	515
14.7. VYUŽITÍ INTEGROVANÉ KAMERY	517
KAPITOLA 15 - PŘÍSTUP ZE ZAŘÍZENÍ ANDROID	519
15.1. PODPOROVANÉ FUNKCE	519
15.2. SPUŠTĚNÍ A PŘIHLÁŠENÍ	519
15.3. SEZNAM KAMER A ŽIVÉ VIDEO	521
15.4. POHLEDY VÍCE KAMER	523
15.5. PŘEHRÁVÁNÍ ZÁZNAMU	523

15.6. NASTAVENÍ	525
15.7. NOTIFIKACE	527
15.8. VYUŽITÍ INTEGROVANÉ KAMERY	528
15.9. ANDROID TV	530
15.9.1. VIDEO STĚNA	531
KAPITOLA 16 - APLIKACE PRO MONITORING OBRAZOVKY	532
16.1. INSTALACE A ZPROVOZNĚNÍ	532
16.2. NASTAVENÍ	534
KAPITOLA 17 - PŘÍLOHA 1 – KONFIGURACE SÍTĚ	536
17.1. ADMINISTRAČNÍ SERVER	536
17.2. KAMEROVÝ SERVER	536
KAPITOLA 18 - PŘÍLOHA 2 – ATEAS API	538
18.1. PRINCIP KOMUNIKACE	538
18.2. ATEAS API PRO ADMINISTRAČNÍ SERVER	539
18.2.1. EXTERNÍ UDÁLOSTI	539
18.2.2. VIDEO STĚNA	539
18.2.3. REGISTRAČNÍ ZNAČKY	541
18.2.4. DATABÁZE OBLIČEJŮ	542
18.2.5. SPRÁVA UŽIVATELŮ A SKUPIN	549
18.2.6. SPRÁVA ZAŘÍZENÍ	554
18.2.7. NOTIFIKACE UDÁLOSTÍ	558
18.2.8. NOTIFIKACE PŘIHLÁŠENÍ	562
18.3. ATEAS API PRO KAMEROVÝ SERVER	563
18.3.1. EXTERNÍ UDÁLOSTI	563
18.3.2. METADATA	564
18.4. PARAMETRICKÉ SPOUŠTĚNÍ APLIKACÍ	565
18.4.1. ADMINISTRAČNÍ SERVER	565
18.4.2. KAMEROVÝ SERVER	565
18.4.3. KAMEROVÝ KLIENT	566
KAPITOLA 19 - PŘÍLOHA 3 – EXTERNÍ ANALYTICKÁ DATA	568
19.1. PŘEDPOKLADY	568

19.2. INTEGRACE SE SYSTÉMEM VTRACK	568
19.2.1. PŘIPOJENÍ METADAT ZE SERVERU	568
19.2.2. PŘIPOJENÍ METADAT Z KAMERY	569
19.2.3. PROPOJENÍ UDÁLOSTÍ	570
KAPITOLA 20 - PŘÍLOHA 4 – ZDROJE OPENSTREETMAP	572
20.1. TVORBA MAP Z VOLNÝCH MAPOVÝCH ZDROJŮ	572
20.1.1. VÝBĚR ÚZEMÍ A STAŽENÍ DAT	572
20.1.2. PŘEVOD DAT	573
20.1.3. POUŽITÍ DAT	573
20.1.4. PODPORA RŮZNÝCH ÚROVNÍ DETAILŮ	574
20.2. TVORBA MAP Z RASTROVÝCH PODKLADŮ	574
KAPITOLA 21 - PŘÍLOHA 5 – JSON INTEGRACE DAT	576
21.1. PŘEDPOKLADY	576
21.2. INTEGRACE APLIKACE CAMMRA	576
21.2.1. PŘÍJEM METADAT PŘES TCP	576
21.2.2. PŘÍJEM METADAT PŘES HTTP	576
21.2.3. METADATA A UDÁLOSTI	577
21.2.4. GRAFICKÉ VÝSTUPY	577
KAPITOLA 22 - PŘÍLOHA 6 – INTEGRACE AXIS BODY WORN	578
22.1. PROPOJENÍ SE SERVEREM ATEAS	578
22.2. PŘIDÁNÍ KAMER A UŽIVATELŮ	581
22.3. PROVOZ SYSTÉMU	582
KAPITOLA 23 - PŘÍLOHA 7 – CERTIFIKÁTY	583
23.1. ÚVOD	583
23.2. PŘEDPOKLADY	583
23.3. CERTIFIKÁTY	586
23.3.1. ACME PROTOKOL	587
23.3.2. WILDCARD CERTIFIKÁTY	588
23.4. POUŽITÍ EXISTUJÍCÍHO CERTIFIKÁTU ORGANIZACE	589
23.4.1. ZÍSKÁNÍ CERTIFIKÁTU	589
23.4.2. EXPORT CERTIFIKÁTU	590

23.4.3. NASAZENÍ CERTIFIKÁTU	591
23.4.4. ÚPRAVA DNS ZÁZNAMU	591
23.4.5. TEST CERTIFIKÁTU	592
23.5. POUŽITÍ NOVÉHO CERTIFIKÁTU	593
23.5.1. VYTVOŘENÍ KOŘENOVÉHO CERTIFIKÁTU	594
23.5.2. VYTVOŘENÍ CERTIFIKÁTU SERVERU	595
23.5.3. NASAZENÍ CERTIFIKÁTU	598
23.5.4. PŘEDBĚŽNÝ TEST CERTIFIKÁTU	598
23.5.5. PROKÁZÁNÍ PŮVODU SERVERU	600
23.5.6. ZÁVĚREČNÝ TEST CERTIFIKÁTU	603

Kapitola 1 - Instalace

1.1. Obecné předpoklady

Produkty systému ATEAS Security vyžadují pro své fungování operační systém od společnosti Microsoft. Celá instalace produktů ATEAS Security je snadná a zabere pouze několik minut. Pro provedení instalace je zapotřebí být do systému Windows přihlášen jako administrátor. Pokud to bude instalátor vyžadovat, bude nutné nainstalovat rozhraní Microsoft .NET 4. generace a to ve verzi alespoň 4.8. Pro ATEAS Screen Recoder postačí .NET verze 4.0, což umožňuje jeho instalaci na starší počítače.

POZNÁMKA

Ve většině případů je rozhraní .NET již součástí Vašeho operačního systému.

Se systémem ATEAS Security můžete využívat komfortu v podobě automatických aktualizací aplikací. Při upgrade systému tak stačí z prostředí klienta stáhnout a nainstalovat nové administrační jádro systému (ATEAS Administrator) a ostatní aplikace budou aktualizovány automaticky).

V každé edici produktu ATEAS Security je nutné provést instalaci třech základních aplikací ATEAS Security:

1. ATEAS Security Administrator – systémový server ATEAS Security, slouží k centrálnímu přihlašování do systému a centrálnímu řízení událostí.
2. ATEAS Security Server – kamerový server ATEAS Security, slouží ke komunikaci s kamerami a video servery, řízení toků videa a zvuku směrem ke klientům, provádí záznam a vyhodnocování událostí v systému.
3. ATEAS Security Observer – klientská aplikace ATEAS Security, je jedinou aplikací v systému s uživatelským rozhraním sloužící k plnému přístupu k systému a jeho administraci (kompletně nastavuje chování serverů, kamer, záznamu apod.).

Kromě těchto aplikací je možné do systému instalovat i dodatečné nadstavbové moduly či komponenty např. aplikaci ATEAS Screen Recorder emulující kameru na běžném počítači nebo ATEAS Security LPR Engine pro detekci RZ vozidel.

V edici HOME se provádí instalace obou serverových aplikací na jeden cílový počítač. Klientskou aplikaci je možné instalovat kdekoliv, taktéž samozřejmě přímo na počítač, kde jsou nainstalovány serverové aplikace. Oproti edici PROFESSIONAL je však omezen současný přístup do systému na dva přístupy.

V edici PROFESSIONAL se zpravidla instaluje ATEAS Administrator a ATEAS Server na dedikovaný počítač (server) pro kamerový systém, na kterém bude probíhat záznam a řízení a vyhodnocování událostí. ATEAS Observer se poté instaluje na příslušný počet klientských stanic, které budou mít systému přístup.

V edici UNLIMITED je instalace stejná jako v případě edice PROFESSIONAL s tím, že je možné produkt ATEAS Server instalovat na další dodatečné počítače (servery), ke kterým jsou připojeny další kamery a zařízení.

1.2. Shodný postup instalace

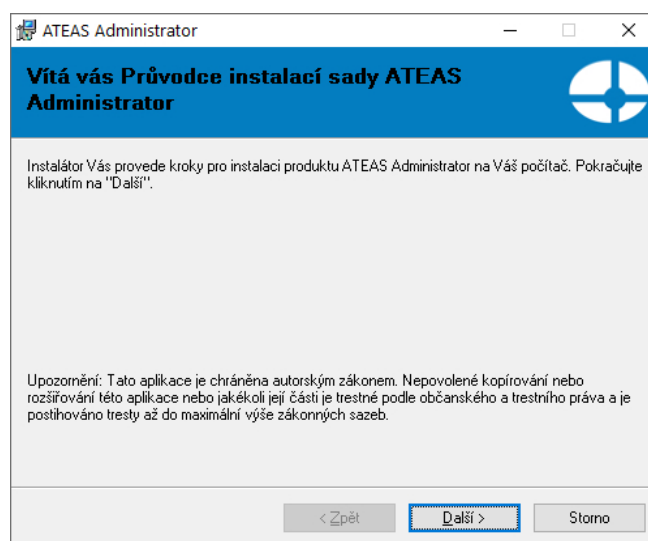
Všechny tři uvedené aplikace se instalují zcela analogicky se stejným instalačním průvodcem. Odkazy na instalaci všech těchto aplikací včetně dalších důležitých odkazů naleznete přímo na stránce, která se automaticky otevře po vložení či připojení instalačního média. K dispozici jsou tyto odkazy:

- úvodní kapitola dokumentace produktu o instalaci systému,
- instalace administračního serveru systému,
- instalace kamerového serveru systému,
- instalace kamerového klienta systému,
- přístup na klienty iOS a Android v příslušných obchodech (zdarma),
- instalace aplikace pro monitoring počítače.

Kamerové servery, klientské aplikace a všechny další aplikace je možné též instalovat pohodlně z webového rozhraní administračního serveru. Oproti odkazům přímo na úvodní stránce instalačního média jsou zde navíc i odkazy na důležité dokumenty, kompletní dokumentaci k produktu v tiskové kvalitě a ukázkovou aplikaci pro ATEAS API.

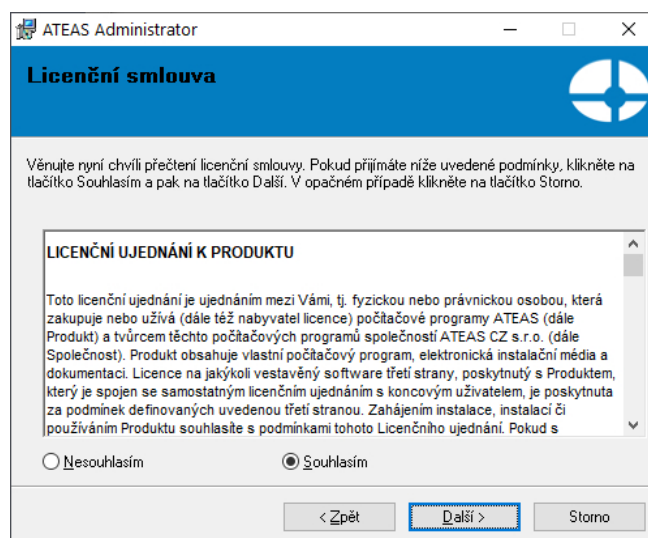
Pořadí, v jakém budete tyto tři produkty instalovat, je libovolné. Zde si ukážeme průběh instalačního průvodce pro ATEAS Security Administrator, u zbylých dvou aplikací je průběh zcela analogický s několika málo drobnými změnami, které jsou popsány dále v této kapitole.

Krok 1 – Úvítací obrazovka instalátoru.



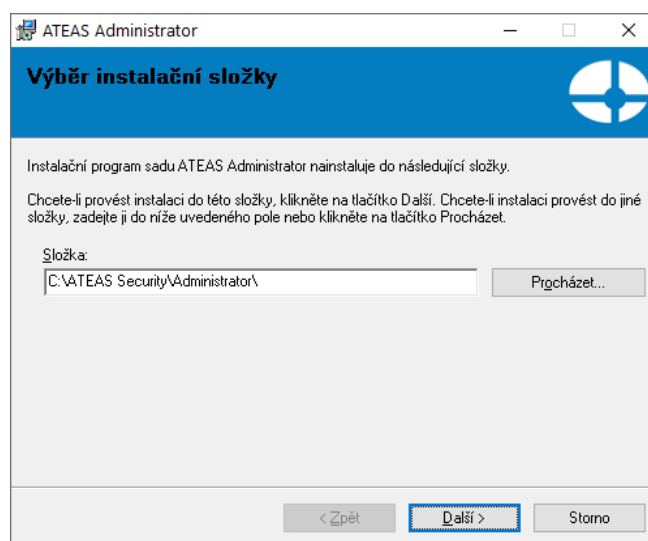
V instalaci pokračujte stisknutím tlačítka **DALŠÍ**.

Krok 2 – Licenční ujednání.



Označte volbu Souhlasím a v instalaci pokračujte stisknutím tlačítka **DALŠÍ**.

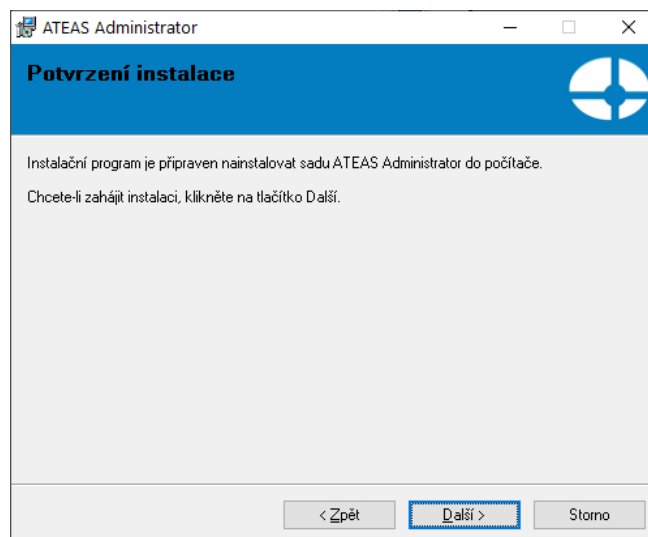
Krok 3 – Výběr instalační složky.



V této části instalátoru je nutné vybrat cílovou složku, kam bude aplikace nainstalována. Změnu disku provedete nejjednodušším způsobem tak, že přepíšete úvodní písmeno v textovém poli složka.

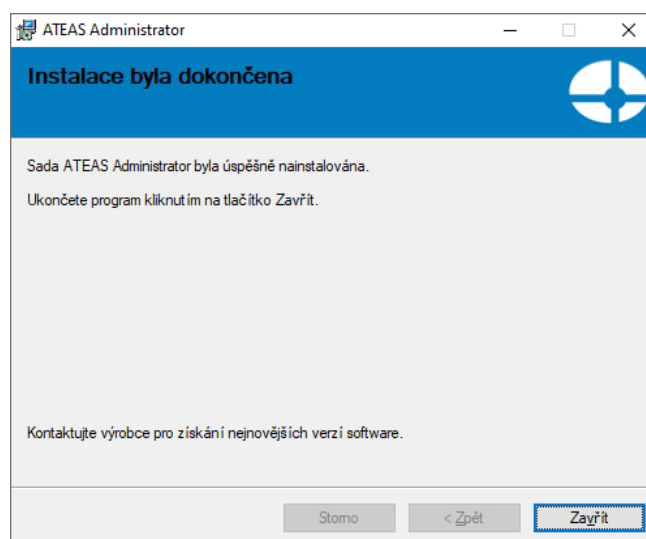
V instalaci pokračujte stisknutím tlačítka **DALŠÍ**.

Krok 4 – Potvrzení instalace.



V instalaci pokračujte stisknutím tlačítka **DALŠÍ**.

Krok 5 – Dokončení instalace.



Tlačítkem **ZAVŘÍT** je instalace dokončena.

1.3. Specifika administračního serveru

Při instalaci administračního serveru se ještě před zahájením samotné instalace zobrazuje doplňkový dialog, který upozorňuje na skutečnost, že při aktualizaci systému na novější verzi nebude možné systém aktivovat pokud není aktivní služba ATEAS PMA. Před zahájením aktualizace je tedy nutné se ujistit, že pro dané ATEASID byla aktivována služba ATEAS PMA.

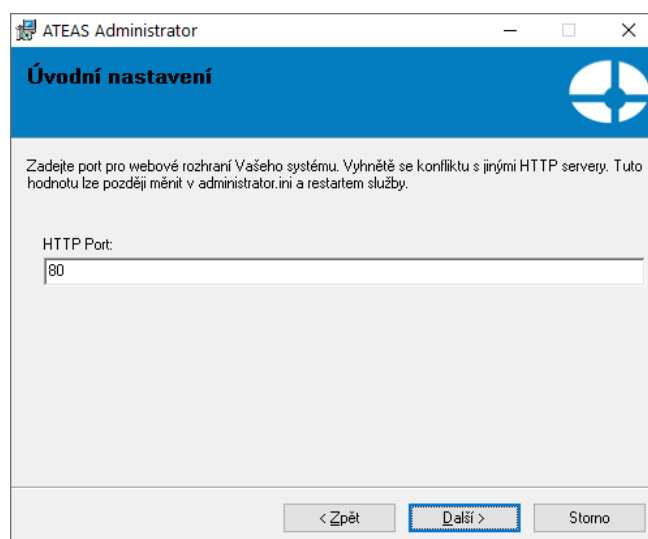
POZNÁMKA

Ve zkušební verzi lze nové verze produktu instalovat bez omezení.

V průběhu instalace administračního serveru se zobrazí dialog, ve kterém můžete zadat číselnou hodnotu pro HTTP port, na kterém bude administrační port komunikovat s webovými prohlížeči. Přes tento port nepovede jiná komunikace, používané porty pro řídicí či datovou komunikaci naleznete v příloze. Přes webový prohlížeč lze však na zadaném portu pohodlně nainstalovat či stáhnout klientskou aplikaci pro přístup do systému a není tak nutné používat CD.

POZNÁMKA

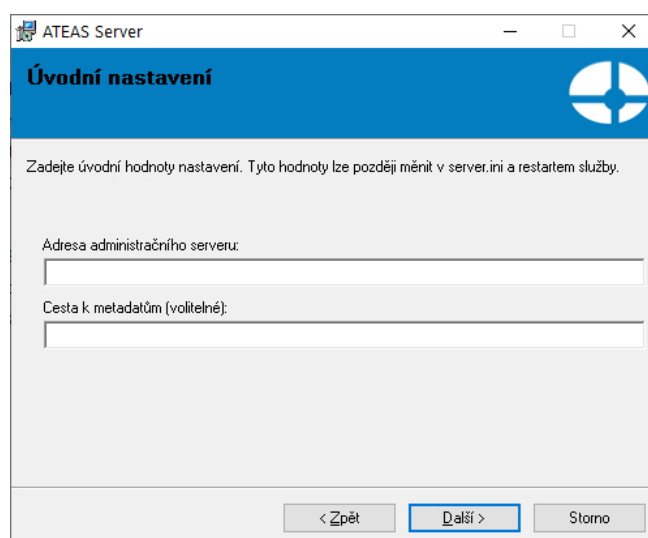
Pomocí webového prohlížeče lze stáhnout či nainstalovat i kamerový server, jeho připojení do systému však může provést pouze administrátor systému.



Implicitní hodnota portu HTTP je 80. V takovém případě lze na administrační server z webového prohlížeče přistoupit přímo přes jeho adresu např. 10.0.0.1. Pokud bude použit jiný port, je nutné ho doplnit do adresy v prohlížeči (např. 10.0.0.1:999). HTTP port by neměl být obsazen žádným jiným webovým serverem jako je Apache či IIS atd. V budoucnu lze tuto hodnotu změnit v souboru administrator.ini v klíči HTTPPORT v instalačním adresáři a restartem služby ATEAS Administrator.

1.4. Specifika kamerového serveru

V průběhu instalace kamerového serveru budete dotázáni na adresu či název (jméno počítače či DNS) administračního serveru. Každý kamerový server musí být připojen k administračnímu serveru, který je vždy v systému pouze jeden.



Pro vyplnění adresy platí následující pravidla a doporučení:

Edice HOME a PROFESSIONAL: Adresa administračního serveru je shodná a s adresou kamerového serveru, neboť jsou obě serverové aplikace instalovány na jeden počítač (server). Vyplňte tedy lokální IP adresu počítače nebo serveru (např. 10.0.0.1 nebo 192.168.1.1 atd.).

Edice UNLIMITED: V edici UNLIMITED může existovat neomezené množství kamerových serverů kdekoli v lokální či propojené síti či internetu. Vyplňte adresu, na které je možné provést spojení s administračním serverem. Touto adresou může být adresa v lokální síti či např. WAN adresa směrovače s NAT, který přesměruje komunikaci na administrační server.

POZNÁMKA

Pro fungování serverových služeb v prostředí s NAT viz příloha o síťových portech, které musí být pro aplikace ATEAS Security otevřeny.

V budoucnu lze tuto hodnotu změnit v souboru server.ini v klíči ADMIN v instalačním adresáři a restartem služby ATEAS Server.

Volitelně je možné již během instalace nastavit, že metadata analýzy videa budou ukládána do vlastního umístění. I toto umístění je možné v budoucnu změnit v souboru server.ini.

1.5. Instalační složka

Výchozím umístěním pro instalaci serverů je složka ATEAS Security na systémovém disku. Toto umístění však lze během instalace změnit. U klienta je výchozím umístěním pro instalaci systémová složka pro 64-bitové aplikace. Každý účet Windows má pak samostatnou datovou složku se svým nastavením, exporty či mapami, a to opět v systémové složce pro uživatelská data aplikací.

TIP

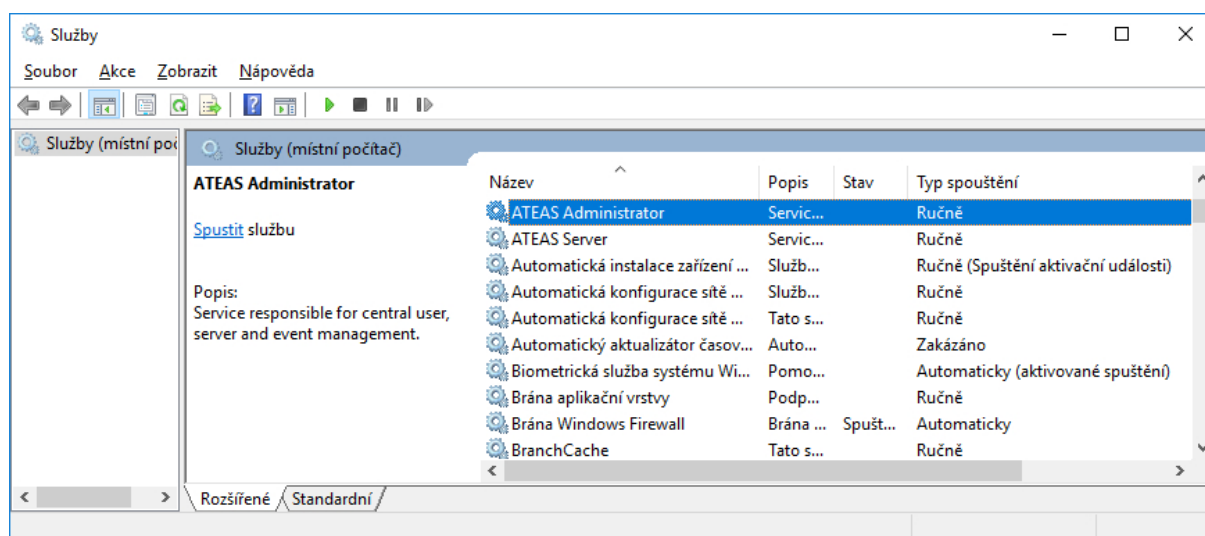
Každý uživatel tak může mít své vlastní automatické přihlášení dle svého Windows účtu.

1.6. Po instalaci

Serverové aplikace (ATEAS Administrator a ATEAS Server) budou ve Vašem počítači nebo na Vašem serveru existovat jako služby (services), které nemají žádné uživatelské ovládání. Veškeré ovládání,

správa systému a nastavení jsou již prováděny z prostředí klientské aplikace ATEAS Observer, pro kterou instalátor automaticky vytvoří v nabídce Start programovou skupinu ATEAS Security a v ní příslušného zástupce. Zástupce pro spuštění klientské aplikace je také umístěn přímo na plochu.

Po instalaci jsou obě serverové aplikace spuštěny automaticky a jejich spouštění je nastaveno na automaticky (viz následující obrázek). To znamená, že obě aplikace jsou nastartovány automaticky při startu systému Windows (nezávisle na tom, jestli se do systému přihlásí uživatel) a jsou též automaticky ukončeny při ukončení systému Windows.



Do služeb se v systému Windows dostanete takto:

Česká verze operačního systému: Start – Ovládací panely – Nástroje pro správu – Služby.

Anglická verze operačního systému: Start – Control panel – Administrative tools – Services.

1.7. Konfigurační položky administračního serveru

Konfigurační položky administračního serveru jsou umístěné v souboru administrator.ini v instalační složce administračního serveru. Jejich změna je možná přímo v tomto souboru pomocí libovolného textového editoru. Po změně vždy musí následovat restart služby administračního serveru.

Položka HTTPPORT (implicitně 80): Tato položka je automaticky nastavena na hodnotu zadanou v průběhu instalace a udává port, na kterém administrační server zobrazuje domovskou stránku Vašeho kamerového systému, provozuje webového klienta a řídí automatické aktualizace v systému.

Položka HTTPSPORT (implicitně 443): Tato položka udává port, na kterém administrační server zobrazuje domovskou stránku Vašeho kamerového systému a provozuje webového klienta při použití zabezpečené verze protokolu http.

Položka WEBCLIENT (implicitně OFF): Povoluje nebo zakazuje webový přístup do systému (hodnota OFF nebo ON).

Položka WEBFORCETLS (implicitně OFF): Pokud je hodnota nastavena na ON, budou citlivé části webového obsahu povinně používat https protokol. To se týká např. provozu webového klienta či fungování automatických aktualizací serverů a klientů. Pro tuto funkci musí být řádně zprovozněn certifikát. Postup nasazení je součástí této dokumentace.

Položka SERVICEUSER (implicitně nepoužito): Udává uživatelské jméno při přihlášení služby.

Položka SERVICEPASSWORD (implicitně nepoužito): Obsahuje v šifrované podobě heslo pro přihlášení služby.

Položka REALTIME (implicitně 0): Nastavením na hodnotu 1 bude služba spuštěna s maximální prioritou procesu. To umožňuje překonat některá úsporná nastavení hardware, pokud služba nedostává dostatek procesorového času pro zpracování paketů ze sítě.

POZNÁMKA

Položky pro přihlášení služby jsou účinné při reinstalaci služby, nikoliv pouze při jejím restartu. Implicitní přihlášení služby je pod místním systémovým účtem Local System.

1.8. Konfigurační položky kamerového serveru

Konfigurační položky kamerového serveru jsou umístěné v souboru server.ini v instalační složce kamerového serveru. Jejich změna je možná přímo v tomto souboru pomocí libovolného textového editoru. Po změně vždy musí následovat restart služby kamerového serveru.

Položka ADMIN (implicitně 127.0.0.1): Udává název nebo adresu administračního serveru v systému, ke kterému se má daný kamerový server připojovat a jehož má být součástí. Tato hodnota je automaticky nastavena na hodnotu zadanou v průběhu instalace.

Položka METADATAPATH (implicitně nepoužito): Udává plnou cestu k umístění, kam bude server ukládat metadata při analýze videa a pro forenzní vyhledávání. Ve výchozím stavu to bude přímo v instalační složce serveru.

Položka SERVICEUSER (implicitně nepoužito): Udává uživatelské jméno při přihlášení služby.

Položka SERVICEPASSWORD (implicitně nepoužito): Obsahuje v šifrované podobě heslo pro přihlášení služby.

Položka WANKEY (implicitně nepoužito): Tato položka definuje unikátní klíč kamerového serveru při cloudovém režimu připojení kamerového serveru.

Položka HTTPPORT (implicitně 8080): Udává port http serveru služby kamerového serveru, který může být využit některými systémy jako je třeba stažení dat z nositelných kamer.

Položka HTTPUSER (implicitně root): Udává uživatelské jméno pro přihlášení k http serveru.

Položka HTTPPASS (implicitně pass): Udává heslo pro přihlášení k http serveru.

Položka REALTIME (implicitně 0): Nastavením na hodnotu 1 bude služba spuštěna s maximální prioritou procesu. To umožňuje překonat některá úsporná nastavení hardware, pokud služba nedostává dostatek procesorového času pro zpracování paketů ze sítě.

Položka DECODESTRICTMODE (implicitně 1): Udává, jak striktně se postupuje při dekódování videa. Hodnota 0 obsahuje pouze výkonově nenáročnou kontrolu bitstreamu a povoluje algoritmy opravy poškození. Hodnota 1 přidává některé dodatečné kontroly rozsahu paměťových operací a vypíná většinu algoritmů opravy videa, hodnota 2 přidává podrobnější kontrolu bitstreamu a hodnota 3 požaduje plnou kompatibilitu se standardy vč. případů, kdy by odstranění chyby bylo bez následku. Hodnoty 2 a 3 mohou znamenat navýšení spotřeby výkonu. Hodnota ovlivňuje dekódování H264/5 na CPU. Dekódování na GPU a AV1 video nejsou ovlivněny.

Položka LOCALIP (implicitně nepoužito): V praxi lze použít pro výběr správného síťového rozhraní pro připojení k administračnímu serveru systému, tak aby mohl být kamerový server správně identifikován. Je to však nutné pouze v neobvyklých případech, kdy kamerový server nemůže použít síťových rozhraní určit automaticky. Více také viz kapitola Více síťových karet v počítači.

Položka MULTICASTSOURCEIP (implicitně nepoužito): Pomocí této položky je možné určit síťové rozhraní pro multicastové vysílání. Více také viz kapitola Více síťových karet v počítači.

Položka DLNA (implicitně nepoužito): Tato položka určuje síťové rozhraní pro vysílání videa pomocí standardu DLNA. Pokud není vyplněno, je rozhraní vybráno automaticky.

Položka FORCEDSERVERID (implicitně nepoužito): Běžně jsou kamerové servery v systému identifikovány pomocí jejich adres a získají tak jednoznačné číslo v systému, které přiřadí administrátor. Při připojení více serverů z jedné adresy může být nutné je odlišit pomocí této položky.

POZNÁMKA

Položky pro přihlášení služby jsou účinné při reinstalaci služby, nikoliv pouze při jejím restartu. Implicitní přihlášení služby je pod místním systémovým účtem Local System.

1.9. Konfigurační položky kamerového klienta

Konfigurační položky kamerového klienta jsou umístěné v souboru observer.ini v instalační složce klienta. Jejich změna je možná přímo v tomto souboru pomocí libovolného textového editoru. Po změně vždy musí následovat restart klienta.

Položka MUTEXLEVEL (implicitně 1): Udává, že je použit systémový objekt typu mutex pro zabránění dvojího spuštění klienta. Pokud je klient spuštěn v terminálovém režimu (např. pomocí technologie virtualizace pracovních stanic za využití GPU akcelerace), může být v závislosti na zvolené hloubce virtualizace nutné tuto ochranu vypnout nastavením na hodnotu 0. Více také viz kapitoly o GPU akceleraci.

Položka DECODESTRICTMODE (implicitně 1): Udává, jak striktně se postupuje při dekódování videa. Hodnota 0 obsahuje pouze výkonově nenáročnou kontrolu bitstreamu a povoluje algoritmy opravy poškození. Hodnota 1 přidává některé dodatečné kontroly rozsahu paměťových operací a vypíná většinu algoritmů opravy videa, hodnota 2 přidává podrobnější kontrolu bitstreamu a hodnota 3 požaduje plnou kompatibilitu se standardy vč. případů, kdy by odstranění chyby bylo bez následku. Hodnoty 2 a 3 mohou znamenat navýšení spotřeby výkonu. Hodnota ovlivňuje dekódování H264/5 na CPU. Dekódování na GPU a AV1 video nejsou ovlivněny.

1.10. Automatické aktualizace

Instalace aplikací ATEAS Security velmi snadná a rychlá s podporou komfortu automatických aktualizací systému. Automatické aktualizace probíhají jak na kamerových serverech (služba ATEAS Server), tak i pro klienty systému (ATEAS Observer). Při aktualizaci celého systému je tak možné pouze reinstalovat administrační jádro systému (ATEAS Administrator) a zbytek systému bude

aktualizován automaticky. Novou verzi systému (administračního serveru) lze získat buď přímo z instalačního média ATEAS, které je k dispozici ve formátu ISO, nebo ji lze stáhnout přímo z dialogu kontroly nové verze systému, více viz kapitola Informace o verzi dále v textu.

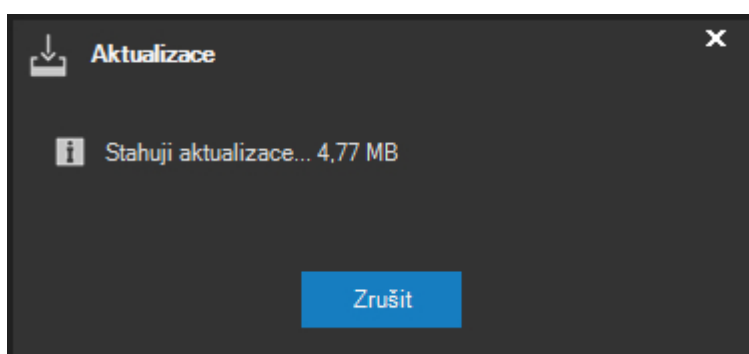
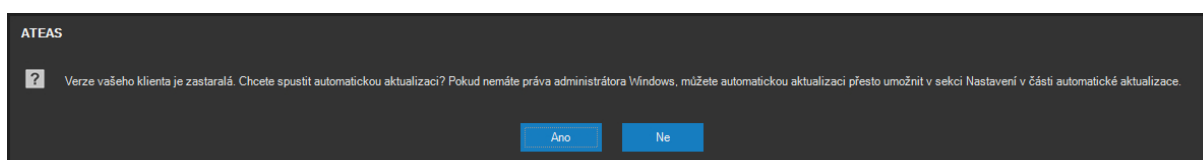
POZNÁMKA

Při reinstalaci administračního serveru systému je automaticky nahrazena starší verze produktu, není nutné provádět ruční odinstalaci.

Kamerové servery, které jsou po dobu instalace administračního jádra odpojeny (bez přerušení základních funkcí), jsou po automatickém znovu připojení k administračnímu serveru schopny stáhnout a spustit aktualizaci a obnovit provoz.

Automatické aktualizace nejvíce ulehčí práci na větších systémech s mnoha klienty nebo u UNLIMITED edicí s mnoha kamerovými servery, které se po aktualizaci administračního jádra aktualizují a restartují samy.

Klienti systému jsou při reinstalaci administračního jádra odpojeni a musí se znovu přihlásit do systému. Po přihlášení je klient schopen stáhnout a spustit automatickou aktualizaci. Automatická aktualizace klienta je doprovázena uživatelským rozhraním.



POZOR

Aby mohla automatická aktualizace úspěšně proběhnout, je nutné, aby byl na administračním serveru dostupný port pro HTTP komunikaci, po kterém jsou aktualizace stahovány. Tento port (viz příloha o portech) je implicitně nastaven na 80 a lze ho změnit v souboru administrator.ini.

POZNÁMKA

Pokud se jedná o počítač zařazený ve video stěně (tj. je na něm aktuálně přihlášen uživatel vytvořený jako účet video stěny), aktualizace bude zahájena automaticky bez nutnosti potvrzení zprávou tlačítkem **ANO**, neboť počítače video stěny často nemusí mít připojena periferní zařízení.

1.11. Instalace mobilního klienta

Aplikace pro mobilní přístup k systému je možné spustit či instalovat pomocí odkazů na instalačním CD anebo na adrese administračního serveru Vašeho systému.

Aplikace pro iOS vyžaduje operační systém iOS, kterým jsou osazena zařízení od společnosti Apple - iPhone, iPad. Aplikace je spuštěna po kliknutí do online obchodu s aplikacemi pro iOS (App Store). Aplikace je k dispozici zdarma.

Aplikace pro OS Android vyžaduje operační systém Android, kterým jsou osazena nejrůznější zařízení typu chytrých telefonů a tabletů. Aplikace je spuštěna po kliknutí do online obchodu s aplikacemi pro Android (Google Play). Aplikace je k dispozici zdarma.

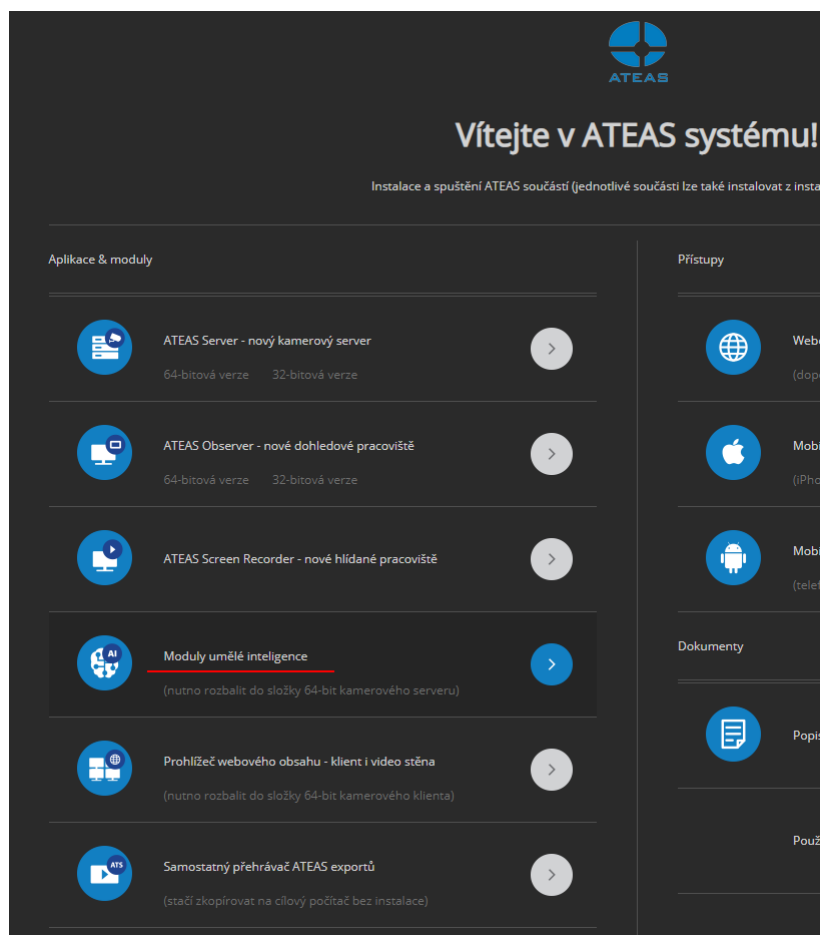
Aplikace pro Android může být také instalována do zařízení typu televize či displej s operačním systémem Android s ovládáním pomocí dálkového ovladače anebo jako součást video stěny. K instalaci může být použito stejné APK jako v případě mobilního telefonu či tabletu. Pokud aplikace detekuje, že je spuštěna v zařízení typu televize či displej, automaticky zvolí optimalizované uživatelské rozhraní.

POZNÁMKA

Některé Android displeje nemají implementovanu možnost být rozpoznán jako displej a aplikace se spustí s rozhraním pro telefon. V takovém případě je třeba pro instalaci použít APK, které obsahuje pouze rozhraní pro televize a displeje.

1.12. Instalace neuronových sítí

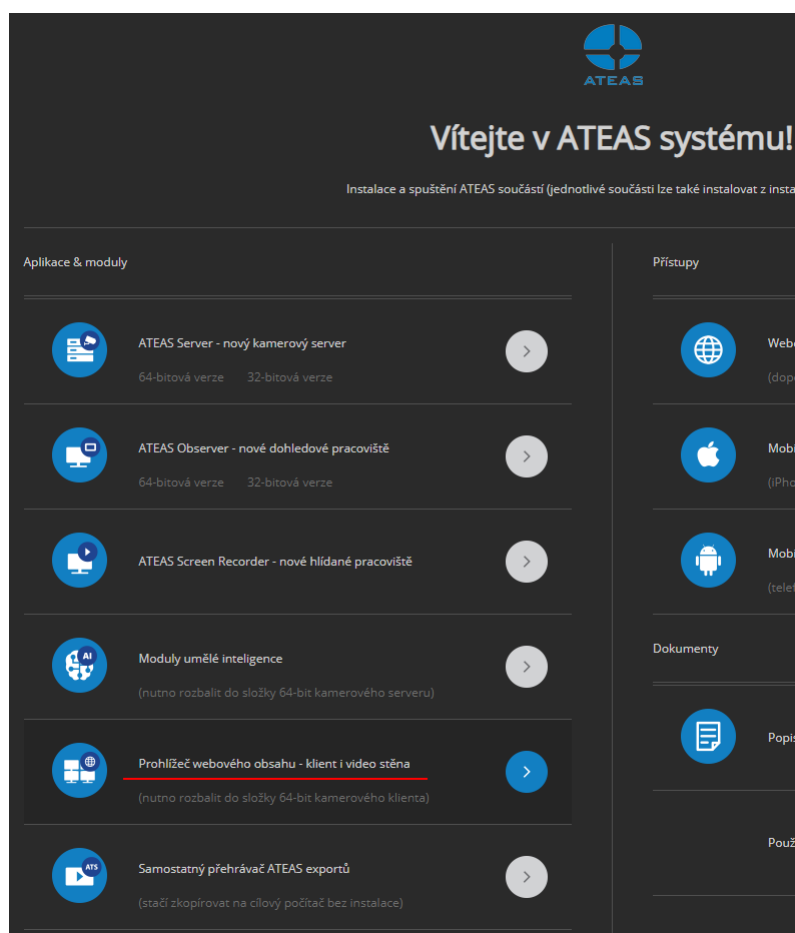
Instalaci neuronové sítě lze provést velmi jednoduše tak, že stáhneme archiv přímo z webu administračního serveru systému a provedeme jeho rozbalení do instalační složky kamerového serveru, který má být umělou inteligencí a možností analýzy vybaven.



Po instalaci je pak možné pokračovat v administraci serverů pomocí tlačítka **DNN**.

1.13. Instalace doplňku pro webový obsah

ATEAS klient anebo i video stěna mohou kromě kamer zobrazit také libovolný webový obsah. K tomu však musí být do klienta instalován doplněk webového prohlížeče dostupný z webu administračního serveru.



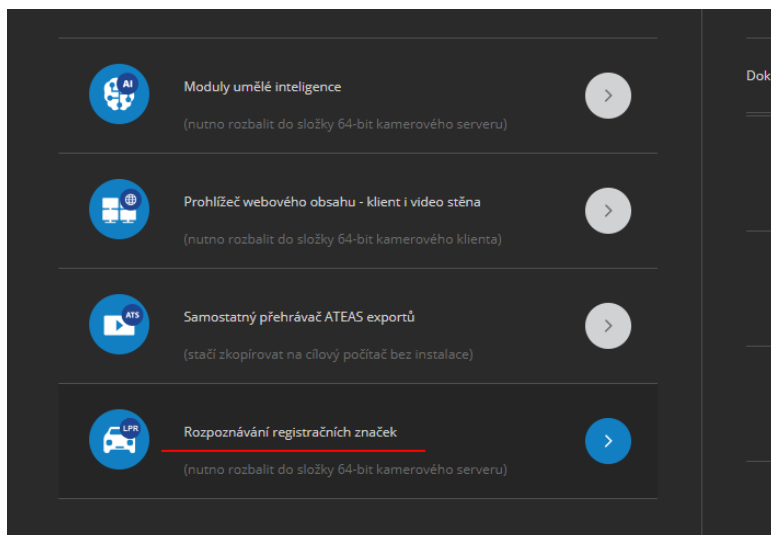
Archiv musí být rozbalen do instalační složky klienta ATEAS.

POZNÁMKA

Webový doplněk může být používán jen s 64-bit edicí klienta a nemůže být použit pro monitory s operačním systémem Android, které mohou být součástí video stěny.

1.14. Instalace dalších doplňků – LPR, UIC

Instalaci dalších doplňků jako je rozpoznávání registračních značek vozidel, rozpoznávání UIC identifikátorů vagónů a dalších lze provést jednoduchým rozbalením archivu do instalační složky kamerového serveru. Odkazy na příslušné doplňky jsou k dispozici na hlavní webové stránce Vašeho administračního serveru. Následující obrázek zobrazuje odkaz na modul rozpoznávání RZ vozidel.



Po instalaci je pak možné pokračovat v administraci doplňků.

POZNÁMKA

Funkce rozpoznávání registračních značek vozidel či dalších modulů mohou vyžadovat dodatečnou licenci.

1.15. IPv6 kompatibilita

Aktuální nedostatek veřejných IPv4 adres je hlavním hnacím motorem pro postupující rozvoj využití adres IPv6. V oblasti kamerových systémů se přechod na IPv6 jako první dotkne samotných uživatelů přistupujících do systému z IPv6 (mobilních) sítí, ve kterých IPv4 adresy již nebudou zařízením vůbec přidělovány. Z tohoto důvodu ATEAS pro komunikaci mezi jednotlivými prvky systému (uživatelé, servery, kamery) podporuje též protokol IPv6.

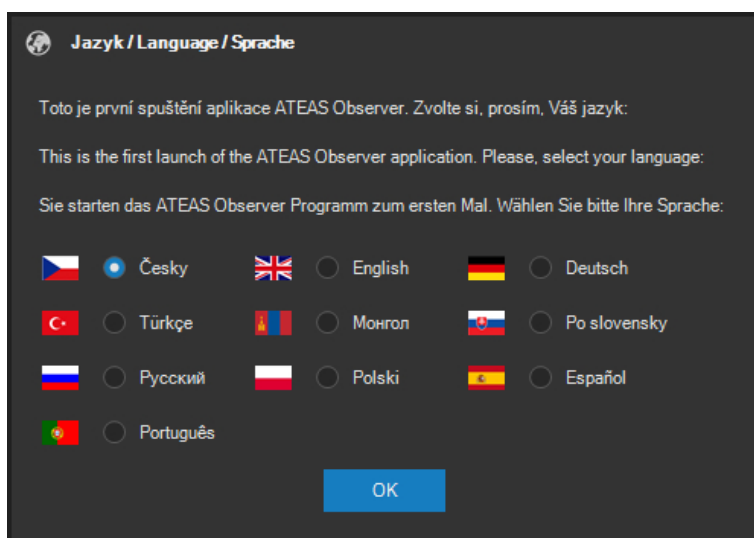
Kapitola 2 - První spouštění

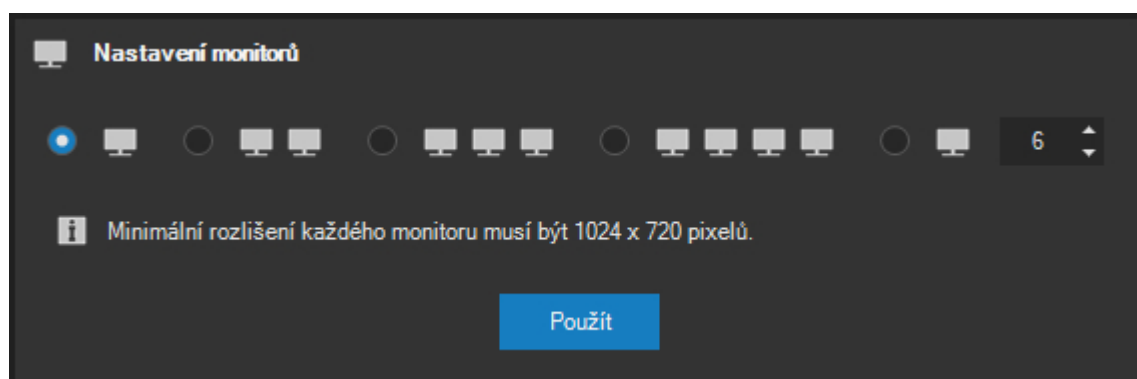
2.1. První přihlášení a zadání licenčního klíče

POZNÁMKA

Pro více informací o aktivaci licence a získání aktivačního klíče si přečtěte subkapitolu Aktivace produktu a upgrade licenčního klíče (součástí administrační části). Pokud ještě nemáte systém aktivován, je tato dokumentace dostupná na adrese Vašeho administračního serveru (přes internetový prohlížeč). Subkapitola obsahuje také zajímavé informace pro hackery.

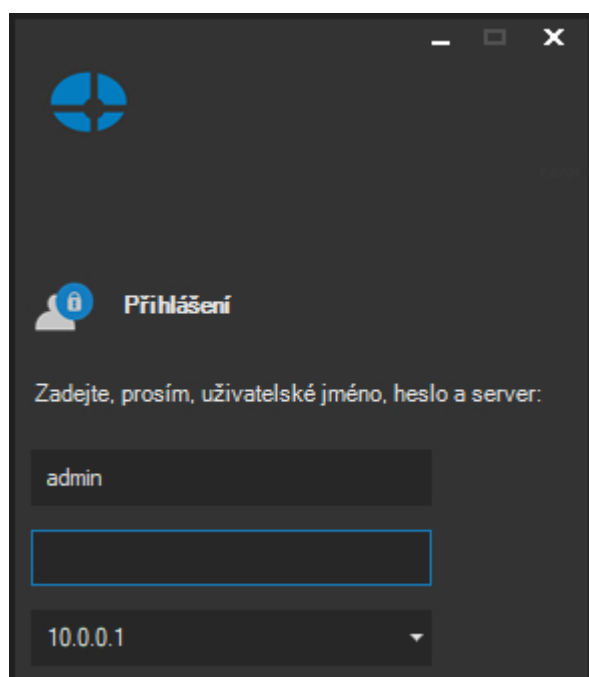
Při prvním spouštění aplikace na dané stanici jsou vyvolány dialogy pro základní nastavení aplikace ještě před jejím spuštěním, to se týká nastavení jazyka a počtu monitorů. V obou případech je zapotřebí vybrat některou z nabízených možností (jazyk může být předvybrán dle nastavení operačního systému) a pokračovat tlačítkem **OK** nebo **POUŽÍT**. Více o nastavení monitorů se dozvíte v části o lokálním nastavení aplikace, kde lze tyto volby kdykoliv změnit.



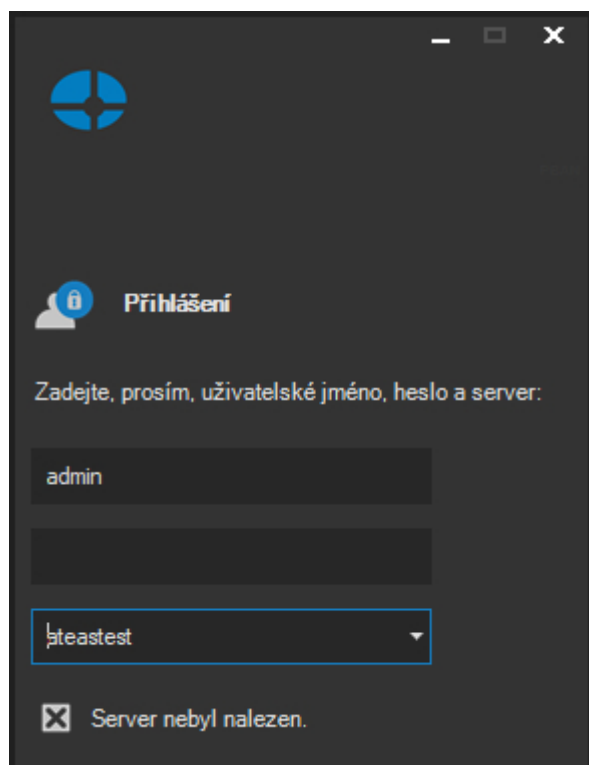


Po spuštění klientské aplikace ATEAS Security Observer bude systém vyžadovat zadání uživatelského jména, hesla a serveru pro přihlášení. V systému je předdefinován administrátorský účet **admin** s heslem **admin**. Systém neakceptuje shodu uživatelského jména a hesla a vynutí si při prvním přihlášení změnu hesla na jiné. Do pole server je možné zadat IP adresu nebo název serveru, kde je zprovozněn administrační server ATEAS Security. Po úspěšném přihlášení je název nebo adresa serveru uložena a není nutné ji příště znovu zadávat.

Klientská aplikace si pamatuje poslední přihlášení a při opětovném přihlášení je nejen automaticky vyplněna hodnota serveru pro přihlášení, ale také je k dispozici seznam naposledy použitých serverů. Ze seznamu je možné vybrat libovolnou položku anebo je možné využít automatického doplňování při psaní z klávesnice. Rozbalovací seznam je vždy seřazen podle data přihlášení k serverům a to sestupně od naposledy použitých názvů či adres.



Pokud se Vám nepodaří přihlásit do systému, aplikace vždy zobrazí důvod neúspěšného přihlášení, jak ukazuje následující obrázek:



Mezi nejčastější důvody pro neúspěšné přihlášení do systému patří:

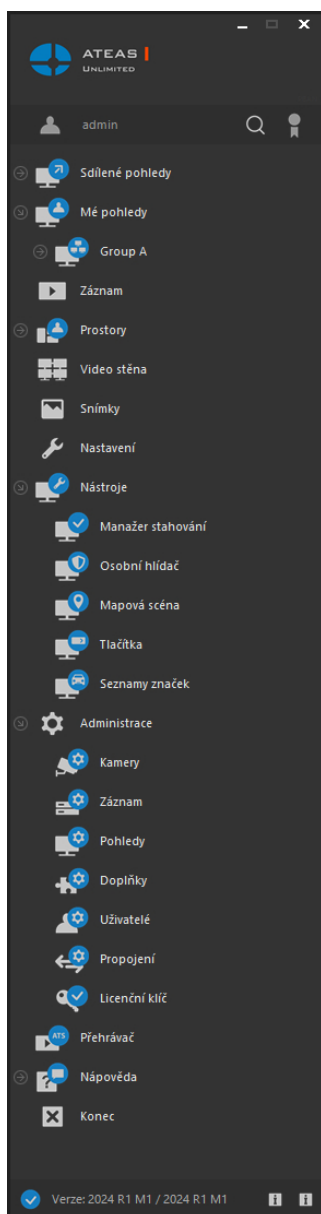
- chybně zadané uživatelské jméno anebo heslo, u hesel jsou vždy rozlišována velká a malá písmena,
- chybná adresa nebo název serveru,
- problémy s připojením do sítě,
- překročení limitu současných přístupů do systému dle aktuální licence,
- neplatná (stará) verze klientské aplikace,
- duplicitní přihlášení (s možností odhlásit sám sebe z jiného desktop klienta).

Systém neakceptuje shodu uživatelského jména a hesla a vynutí si tudíž po Vašem prvním přihlášení pod účtem admin změnu Vašeho administrátorského hesla (stejně tak si vynutí změnu hesla uživatelem po jeho resetu administrátorem nebo při prvním přihlášení u nového uživatelského účtu). Pro nové heslo do systému platí některá pravidla, která je nutné mít na paměti:

- minimální délka hesla je 4 znaky (pokud administrátor systému neupravil uživatelskou politiku tak, aby minimální délka byla vyšší nebo aby požadované heslo bylo silné),
- u hesel se rozlišují velká a malá písmena,

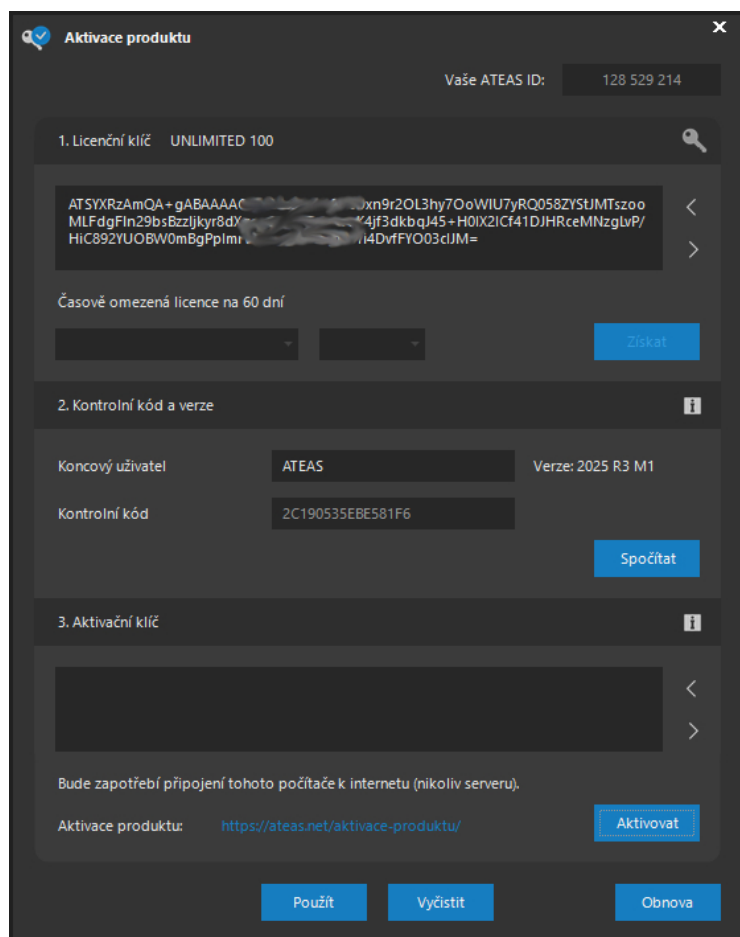
- není možné zadat heslo shodné s uživatelským jménem (bez respektu na velká a malá písmena).

Po úspěšném přihlášení se objeví hlavní nabídka aplikace, zobrazí se logo odpovídající aktuálně instalované edici produktu (HOME, PROFESSIONAL, UNLIMITED) a ve spodní části se objeví indikátor spojení s administračním serverem.



Spojení ke všem kamerovým serverům a k administračnímu serveru jsou udržována automaticky a při rozpadu se obnovují, spojení k administračnímu serveru je indikováno symbolem v levém spodním rohu v okně hlavní nabídky.

Po prvním spuštění klientské aplikace administrátorem je nutné do systému zadat licenční číslo, které umožní další práci.



Do části Licenční klíč je nutné zadat Vámi zakoupené licenční číslo produktu. Toto licenční číslo je možné zkopírovat nebo vložit přímo z licenčního souboru, který byl přiložen k aktivačnímu e-mailu. Vložení licenčního klíče přímo ze souboru lze provést pomocí tlačítka s bílou šipkou. Více informací naleznete v části dokumentace o aktivaci produktu v plné verzi tohoto dokumentu, který je též k dispozici na adrese Vašeho administračního serveru.

Nemáte-li zakoupené licenční číslo, je možné automaticky získat zkušební licenci na 60 dní. K tomu stačí vybrat edici, počet kamer a použít tlačítko **ZÍSKAT**. Z testovací licence je možné kdykoliv přejít na zakoupenou licenci bez časového omezení.

POZOR

Licenci v systému není možné ponížít na nižší edici nebo nižší počet kamer. Na to je třeba pamatovat, pokud plánujete pozdější přechod na zakoupenou licenci.

Po zadání licenčního čísla je nutné zadat název koncového uživatele této licence a tlačítkem **SPOČÍTAT** vygenerovat kontrolní kód.

POZOR

Název koncového uživatele musí být uveden dle skutečnosti. Název si mohou uživatelé systému zobrazit a v případě nesouladu by měli žádat o zjednání nápravy. Systém s nepravdivým označením koncového uživatele je považován za nesprávně licencovaný.

POZNÁMKA

Název koncového uživatele je opatřením na zvýšení bezpečnosti poskytování licencí. Vyplněné názvy uživatelů nejsou výrobcem nijak monitorovány či ukládány a při aktivaci systému nejsou přenášeny na licenční server.

POZNÁMKA

Kromě názvu koncového uživatele licence jsou součástí výpočtu kontrolního kódu také základní vlastnosti počítače, kde je instalován administrační server systému.

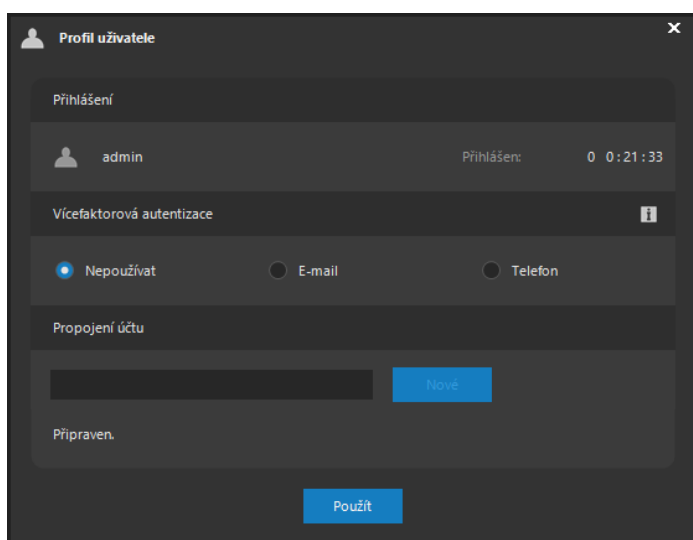
Kromě licenčního čísla je třeba také získat aktivační klíč a to buď online pomocí tlačítka **AKTIVOVAT** nebo pomocí odkazů uvedených ve spodní části okna. V každém případě je však nutný přístup k internetu a k serverům ATEAS (nikoliv však nutně z počítačů s nainstalovaným programovým vybavením ATEAS).

V licenčním dialogu se nachází také tlačítko **OBNOVA**, pomocí kterého je možné obnovit konfiguraci systému po jeho čisté instalaci. Více o zálohách nastavení a jejich obnově se dozvíte v kapitole o správě serverů.

Tlačítkem **ZRUŠIT** lze ukončit tento dialog bez zadání licenčního čísla.

2.2. Vícefaktorové ověření

Administrátor systému může jako součást uživatelské politiky aktivovat možnost či povinnost vícefaktorového ověření uživatele. V takovém případě má uživatel možnost (či k tomu bude přinucen) kliknutím na své uživatelské jméno v hlavním okně zobrazit dialog vícefaktorového ověření.



V horní části dialogu je zobrazen údaj o době, po kterou je uživatel v systému přihlášen. Pro aktivaci vícefaktorového ověření je nutné vybrat jednu z podporovaných (a administrátorem povolených) metod a tlačítkem **NOVÉ** zahájit proces propojení.

V případě e-mailové adresy je nutné kliknout na odkaz v zaslaném ověřovacím e-mailu. V případě mobilního ověření je nutné se přihlásit z mobilní aplikace. V dialogu je vždy zobrazen zbývajících čas pro potvrzení propojení.

POZOR

Nástroj vícefaktorového ověření je účinnou obranou před vyzrazením přihlašovacích údajů vždy pouze v případě, že je druhý faktor nastaven ještě před vyzrazením, nikoliv až poté.

Jakmile je propojení vytvořeno, bude při vícefaktorovém přihlášení vždy nutné potvrdit odkaz v zaslaném ověřovacím e-mailu anebo potvrdit přihlášení v mobilní aplikaci. Mobilní aplikace vždy zobrazí uživatelské jméno, adresu klienta a systému a čas přihlášení spolu s tlačítky **POTVRDIT** a **IGNOROVAT**.

TIP

V operačním systému iOS lze notifikaci odbavit i bez spuštění aplikace přidržením notifikace a zobrazením možností.

2.3. Identifikátor ATEAS ID Vaší instalace

Po zadání licenčního klíče a aktivaci systému se v pravém horním rohu licenčního dialogu zobrazí identifikátor ATEAS ID. Tento identifikátor je jedinečným a trvalým označením Vaší kopie software a měl by být používán pro veškeré technické a procesní záležitosti týkající se Vaší instalace. ATEAS ID je vždy devítimístný numerický identifikátor.

Používání ATEAS ID ulehčuje též evidenci Vašich instalací, pokud jste instalační firma, neboť ATEAS ID zůstává nezměněné při všech běžných úkonech se systémem:

- Při rozšíření systému dochází ke změně licenčního klíče (a tím i aktivačního klíče), nicméně přidělené ATEAS ID zůstává stále shodné.
- Při přesunu systému na jiný hardware a deaktivaci licence dochází ke změně kontrolního kódu pro Vaši licenci (a tím i aktivačního klíče), nicméně přidělené ATEAS ID zůstává stále shodné.
- Při přechodu na novou verzi systému dojde při reaktivaci nové verze ke změně aktivačního klíče, nicméně ATEAS ID zůstává stále shodné.

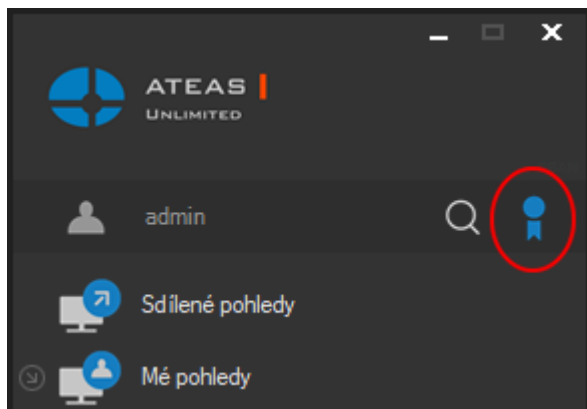
2.4. Certifikované instalace

Vaše instalace může být certifikovaná. To znamená, že byla provedena instalační firmou splňující předpoklady pro provedení certifikované instalace, ke kterým patří zejména absolvování autorizovaných administrátorských školení ATEAS v různých úrovních. Instalační certifikát je generován a automaticky nahrán do systému během aktivace licenčního čísla. Certifikát má formu XML souboru nahraného v podsložce certificates v instalační složce Vašeho administračního serveru.

POZNÁMKA

Při ruční aktivaci licenčního čísla na webu ATEAS je certifikát generován také a je vytvořen odkaz na jeho stažení. Tento soubor pak musí být umístěn do výše zmíněné složky. Následovat musí restart administračního serveru.

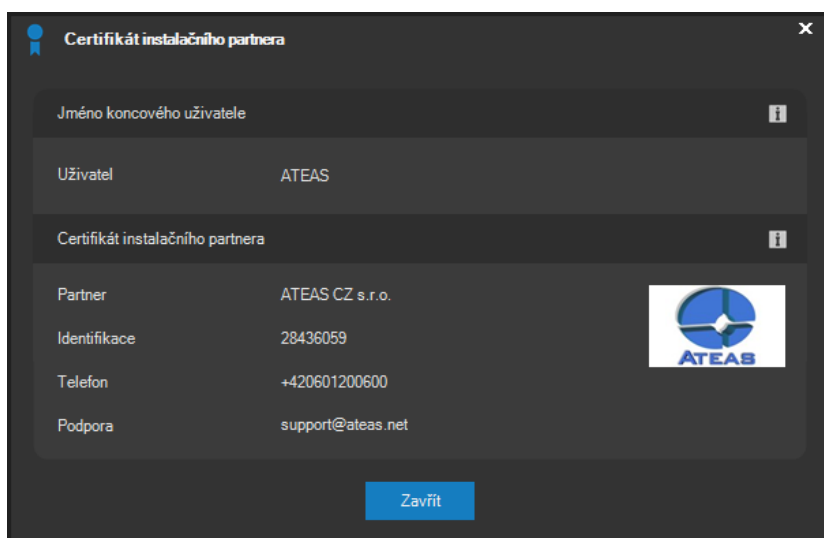
O tom, že Váš systém je certifikovanou instalací, informuje výrazná barva symbolu certifikátu v levém horním rohu okna s hlavní nabídkou aplikace.



Certifikát má dále tyto vlastnosti:

- Certifikát je digitálně podepsán přímo na serverech ATEAS a nemůže být vytvořen nikým jiným.
- Certifikát je vázán a vydáván pro konkrétní ATEAS ID a není přenositelný.
- Certifikát obsahuje označení instalačního partnera a jeho identifikaci včetně loga, volitelně může obsahovat telefonní či online kontakty na podporu.

Tyto údaje je možné kdykoliv zobrazit kliknutím na ikonu certifikátu.



Kromě certifikátu instalačního partnera se v tomto dialogu zobrazuje také jméno či název koncového uživatele licence. Při aktivaci systému musí být správný název koncového uživatele vyplněn pro vytvoření kontrolního kódu Vaší instalace.

POZOR

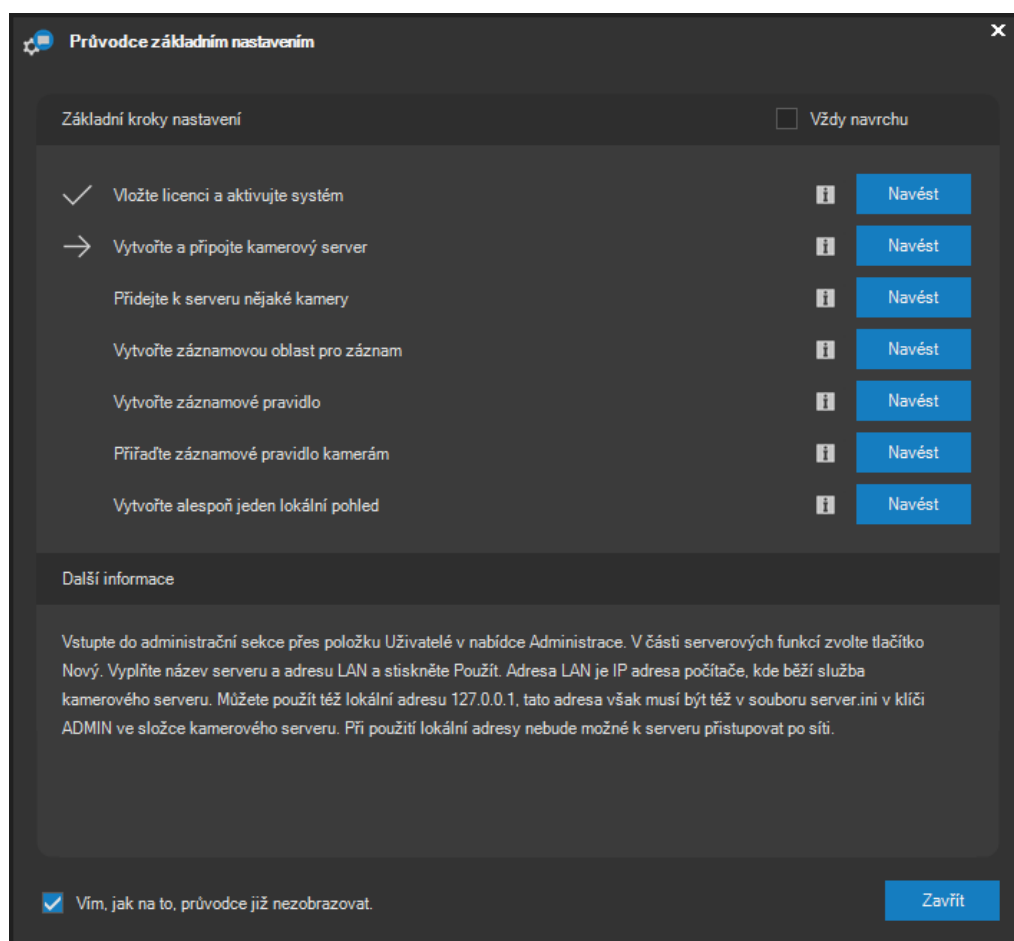
Pokud se Vám zobrazuje jiný název koncového uživatele systému, měl byl Váš instalační partner zjednat nápravu. Systém s chybným označením koncového uživatele je považován na nesprávně licencovaný.

POZNÁMKA

Pokud není v systému certifikát instalačního partnera k dispozici, má ikona certifikátu v okně hlavní nabídky šedou barvu a žádný certifikát nelze zobrazit. Údaje o názvu koncového uživatele však budou zobrazeny vždy.

2.5. Průvodce základním nastavením

Po prvním úspěšném přihlášení do systému se automaticky spustí průvodce základním nastavením systému. Tento průvodce Vás provede několika základními kroky, které jsou běžně potřeba pro zprovoznění stěžejních funkcí kamerového systému jako je přidání kamer, nastavení záznamu a vytvoření živého pohledu.



Průvodce nastavením je přehledně organizován do několika základních kroků, které pokrývají oblast vložení licence a aktivace systému, vytvoření kamerového serveru, připojení kamer k serveru, vytvoření oblasti pro záznam a vytvoření záznamového pravidla, přiřazení záznamového pravidla ke kamerám a vytvoření alespoň jednoho lokálního kamerového pohledu. Průvodce v průběhu nastavování zobrazuje informaci, které kroky již byly provedeny a který krok je aktuálně nutné provést.

Ve spodní části okna průvodce se pro každý krok zobrazuje podrobný návod, jak daný krok provést. U každého kroku je k dispozici též tlačítko **NAVÉST**, které pro Vás automaticky otevře příslušné okno s nastavením, kde je potřeba provést danou akci. Podrobnější informace k libovolnému kroku je možné kdykoliv vyvolat pomocí modrého tlačítka se symbolem informace.

Pokud nechcete pro nastavení systému používat průvodce, můžete ho deaktivovat zaškrtnutím příslušné položky při spodním okraji okna. V takovém případě se již průvodce nebude zobrazovat.

POZNÁMKA

Průvodce je možné ovšem kdykoliv opět aktivovat ručně pomocí volby Průvodce nastavením z nabídky Nápověda.

POZNÁMKA

Průvodce se automaticky zobrazuje pouze master administrátorovi systému (administrátorovi s číslem 1), který má oprávnění ke všem krokům v instalačním průvodci, a to pouze v případě, kdy není některý z kroků nastavení proveden. Pokud jsou všechny kroky provedeny, průvodce se nezobrazí.

POZNÁMKA

Případní další administrátoři systému mohou sice průvodce zobrazit ručně, nezobrazuje se jim však automaticky. Běžní uživatelé systému nemohou průvodce zobrazit vůbec.

Okno průvodce se zobrazuje přes všechna jiná otevřená okna, abyste měli aktuální krok nastavení vždy před očima. Zobrazení průvodce přes ostatní okna lze však vypnout zrušením zaškrtnutí volby Vždy navrchu.

2.6. Vlastní názvy pro přihlášení

Do textového pole pro zadání serveru je při přihlášení možné zadat jednak IP adresu serveru, jednak také jeho jméno (např. DNS název nebo název v lokální síti). Tyto názvy se pak zobrazují v rozbalovacím seznamu, který nabízí historii posledních úspěšných přihlášení seřazenou chronologicky s názvy naposledy použitými jako prvními.

POZNÁMKA

Historie může obsahovat až 25 položek přihlášení.

Jelikož v praxi může přihlašování k různým kamerovým systémům pomocí jednoho klienta vytvořit nepřehledný seznam IP adres, které nelze na první pohled přiřadit konkrétním systémům, je možné je nahradit názvy vlastními.

POZNÁMKA

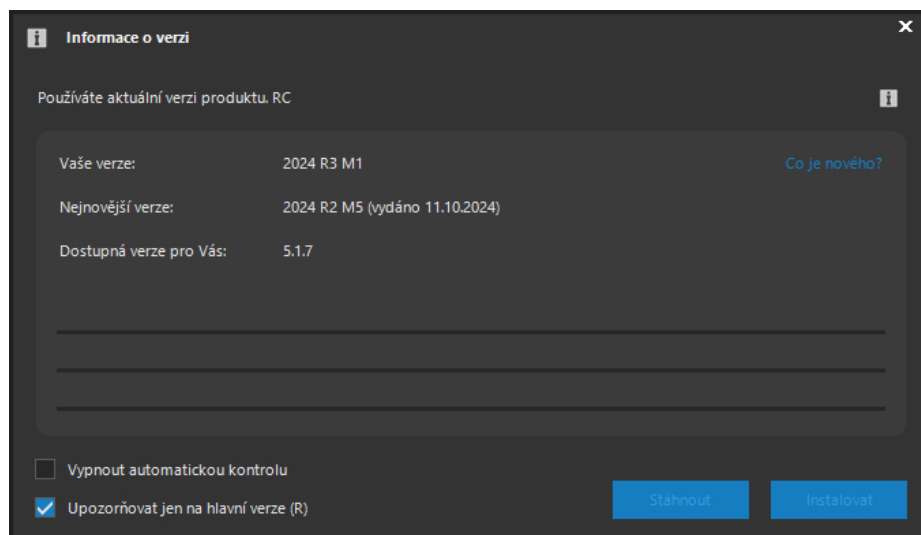
Zde máme na mysli přihlašování k více různým kamerovým systémům, kde každý má svůj vlastní licencovaný administrační server a nikoliv situaci, kdy existuje více serverů v rámci jednoho kamerového systému. Zde se samozřejmě uživatel přihlašuje centrálně pouze jednou a může v rámci edice UNLIMITED získat přístup ke všem serverům současně.

Vlastní názvy pro servery při přihlášení (tzv. alias názvy) je možné tvořit v části Nastavení v sekci Historie přihlášení, kde je uveden popis této funkce. Vedle toho je také možné alias vytvořit též přímým zápisem ihned při přihlášení a to tak, že za skutečný síťový název či adresu serveru doplníme alias do kulatých závorek např. 10.0.0.10 (alias).

V lokálním nastavení nebo pomocí postupu uvedeného v předchozím odstavci vytvořené alias názvy lze poté používat stejným způsobem jako názvy síťové, stačí je zapsat do pole serveru při přihlášení.

2.7. Informace o verzi

Ve spodní části okna s hlavní nabídkou se v pravém spodním rohu nachází informační symboly (vedle indikátoru spojení s administračním serverem a informace o aktuální verzi). Pokud je počítač, na kterém je spuštěna klientská aplikace, současně připojen k internetu, je možné kliknutím na symbol vpravo ověřit nejvyšší dostupnou verzi platformy ATEAS.

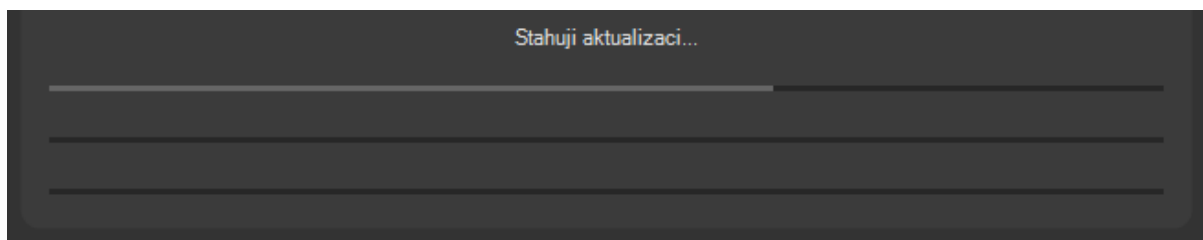


Klientská aplikace kontaktuje servery ATEAS a zjistí aktuálně dostupnou nejvyšší verzi a datum jejího vydání. Dále se Vám také zobrazí informace, zdali používáte aktuální nebo starší verzi produktu a nejvyšší verzi dostupnou pro Vás.

Implicitně je klientská aplikace nastavena tak, že je kontrola nové verze prováděna automaticky, na novou verzi tedy budete upozorněni. Tuto automatickou kontrolu lze vypnout zaškrtnutím příslušné volby při spodním okraji okna.

Výchozí nastavení bude upozorňovat pouze na hlavní verze ATEAS s jiným označením roku či R. Pokud byste chtěli být upozorněni i na drobné změny ve verzi s jiným označením M, pak zrušte aktivaci volby Upozorňovat jen na hlavní verze.

Uživatel s právy master administrátora systému může v případě dostupnosti nové verze systému provést její stažení pomocí tlačítka **STÁHNOUT**. První řádek ukazuje průběh stahování.



POZNÁMKA

Nejnovější verze systému bude stažena jen tehdy, pokud na ni na základě Vašeho ATEAS PMA máte nárok a budete ji moci aktivovat. V opačném případě je možné automaticky stáhnout i starší verzi systému, tato však musí být alespoň 2023 R1 M1.

Po dokončení stahování je automaticky ověřena integrita souboru, průběh této operace je zobrazen ve druhém řádku. Třetí řádek pak ukazuje průběh nahrávání aktualizace na administrační server systému.

POZNÁMKA

Servery kamerového systému tedy nemusí být v průběhu automatické aktualizace připojeny k internetu.

Po nahrání aktualizace na administrační server bude možné pomocí tlačítka **INSTALOVAT** zahájit reinstalaci administračního serveru systému. To znamená, že dojde k odpojení klienta a po jeho automatickém připojení bude případně nutné provést aktualizaci samotného klienta a aktivaci nové verze systému. Tento průběh spolu s automatickou aktualizací všech kamerových serverů v systému je popsán v kapitole Automatické aktualizace.

POZNÁMKA

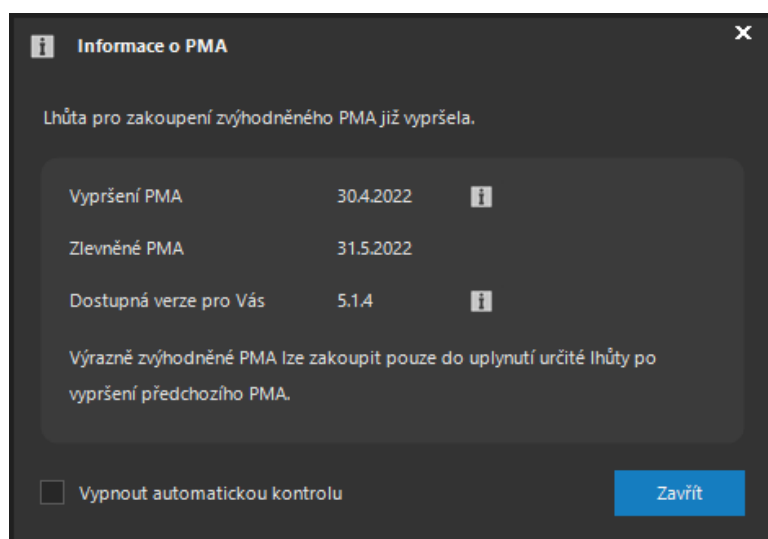
Novou verzi můžete po instalaci úspěšně aktivovat pouze tehdy, máte-li na ní nárok (volné aktualizace po nákupu licenčního čísla či samostatná smlouva o podpoře produktu PMA).

POZNÁMKA

Ve spodní části okna hlavní nabídky aplikace jsou po přihlášení k dispozici označení verze klientské aplikace a za ním následuje označení verze systému, ke kterému se uživatel přihlásil. Klientská aplikace je zpětně kompatibilní a může přistupovat ke starším verzím systému.

2.8. Informace o PMA

Ve skupině informačních symbolů v pravém dolním rohu okna s hlavní nabídkou aplikace slouží symbol vlevo k ověření stavu PMA pro Vaši instalaci.



Služba ATEAS PMA garantuje možnost aktualizace Vašeho systému na nejnovější dostupnou verzi. Abyste mohli aktualizaci provést, je třeba mít aktivovanou službu ATEAS PMA. Pokud je služba PMA obnovována pravidelně, je možné ji získat za výrazně výhodnějších podmínek. Z tohoto důvodu, pokud je aplikace připojena k internetu, si můžete datum vypršení služby a datum, do kdy je nutné obnovit PMA, ověřit přímo ve Vaší aplikaci. S nákupem libovolné licence ATEAS získáváte dvouleté PMA zdarma.

Implicitně je klientská aplikace nastavena tak, že je kontrola vypršení prováděna automaticky, na blížící se datum vypršení tedy budete upozorněni. Tuto automatickou kontrolu lze vypnout zaškrtnutím příslušné volby při spodním okraji okna a kliknutím na tlačítko **ZAVŘÍT**.

Zobrazená dostupná verze pro Vás určuje maximální verzi systému, kterou můžete instalovat a aktivovat. Pokud Vaše ATEAS PMA již vypršelo, může být tato verze nižší než nejnovější verze systému.

2.9. Hlavní menu aplikace

Hlavní nabídka aplikace se zobrazí po úspěšném přihlášení a má následující položky a význam:

Sdílené pohledy – pohledy definované administrátorem s přístupem všech uživatelů.

Mé pohledy – pohledy definované uživatelem bez přístupu ostatních uživatelů.

Záznam – přístup k záznamu z kamer.

Prostory – nepovinná položka obsahující rozložení více dohledových oken včetně pohledů či mapového okna, aktivuje se v části nastavení pracovních prostorů.

Video stěna – nepovinná položka zpřístupňující ovládání video stěny či vzdálených monitorů, pokud je v systému administrátorem video stěna vytvořena.

Snímky – přístup k náhledu uložených snímků.

Nastavení – lokální nastavení stanice.

Nástroje – přístup k vybraným nástrojům jako je manažer stahování, osobní hlídač, mapa, uživatelská tlačítka, databáze obličejů či seznamy RZ vozidel.

Administrace – možnost správy kamer a jejich nastavování, správa záznamu, pohledů a video stěny, doplňků, uživatelů, oprávnění, serverů, integrační možnosti, upgrade licenčního čísla (aktivace).

Nápověda – otevře dokumentaci k produktu.

Konec – ukončení aplikace.

Nad hlavní nabídkou je zobrazen údaj o aktuálně přihlášeném uživateli a tlačítko pro vyhledávání, které je zejména vhodné, pokud sdílené či vlastní pohledy obsahují velké množství pohledů členěných do složité stromové struktury s více úrovněmi.

2.10. Automatické startování aplikací

Služby ATEAS Administrator a ATEAS Server jsou po instalaci nastaveny na automatické spouštění a nevyžadují žádnou uživatelskou obsluhu.

Klientskou aplikaci ATEAS Observer lze pomocí lokálního nastavení také spouštět automaticky po startu Windows a automaticky přihlásit konkrétního uživatele. Navíc lze pomocí automatického načtení pracovního prostoru zajistit otevření definovaných pohledů a jejich umístění na příslušné monitory. Více viz kapitola o lokálním nastavení.

POZOR

Při automatickém přihlášení uživatele je nutné dbát zvýšené opatrnosti. Automaticky přihlášený uživatel nemusí zadávat své heslo a jeho účet tak může být zneužit. Proto je vhodné používat automatické přihlášení pro univerzální uživatele s nízkými oprávněními.

2.11. Vyhledávání, filtrování a řazení

Klientská aplikace nabízí ve svých nejrůznějších částech seznamy dat systému – např. seznam kamer, uživatelů, serverů, událostí, externích prvků a mnoho dalších. Data jsou prezentována buď v podobě tabulky anebo seznamu se stromovou strukturou. Ve všech těchto strukturách lze pomocí stisku kombinace kláves CTRL-F aktivovat vyhledávání pomocí vestavěného vyhledávacího panelu.

X		PN0	Smazat
ID	Název	Typ	Adresa
	5 Wisenet	PN0-A9081R	109.202.74.6
	6 Wisenet	PN0-A9081R	109.202.74.6

Zápisem textu do vyhledávacího pole dojde k automatickému filtrování všech záznamů v tabulce, přičemž zobrazeny budou pouze ty, které vyhovují zadání. Pro vyhledávání a filtry platí následující pravidla:

- Zadávaný text je automaticky vyhledáván ve všech sloupcích tabulky.
- Zadání více slov oddělených mezerou vyhledá všechny záznamy, kde alespoň jeden sloupec obsahuje alespoň jedno z těchto slov (logické OR).
- Abychom vynutili vyhledání záznamů, které obsahují více zadáných slov současně, použijeme před slovem symbol + (logické AND).
- Pro vyhledání celého výrazu obsahujícího mezery lze celý výraz uvést v uvozovkách.
- Pokud chceme omezit vyhledávání jen na některý sloupec, lze před hledaný výraz uvést název sloupce a za ním dvojtečku následovanou vyhledávaným výrazem.
- Nalezené hledané výrazy jsou ve vyfiltrovaných výrazech automaticky zvýrazněny.
- Tlačítko **SMAZAT** smaže všechna zadaná vyhledávaná slova.

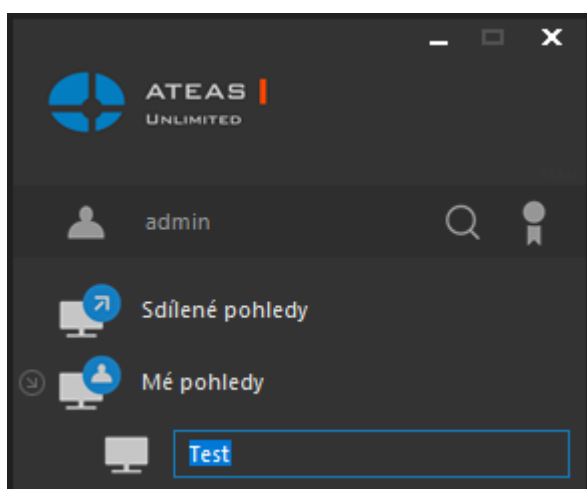
Řazení seznamů se provede jednoduše kliknutím na záhlaví příslušného sloupce. Opětovné kliknutí způsobí změnu řazení z vzestupného na sestupné a opačně. Chceme-li data seřadit podle více sloupců, použijeme při volbě dalšího sloupce v pořadí klávesu SHIFT.

TIP

Texty je možné ze seznamů vybírat a kopírovat pomocí opakovaného kliknutí do buňky tabulky.

2.12. Přejmenovávání položek

V závislosti na přidělených oprávněních je možné některé položky v hlavním menu přejmenovat použitím editačního symbolu. Týká se to např. názvů lokálních či sdílených pohledů, prostorů apod.

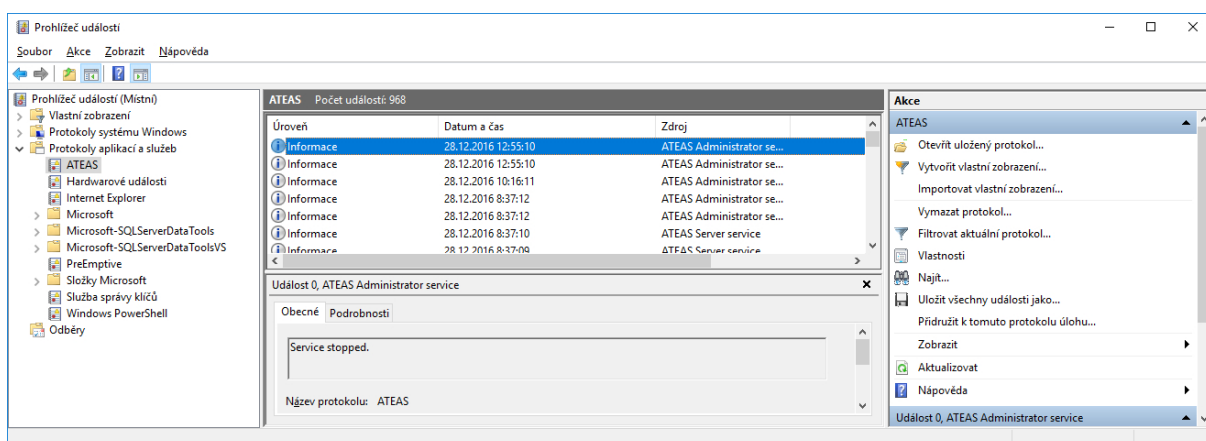


2.13. Klientský terminálový přístup

Technologie virtualizace pracovních stanic přináší nesporné výhody pro provoz informačních systémů v enterprise řešeních. Díky podporovaným technologiím GPU akcelerace aplikacemi ATEAS (klient i server) lze nyní do takové architektury plně integrovat také provoz kamerových systémů. Klientská aplikace umí využít akcelerace pomocí serverových GPU (Tesla), a může tak být spuštěna pro větší počet klientů pomocí využití GPU akcelerace, bez které by vícenásobně spuštění klienti nárokuje plynulé video ve vysokém rozlišení okamžitě přetížili procesory serveru. Bližší informace jsou uvedeny v kapitolách o GPU akceleraci.

2.14. Protokoly

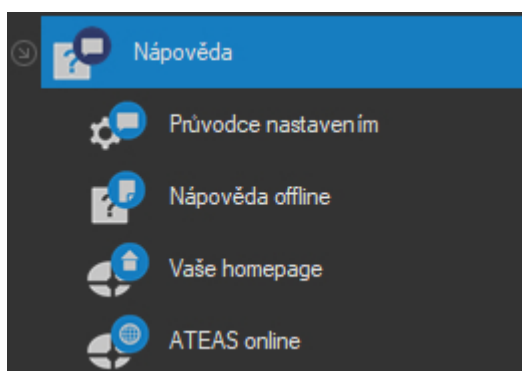
Po instalaci libovolné aplikace systému ATEAS Security je v systému vytvořen nový událostní protokol s názvem ATEAS, do kterého jsou zapisovány veškeré důležité okolnosti běhu aplikací. Tento protokol je dostupný v Ovládacích panelech, Nástrojích pro správu, Prohlížeč událostí. V případě havárie nebo nestandardního chování systému protokol může obsahovat důležité diagnostické údaje. Kromě zápisu do tohoto systémového protokolu spravovaného Windows, obsahuje ATEAS Security vlastní systémový log dostupný v části administrace uživatelů s možností historického náhledu, filtrování a okna živého náhledu (live spy).



Kapitola 3 - Pomoc

3.1. Dokumentace a nápověda

V podnabídce nápověda jsou k dispozici následující odkazy.



Administrátoři systému mohou spustit průvodce nastavením, který je provede základními kroky pro úvodní nastavení systému.

Nápověda offline otevírá offline uloženou kompletní dokumentaci k produktu ve formátu PDF či CHM. Odkaz Vaše homepage otevře ve Vašem výchozím internetovém prohlížeči domovskou stránku administračního serveru (není nutné připojení k internetu), na které jsou k dispozici vedle kompletní dokumentace v tiskové kvalitě také některé další dokumenty a také instalátory aplikací systému.

Posledním odkazem (nutné připojení k internetu) je domovská stránka výrobce systému s kontaktními údaji a s možností přihlášení do partnerské sekce.

Kapitola 4 - Dohled

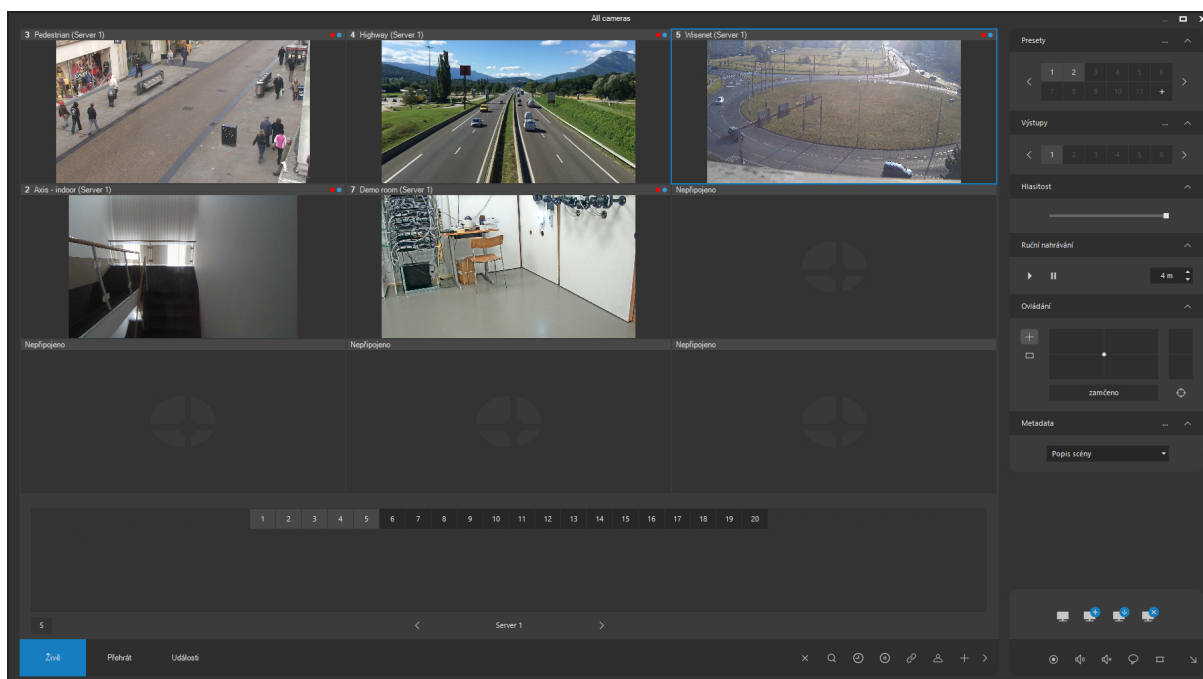
4.1. Pohledy

4.1.1. Správa pohledů

Pohledem nazýváme definované uspořádání kamer na obrazovce počítače (v dohledovém okně). Při práci s dohledovým oknem tak může uživatel jednoduše přepínat mezi pohledy a změnit tak jedním kliknutím kamery na svém monitoru jejich počet a jejich uspořádání.

V hlavní nabídce jsou dvě položky, které otevírají podnabídku pohledů.

Sdílené pohledy obsahují pohledy viditelné a přístupné pro všechny uživatele systému, **Mé pohledy** obsahují pohledy, které si z dostupných kamer vytvoří sám uživatel. Tyto pohledy nejsou pro jiné uživatele viditelné. Jedno dohledové okno může obsahovat až 100 kamer, maximální počet dohledových oken je 16. Pro zobrazení většího počtu kamer v detailu lze využít vestavené video stěny (viz příslušné kapitoly).



Ovládání dohledového okna

Dohledové okno může mít buď maximalizovanou podobu (bez dodatečných ovládacích prvků) nebo standardní podobu se zobrazenými ovládacími prvky. Do maximalizovaného tvaru lze dohledové okno převést pomocí kliknutí na ovládací prvek v pravém dolním rohu boční ovládací lišty. Zpět do podoby s ovládacími prvky je dohledové okno možné přepnout pouhým najetím ukazatele myši do aktivního prostoru pravého dolního rohu maximalizovaného okna. Pro přepínání lze využít také klávesu F12.

Pokud je dohledové okno ve své standardní podobě se zobrazenými ovládacími prvky, je možné na spodní ovládací lištu přepínat mezi těmito skupinami ovládacích prvků (kartami):

Na kartě **Živě** je možné provádět funkce související s pohledy, na kartě **Události** jsou k dispozici události v systému a je možné zde provádět přepínání mezi událostmi. Karta **Přehrát** otevírá možnost přímého přístupu k přehrávání (vyvolání záznamu) aktivního pohledu. Boční ovládací lišta obsahuje přístup k funkcím vybrané kamery.

Přepínání pohledů

Přepínání pohledů se provádí jednoduše výběrem pohledu z nabídky **Sdílené pohledy** nebo **Mé pohledy**. Zvolený pohled je přepnut do posledního aktivního dohledového okna. To je důležité, pokud máte otevřeno více dohledových oken (viz otvírání dalších oken).

Pokud není otevřeno primární dohledové okno (okno, ve kterém je možné pohledy spravovat), bude při volbě pohledu vždy otevřeno nezávisle na dalších dohledových oknech.

POZNÁMKA

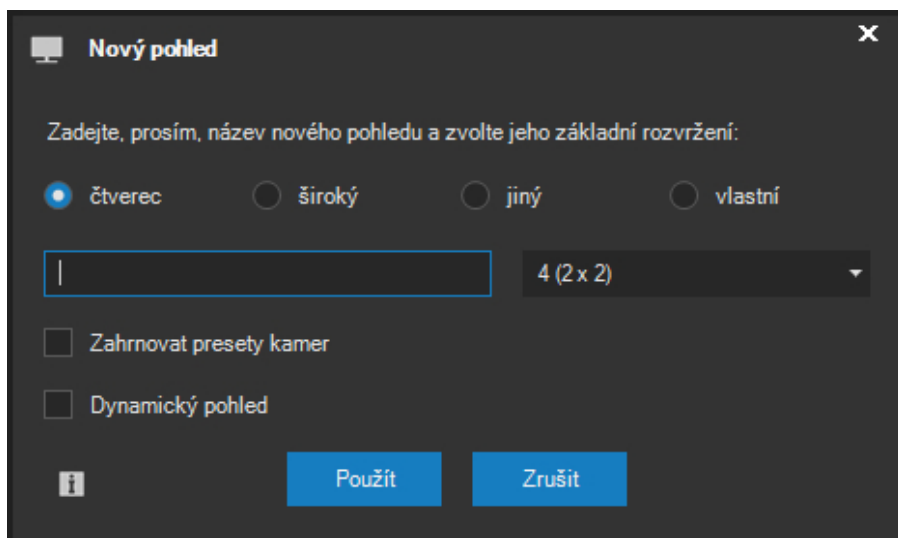
Pokud není vytvořen žádný pohled, bude primární dohledové okno otevřeno už při kliknutí na položku **Mé pohledy**.

Vytvoření nového pohledu



Na kartě Pohledy zvolíme tlačítko Vytvořit nový pohled. Aplikace zobrazí dialogové okno, ve kterém je nutné zadat název nového pohledu a určit jeho základní rozvržení (tj. počet kamer, které budou daný pohled tvořit). Pro každý z typů rozvržení (čtvercové, široké, jiné) je možné vybrat z rozbalovacího seznamu konkrétní rozvržení pohledu. Čtvercové rozlišení vždy obsahuje shodný počet kamer v horizontálním a vertikálním směru, široké rozlišení nabízí režimy s vyšším počtem kamer

v horizontálním směru než ve vertikálním (v přibližných poměrech 16:9) a jiná rozlišení nabízejí různou velikost oken pro jednotlivé kamery. Maximální počet pro čtvercové rozlišení je 11 x 11, tedy celkem 121 kamer, pro široký typ rozvržení je to 13 x 9, resp. 14 x 8, tedy 117, resp. 112 kamer.



Ve skupině jiných pohledů jsou k dispozici tzv. středové (centrické) pohledy. Středové pohledy jsou vždy v režimu 1 + N s jedním větším oknem kamery uprostřed pohledu a N okny pro kamery uspořádanými kolem něj. Kromě této orientace mají středové pohledy některá další specifika, která zvyšují uživatelské vlastnosti těchto pohledů:

- Pokud je kamera umístěná po obvodu pohledu přepnuta do detailu dvojitým kliknutím na její záhlaví, bude detail zobrazen nikoliv dle nastavení pro hotspot monitor, ale přímo ve středu tohoto pohledu.
- Pro zobrazení videa ve středovém okně pohledu je použita primární snímková frekvence.

Povolení přepnutí stejné kamery do jednoho pohledu vícekrát je automaticky aktivováno při volbě centrického pohledu a deaktivováno při výběru pohledu jiného. Tento stav je indikován pomocí tlačítka se symbolem čísla 1 vpravo od přehledu kamer, které představuje zámek pro vícečetné přepnutí jedné kamery do pohledu. Tento zámek však lze libovolně měnit.

POZNÁMKA

Zámek budeme chtít vypnout i v jiném než centrickém pohledu v situaci, kdy budeme chtít zobrazit jednu kameru ve dvou oknech s různou úrovní digitálního přiblížení.

Kromě pohledů zařazených mezi jiné pohledy je také možné vytvářet vlastní. Při tvorbě vlastních pohledů nevybíráme hotové rozvržení kamerových oken v pohledu, ale tvoříme toto rozvržení sami pomocí editoru rozvržení. Editor rozvržení spustíme po označení přepínače Vlastní a po stisku tlačítka **UPRAVIT**. Práce s editorem rozvržení pohledů je popsána v následující subkapitole.

Po potvrzení tlačítkem **POUŽÍT** bude pohled vytvořen a bude automaticky přepnut do primárního dohledového okna. Zároveň bude nový pohled zobrazen jako položka v hlavním menu aplikace, odkud je možné provádět jeho rychlou volbu.

Při vytváření nového pohledu lze také zaškrtnout ovládací prvek Zahrnovat presety kamer. V takovém případě bude aktuální pohled při svém uložení také obsahovat poslední prepozice kamer, na které byly otočné kamery v pohledu přepnuty. Při aktivaci takového pohledu budou dané kamery na příslušné presety automaticky natočeny. Pomocí této funkce lze tedy definovat dva různé pohledy sestávající ze stejných kamer (při každém z pohledů se otočné kamery natočí na jiné presety).

Aktivací funkce Dynamický pohled bude pozměněno chování vytvořeného pohledu v případě, že tento pohled bude administrátorem systému označen jako sdílený. Změna v chování spočívá v tom, že pohled bude automaticky měnit své rozvržení podle toho, ke kolika kamerám z pohledu bude mít přístup uživatel, který pohled zobrazuje. Různí uživatelé tak mohou stejný pohled vidět v různém rozvržení. Více o sdílených pohledech a skupinách pohledů se dozvíte v subkapitole Správa pohledů v kapitole Administrace systému.

Úprava pohledu

Aby byly v pohledu zobrazeny nějaké kamery, je nutné je do pohledu přepnout. Toto přepnutí (volba) kamer do pohledu se provádí vždy jen při editaci pohledu, pohled je uložen vždy včetně informace o kamerách a jejich rozvržení.

POZNÁMKA

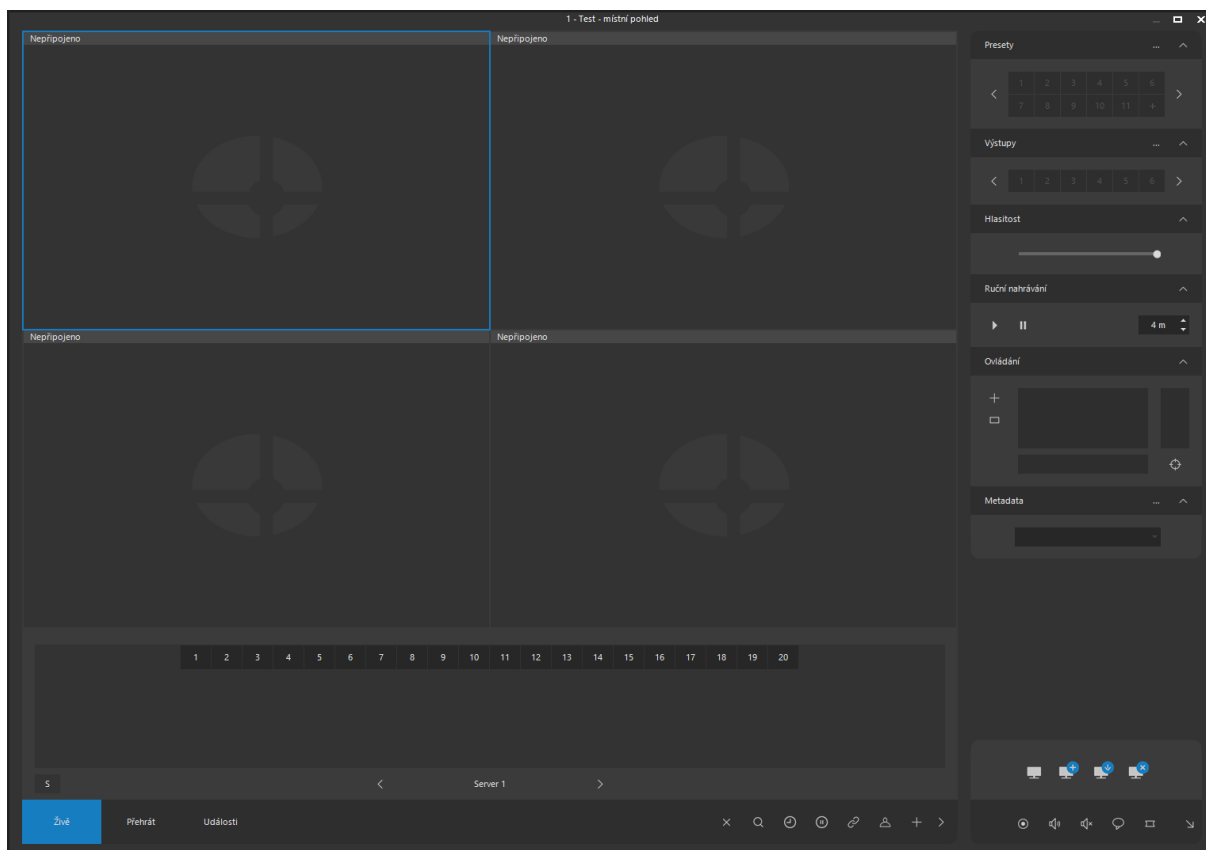
V rámci pohledu lze též definovat automaty či túry, o kterých je psáno v dalších subkapitolách. Zde je popisováno pouze základní přepínání kamer do pohledu.

Kamery je možné do pohledu přepínat dvěma způsoby. Prvním způsobem je výběr pozice následovaný výběrem kamery, tímto způsobem lze přepnout vždy jednu kameru. Druhým způsobem je možnost přetažení myši či dotykem, tímto způsobem je možné provádět najednou přepnutí též více kamer. Dále je k dispozici také funkce automatického vyplnění pohledu, popis následuje v dalším textu.

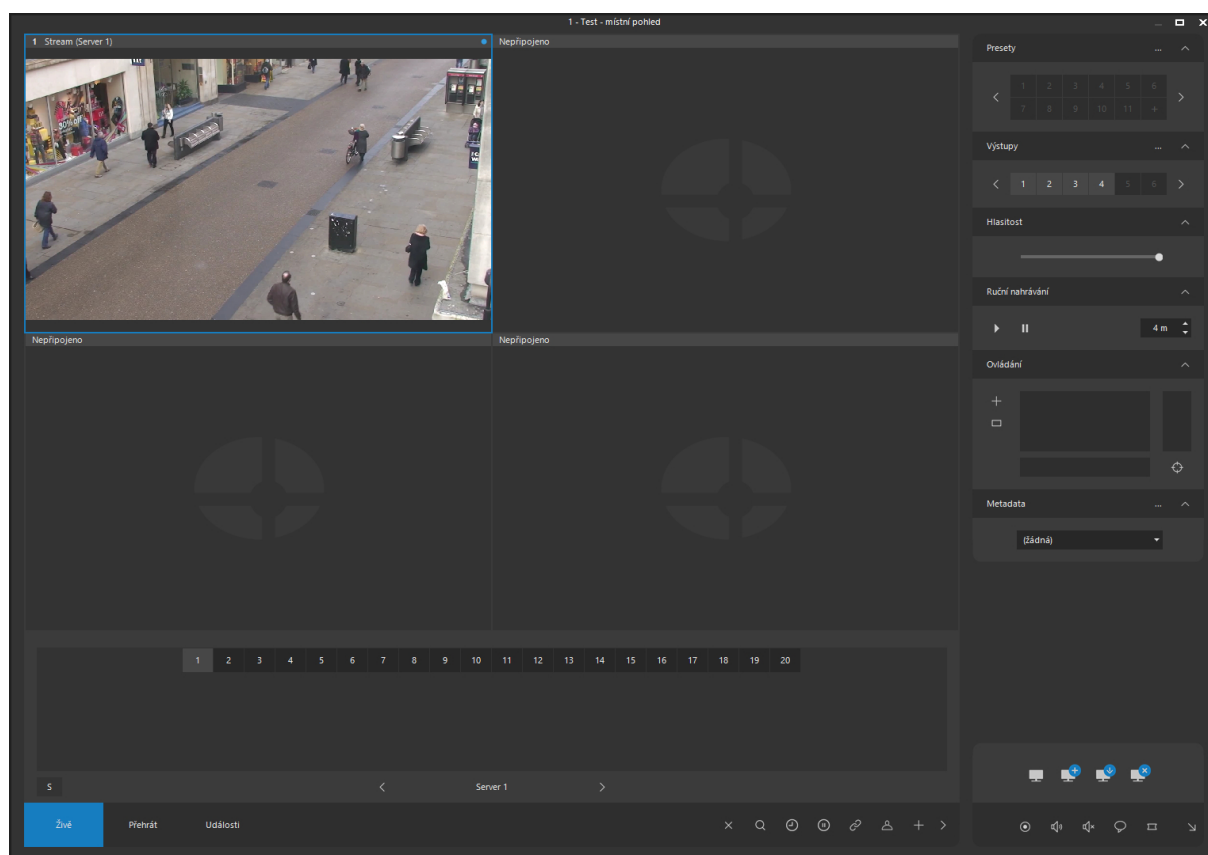
Přepnutí jedné kamery

Přepnutí kamery na dané místo pohledu se provede následovně:

- provedeme výběr některého místa pohledu, kolem vybraného místa se vytvoří výběrový rámeček,

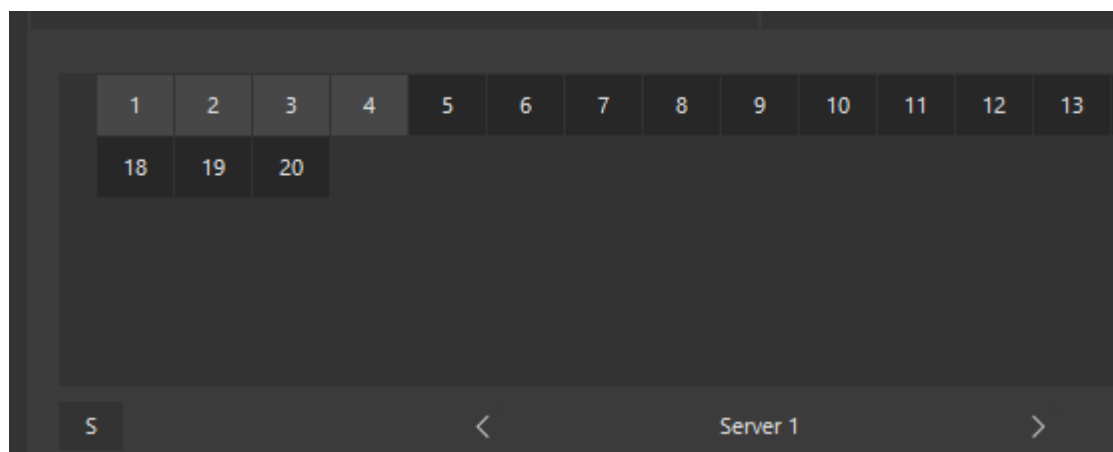


- na kartě Živě provedeme volbu kamery kliknutím na její číslo (výběr kamery je zjednodušen zobrazením tooltipu s názvem kamery a – pokud má uživatel oprávnění – i její adresy), poté je kamera přepnuta na dané místo v pohledu.



Popsaným způsobem lze zaplnit všechna místa v pohledu. Přemístit již umístěnou kameru lze jednoduše přetažením za záhlaví dané kamery na jiné místo v pohledu. Implicitně je použit primární stream kamery. Pro přepnutí sekundárního streamu je nutné aktivovat sekundární přepínač v levém dolním rohu se symbolem S.

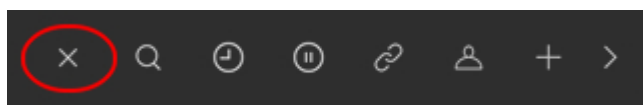
Čísla kamer jsou zobrazena vzestupně od čísla 1. Pro zvýšení přehlednosti jsou v případě chybějících čísel kamer v řadě vkládány prázdné pozice. Zároveň jsou všechny kamery, které již jsou součástí pohledu, zobrazeny výraznější barvou, jak ukazuje následující obrázek.



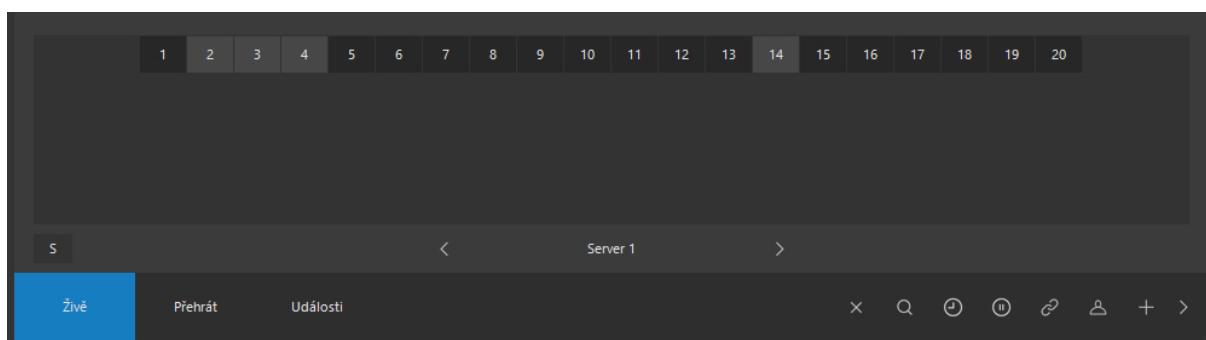
POZNÁMKA

Tímto způsobem lze jednoduše vytvářet přehledné sekce kamer dle seskupení jejich čísel.

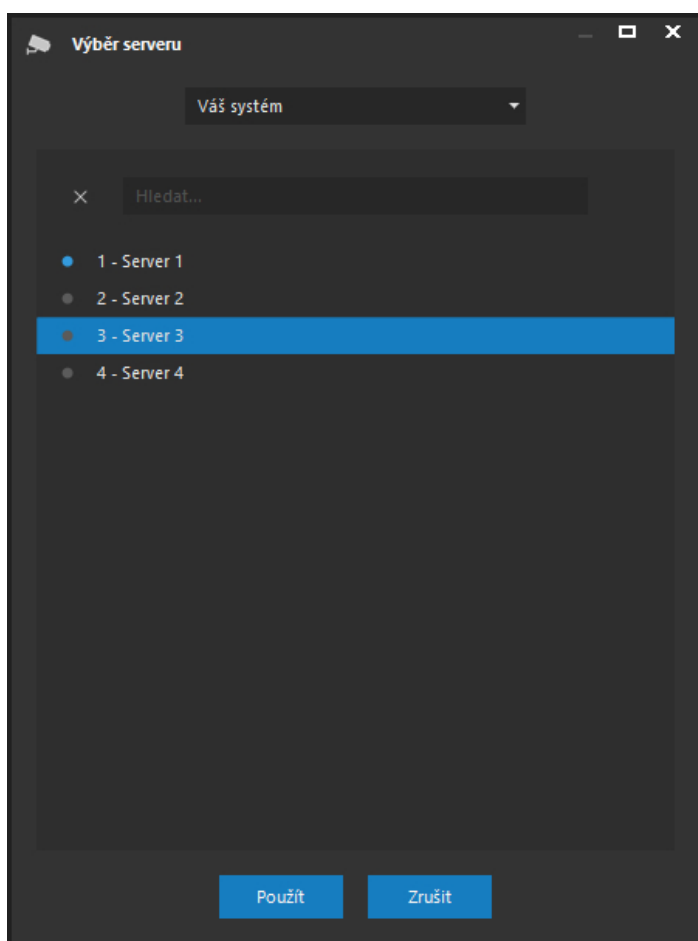
Pokud chcete dané místo v pohledu skutečně uvolnit, tj. nikoliv obsadit jinou kamerou, je možné po výběru tohoto místa použít tlačítko Vypnout okno.



Výběr kamer je možné provádět i z různých serverů. Tímto serverem mohou být dle Vaší edice produktu ATEAS Security např. přímo Váš počítač, na kterém provádíte dohled, nebo specializované servery v síti. K jednomu serveru může být připojeno až 999 kamer, pokud však z nejrůznějších důvodů Váš administrátor konfiguruje systém z více serverů, je nutné mezi nimi přepínat a zobrazit tak vždy jinou sadu kamer.



Kliknutím na název serveru lze zobrazit kompletní přehled serverů v systému (přesněji pouze ty servery, ke kterým máte zřízení přístup) nebo lze použít šipky pro listování. Výběrem serveru ze seznamu a stisknutím tlačítka **POUŽÍT** nebo dvojitým kliknutím lze vybrat daný server. Okno serverů také ukazuje momentální stav všech serverů (online nebo offline).



Pokud pro Vás administrátor systému aktivoval funkci vícenásobného přihlášení (ATEAS Interlogin), bude možné se v seznamu systémů přepnout i na jiné systémy, než je Váš systém.

POZNÁMKA

Zatímco přepnutí na jiný kamerový server téhož kamerového systému zobrazí pouze jiná čísla kamer na novém serveru, přepnutí do jiného kamerového systému způsobí též uzavření aktuálního pohledu.

Přepínání pomocí přetažení

Přepínání kamer je možné provádět také pomocí přetažení čísel kamer myší. Jedná se o standardní techniku, při které stisknete symbol kamery a přetáhnete na zvolenou pozici v pohledu. Během této operace bude barevný rámeček indikovat cílovou pozici v pohledu, kde bude kamera zobrazena, pakliže uvolníte stisk.

Pokud použijete klávesu CTRL, je možné provést výběr více kamer. Použití klávesy SHIFT provede také výběr více kamer, nicméně jsou do výběru vždy zahrnuty všechny kamery mezi označovanými čísly.

POZNÁMKA

Při přetažení více kamer současně je zobrazeno také odpovídající množství barevných rámečků indikujících cílovou pozici.

Pokud se na cílových pozicích již nacházejí nějaké kamery, jsou tyto při běžném přetažení nahrazeny novými, dojde tedy k přepsání výběru. Pokud byste chtěli kamery umístit do pohledu v režimu vkládání (nikoliv přepisování) tak, že na cílové pozici bude vytvořeno volné místo a stávající kamery budou posunuty v pohledu dále, lze pro přetažení použít pravé tlačítko myši.

Kamery lze také přetahovat přímo mezi sebou. Při této akci dojde k záměně pozic kamer.

Expanze rozvržení pohledu

Pomocí přetažení kamer myši popsaného výše lze také provést automatickou expanzi pohledu o nové řady, sloupce či obojí zároveň. Pro automatickou expanzi o nový sloupec (či řadu) stačí kurzor myši umístit během přetažení do blízkosti začátku prvního či konce posledního sloupce (či řady) a nový sloupec (či řada) bude automaticky nabídnut jako možnost pro umístění kamery.

POZNÁMKA

Tuto expanzi však nelze provést u pohledů s vlastním designem navrženým v editoru, středových a jiných pohledů. Expanzí také nelze překonat maximální počet 121 pozic v pohledu.

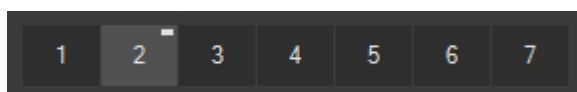
Automatické vyplnění pohledu

Pomocí této funkce lze aktuální pohled automaticky vyplnit kamerami vybraného kamerového serveru. Vyplnění se vždy provádí od pozice právě vybraného okna pohledu přes všechna následující okna pohledu (nebo po dosažení nejvyššího čísla kamery daného serveru). Automatické vyplnění využijete zejména při větším počtu kamer v systému, kdy můžete jedním kliknutím obsadit všechny pozice v pohledu.

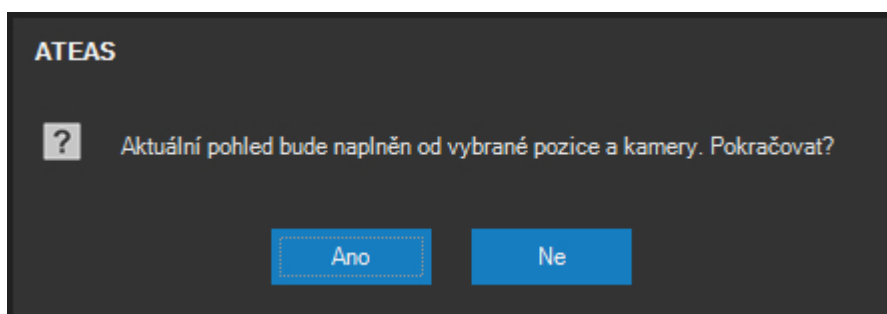
POZOR

Při automatickém vyplnění pohledu se mohou změnit také již obsazená okna pohledu.

Pokud chcete provést automatické vyplnění pohledu počínaje konkrétní kamerou, je třeba kliknout na symbol vyplnění umístěný vpravo nad číslem aktivní kamery, viz následující obrázek.



Vyplnění poté nastane po potvrzení zprávy.

**POZNÁMKA**

Funkce automatického vyplnění pohledu je automaticky přerušena, pokud je při vyplňování dosaženo poslední pozice v pohledu, poslední zobrazené kamery anebo mezery mezi kamerami v prvku zobrazujícím čísla kamer.

Uložení pohledu

Po úpravě pohledu a rozmístění všech potřebných kamer musí být pohled uložen. Uložení můžete provést kliknutím na tlačítko Uložit pohled.

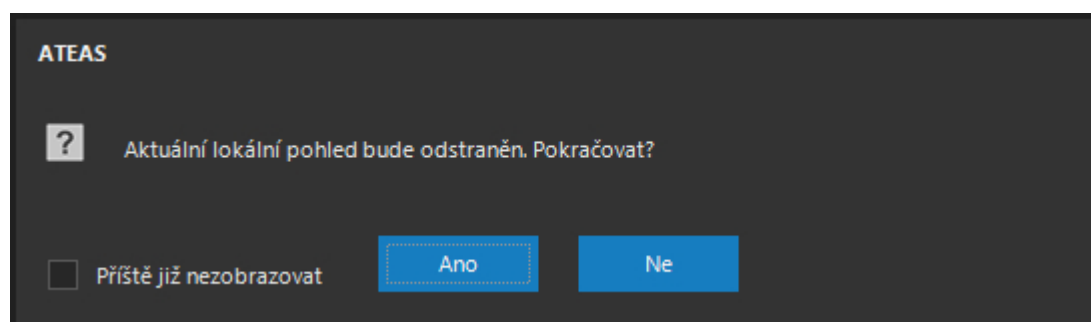
Pokud opomenete po úpravě pohledu jeho uložení a pohled bude nutné vypnout nebo přepnout na jiný, aplikace se na uložení pohledu zeptá, změny tedy nebudou ztraceny.

TIP

Pokud je aktuální pohled jiný než lokální či sdílený (např. otevřený z mapy či událostní), bude možné po stisku tohoto tlačítka zadat před uložením jeho název.

Odstranění pohledu

Aktuálně vybraný pohled také můžete odstranit. K odstranění pohledu použijte tlačítko Odstranit pohled. Pohled bude odstraněn až po potvrzení následující zprávy (po stisku tlačítka **ANO**).

**POZNÁMKA**

Stejným způsobem může administrátor odstranit i pohled sdílený.

Indikátory

Každá pozice, do které byla v rámci pohledu přepnuta kamera, je vybavena vlastními indikátory. Jedná se o malé barevné symboly při pravém okraji záhlaví okna s názvem kamery. Jsou k dispozici tři indikátory.



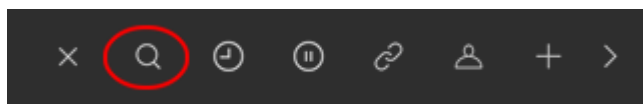
Pravý indikátor je zobrazen modře, pokud je zobrazené video živé. Při přehrávání záznamu pak indikuje, že video je pro přehrávaný čas k dispozici.

Prostřední indikátor je zobrazen červeně, pokud probíhá záznam. Pokud záznam neprobíhá, ale je tvořen předpoplachový buffer na serveru, je zobrazen žlutě.

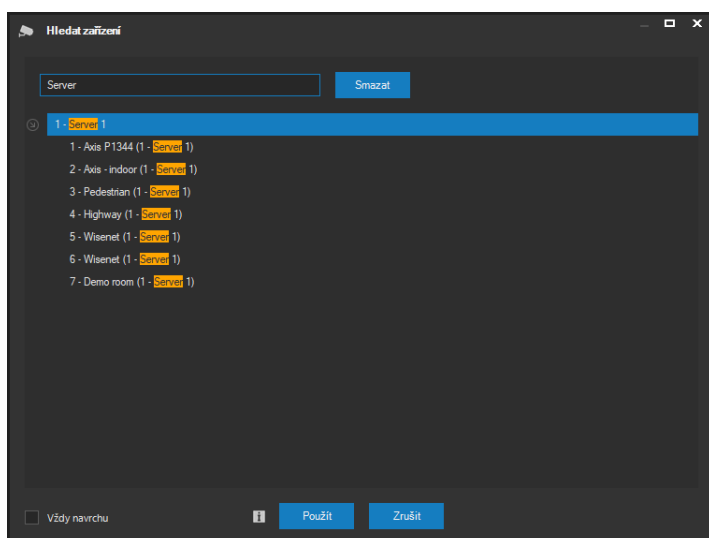
Levý indikátor je zobrazen bíle, pokud je aktivován šifrovaný přenos ze serveru. Pokud je úspěšně ověřen certifikát zařízení při přenosu https protokolem, indikátor je zobrazen fialově. Pokud platí obě skutečnosti současně, je indikátor zobrazen zeleně.

4.1.2. Vyhledávání kamer podle názvu

Při přepínání kamer do pohledu se lze primárně orientovat podle identifikace serveru a čísel kamer. V rozsáhlejších systémech však může být vhodná možnost vyhledávání kamer podle názvu přes všechny servery. K tomu slouží tlačítko vyhledávání.



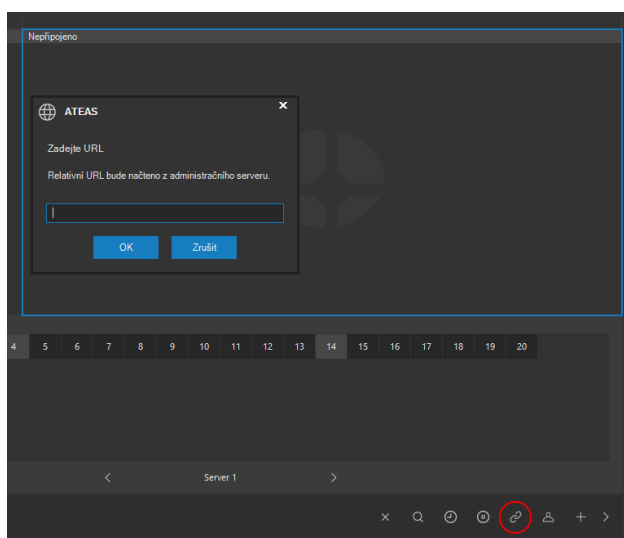
Dialog vyhledávání umožňuje začít psát název kamery, který bude vyhledán mezi všemi kamerami na všech serverech, ke kterým má uživatel přístup.



Po výběru konkrétní kamery z nabízených výsledků dojde k jejímu přepnutí do pohledu. Kamery lze do pohledu vkládat opakovaně i bez zavření okna dvojitým kliknutím na kameru.

4.1.3. Zobrazení webového obsahu

Kromě kamer lze na jednotlivé pozice pohledu přepnout také libovolný webový obsah. Okno pohledu podporuje nejnovější technologie zobrazení webového obsahu včetně HTML5, CSS3 a JavaScriptu. Webový obsah lze zobrazit pomocí tlačítka se symbolem webu, jak ukazuje následující obrázek.



POZNÁMKA

Možnost přepnout do pohledu webový obsah je vázána na příslušné uživatelské oprávnění.

Jako URL je možné použít libovolnou adresu s protokolem http nebo https. Pokud je použita relativní adresa, tj. adresa bez protokolu, bude adresa automaticky vyhledána v kontextu administračního serveru systému.

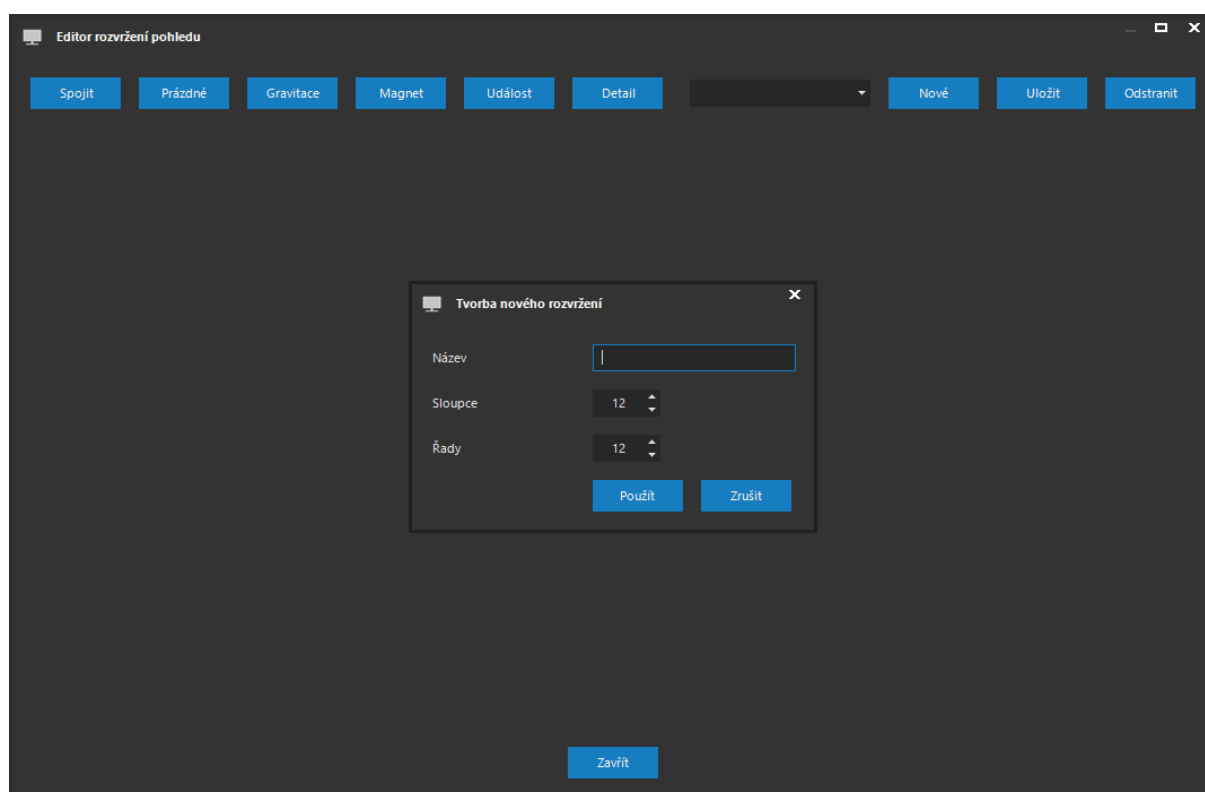
Po uložení je webový obsah automaticky součástí pohledu, který může být sdílen ostatním uživatelům.

POZNÁMKA

Velmi podobnou funkcí pro zobrazení webového obsahu disponuje i video stěna.

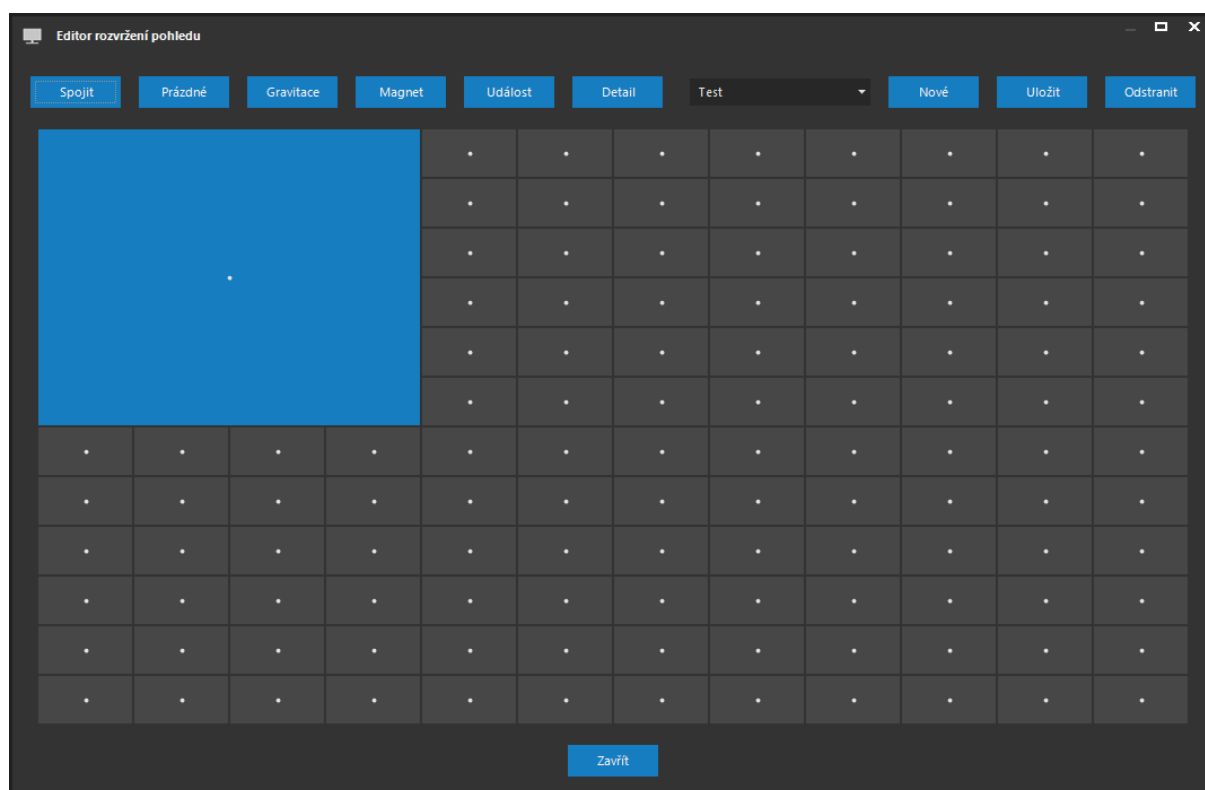
4.1.4. Editor rozvržení pohledů

Při tvorbě vlastních pohledů nevybíráme rozvržení pohledu z předem připravených skupin rozvržení (jako jsou čtvercová či širokoúhlá rozvržení), ale rozvržení si vytvoříme sami přímo v editoru. Nové rozvržení vytvoříme pomocí tlačítka **NOVÉ**.



V prvním kroku je nutné zadat pro nové rozvržení nějaký název a výchozí počet sloupců a řádků, které bude rozvržení obsahovat. Tyto hodnoty lze nastavit v rozsahu 1 – 20. Výchozí matice před případnou další úpravou rozvržení tedy může být rozdělena do maximálně 400 oken.

Rozvržení můžeme dále upravovat tak, že učiníme výběr několika oken v zobrazené matici a tlačítkem **SPOJIT** provedeme jejich spojení do jednoho okna. Tento postup můžeme opakovat dle libosti až do dosažení výsledného rozvržení. Při označování oken editor vždy automaticky výběr doplňuje tak, aby vznikl nejmenší možný obdélník.



Při postupném spojování oken v rozvržení se lze kdykoliv vrátit zpět do výchozí podoby. Tlačítko **PRÁZDNÉ** slouží k návratu do podoby s původním výchozím počtem sloupců a řádků.

Hotové rozvržení můžeme kdykoliv uložit pomocí tlačítka **ULOŽIT**, nebo smazat pomocí tlačítka **ODSTRANIT**.

POZOR

Přestože rozvržení může být na začátku rozděleno až do 400 pozic, uložit ho můžeme pouze tehdy, je-li jejich počet maximálně 121. To souvisí s maximální hranicí zobrazených kamer v jednom pohledu.

Úprava fyziky pohledu

V každém z oken v editoru rozvržení je zobrazen symbol tečky, který určuje gravitaci aplikovanou v tomto okně. Implicitně je gravitace nastavena na střed. Gravitace v okně s kamerou určuje, kam bude přitahována oblast videa v tomto okně. A to nejen v situaci, kdy je nativní rozlišení menší než oblast pro zobrazení videa, ale také v opačném případě při zapnuté volbě dodržení původního poměru stran. V této situaci totiž často vznikají svislé nebo vodorovné pruhy vedle videa.

Úpravou gravitace lze docílit efektu, při kterém bude zobrazované video buď umístěno ve středu nebo přitáhuto do jedné z těchto pozic v okně: vlevo na střed, vlevo nahoru, na střed nahoru, vpravo nahoru, vpravo na střed, vpravo dolů, na střed dolů nebo vlevo dolů.

Změna gravitace se provede tak, že stiskneme tlačítko **GRAVITACE** a poté klikneme do prostoru okna, jehož gravitaci chceme změnit. Gravitace bude nastavena na hodnotu, která nejvíce odpovídá bodu, kde bylo provedeno kliknutí.

POZNÁMKA

Změny gravitace lze využít zejména pro vytváření pohledů, které budou obsahovat video z kamer vybavených více objektivy, které mohou dohromady tvořit jednu scénu.

Pomocí tlačítka **MAGNET** lze ovlivnit další aspekt zobrazení kamery v pohledu. Podporován je pouze horizontální magnet. Pokud je aktivován, šířka okna se zobrazeným videem je automaticky upravena na velikost videa tak, aby nevznikaly žádné svislé pruhy bez zobrazeného videa a okna kamer vlevo a vpravo od zmagnetizovaného okna jsou přitažena co nejbližší k danému oknu.

Zmagnetizování okna se provede jeho označením při stisknutí tlačítka **MAGNET**. Zmagnetizování okna je indikováno dvěma svislými čarami u krajů okna.

POZNÁMKA

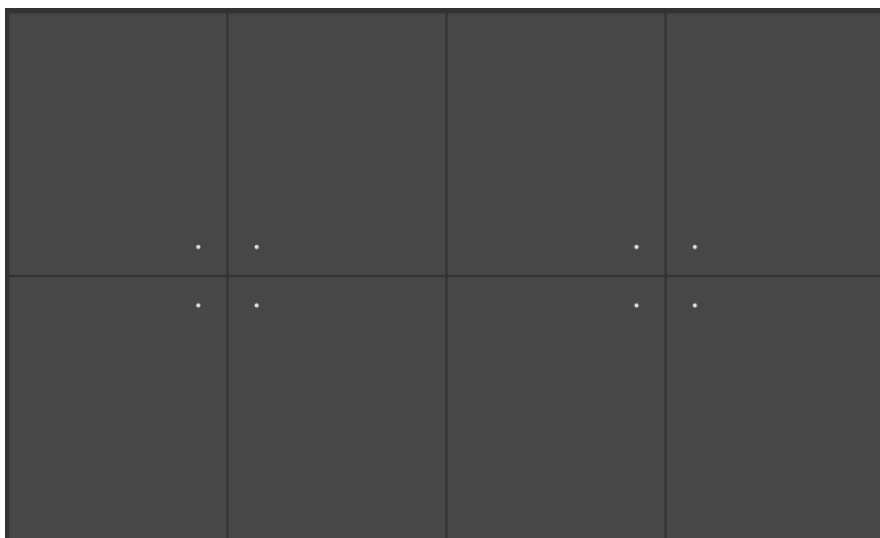
Pokud je zmagnetizováno více oken vedle sebe, magnet se přenesení až na první okno, které zmagnetizované není, pokud existuje. Pokud neexistuje, magnet je přenesen až na hranu dohledového okna. Pokud je však magnet přenesen na obě hrany okna, je aplikován rovnoměrně, a efekt nebude viditelný.

POZNÁMKA

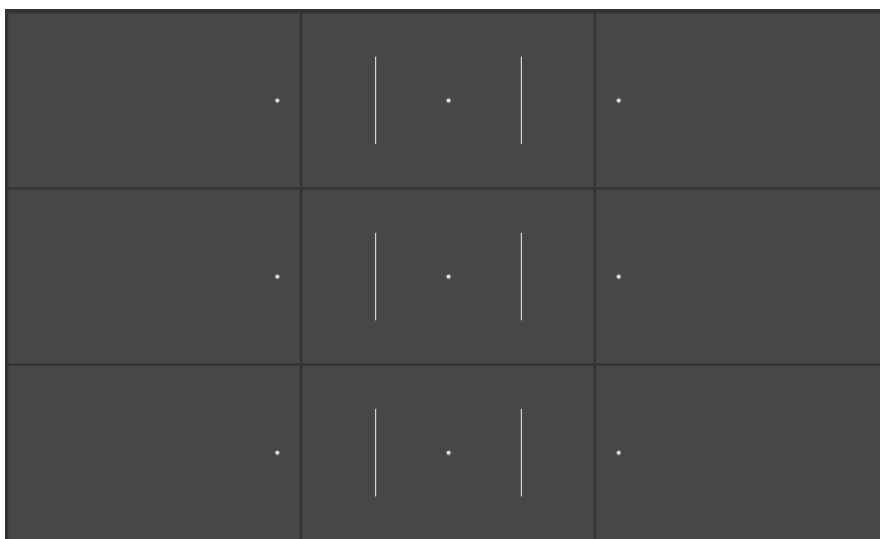
Pro ukončení nastavování gravitace či magnetu je nutné dané tlačítko uvolnit.

Příklady pro změnu fyziky

Příklad pro pohled obsahující 8 kamer, kde vždy čtyři kamery patří do jedné skupiny:



Příklad pro pohled obsahující 9 kamer, kde každá řada v pohledu obsahuje kamery sdružené v zařízení se třemi objektivy:



POZNÁMKA

Pokud je gravitace okna nastavena při horním okraji okna, je z důvodu vylepšení vizuálního dojmu automaticky skryto záhlaví okna kamery s jejím názvem. Přepnutí do detailu je v tomto případě (pouze v tomto případě) nutné provést dvojitým kliknutím do plochy videa.

POZNÁMKA

Změněná fyzika pohledu je samozřejmě aplikována i v situaci, kdy je takový pohled sdílen.

Pomocí tlačítka **UDÁLOST** lze vybrané pozice označit za událostní. Pokud je aktivní pohled, který obsahuje alespoň jednu událostní pozici, zobrazení události probíhá podle odlišných pravidel. Namísto zobrazení událostního pohledu v současném nebo novém dohledovém okně (dle nastavení) jsou pro zobrazení všech kamer připojených k události s příznakem zobrazit událost použity událostní pozice v dohledovém okně beze změny ostatních pozic.

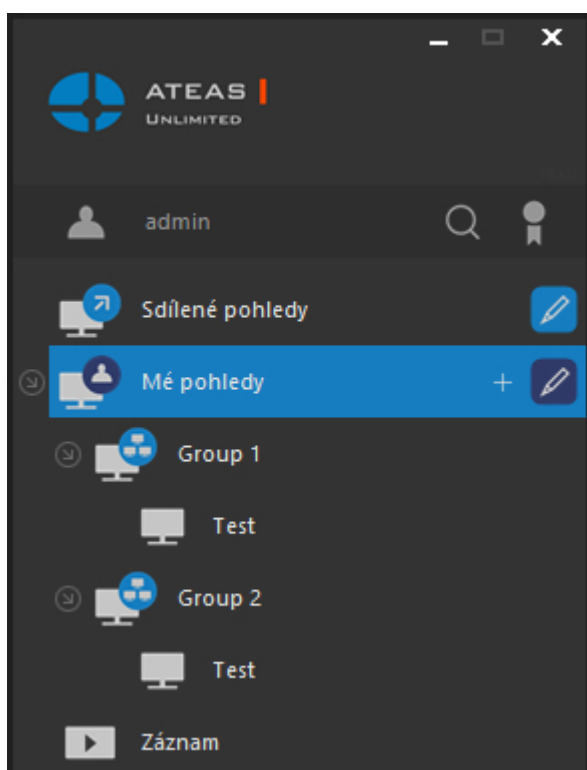
V takovémto případě dochází také k posunu předchozích událostí na další událostní pozice, takže událostí může být zobrazeno i více. Velmi podobný efekt mají událostní monitory na video stěně, kde též dochází k posunu událostí po monitorech.

Událostí pozice jsou v editoru vizuálně indikovány horizontální čarou a v pohledu mohou být odlišeny vlastním barevným indikátorem dle lokálního nastavení klienta.

Pomocí tlačítka **DETAIL** je možné některé pozice označit za cílové pozice pro zobrazení detailu. Tím lze docílit podobného efektu jako u centrických pohledů s jednou větší pozicí uprostřed sloužící pro zobrazení detailu. Do pozic označených jako pozice pro detail budou při zobrazení detailu kamery zobrazovány postupně.

4.1.5. Organizace pohledů

Pokud bude výsledný počet pohledů, které vytvoříte, přesahovat hranici, u které se ještě budete moci bez problémů orientovat v základní nabídce aplikace, lze doporučit přistoupit k organizaci pohledů. Organizace pohledů je způsob jak jednotlivé pohledy rozdělit do skupin pro snadnější orientaci v pohledech. Základní nabídka zohlední organizaci pohledů vytvořením dodatečné úrovně nabídky, která bude zobrazovat skupiny pohledů a teprve po volbě skupiny bude k dispozici seznam pohledů, jak ukazuje následující obrázek.



Organizace pohledů se provádí intuitivně přímo v nabídce pohledů. Pro zahájení editace je nutné aktivovat editační tlačítko vedle označení Mé pohledy nebo Sdílené pohledy.

Pomocí symbolu plus lze na dané úrovni vytvořit a pojmenovat novou skupinu pohledů, pomocí symbolu minus lze provést její odstranění.

Pohledy či celé skupiny pohledů lze poté přesouvat nebo kopírovat v rámci celé struktury lokálních nebo sdílených pohledů v závislosti na oprávněních uživatele. Přesun či kopie se provede přetažením myši do cílového umístění. Při přetažení v rámci lokálních či sdílených pohledů se implicitně provede přesun, při přetažení mezi lokálními a sdílenými pohledy kopie.

TIP

Toto chování lze ovlivnit současným přidržením kláves CTRL nebo SHIFT.

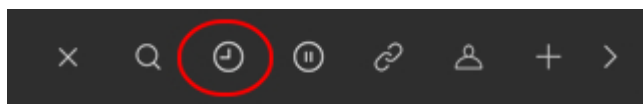
TIP

Pohled či skupinu lze přetáhnout i přímo do skupiny, ve které se již nachází. Takto lze rychle vytvořit kopii vybraného pohledu či skupiny.

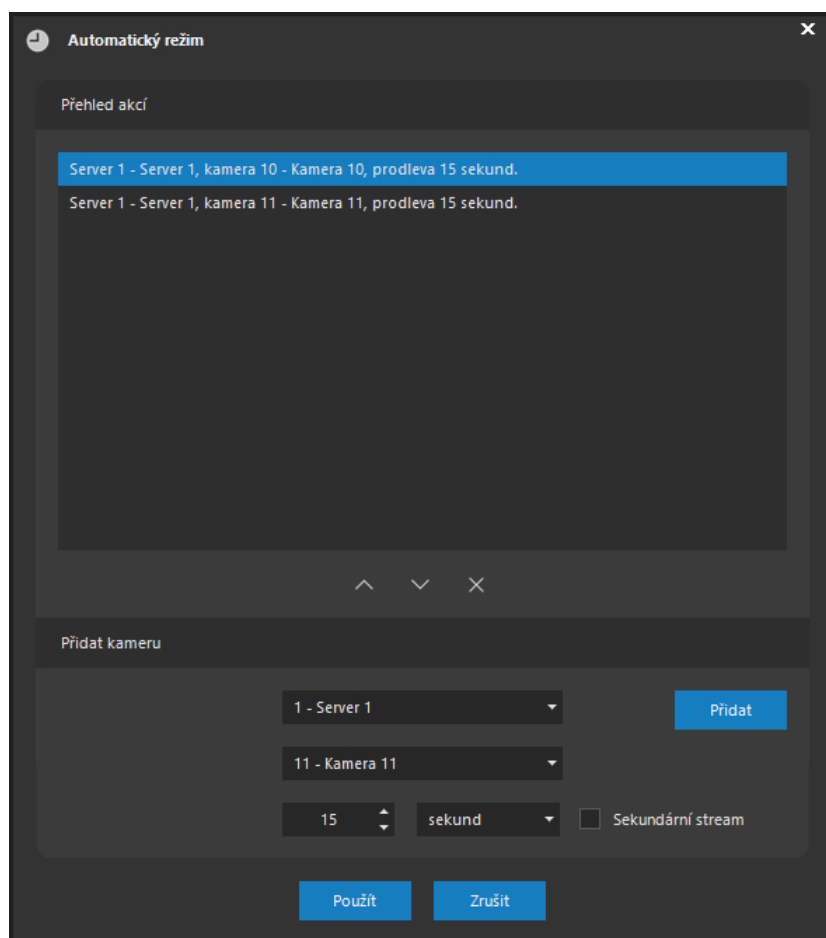
4.1.6. Automaty

Automaty jsou jednou z možností rozšíření pohledů. Namísto jedné staticky umístěné kamery na dané místo pohledu je možné danému místu pohledu přiřadit automat, který bude zajišťovat periodické přepínání vybraných kamer.

Přiřazení automatu se provede stisknutím tlačítka Automatický režim.



V následujícím dialogu je možné vytvořit automat, který bude po stisknutí tlačítka **POUŽÍT** aplikován na vybrané místo pohledu. Automat je uložen spolu s pohledem, tzn. že při příštím přepnutí tohoto pohledu budou též nastartovány všechny automaty v pohledu.



Automatický režim

Přehled akcí

- Server 1 - Server 1, kamera 10 - Kamera 10, prodleva 15 sekund.
- Server 1 - Server 1, kamera 11 - Kamera 11, prodleva 15 sekund.

Přidat kameru

1 - Server 1

11 - Kamera 11

15 sekund

☐ Sekundární stream

Přidat

Použít Zrušit

Každý automat sestává z neomezeného počtu akcí spočívající v přepnutí dané kamery na dané místo pohledu, kde je automat aplikován. Akci lze přidat vyplněním položek v části Přidat kameru a použitím

tlačítka **PŘIDAT**. Pokud je aktivní volba Sekundární stream, bude součástí automatu sekundární stream dané kamery.

POZNÁMKA

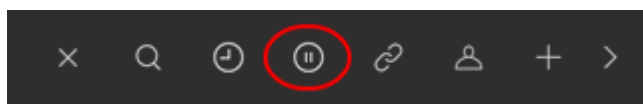
Minimální prodleva jsou čtyři sekundy, maximální jedna hodina.

Akci je možné z automatu odstranit tak, že ji vybereme a stiskneme tlačítko pro odstranění akce. Pomocí šipek pro přesun je také možné měnit pořadí již zařazených akcí.

Tlačítkem **POUŽÍT** bude automat aplikován pro vybranou pozici v pohledu. Automat lze jednoduše vypnout tak, že na místo, kde je aktuálně automat použit, přepnete kteroukoliv kameru nebo provedete vypnutí tohoto okna.

Ovládání automatů v pohledu

Automaty na daných pozicích pohledu jsou uloženy spolu s pohledem a automaticky opět spuštěny při jeho otevření. Pokud kameru, která je součástí automatu, přepneme do detailu (ve stejném dohledovém okně), dojde k automatickému přerušení automatu. Po návratu z detailu pak automatický režim pokračuje v místě přerušení. Pokud chceme automat přerušit bez přepnutí do detailu, můžeme k tomu využít tlačítko pro přerušení automatu.



Opětovné kliknutí na tlačítko způsobí pokračování automatu.

POZNÁMKA

Pokud chceme dočasně přerušit automatické režimy na všech pozicích pohledu najednou, použijeme pravé tlačítko. Při opětovném použití pravého tlačítka jsou všechny automatické režimy opět obnoveny. Pokud jsou automatické režimy v různém stavu, je stav upraven podle vybraného (nebo prvního) automatického režimu v pohledu.

4.1.7. Túry

Další možností rozšíření statických pohledů jsou vedle automatů také túry. Túry se vždy týkají dané kamery (nikoliv jako v případě automatu daného okna) a obsahují předdefinovaný pohyb pro danou kameru.

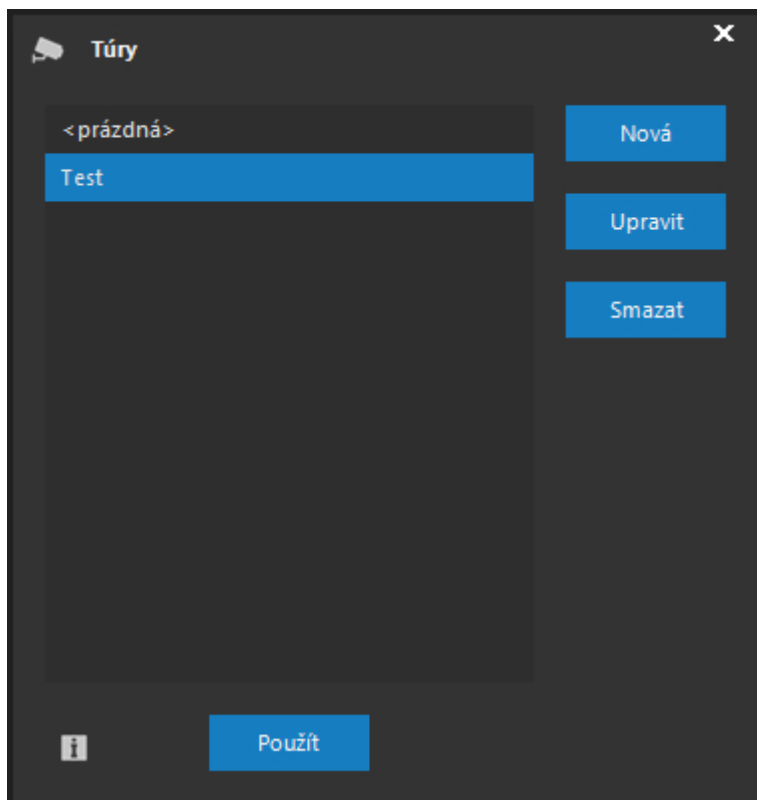
POZNÁMKA

Přístup k túrám mají pouze uživatelé s příslušným oprávněním. Přitom je možné rozlišovat, kteří uživatelé mohou túry pouze spouštět anebo také vytvářet či upravovat nebo mazat.

Pro každou otočnou kameru v systému může být vytvořeno a uloženo libovolné množství túr. Aktivní může být v daném okamžiku pouze jeden. Seznam túr pro danou kameru lze zobrazit tlačítkem Túra, které se nachází vedle přehledu presetů kamery.



Po stisku tohoto tlačítka se zobrazí přehled túr. Túra, ve které se daná kamera aktuálně nachází, je automaticky v seznamu označena.



Novou túru lze vytvořit stisknutím tlačítka **NOVÁ** a zadáním názvu, poté se túra objeví v seznamu. Odstranění se provede stisknutím tlačítka **SMAZAT**. Aktivace vybrané túry se provede tlačítkem **POUŽÍT**. Ukončení túry se provede výběrem první položky v seznamu.

Túru můžete pro kameru použít, pouze má-li definována alespoň jednu akci. V opačném případě se zobrazí varovná zpráva a túra nebude použita.

POZOR

Pokud je kamera v túře a některý z uživatelů bude kameru ovládat, túra bude přerušena. K jejímu obnovení dojde automaticky po uběhnutí časového intervalu od posledního ručního pohybu kamery, který lze nastavit v dialogu úpravy túry.

POZNÁMKA

Túry jsou řízeny příslušným kamerovým serverem a nejsou nijak závislé na uživateli, který je spustil (uživatel musí mít pro aktivace túry oprávnění). Túry jsou obnoveny též po restartu či výpadku serverů.

POZNÁMKA

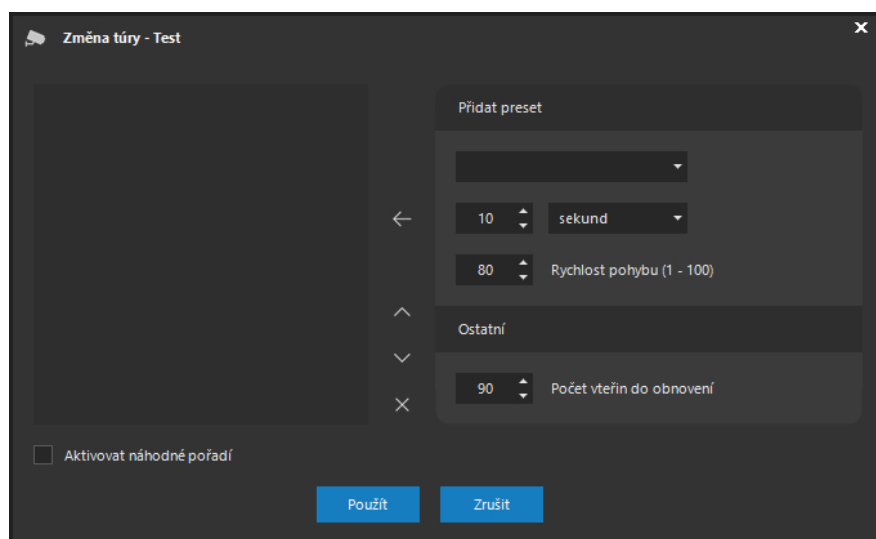
Túra bude také dočasně přerušena při události, pokud je předmětná kamera součástí událostního scénáře a má v jeho rámci definován pohyb na preset nebo přepnutí do jiné (poplachové) túry.

POZNÁMKA

Pomocí vytvoření túry, která bude obsahovat pouze jeden preset kamery, lze jednoduše docílit automatického návratu otočných kamer do výchozích (home) pozic.

Úprava túry

Aby mohla být nově vytvořená túra použita, je nutné ji editovat. Editace túry se provede stisknutím tlačítka **UPRAVIT**.

**POZOR**

Před vytvořením túry je nutné definovat pro danou kameru prepoziční body.

V seznamu akcí je uveden přehled všech prepozičních bodů, mezi nimiž se bude kamera cyklicky přesouvat. Akce tedy sestává z čísla prepozičního bodu, dále z rychlosti přesunu na tento bod v rozmezí 1 – 100 a z časové prodlevy do další akce.

POZOR

Parametr rychlosti nemusí podporovat všechny kamery.

Novou akci lze přidat vyplněním položek v části Přidat preset a stisknutím tlačítka šipky. Pomocí dalších tlačítek vedle seznamu akcí lze vybranou akci odstranit nebo měnit jejich pořadí.

Pro každou túru je také možné nastavit dobu, po kterou bude túra přerušena, pokud bude kameru manuálně ovládat oprávněný uživatel (jedná se tedy o dobu, která uplyne mezi posledním příkazem ručního ovládání od uživatele (z obrazu, joysticku apod.) do doby, kdy túra bude automaticky obnovena. Časový interval se nastavuje ve vteřinách v rozsahu od 10 vteřin do 60 minut. Implicitně je interval nastaven na 90 sekund.

Pod seznamem akcí je k dispozici volba Aktivovat náhodné pořadí. Pokud je tato volba pro vybranou túru aktivována, nebudou jednotlivé akce (pohyby na preset) spuštěny v definovaném pořadí, ale

v pořadí zcela náhodném. Pro pozorovatele je poté pohyb kamer a její příští nasměrování v každém okamžiku neodhadnutelné.

4.1.8. Otevření dalších oken

Další dohledová okna lze otevřít pomocí níže zobrazeného tlačítka až do celkového počtu 16 dohledových oken. Vybraný pohled bude vždy zobrazen v posledním aktivním okně. Pozice a rozměry všech oken spolu s informací o zobrazených pohledech lze uložit v rámci prostoru, a všechna okna tak lze otevřít jedním kliknutím v hlavní nabídce aplikace.



4.2. Události a poplachový pohled

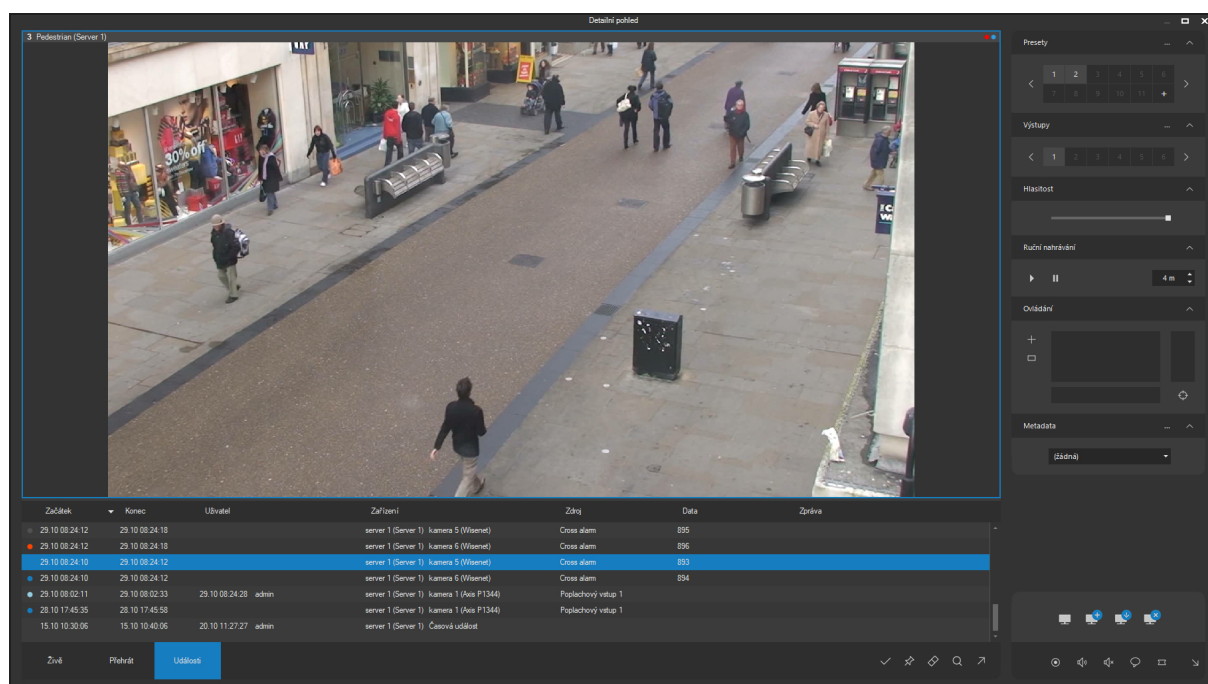
4.2.1. Příjem události

Libovolné dohledové okno může být konfigurováno pro příjem událostí v systému. Při příjmu události může dojít k automatickému přepnutí pohledu na administrátorem předdefinovaný událostní pohled, který bude zobrazovat danou událost.

Událost v systému vznikne, pokud je aktivován některý z aktuálně monitorovaných událostních vstupů. Událostním vstupem může být např. detekovaný pohyb v definovaném poli kamery, aktivace nebo deaktivace alarmového vstupu nebo aktivace připojeného čidla.

Chování aplikace při příjmu události je ovlivněno dílem nastavením ze strany administrátora (definice událostního pohledu), dílem ze strany uživatele (volba dohledového okna), dílem také aktuální situací v systému, viz popis dále. Uživatel má možnost určit dohledové okno, na kterém budou na kartě **Události** zobrazovány systémové události.

Při příjmu události se na kartě **Události** objeví řádek popisující vzniklou událost.



Mezi údaje, které se při příjmu události objeví na kartě **Události** patří:

- Stupeň závažnosti identifikovaný symbolem na začátku řádku. V systému se standardně rozlišuje mezi běžnými událostmi a událostmi typu alarm (běžné události nevyvolávají automatickou změnu pohledu v dohledovém okně). Běžné události může uživatel dokonce odfiltrovat tak, že vůbec nejsou v jeho dohledových oknech zobrazovány. Alarmy jsou uživateli zobrazeny vždy. Porušení dveřního kontaktu na dveřích může tak např. v denní době považováno za běžnou událost, zatímco v noci za událost poplachovou a systém bude v obou případech reagovat jinak.
- Datum a čas začátku a konce události, pokud konec události již nastal.
- Doba převzetí či uzavření poplachu a jméno uživatele, pokud je aktivován rozšířený režim řešení.
- Kamera (nebo jiný zdroj události), který vyvolal událost. Kamerový bod je určen identifikací serveru a identifikací kamerového bodu.
- Zdroj události na daném kamerovém bodu. Zdrojem události může být např. připojené čidlo nebo detekce pohybu apod. Zdroj události může být buď identifikován svým implicitním názvem (např. poplachový vstup 1) nebo symbolickým názvem (např. dveřní kontakt v hale).
- Další data k události. Může se jednat o doplňující informaci či upřesnění zdroje události (např. RZ vozidla).
- Uživatelská zpráva, která pro případ této události může obsahovat nejrůznější doplňující údaje jako např. pokyny pro obsluhu apod.

TIP

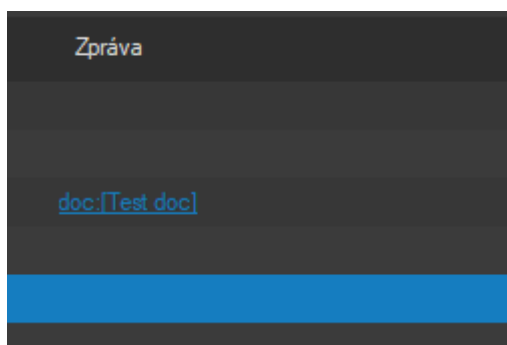
Nevyužívané sloupce mohou být skryty pomocí kontextové nabídky, pořadí a rozměry sloupců mohou být měněny přetažením myši. Tato nastavení jsou pak součástí uloženého prostoru.

Příjem události může vyvolat i automatickou změnu pohledu v daném dohledovém okně, také může být dle nastavení doprovázen i zvukovou notifikací pro upozornění obsluhy. Automaticky nebude pohled přepnut na událostní, pokud se jedná o běžnou událost nebo pokud od posledního přepnutí vyvolaného událostí neuběhl minimální nastavený časový interval. Tím je zajištěno, že při současném nebo časově zhuštěném příjmu více událostí nebude pohled neustále měněn, což by vedlo k zahlcení obsluhy. Příjem události je však zajištěn vždy, takže uživatel je bez automatického přepnutí pohledu informován, že došlo k další události. Události jsou na kartě **Události** řazeny od nejnovějších a jejich počet je nastavitelný. Způsob řazení může být kdykoliv změněn kliknutím na záhlaví konkrétního sloupce či sloupců.

POZNÁMKA

Událostní pohled, který pro danou událost definuje administrátor, může sestávat z různého počtu libovolných kamer, není tedy podmínkou, že se uživateli zobrazí vždy kamera, která událost vyvolala. Ta nemusí být vždy pro sledování událostí nejvhodnější a navíc je účelné při události přepnout uživateli i další kamery, které mohou být pro posouzení události a odhad situace klíčové.

Namísto uživatelské zprávy může být zobrazen také odkaz na dokument ve formátu PDF, který může obsahovat dodatečné textové i grafické informace k události.



Kliknutím na odkaz se otevře okno, ve kterém bude zobrazen příslušný dokument.

POZNÁMKA

Okno s otevřeným dokumentem zůstane otevřené i během další práce s dohledovým oknem, a operátor tak může mít dokument zobrazen současně s dohledovým oknem. Při kliknutí na jiný odkaz dokumentu bude obsah okna nahrazen posledním vyžádaným dokumentem.

Uživatel má možnost aktuálně vybraný událostní pohled zafixovat na obrazovce a zabránit tak automatickým změnám pohledu i po uplynutí ochranné doby pro základní posouzení události. To lze provést tlačítkem Podržet aktuální pohled.



Tlačítko zůstane po stisknutí ve stisknutém stavu, automatické změny pohledů budou obnoveny až po jeho opětovném stisknutí.



Pomocí tohoto tlačítka se symbolem gumy je možné vyčistit aktuální seznam událostí, který zobrazuje vždy nastavený počet nejnovějších událostí v systému z pohledu oprávnění daného uživatele či skupiny.

POZNÁMKA

Vyčištěním nelze odstranit poplachy určené k odbavení, které vyžadují aktivní reakci operátora.

4.2.2. Příjem akcí

Kromě událostí či událostí se statutem poplach může klientská aplikace v okně pro příjem událostí přijímat a zobrazovat také některé další skutečnosti, které nemají statut události a není možné či logické pro ně definovat kamerový scénář, kterým by systém na takovou skutečnost reagoval. Těmto skutečnostem se říká systémové akce a jsou zobrazeny pouze z důvodu upozornění obsluhy. V současnosti jsou zobrazovány tyto systémové akce:

- ztráta spojení či výpadek kamerového serveru (s významností poplachu),
- ztráta spojení či výpadek administračního serveru (s významností poplachu),

- obnova spojení s administračním serverem (s významností události),
- obnova spojení s kamerovým serverem (s významností události).

4.2.3. Přepínání událostí

Mezi jednotlivými událostmi, které se postupně objevují v seznamu na kartě **Události** je možné provádět přepínání. Výběrem řádku s událostí docílíte přepnutí do událostního pohledu přiřazeného administrátorem k této události.

POZNÁMKA

Přepnutí se samozřejmě provede vždy a nezávisle na závažnosti a uplynulším času od posledního přepnutí.

Začátek	Konec	Uživatel	Zařízení	Zdroj	Data	Zpráva
29.10.08:50:20	29.10.08:50:22		server 1 (Server 1) kamera 3 (Pedestrian)	Cross	659	
29.10.08:50:17	29.10.08:50:21		server 1 (Server 1) kamera 5 (Wienet)	Cross alarm	310	
29.10.08:50:17	29.10.08:50:21		server 1 (Server 1) kamera 6 (Wienet)	Cross alarm	311	
29.10.08:50:17	29.10.08:50:20		server 1 (Server 1) kamera 3 (Pedestrian)	Cross	612	
29.10.08:45:42	29.10.08:46:04		server 1 (Server 1) kamera 1 (Axis P1344)	Poplachový vstup 1		doc [Test.doc]
28.10.17:45:35	28.10.17:45:58		server 1 (Server 1) kamera 1 (Axis P1344)	Poplachový vstup 1		
15.10.10:30:06	15.10.10:40:06	20.10.11:27:27 admin	server 1 (Server 1) časová událost			

4.2.4. Rozdělení okna

Dohledové okno je rozděleno na část zobrazení pohledu a části ovládací. Mezi těmito částmi se nachází aktivní oblast, kterou je možné použít pro změnu poměru velikostí těchto částí okna. Takto lze tedy např. zvětšit prvek se zobrazenými čísly kamer nebo seznam zobrazených událostí. Tato změna je velmi vhodná tehdy, pokud seznam obsahuje značné množství událostí anebo pokud v nich chceme dále vyhledávat nebo je filtrovat.

POZNÁMKA

Pro rychlé zvětšení ovládací části lze použít též dvojité kliknutí na aktivní oblast sloužící ke změně rozměrů. Má-li ovládací část výchozí velikost, provede dvojité kliknutí změnu rozměrů tak, že velikost pohledu a ovládací části budou upraveny přesně na polovinu velikosti okna. Opětovné dvojité kliknutí provede návrat do výchozí podoby.

4.2.5. Samostatné událostní okno

Pomocí tlačítka uvolnění událostí z pohledu je možné události zobrazit v samostatném okně.



Samostatné událostní okno se chová velmi podobně jako události zobrazené přímo v dohledovém okně. Základní funkce výběru událostí, synchronizace času pro přehrávání, synchronizace mapy, vyhledávání v událostech atd. jsou shodné. V samostatném událostním okně jsou také k dispozici stejná tlačítka pro uzavření poplachu, fixaci pohledu a vyčištění seznamu událostí jako v dohledovém okně.

Události							
Začátek	Konec	Uživatel	Zařízení	Zdroj	Data	Zpráva	
29.10 08:12:45	29.10 08:12:46		server 1 (Server 1) kamera 5 (Wisenet)	Cross alarm	719		
29.10 08:12:45	29.10 08:12:46		server 1 (Server 1) kamera 6 (Wisenet)	Cross alarm	720		
29.10 08:12:43	29.10 08:12:45		server 1 (Server 1) kamera 6 (Wisenet)	Cross alarm	721		
29.10 08:12:43	29.10 08:12:45		server 1 (Server 1) kamera 5 (Wisenet)	Cross alarm	720		
29.10 08:12:42	29.10 08:13:00	admin	server 1 (Server 1) kamera 1 (Axis P1344)	Poplachový vstup 1			
29.10 08:12:37	29.10 08:12:43		server 1 (Server 1) kamera 5 (Wisenet)	Cross alarm	717		
29.10 08:12:37	29.10 08:12:43		server 1 (Server 1) kamera 6 (Wisenet)	Cross alarm	718		
29.10 08:12:34	29.10 08:12:37		server 1 (Server 1) kamera 5 (Wisenet)	Cross alarm	715		
29.10 08:12:34	29.10 08:12:37		server 1 (Server 1) kamera 6 (Wisenet)	Cross alarm	716		
29.10 08:12:32	29.10 08:12:34		server 1 (Server 1) kamera 5 (Wisenet)	Cross alarm	716		
29.10 08:12:32	29.10 08:12:34		server 1 (Server 1) kamera 6 (Wisenet)	Cross alarm	717		
29.10 08:12:29	29.10 08:12:32		server 1 (Server 1) kamera 6 (Wisenet)	Cross alarm	714		

Samostatné událostní okno může být pomocí ovládacích prvků ve spodní části opatřeno příznakem Vždy navrchu a může být také zpětně integrováno do libovolného dohledového okna.

POZNÁMKA

Nastavení cílového dohledového okna anebo samostatného okna pro příjem událostí automaticky mění lokální nastavení v části Monitory a obrazovky. Samostatné událostní okno je také součástí uloženého prostoru a může být v rámci prostoru opět otevřeno na předdefinované pozici a v dané velikosti.

4.2.6. Řešení poplachů

Pokud administrátor aktivuje pro některé zdroje událostí režim řešení poplachů, bude nutné každý poplach s aktivovaným režimem řešení nejdříve vyřešit, aby mohl být později odstraněn z dohledového okna. Vyřešený poplach (Vámi nebo jiným uživatelem) změní barvu své ikony na modrou. Na obrázku níže jsou zobrazeny všechny barevné možnosti pro ikony v seznamu událostí –

běžná událost, poplach, poplach s aktivovaným režimem řešení, Vámi přijatý a ještě neuzavřený poplach, vyřešený poplach a přijatý poplach jiným uživatelem.

Začátek	Konec	Uživatel	Zařízení	Zdroj	Data	Zpráva
29.10.08.50.20	29.10.08.50.22		server 1 (Server 1) kamera 3 (Pedestrian)	Cross	659	
29.10.08.50.17	29.10.08.50.21		server 1 (Server 1) kamera 5 (Wirenet)	Cross alarm	310	
29.10.08.50.17	29.10.08.50.21		server 1 (Server 1) kamera 6 (Wirenet)	Cross alarm	311	
29.10.08.50.17	29.10.08.50.20	20.10.11.27.27 admin	server 1 (Server 1) kamera 3 (Pedestrian)	Cross	612	
29.10.08.45.42	29.10.08.46.04	20.10.11.27.27 admin	server 1 (Server 1) kamera 1 (Axis P1344)	Poplachový vstup 1		doc.[Text.doc]
29.10.17.45.35	28.10.17.45.58	20.10.11.27.27 admin2	server 1 (Server 1) kamera 1 (Axis P1344)	Poplachový vstup 1		
15.10.10.30.06	15.10.10.40.06	20.10.11.27.27 admin	server 1 (Server 1) Časová událost			

Pro vyřešení vybraného poplachu je nutné provést dvojité kliknutí na daný poplachový řádek, případně použít tlačítko Uzavřít poplach. V následujícím dialogu je pak nutné doplnit komentář k vyřešení poplachu, případně explicitně zvolit možnost uzavření bez komentáře.

Uzavření poplachu

X

☐ Bez komentáře

-- Vytvořit nový text --

↑

Odstranit

Zbývající počet znaků:

200 (200)

Přijmout

Uzavřít

Zrušit

Poplach lze v tomto okně buď rovnou uzavřít anebo přijmout. Vyřešení i přijetí poplachu automaticky změní barevný indikátor všem uživatelům, kteří mají tento poplach zobrazen (barvy jsou odlišné).

Přijetí poplachu indikuje ostatním uživatelům (a pozdější kontrole deníku poplachů), že se daný uživatel poplachem zabývá a že ho dříve či později uzavře. To je vhodné např. v situaci, kdy pro uzavření poplachu není ještě k dispozici dostatek informací. Rozhodným časem pro hodnocení

operátora je čas přijetí (pokud k němu před uzavřením došlo). Přijaté poplachy (aktuálním či jinými uživateli) jsou od sebe barevně odlišeny, viz přehled barevných signalizací výše.

Pro rychlé odbavení poplachu je možné použít nějaký z předdefinovaných textů v rozbalovacím seznamu nad textovým polem pro zápis komentáře. Má-li uživatel přiděleno oprávnění pro rozšířené událostní funkce, může zároveň tyto předdefinované texty měnit, mazat anebo vytvořit nové.

Zapsaný text do pole komentáře lze mezi předdefinované texty uložit pomocí bílé šipky umístěné vpravo od textového pole. Pokud je v rozbalovacím seznamu vybrán konkrétní text, bude nahrazen. Pokud je vybrána první hodnota v seznamu, bude vytvořen nový text. Smazat předdefinovaný text lze pomocí tlačítka se symbolem křížku vedle rozbalovacího seznamu.

POZNÁMKA

Jednotlivým předdefinovaným textům jsou automaticky přiřazeny číselné hodnoty, výběr textové položky ze seznamu lze rychle učinit také přímo zadáním kódu z klávesnice.

POZNÁMKA

Údaje o vyřešení poplachu včetně informace o uživateli a čase vyřešení jsou k dispozici v deníku událostí v okně Záznam, kde je také možné doplňovat dodatečné komentáře k řešení.

4.2.7. Událostní pozice v dohledovém okně

Pomocí editoru pohledů lze v pohledu vytvořit událostní pozice (více viz popis editoru pohledů). Pokud jsou událostní pozice v pohledu vytvořeny, je událost zobrazena přímo na těchto událostních pozicích bez toho, aby došlo ke změně na ostatních pozicích v pohledu. Starší události jsou automaticky posouvány do dalších událostních pozic v okně.

Konfigurace pohledu s událostními pozicemi je zejména vhodná pro dohled na jednom monitoru a může být alternativou k funkci automatického navrácení z událostního pohledu.

TIP

Událostní pozice jsou zvýrazněny vlastním indikátorem, jehož barvu lze měnit v lokálním nastavení klienta.

4.3. Záznam pohledu

4.3.1. Přehrávání pohledu

Libovolný pohled (lokální, sdílený, událostní či detailní) je možné přepnout do režimu přehrávání, čímž je možné získat okamžitý a rychlý přístup k záznamu právě sledovaných kamer. Toto přepnutí se provede výběrem karty Přehrávání ve spodní ovládací liště.

POZNÁMKA

Do režimu přehrávání lze však přepnout maximálně pohled obsahující 16 oken. Lze tedy současně přehrávat maximálně 16 kamer.

Po přepnutí na kartu Přehrávání dojde k zastavení obrazu ze všech kamer a bude možné online přehrávat zaznamenaná data. Datum a čas se během přehrávání záznamu zobrazuje v pravé části karty Přehrávání. Pro vybranou kameru je automaticky přehráván také zvuk, pokud je v záznamu k dispozici.

Při přepnutí do přehrávání pohledu je čas přehrávání automaticky nastaven na poslední hodnotu při minulém přehrávání. Pokud však provedeme přepnutí z událostního pohledu, bude čas vždy automaticky nastaven na začátek poslední vybrané události.

Přehrávání pomocí ovládacího prvku přehrávače



Pomocí tohoto ovládacího prvku je možné přehrávat záznam aktuálního pohledu. Skupina dvou tlačítek vlevo na tomto ovládacím prvku slouží ke změně rychlosti přehrávání v rozmezí šestnáctinásobného zpomalení až šestnáctinásobného zrychlení. Skupina třech větších tlačítek uprostřed ovládacího prvku slouží ke změně směru či zastavení přehrávání. Dvě tlačítka vpravo mohou být použita pro rychlý přesun o daný časový interval vpřed či vzad. Tento časový interval je nastavitelný po kliknutí na jeho aktuální hodnotu. V následujícím okně lze pak zvolit předdefinovaný nebo nastavit vlastní časový interval, který po stisku tlačítka **POUŽÍT** bude přiřazen tlačítkům rychlého přechodu. Hodnota 1 snímek je časově nezávislá a umožňuje přechod mezi jednotlivými snímky.

 Rychlý přechod

☐ 1 snímek

☐ 1 sekunda

☐ 1 minuta

☒ 10 minut

☐ 1 hodina

☐ Vlastní

10

↑

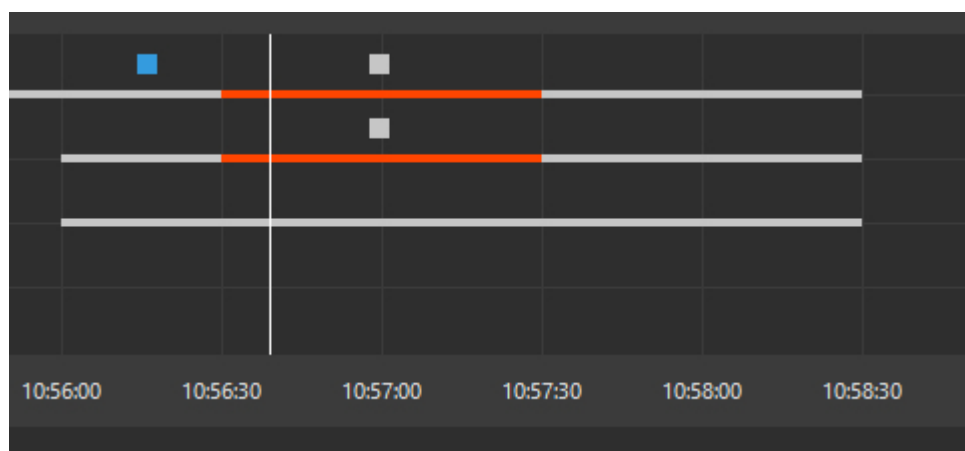
↓

sekund

Použít

Zrušit

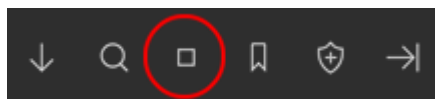
Přehrávání pomocí časové osy



Tento ovládací prvek graficky ukazuje, ve kterém čase je pro přehrávané kamery k dispozici záznam. Každá řada grafu ukazuje dostupnost zaznamenaných dat pro jednu z kamer, která je součástí přehrávaného pohledu. Barevně je odlišen událostní záznam (záznam při události), tj. situace, kdy daná kamera reaguje na událost pořizováním záznamu. Pokud je na tomto ovládacím prvku více řad, jsou řazeny podle jejich výskytu v pohledu (nejprve po řádcích, poté po sloupcích). Maximální počet současně zobrazených řad je 9. Pokud je přehráván pohled sestávající z více než 9 kamer (maximálně 16), je zobrazena vždy pouze jedna řada pro aktuálně vybranou kameru.

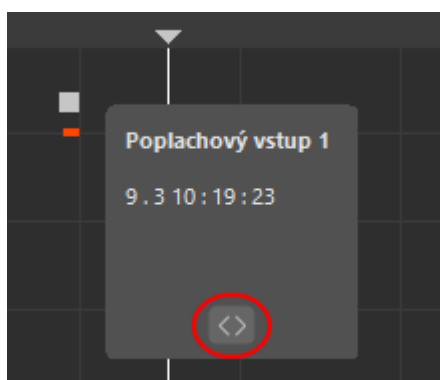
U jednotlivých časových řad mohou být také zobrazeny dodatečné popisné informace vztahující se k událostem a záložkám. Tyto informace mají podobu barevných čtvercových indikátorů, které při

setrvání kurzoru myši nad nimi zobrazí dodatečné informace. Funkci lze aktivovat pomocí tlačítka zobrazení událostí.

**TIP**

Jednotlivé události kamer či externí události mohou mít odlišné barvy pro snadnou a přehlednou orientaci na časové ose záznamu.

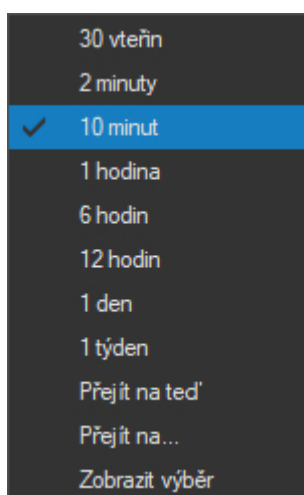
Dodatečně zobrazená informace nad událostí či záložkou je vybavena tlačítkem pro nastavení filtru, pomocí kterého lze konkrétní událost určenou serverem, kamerou a typem události či konkrétní záložku určenou serverem a kamerou použít jako filtr při procházení záznamu.



Po stisku tohoto tlačítka pak budou šipky pro rychlý přesun v prvku pro ovládání přehrávání automaticky posouvat časovou osu na další či předchozí výskyt této události či záložky a to až do doby výběru jiné události nebo přepnutím zpět na časový interval či snímek.

Vertikální bílá středová linie ukazuje čas záznamu. Ten vždy odpovídá časovému údaji zobrazenému na kartě **Přehrát**. Pomocí tohoto ovládacího prvku lze provádět rychlé přesuny v čase pomocí pohybu myši při stisknutí levém tlačítku (přetažení myši).

Tento ovládací prvek má nastavitelné časové rozlišení. Změnu časového rozlišení lze vyvolat vyvoláním kontextové nabídky tohoto prvku (stiskem pravého tlačítka myši), kde lze vybrat některý z předdefinovaných časových rozlišení. Rychlejší a jednodušší možností pro změnu rozlišení časové osy (zoom) je použití kolečka myši.

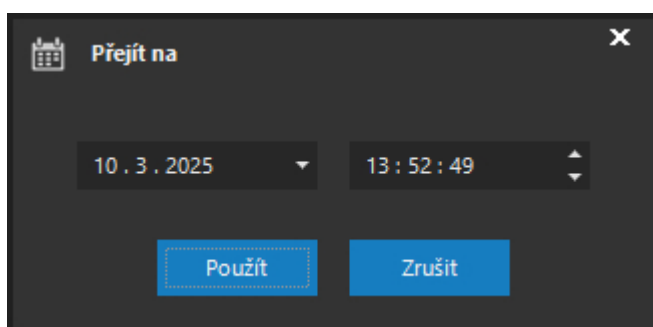


Volba Přejít na teď umožňuje rychlý přechod na aktuální datum a čas, tedy na nejnovější záznam.

POZNÁMKA

Tato funkce je užitečná zejména proto, že při aktivaci přehrávání záznamu na kartě Přehrávání je datum a čas záznamu automaticky nastaven na poslední přehrávaný úsek, a tudíž může být zapotřebí se rychle přesunout k poslednímu dostupnému záznamu.

Další volbou v této kontextové nabídce je položka Přejít na, pomocí které je možné otevřít jednoduchý dialog pro přímé zadání data a času pro přechod na konkrétní časový okamžik včetně možnosti zobrazit kalendář.



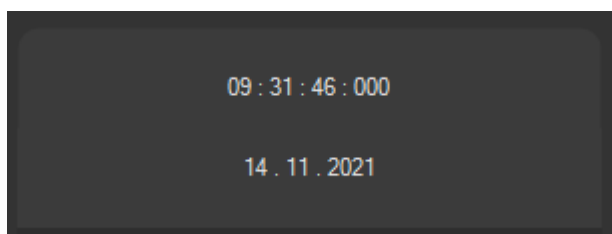
Volba Zobrazit výběr umožňuje zobrazit hranice intervalu přímo v časové ose přehrávání a provede zároveň jejich přesun do viditelné oblasti. Stejnou funkci má i dvojité kliknutí myši do časové osy.

POZNÁMKA

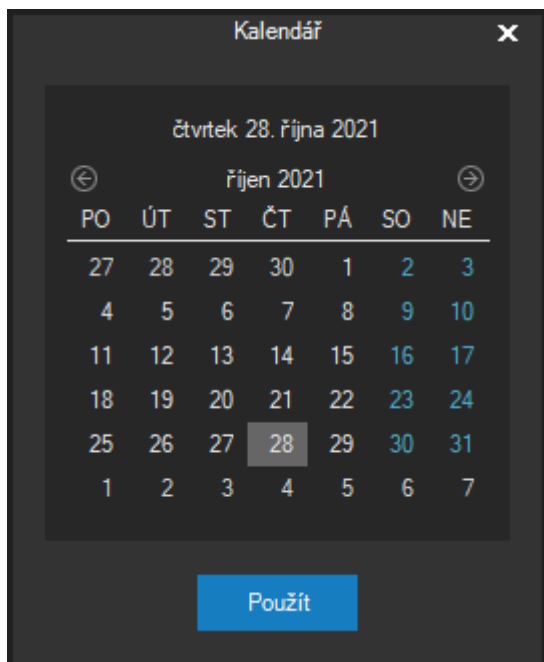
Stejně jako v živém pohledu je možné také během přehrávání pohledu dvojitým kliknutím na záhlaví okna kamery zobrazit detail kamery a následným dvojitým kliknutím provést přepnutí zpět do pohledu.

Výběr data a času v prvku se zobrazeným časem

Stejnou funkci jako volba Přejít na... má též kliknutí na symbol času v prvku, kde se zobrazuje aktuální datum a čas přehrávání.



Pokud klikneme na symbol kalendáře, můžeme pohodlně vybrat jiné datum při zachování aktuálního času přehrávání.



4.3.2. Automatické přehrávání

Pokud je aktivována funkce automatického přehrávání, bude možné plynule přehrávat pohled i v situaci, kdy pro vybranou kameru není v určitých intervalech k dispozici záznam. Jinými slovy, mezery při přehrávání videa budou automaticky přeskočeny a to během přehrávání oběma směry a při libovolně nastavené rychlosti přehrávání.



Tato funkce je zejména vhodná, pokud pro kameru provádíme záznam pouze při události.

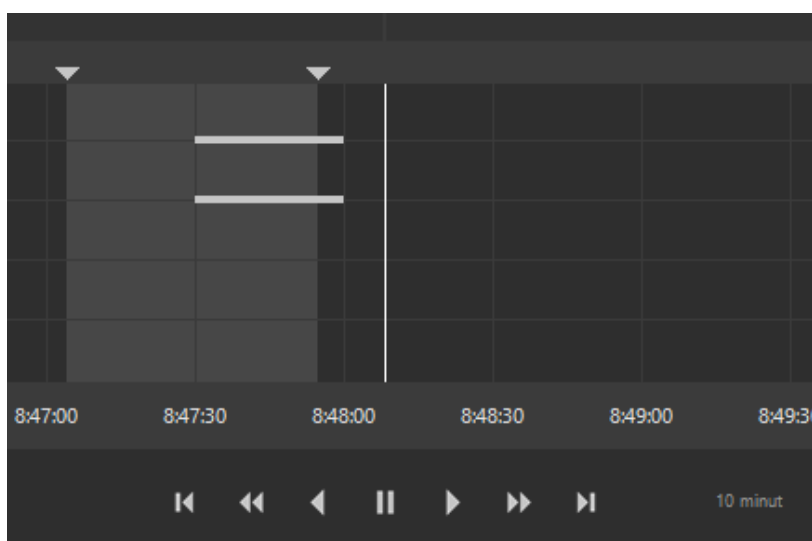
POZNÁMKA

Pokud přehrávaný pohled sestává z více kamer, váže se funkce automatického přehrávání vždy k vybrané kameře.

4.3.3. Stažení záznamu

Přímo z dohledového okna je možné provádět export dat ze záznamových oblastí kamerového serveru. Při tomto exportu dojde k vytvoření kopie dané sekvence na Vašem lokálním disku mimo záznamovou oblast kamerového serveru. Exportovaná sekvence je tak uložena trvale a může být dále přehrávána, upravována či exportována do jiných formátů.

Určení intervalu pro stažení lze provést přímo na časové ose přehrávání záznamu pomocí šipek pro určení intervalu.



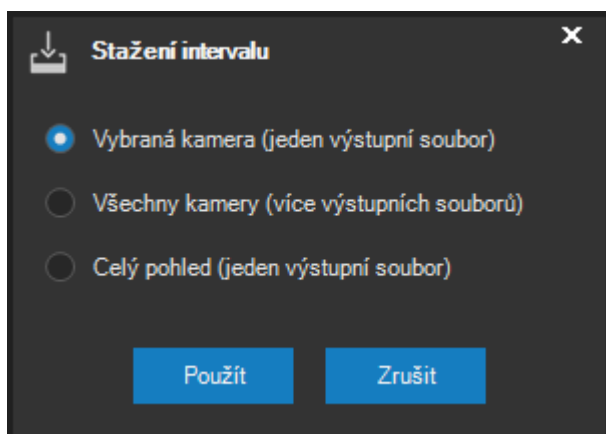
Při posunu šipek se automaticky synchronizuje celý pohled kamer a je průběžně zobrazován odpovídající čas, aby bylo možné daný interval nastavit co nejpohodlněji. Přesné zadání začátku či konce intervalu lze provést dvojitým kliknutím na jednu z šipek, který aktivuje funkci Přejít na.

Pokud jsou v daném okamžiku hranice intervalu mimo zobrazenou oblast časové osy, lze dvojitým kliknutím na časovou osu interval nastavit do viditelné oblasti. Ten samý efekt má funkce Zobrazit výběr v kontextové nabídce časové osy.

Zahájit stahování lze provést pomocí následujícího tlačítka.



Po stisknutí tohoto tlačítka bude zobrazen dialog, ve kterém je možné zvolit způsob ukládání dat.



První volba znamená, že budou stažena data pouze pro vybranou kameru. Druhá volba provede stažení daného intervalu pro všechny kamery v pohledu s tím, že pro každou kameru bude vytvořen samostatný výstupní soubor. Třetí volba provede také stažení daného intervalu pro všechny kamery, ale s tím rozdílem, že bude vytvořen pouze jeden výstupní soubor, který bude obsahovat data všech kamer. Při této poslední možnosti je ve výsledném souboru vždy zachováno i rozvržení pohledu s výjimkou pohledů s vlastním rozvržením.

POZNÁMKA

Pokud zvolíte třetí možnost (stažení všech kamer pohledu do jednoho výstupního souboru), musí být v okně Manažera stahování jako cíl stahování zvolena Vlastní složka a současně musí být všechny kamery v pohledu připojené k jednomu serveru.

POZNÁMKA

Každé dohledové okno si pamatuje poslední použitou možnost a bude Vám ji při Vaší práci se systémem automaticky nabízet jako výchozí.

TIP

Součástí exportovaných dat mohou být i textová data transakcí, pokud jsou transakce zobrazeny na některých pozicích v pohledu.

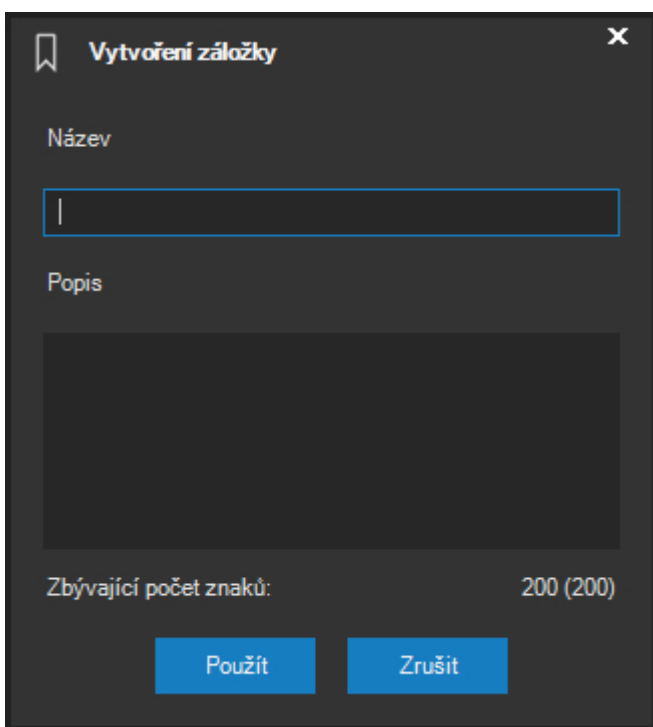
Označený interval pro stažení záznamové sekvence musí být v rozsahu 5 vteřin až 40 dní. V opačném případě bude aplikace reagovat varovnou zprávou a stahování nebude zahájeno.

Je-li interval pro stažení delší než 30 minut, bude provedeno automatické rozdělení intervalu pro snazší manipulaci se staženými daty.

Stahování dat ze záznamových oblastí jednotlivých kamerových serverů je prováděno pomocí inteligentního manažera stahování, který je popsán v samostatné kapitole. Manažer stahování eviduje požadavky na stažení jako své úkoly, které postupně či paralelně provádí.

4.3.4. Vkládání záložek

Tlačítko pro vložení záložky se nachází ve skupině tlačítek funkcí záznamu pohledu. Záložky jsou uživatelem doplněné informace vztahující se k určitým okamžikům zaznamenaného videa. Po stisku tlačítka se zobrazí následující dialog pro vložení záložky.



Každá záložka musí mít definován nějaký nadpis a volitelně je možné dopsat podrobnější komentář limitovaný délkou 200 znaků.

POZNÁMKA

Vkládání záložek je možné, pouze pokud je uživateli přiděleno příslušné oprávnění pro přístup k záložkám.

POZNÁMKA

Záložku bude možné vložit pouze tehdy, jsou-li poblíž časového okamžiku pro vložení záložky pro vybranou kameru k dispozici nějaká zaznamenaná data na serveru.

4.3.5. Inteligentní vyhledávání

Pokud se libovolné dohledové okno nachází v režimu přehrávání, je možné provádět inteligentní vyhledávání v zaznamenaných datech. Inteligentní vyhledávání umožňuje provádět rychlé vyhledání objektů dle jejich typů, počtu, směru pohybu, doby setrvání ve vymezeném prostoru, barev apod.

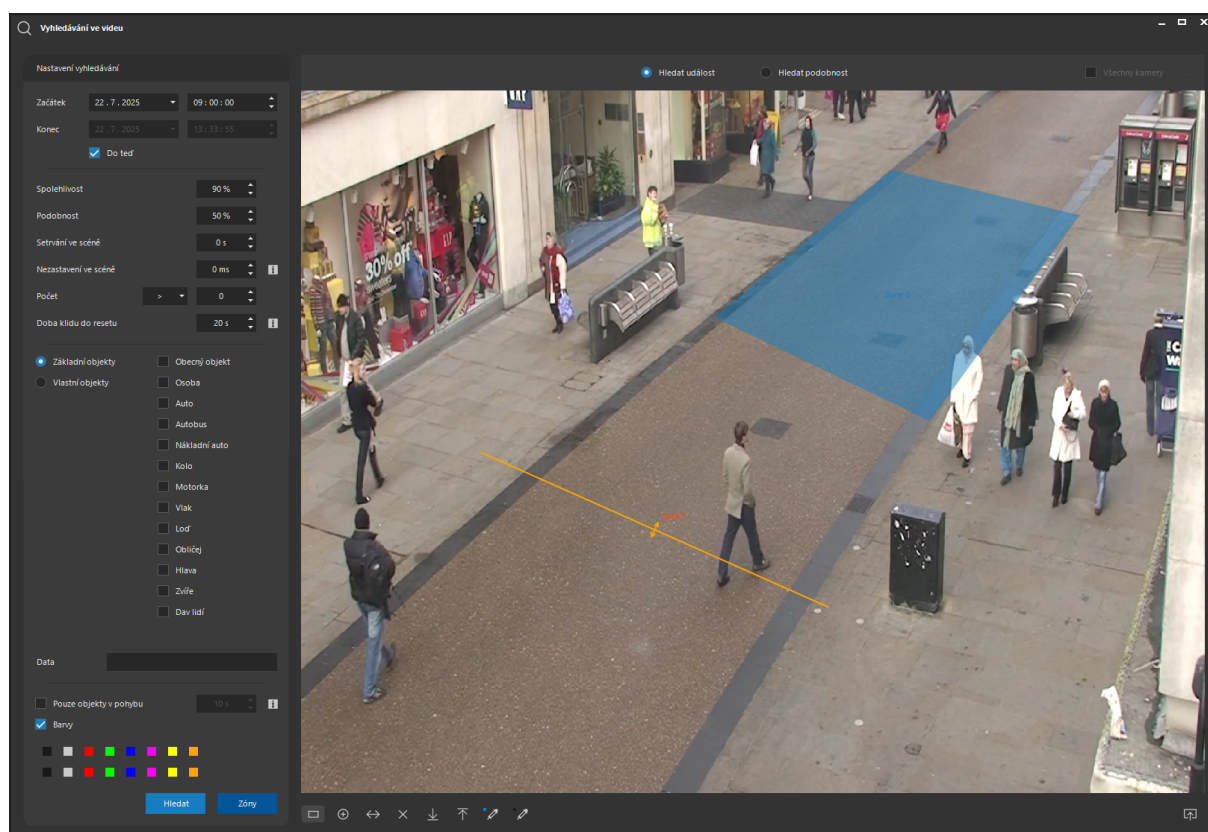
POZOR

Aby mohla funkce inteligentního vyhledávání generovat nějaké výsledky, musí administrátor systému aktivovat neuronovou síť a ukládání analytických metadat pro vybrané kamery.

Před samotným spuštěním funkce je nutné vybrat kameru a aktivovat funkci.



Tlačítkem Vyhledávání ve videu bude otevřeno následující okno, ve kterém je možné spustit funkci vyhledávání. Pokud je již okno vyhledávání otevřeno, bude aktualizován obrázek pro definice události či výběr objektu. V horní části okna lze vybrat mezi vyhledáním události (definicí podmínek) či podobnosti (definicí vzoru).



POZNÁMKA

Pokud byl na otočné kamery předem aktivován preset, bude vyhledávání omezeno pouze na objekty svázané s tímto presetem.

V části Nastavení vyhledávání je možné omezit časový úsek pro vyhledávání. Pokud je aktivována volba Do teď, je vyhledávání provedeno až do současnosti.

Volby Spolehlivost, Podobnost, Setrvání ve scéně, Nezastavení ve scéně, Počet a Doba klidu do resetu vstupu mají stejný význam jako v případě nastavení analytických zdrojů události. V případě inteligentního vyhledávání jsou však tyto hodnoty uplatněny na uložená neuronová metadata až při vyhledávání. V libovolné zóně je tak možné vyhledat objekty s danou spolehlivostí detekce, s daným časem setrvání objektů v zóně, v daném počtu v jedné zóně apod.

V části Objekty lze vybrat typy objektů, které budou vyhledány. Objekty jsou rozdělené do dvou skupin, je možné provádět výběr současně z obou dvou. V základní skupině jsou uvedeny objekty, které jsou podporovány volně dostupnými neuronovými sítěmi ATEAS, ve vlastní skupině jsou zobrazeny typy objektů, které si vytvoříte sami. Více viz kapitola o vlastních typech objektů.

První položka Obecný objekt prohledává metadata generovaná pokročilým detektorem pohybu, nikoliv neuronovou sítí. Pro použití této volby tedy stačí u příslušné kamery aktivovat pořizování těchto metadat.

POZNÁMKA

Při vyhledávání nelze kombinovat výběr obecného objektu a objektů neuronových sítí.

V části Data je možné omezit vyhledávání vybraných typů objektů na objekty doplněné o konkrétní data. Využívá se např. pro omezení vyhledávání objektu typu obličej pouze na osoby s konkrétním jménem či v konkrétní skupině.

Volba Pouze objekty v pohybu umožní filtrovat vyhledané incidenty tak, že je mohou způsobovat pouze objekty v pohybu. Časová hodnota udává dobu, po kterou musí být objekt v klidu, aby nebyl považován za objekt v pohybu.

V části Barvy je možné omezit vyhledávání jen na objekty s danou převažující barvou či kombinací barev (u osob).

Tlačítkem **ZÓNY** se aktivuje možnost kreslení a úpravy zón či vícebodových čar, kde bude prováděno vyhledávání. Všechna tlačítka pro vytváření a editaci zón pod náhledem videa jsou shodná jako při tvorbě analytických událostních zdrojů, kde jsou také popsána. Tlačítko **HLEDAT** následně zahájí vyhledávání.

Vyhledané výsledky lze stránkovat pomocí tlačítek **PŘEDCHOZÍ** a **DALŠÍ**, pomocí ovládacího prku pod výsledky lze provést rychlý náhled videa před a po události. Dvojitě kliknutí na výsledek vyhledávání provede otevření daného časového okamžiku v režimu přehrávání v dohledovém okně. Pod náhledem výsledků je k dispozici časový údaj prvního vyhledaného výsledku.

TIP

Pomocí klávesy CTRL lze označit i více výsledků vyhledávání, a po dvojitém kliknutí tak otevřít pohled i více kamer v čase, který odpovídá výsledku, na kterém bylo provedeno dvojitě kliknutí.

4.3.6. Vyhledávání dle podobnosti

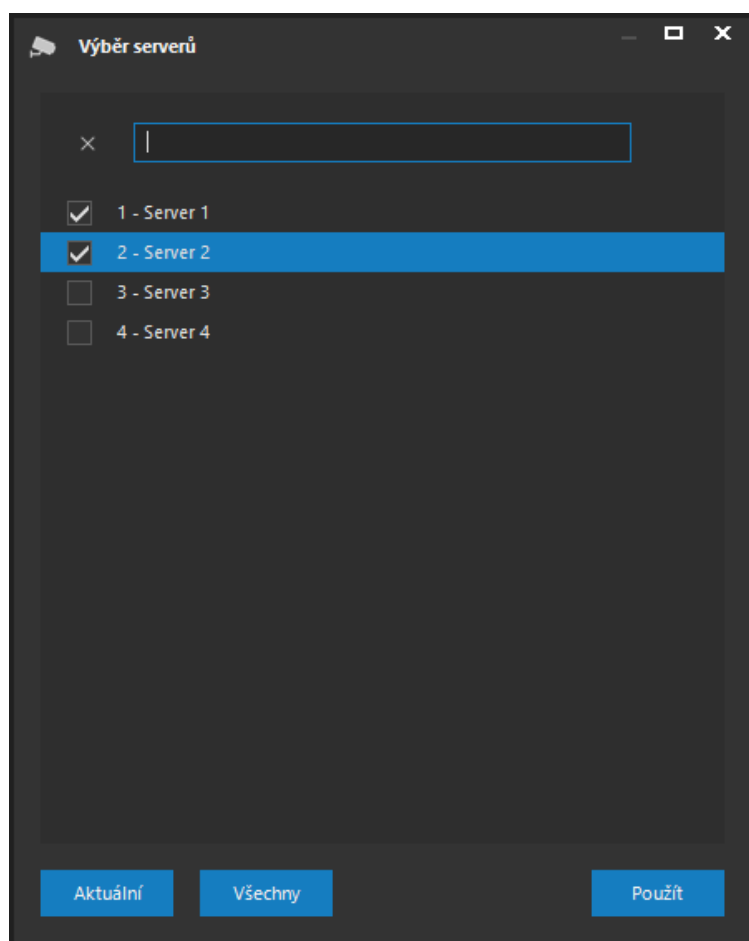
Pokud v systému existuje událost vyvolaná na základě podobnosti (rozpoznání obličeje), je možné ji dohledat i mezi běžnými metadaty včetně jména osoby či skupiny. Pokud v minulosti došlo k rozpoznání na základě podobnosti a je aktivováno ukládání metadat neuronových sítí, je možné provést vyhledání i se zadáním např. jména osoby do pole Data při aktivované volbě Hledat událost.

Pokud není možné použít ani jeden z těchto způsobů, je možné aktivovat volbu Hledat podobnost v horní části okna.

Po aktivaci této volby bude možné vybrat právě jednu uzavřenou zónu, ve které se nachází vzor pro vyhledávání. Následné vyhledávání bude probíhat na základě zadaných parametrů spolehlivosti a podobnosti dle shody s vybraným vzorem. Vyhledávání je možné provádět např. pro obličeje či celé osoby, typ objektu je zjištěn automaticky.

Pokud není hledaný vzor součástí záznamu kamerového systému, je možné do okna importovat obrázek ve formátu jpeg nebo bmp, který lze použít pro označení hledaného vzoru. Import lze provést tlačítkem v pravém spodním rohu okna.

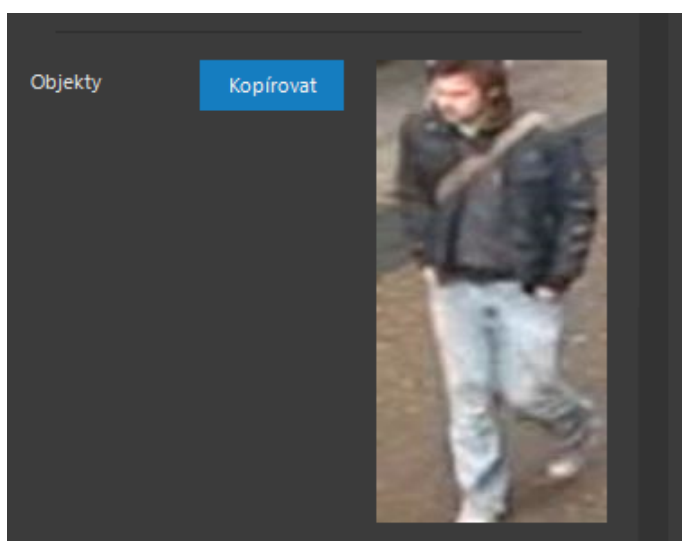
Při vyhledávání dle podobnosti je možné pomocí volby Všechny kamery vyhledávání rozšířit na všechny kamery na daném kamerovém serveru nebo na všechny kamery v systému (na všech kamerových serverech). Pro výběr serverů, které budou zahrnuty do vyhledávání, slouží dialog pro výběr serveru.



Tlačítkem **VŠECHNY** lze zahrnout všechny kamerové servery, tlačítko **AKTUÁLNÍ** aktivuje pouze server, ke kterému patří kamera v okně vyhledávání.

Na výsledek vyhledávání má vliv, zdali má neuronová síť aktivováno sledování či nikoliv. Pokud ano, bude možné výsledky lépe filtrovat a nenabízet opakovaně např. stejnou osobu hned po vypršení nastavené doby pro reset události, protože systém bude vědět, že se jedná o stále stejnou osobu, která ještě neopustila scénu.

Při vyhledávání na základě podobnosti je hledaný vzor zobrazen a může být zkopírován např. do databáze obličejů či do funkce Osobního hlídače. Výsledky vyhledání je možné ve scéně též automaticky přiblížit, pokud je aktivována volba Zoomovat výsledky.

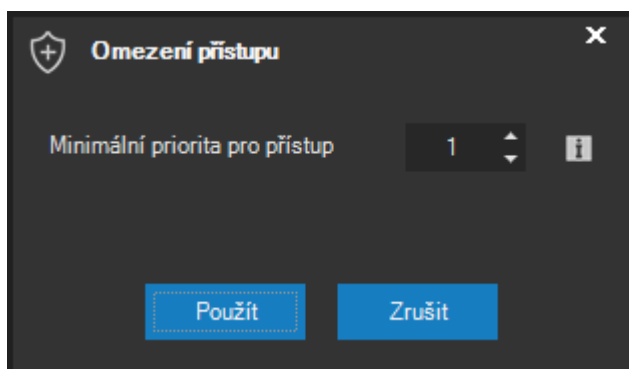


4.3.7. Omezení přístupu k záznamu

Administrátor systému může využít různé nástroje pro omezení přístupu uživatelů k záznamu kamer. Základní nástroj je řízení přístupu ke kamerám pomocí nastavení oprávnění a omezení. Další možností je omezení doby záznamu, ke které může uživatel přistupovat, např. pouze jednu hodinu či den do minulosti. V situaci, kdy chceme uživatelům zamezit v přístupu ke konkrétnímu záznamu, můžeme využít nástroj na omezení přístupu.

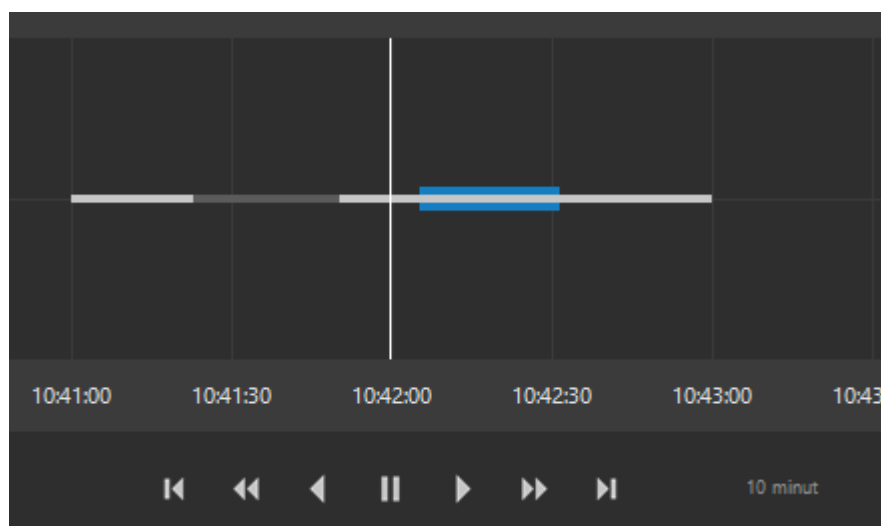


Před aplikací tohoto nástroje musí být vybrána kamera a také interval záznamu jedním ze způsobů popsaných výše v kapitole Uložení sekvencí. Po kliknutí na tlačítko omezení přístupu k záznamu se zobrazí následující dialog.



Pomocí určení minimální priority pro přístup k danému intervalu záznamu lze docílit toho, že uživatelé s nižší prioritou přístupu k záznamu (u dané kamery) nebudou moci přistupovat (přehrávat ani

stahovat) konkrétní části záznamu. Zobrazení v časové ose indikuje, ke kterým částem záznamu byl omezen přístup, a také, jestli naše aktuální nastavená priorita přístupu k záznamu umožňuje nebo neumožňuje záznam prohlížet.



POZNÁMKA

Nastavení minimální priority na hodnotu 0 ruší omezení pro daný interval. Samozřejmě pouze tehdy, je-li naše priorita vyšší než priorita uživatele, který omezení nastavil.

POZNÁMKA

Nástroj může využít každý uživatel v rámci své administrátorem přiřazené maximální priority pro přístup k záznamu. Implicitně má ovšem tato priorita hodnotu jedna, a proto omezení sice lze nastavit, ale v praxi nebude účinné.

4.4. Funkce vybrané kamery

4.4.1. Výběr kamery

Libovolnou kameru v daném pohledu lze vybrat kliknutím kamkoliv do prostoru daného kamerového okna, které je vymezeno záhlavím s číslem, názvem a dalšími údaji ke kameře, plochou pro zobrazení kamerového obrazu a samotným obrazem kamery (pokud je v danou chvíli dostupný). Kolem vybrané kamery se vždy zobrazí modrý rámeček.

POZNÁMKA

Pokud je aktuální pohled složen pouze z jedné kamery, je tato vybrána automaticky.

POZOR

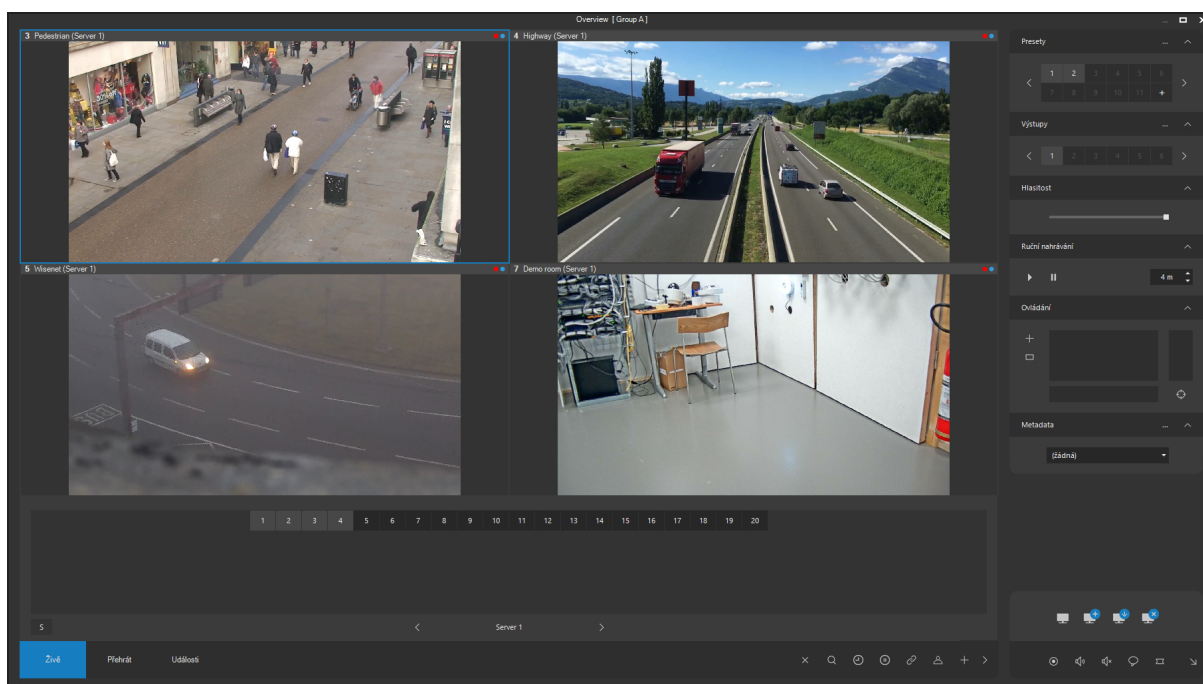
Je lépe vybírat kamery kliknutím na jejich záhlaví než přímo do obrazu. Vzhledem k tomu, že otočné kamery lze ovládat přímo klikáním do obrazu, může vést kliknutí do obrazu k natočení kamery, pokud se jedná o kameru otočnou.

Výběr kamery je též možné provést volbou jejího čísla na numerické klávesnici, podobně jako tomu je u speciálních kamerových klávesnic. Volbu provedeme tak, že na numerické klávesnici postupně stiskneme všechny číslice, které tvoří číslo kamery (např. 1, 2, 3 pro kameru číslo 123), a potvrdíme klávesou ENTER. Výběr kamery je proveden na aktuálně vybranou pozici pohledu.

POZNÁMKA

Implicitně jsou klávesy v numerické části klávesnice používány pro PTZ ovládání kamery. Pokud chcete numerickou klávesnici používat pro výběr kamer, je nutné změnit nastavení numerické klávesnice v lokálním nastavení klienta. Pro PTZ ovládání pomocí klávesnice lze pak dále používat také kurzorové šipky.

4.4.2. Zobrazení detailu



Kteroukoli kameru, která je v aktuálním pohledu a je pro ni dostupný její kamerový obraz, je možné přepnout do detailu. To znamená, že daná kamera bude přepnuta do detailního pohledu, který bude obsahovat pouze jednu kameru. Zcela automaticky a dle nastavení administrátora bude při uplatnění detailu kamerový obraz k dispozici v maximálním možném rozlišení v dané situaci (vzhledem k nativnímu rozlišení kamerového obrazu a rozlišení monitoru) a také ve zvýšené (maximální) snímkové frekvenci.

Přepnutí kamery do detailního pohledu lze provést v libovolném dohledovém okně dvojitým kliknutím na záhlaví daného kamerového okna. Zpětné přepnutí do původního pohledu je možné opět dvojitým kliknutím do záhlaví vybrané kamery v detailním pohledu. Detailní pohled bude také ukončen při volbě jiného pohledu z hlavní nabídky nebo při přepnutí do událostního pohledu.

Cílové dohledové okno, kam bude detailní pohled přepnut, lze nastavit v části Nastavení. Implicitně bude při detailu nahrazen aktuální pohled detailem, dojde tedy k zobrazení detailu v aktuálním dohledovém okně. Toto chování lze však upravit, viz sekce Nastavení.

Výjimku tvoří situace, kdy se nacházíme v tzv. centrickém pohledu (kamery uspořádané kolem jednoho většího kamerového okna), přepnutí do detailu se provádí přímo v rámci pohledu do pozice uprostřed pohledu.

4.4.3. Ukládání snímků

Pro vybranou kameru je možné ukládat snímky. Snímkem se rozumí aktuální stav kamerového obrazu převedený do některého obrazového formátu běžně podporovaného na všech platformách (JPG, BMP apod.). Snímek vybrané kamery je možné uložit pomocí tlačítka Sejmout snímek na boční ovládací liště, která se vždy váže k vybrané kameře.



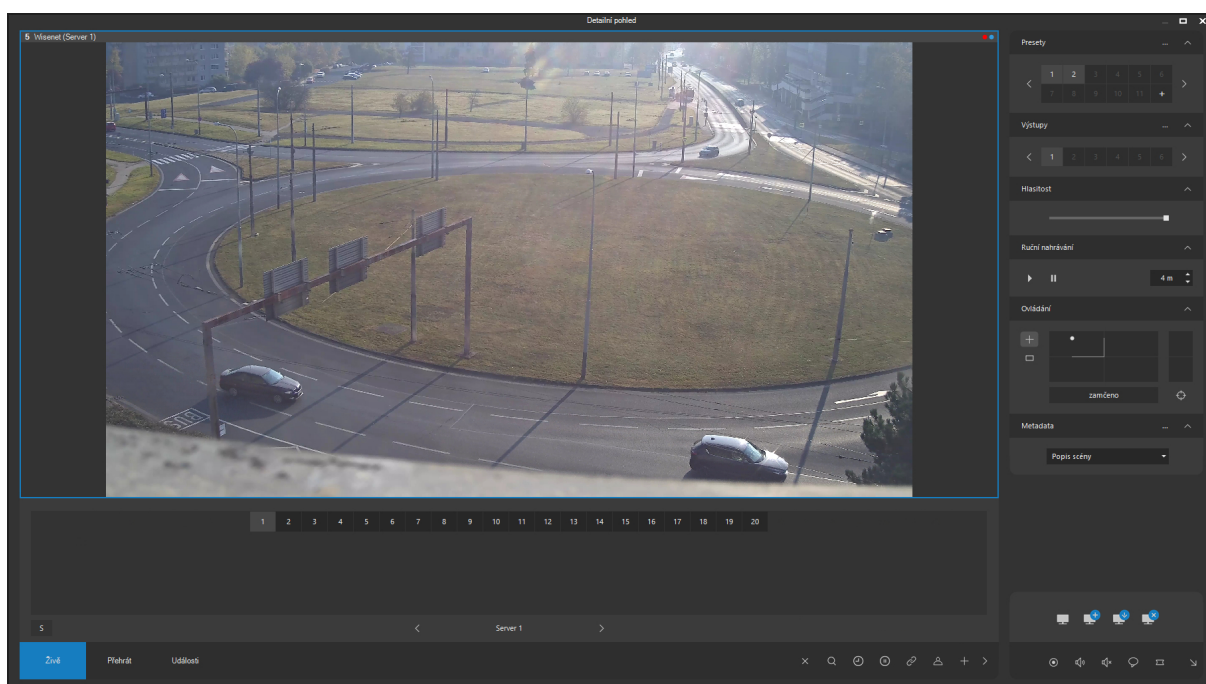
Po uložení snímku dojde k otevření okna s náhledem databáze snímků, ovládání tohoto okna je popsáno v samostatné kapitole.

4.4.4. Ovládání otočné kamery

Ovládání otočných kamer patří k základním funkcím pro vybranou kameru. V systému ATEAS Security máte k dispozici naprosto plnohodnotné a velice citlivé ovládací prvky a mechanismy. Otočné kamery (tj. PTZ a DOME kamery) můžete ovládat několika způsoby.

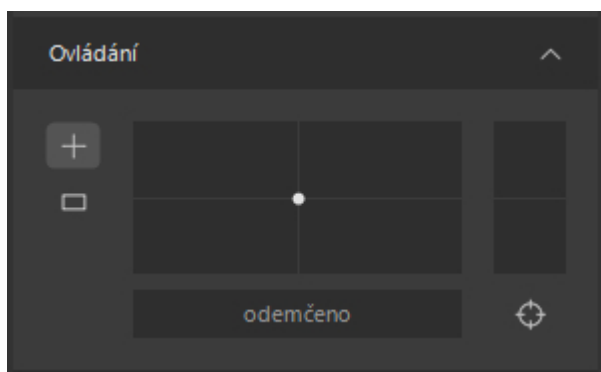
Ovládání kamery v obraze

Ovládání kamery přímo v jejím obraze je velice intuitivní způsob ovládání kamery, při kterém se kamera pohybuje vždy směrem od středu obrazu ke kursoru myši a to rychlostí, která je dána vzdáleností kursoru myši od středu obrazu. Kameru je tak možné tímto způsobem polohovat ve dvou osách ve všech směrech a variabilní rychlostí, přičemž přechody jsou naprosto plynulé.



Při otáčení kamery pomocí myši je pro zahájení pohybu kamery nutné v daném místě kamerového obrazu stisknout levé tlačítko myši a pro ukončení pohybu ho opět uvolnit.

Pro ovládání zoomu je možné (i v průběhu ovládání v obraze) používat kolečko myši, pokud je myš takovým kolečkem vybavena. Veškeré operace ve všech třech osách jsou promítány do ovládacího prvku pro polohování kamer ve spodní části boční ovládací lišty.



Ovládání pomocí ovládacího prvku

Ovládací prvek na výše zobrazeném ovládacím prvku je v podstatě simulátorem tříosého joysticku, pomocí kterého je možné polohovat kameru i přímo za použití myši. V oblasti tohoto ovládacího prvku je možné pohybovat myší a při stisknutém levém tlačítku je opět docíleno pohybu kamery. Stejně jako v případě klikání do obrazu je rychlost pohybu horizontálně a vertikálně dána vzdáleností kursoru myši od středu ovládacího prvku a směr je dán vektorem bodů. Ovládání zoomu je možné pomocí plochy

v pravé části ovládacího prvku, rychlost zoomování je dána kolmou vzdáleností mezi kurzorem myši středovou úsečkou.

Ovládání pomocí pákového ovladače (joysticku)

Pro ovládání kamer je možné použít též pákové ovladače, které se připojí k počítači pomocí rozhraní USB. Pokud jsou pákové ovladače vybaveny všemi třemi osami, je možné docílit plynulého pohybu variabilní rychlostí ve všech třech osách (pan, tilt, zoom). Pokud použitý joystick nemá třetí osu, je možné provádět zoomování pomocí tlačítek joysticku. Funkce pro tlačítka lze nastavit v sekci Nastavení v části joystick.

POZOR

Pro ovládání kamer nejsou zdaleka vhodné všechny joysticky (kvůli nízkým citlivostem a velkým mrtvým a saturačním zónám je u levných modelů pro počítačové hry mnohdy velmi obtížné citlivě kameru ovládat).

POZNÁMKA

Součástí dodávky pro Váš kamerový systém mohou být též speciální tříosé joysticky pro ovládání otočných kamer, které mají vysokou citlivost.

Ovládání pomocí počítačové klávesnice

Otočné kamery je možné ovládat také pomocí počítačové klávesnice a to pomocí šipek na numerické klávesnici s možností vertikálního, horizontálního i šikmého pohybu. Pro ovládání zoomu je možné použít tlačítek plus a minus. Dále je také možné použít tlačítka kurzorových šipek, což je vhodné, pokud je numerická klávesnice používána pro výběr kamer (viz lokální nastavení). Při využití kurzorových šipek samozřejmě chybí možnost ovládání v diagonálních směrech.

Ovládání ostření

Pomocí tlačítka ostření je možné ručně doostřit kameru, pokud nejsme spokojeni s výsledkem funkce automatického ostření. K tomu může dojít v situacích, kdy kamera nemůže objektivně rozhodnout, v jaké vzdálenosti má vzhledem ke snímané scéně ostřit.

Po stisku tlačítka ostření je možné ostření ovládat stejným způsobem jako zoom, a to pomocí všech výše popsaných způsobů včetně např. použití joysticku. Zároveň je také podporována proporcionální rychlost ostření, stejně jako v případě ovládání zoomu. Pro přepnutí zpět na ovládání zoomu je nutné opětovným stisknutím tlačítka uvolnit.

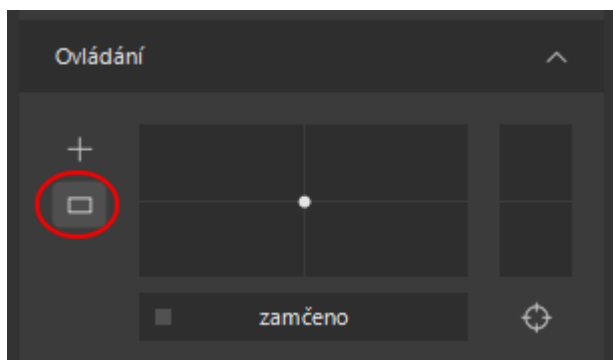
POZNÁMKA

Pokud je aktivováno ovládání ostření, je v ovládacím prvku PTZ použita jiná barva přechodové výplně pro odlišení od ovládání zoomu kamery.

Funkce zoom oblasti

Implicitní způsob ovládání otočné kamery pomocí dotyku nebo klikání myši do obrazu kamery popsaný výše může být přepnut do jiného režimu PTZ ovládání kliknutím na tlačítko pro zoom oblasti.

Rychlejší způsob použití funkce zoom oblasti je ponechání PTZ symbolu ve výchozí podobě (proporcionální ovládání) a použití klávesy Ctrl, která aktivuje rychlou možnost označení oblasti pro provedení zoomu.



V tomto režimu je možné ve videu nakreslit obdélník a kamera bude automaticky natočena a přiblížena, aby co nejlépe zabírala vybranou oblast.

POZOR

Tato funkce není podporována všemi typy kamer.

Některé speciální typy pevných kamer (např. Axis Q6000) umožňují kalibraci přidružené otočné kamery tak, že je možné funkci zoom oblasti použít i v obraze fixních kamer a docílit tím zoom oblasti

na přidružené otočné kameře. Tato funkce spolu s těmito speciálními kamerami umožňuje přiblížit detail scény a neztratit při tom přehled nad celou situací snímanou fixními kamerami.

POZNÁMKA

Dohledové okno si pamatuje naposledy použitý režim ovládání otočné kamery a při příštím výběru otočné kamery v dohledovém okně bude tento režim zvolen automaticky.

4.4.5. PTZ zámky

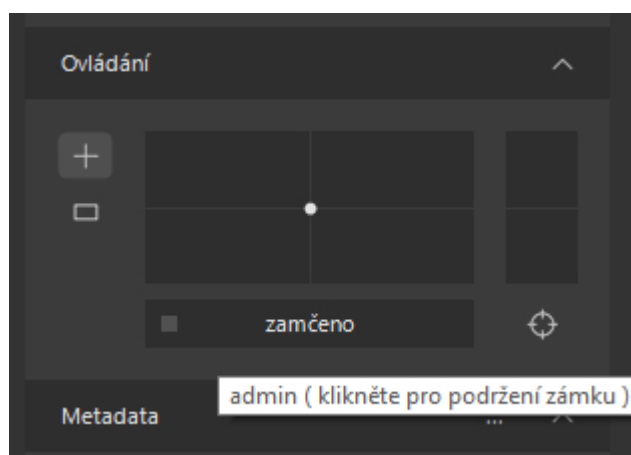
Při současném přístupu více uživatelů k ovládání kamer používají kamerové servery ATEAS inteligentní systém řízení tohoto současného přístupu. Rozhodující je nastavení priorit ovládání (PTZ priorit) pro jednotlivé uživatele a generování tzv. PTZ časových oken. PTZ časová okna jsou popsána v subkapitole Správa uživatelů v části o nastavení oprávnění a priorit PTZ. Princip časového okna spočívá v tom, že kamera je po určitou dobu (trvání PTZ časového okna je v řádu desítek vteřin) nečinnosti ponechána stále pod kontrolou uživatele, který ji naposledy ovládal, aby byla zajištěna kontinuita ovládání. Časové okno může být přerušeno pouze uživatelem s vyšší PTZ prioritou k dané kameře.

Pokud si uživatel potřebuje ovládání kamery vyhradit pro sebe na delší dobu a chce zamezit ostatním uživatelům v ovládání kamery i pro vypršení PTZ časového okna, může uplatnit tzv. PTZ zámek.

POZNÁMKA

Například pokud uživatel potřebuje kameru nasměrovat na určitý bod zájmu, ponechat ji delší dobu v nečinnosti a zároveň zamezit, aby jiný uživatel kameru nasměroval jinam.

Aby uživatel mohl uplatnit PTZ zámek, musí mít pro danou kameru vygenerováno PTZ časové okno, tj. musí ovládání kamery nejprve získat. V takovém případě se kromě informace, že ovládání kamery je zamčeno pro uživatele s jeho jménem, zpřístupní také tlačítko pro aktivaci PTZ zámku. Jméno uživatele se zobrazí při ponechání myši v prostoru pro ovládání zámku.



Po stisku tohoto tlačítka je na kameru aplikován PTZ zámek a kameru nebude moci ovládat žádný uživatel s nižší či stejnou prioritou ani po vypršení PTZ časového okna. Uživatel s vyšší prioritou k ovládání dané kamery může samozřejmě PTZ zámek přerušit, vytvořit si vlastní PTZ časové okno, případně také svůj zámek.

POZNÁMKA

PTZ zámek lze aplikovat na libovolné množství kamer. PTZ zámek však vyžaduje přítomnost uživatele v systému, pokud se uživatel odhlásí nebo jinak ukončí svou činnost, PTZ zámky budou na kamerových serverech zrušeny a ovládání kamer bude uvolněno pro ostatní uživatele.

Uvolnění PTZ zámku lze provést opětovným stiskem tlačítka zámku při vybrané kameře, na kterou byl zámek aplikován.

4.4.6. Speciální PTZ funkce

Pomocí ovládacího prvku pro ovládání otočných kamer (viz předchozí subkapitola) je možné aktivovat speciální PTZ funkce kamery, pokud je daný typ kamery podporuje. Pokud je podporován nějaký typ speciální PTZ funkce, bude možné v pravém horním rohu tyto funkce aktivovat kliknutím na grafický symbol a přepínat pomocí šipek. Aktivace funkce však musí vždy proběhnout pomocí levého tlačítka myši, pravé tlačítko myši provádí deaktivaci zvolené speciální PTZ funkce.

K dispozici jsou tyto speciální funkce:



Funkce automatického sledování (autotracking) – pokud je tato funkce aktivována, kamera je přepnuta do režimu automatického sledování a reaguje na pohyb v obraze tím, že je schopna sama sledovat pohybující se objekty či vozidla.

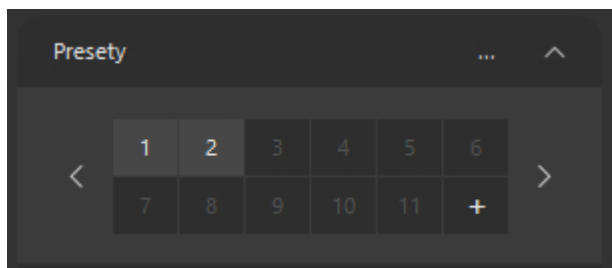
POZOR

K používání speciálních PTZ funkcí se neváže žádné speciální oprávnění v administraci uživatelů. Tyto speciální funkce však mohou používat pouze uživatelé s oprávněním ovládat danou kameru a současně mají vyšší prioritu ovládání (alespoň prioritu 10).

4.4.7. Prepoziční body

Obvyklou funkcí otočných kamer je uložení hodnot pro všechny tři osy (pan, tilt, zoom) v daném bodě. Tento bod se nazývá prepozičním bodem kamery (preset). Tyto body lze pak použít pro rychlý přesun do daného místa.

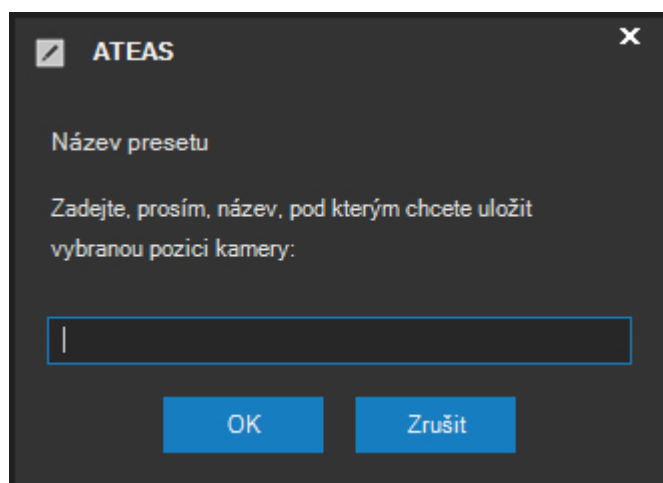
Přepínání kamer do prepozic



Každá kamera může mít předdefinováno až 100 prepozičních bodů. Počet skutečně podporovaných prepozičních bodů závisí na modelu otočné kamery. Obsazené pozice se od neobsazených liší světlejším odstínem šedé. Pokud se pohybujete myší nad jednotlivými prepozičními body, zobrazován název presetu. Kliknutím na bod docílíte polohování vybrané kamery do prepozičního bodu. Pro přístup k dalším presetům je možné posouvat zobrazení pomocí šipek doprava a doleva.

Nastavení prepozičních bodů

Pokud chcete obsadit nebo přepsat některý prepoziční bod, je nejprve třeba nastavit kameru do cílového bodu a poté kliknout na tlačítko se symbolem nastavení, které zvýrazní svou barvu. Po kliknutí na cílovou pozici (1 až 100 dle aktuálně zobrazené sady prepozičních bodů) bude zobrazen dialog pro zadání názvu pro prepoziční bod.



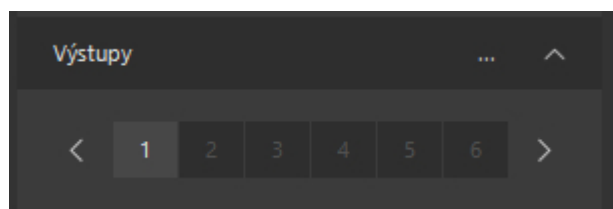
Po potvrzení tlačítkem **OK** dojde k uložení aktuální pozice kamery a k přiřazení danému číslu. Stisknutí nastavovacího tlačítka bude na ovládacím prvku pro prepoziční body automaticky zrušeno, s presety je dále možné pracovat standardně.

Smazání prepozičních bodů

Prepoziční body lze vymazat stejným způsobem jako je lze nastavit, pouze s tím rozdílem, že na konkrétní preset, který má být odstraněn, kliknete pravým tlačítkem myši (symbol nastavení tedy musí být v aktivním zvýrazněném stavu). Po potvrzení zprávy bude preset odstraněn.

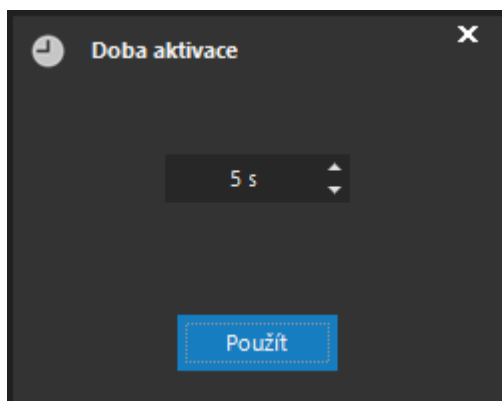
4.4.8. Aktivace výstupů

K některým kamerám či video serverům v systému mohou být připojeny výstupy např. pro ovládání dveřních zámků, závor apod. Tyto výstupy mohou být aktivovány ručně v dohledovém okně (kromě toho mohou být aktivovány automaticky během události). Výstupy vybrané kamery jsou součástí ovládacího prvku výstupů.



Dostupné výstupy mají světle šedivou barvu, nevyužité výstupy splývají s pozadím. Při pohybu myši nad čísly výstupů se zobrazuje název výstupu. Ten může být buď implicitní (např. Výstup 1) nebo symbolický definovaný administrátorem (např. Závor a pod.).

Aktivaci výstupu na určitý počet vteřin je možné provést kliknutím na číslo daného výstupu. Výchozí doba aktivace výstupu je pět vteřin, tuto dobu lze pro každou kameru samostatně změnit pomocí tlačítka nastavení se třemi tečkami.



POZNÁMKA

Pokud je časová prodleva nastavena na hodnotu 0 (nula), výstup bude aktivován natrvalo – nepřejde sám do neaktivního stavu. Ruční deaktivaci výstupu lze provést nastavením hodnoty časového pulzu na hodnotu -1 anebo kliknutím na výstup pravým tlačítkem myši. Pravé tlačítko funguje nezávisle na nastavené hodnotě časového pulzu.

POZNÁMKA

Aplikace si pamatuje naposledy použité hodnoty pro aktivaci výstupů na jednotlivých kamerách a při opakovaném výběru téže kamery (třeba i v jiném dohledovém okně) automaticky nastaví příslušný časový interval. Tyto údaje jsou uchovávány po celou dobu práce klientské aplikace, restartem aplikace dojde k jejich výmazu a nastavení na implicitní hodnoty.

4.4.9. Příjem zvuku

Pokud je pro vybranou kameru k dispozici zvukový zdroj a administrátor pro tuto kameru povolil přenos zvuku, budete moci po výběru kamery automaticky slyšet živý zvuk. Jedinou podmínkou je funkční zvukové zařízení (karta) a připojené reproduktory.

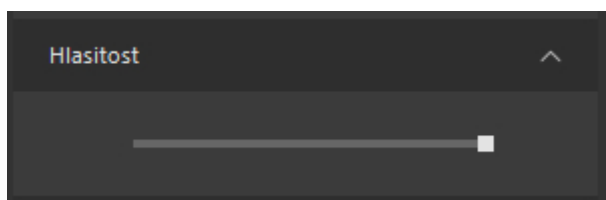
Zvuk můžete v jednom dohledovém okně poslouchat vždy pouze u vybrané kamery. Pokud je spuštěno více dohledových oken, je nutné ručně odpojit zvuk v okně, kde ho nechcete poslouchat. K odpojení a znovu připojení zvuku slouží příslušná tlačítka na boční ovládací liště.



POZNÁMKA

Pokud je v systému video server s více video vstupy a jedním audio vstupem, záleží na nastavení administrátora, kterým video vstupům bude zvuk přiřazen. Zvuk může být přiřazen libovolné kombinaci video vstupů a to pro libovolný formát videa. Pro některé video formáty v závislosti na typu kamery však může být nutné provést přiřazení zvuku video vstupům také přímo v nastavení video serveru.

Hlasitost lze kdykoliv ovlivnit pomocí následujícího ovládacího prvku. Implicitně je hlasitost nastavena na maximum.



Příjem zvuku je pro vybranou kameru k dispozici jak při živém pohledu, tak i při jeho přehrávání ze záznamu.

4.4.10. Stiskni a mluv

Pokud vybrané zařízení podporuje obousměrný zvuk, je možné přímo v dohledovém okně mluvit do kamery. To znamená, že pokud je kamera vybavena reproduktorem zvuku, může operátor na stanici vybavené mikrofonom stisknutím jednoho tlačítka zahájit přenos zvuku směrem ke kameře. Pro tuto funkci je k dispozici tlačítko na panelu funkcí vybrané kamery.

Povolení této funkce závisí na tom, zdali kamera podporuje obousměrný zvuk a také na tom, zdali Vám administrátor systému vysílání zvuku umožnil. U víceportových zařízení (zařízení s více video vstupy), která mají pouze jeden zvukový výstup (a nejčastěji také vstup) lze vždy hovořit jen do zařízení s portem 1.



POZNÁMKA

Pokud chcete mluvit do kamery, je nutné toto tlačítko stisknout a po ukončení přenosu zvuku opětovným kliknutím uvolnit.

Pokud funkcí vysílání zvuku do vybrané kamery již používá jiný uživatel se stejnou nebo vyšší prioritou, mluvení do kamery nelze zahájit a uživatel bude informován zprávou.

Mluvení do více kamer současně

Vaše klientská aplikace umožňuje vysílat zvuk z Vašeho mikrofonu do více kamer či speciálních IP reproduktorů současně. Pokud při stisku tlačítka pro aktivaci přenosu zvuku do kamery použijete namísto levého tlačítka myši pravé tlačítko, bude automaticky aktivováno vysílání zvuku do Všech kamer v pohledu.

POZNÁMKA

Při vysílání zvuku do všech kamer v pohledu je samozřejmě respektováno oprávnění uživatele k této funkci pro kamery v pohledu a vysílání bude možné pouze do kamer, ke kterým má současný uživatel oprávnění přistupovat a pro které má aktivováno oprávnění využití obousměrného zvuku.

POZNÁMKA

Není možné z jednoho dohledového okna vysílat zvuk současně do více kamer připojených k různým serverům (cílový server při vícečetném vysílání zvuku je určen serverem vybrané kamery). Je však možné funkci vysílání zvuku aktivovat ve více dohledových oknech současně, a vysílat tak současně zvuk až do 400 kamer připojených ke 4 serverům.

Pokud funkci vysílání zvuku do některých kamer již používá jiný uživatel se stejnou nebo vyšší prioritou k dané kameře, mluvení do kamery nelze zahájit pro všechny kamery. Uživatel bude o této situaci informován zprávou. Kamery, do kterých zvuk nebyl vysílán anebo do kterých byl zvuk vysílán uživateli s nižší prioritou, bude možné použít.

Automatické ztlumení zvuku

Při práci s obousměrným přenosem zvuku často dochází k situaci, kdy reprodukováný zvuk z kamery je zachycen jejím mikrofonom. Tato situace se označuje jako zvuková zpětná vazba. Může k ní dojít jak na straně kamery, tak na straně klienta. ATEAS nabízí jednoduchou možnost, jak této situaci předejít. Pomocí dvojitého kliknutí na tlačítko pro vysílání zvuku do kamery dojde k automatickému potlačení reprodukce zvuku na klientovi. Funkci lze využít i při vysílání do více kamer současně, kdy použijeme dvojité kliknutí pravým tlačítkem.

POZNÁMKA

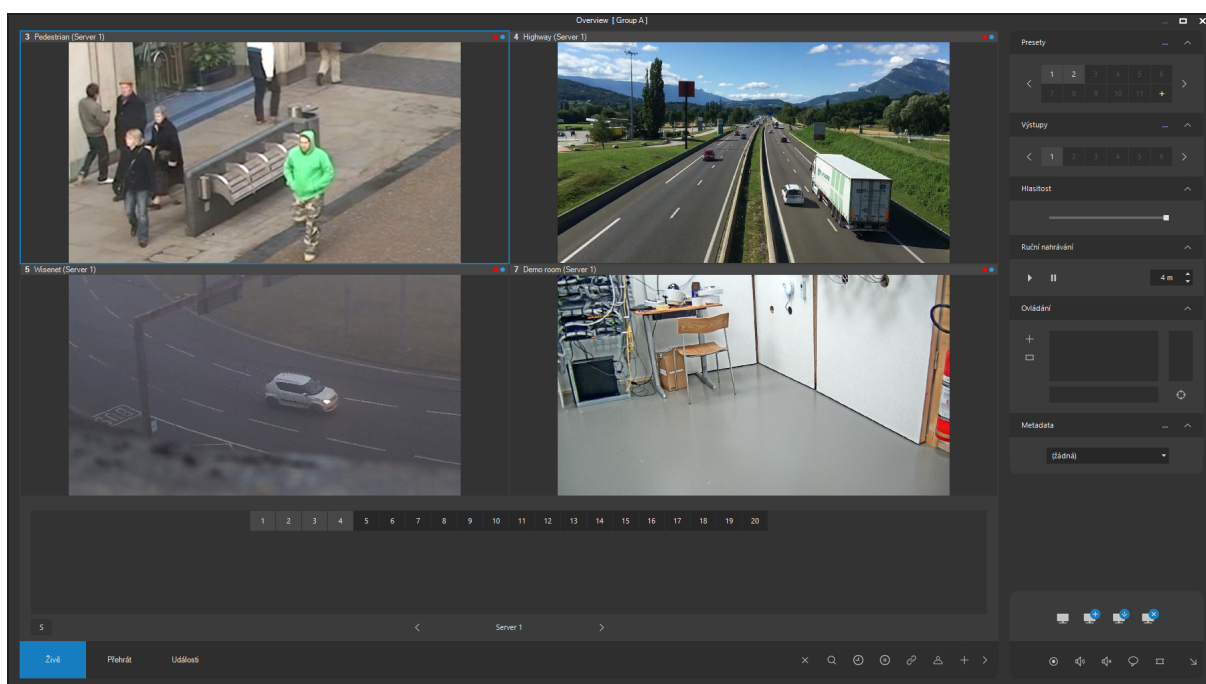
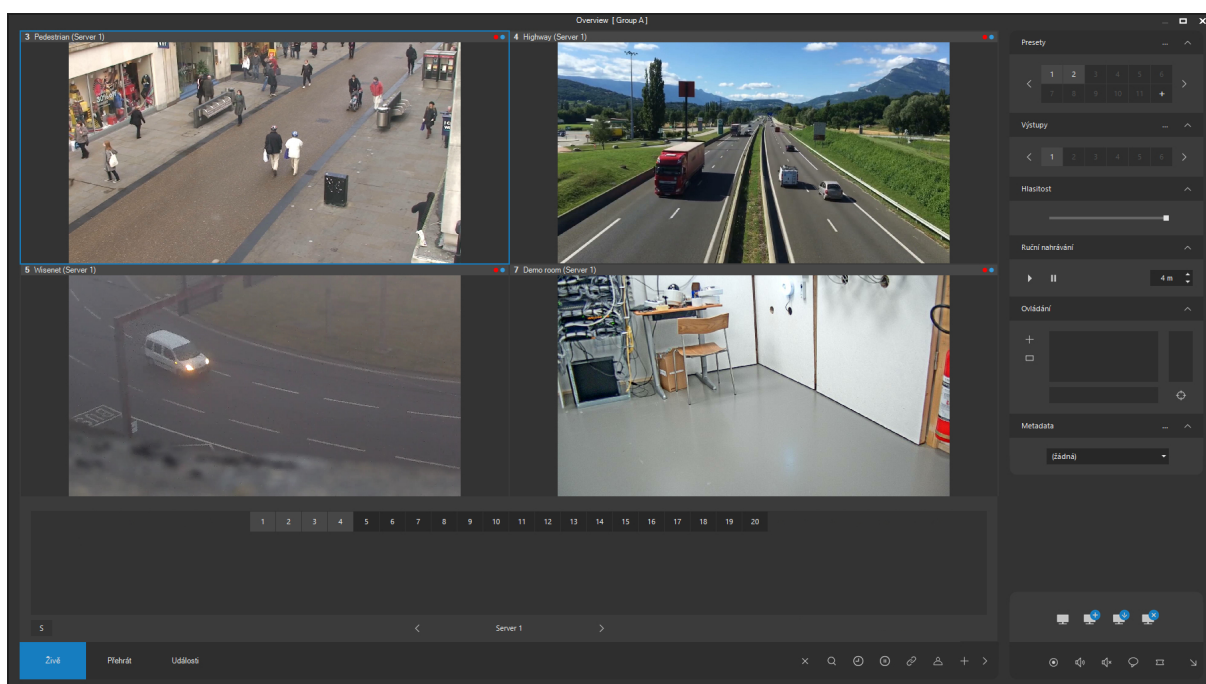
Funkci vysílání zvuku do kamery včetně automatického ztlumení zvuku lze aktivovat i pomocí přednastavené klávesy, kterou je možné libovolně zvolit v lokálním nastavení klienta. Více viz kapitola o lokálním nastavení klávesnice.

4.4.11. Digitální přiblížení

Pro každou vybranou kameru máte možnost provádět digitální přiblížení. Digitálním přiblížením se rozumí zvětšení detailů v obrazu v rámci okna stejné velikosti. Tato funkce je zejména vhodná pro kamery s megapixelovým rozlišením (může být samozřejmě použita pro všechna rozlišení). Předpokladem pro použití funkce je situace, kdy je možné obraz kamery zobrazit ve větší než aktuální velikosti. Do jisté míry se tak jedná o alternativu funkce zobrazení detailu, při které je vybraná kamera přepnuta do nového detailního pohledu. Při použití funkce digitálního přiblížení jsou detaily obrazy zobrazeny i bez nutnosti přepnutí pohledu. Funkce navíc může být použita i na mnoha jiných místech v systému, např.:

- v detailním pohledu, pokud to rozlišení kamery ještě umožňuje,
- v náhledu záznamu,
- při přehrávání záznamu,
- v náhledu a prohlížení snímků,
- v aplikaci ATEAS Media Player.

Následující obrázky ukazují použití funkce digitálního přiblížení u pevné kamery umístěné v pohledu vlevo nahoře.



Digitální přiblížení (resp. oddálení) se ovládá výhradně kolečkem myši. Pokud je obraz digitálně přiblížen, lze provádět také digitální posun po obraze a to stejným způsobem, jakým se provádí manuální ovládání otočné kamery přímo z obrazu kamery. Digitální přiblížení tedy není možné provádět např. pomocí joysticku nebo jeho simulátoru.

Kliknutím prostředním tlačítkem myši (nejčastěji v podobě kolečka) lze provést rychlý reset digitálního přiblížení do výchozí podoby.

POZNÁMKA

Při přepnutí jiného pohledu nebo při změnách rozměru okna je digitální přiblížení resetováno do výchozí podoby (tj. je zobrazen celý obraz).

Digitální přiblížení lze provádět také pro otočné kamery. Vzhledem k tomu, že u otočných kamer jsou operace kolečka myši a klikání do obrazu automaticky přiřazeny PTZ ovládání kamery, je nutné nejprve PTZ operace vypnout. Vypnutí se provede kliknutím na tlačítko právě aktivního režimu PTZ ovládání.

POZNÁMKA

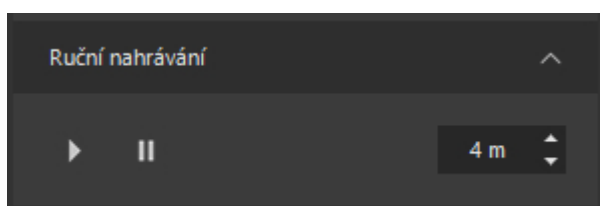
Ve výchozím nastavení systému lze digitální přiblížení provádět pouze do dosažení nativního rozlišení zobrazovaného videa. Větší digitální přiblížení již nezvyšuje kvalitu zobrazované grafické informace (počet obrazových bodů je konečný), nicméně její zvětšení může být v některých případech prospěšné. Aktivaci digitálního přiblížení nad nativní rozlišení videa je možné aktivovat v lokálním nastavení v části Zobrazení videa.

POZNÁMKA

Rychlost digitálního posunu obrazu při digitálním přiblížení je závislá na vzdálenosti ukazatele myši od středu obrazu, ale také se inteligentně přizpůsobuje úrovni digitálního přiblížení, aby bylo docíleno plynulých a očekávaných posunů.

4.4.12. Ruční nahrávání

Od verze 3.9.6 je pro oprávněné uživatele k dispozici funkce ručního nahrávání, jejíž ovládání je dostupné v každém dohledovém okně v pravé části.



POZNÁMKA

Tato funkce je vázána na přidělení příslušného oprávnění administrátorem systému, uživatelé bez tohoto oprávnění nebudou moci funkci použít.

Princip ručního nahrávání spočívá v tom, že uživatel může pomocí tlačítka se symbolem modré šipky vyvolat událost ručního nahrávání. Jedná se o speciální událost, pomocí které lze docílit zahájení nahrávání nebo zvýšení záznamové snímkové frekvence. V systému je tato událost následně také k dispozici v seznamu událostí při prohlížení záznamu kamer.

Zahájení události ručního nahrávání pro vybranou kameru může mít v závislosti na aktuálním nastavení kamery různé účinky. Pokud je v daném čase kamera zaznamenávána pouze při událostech, zahájení události ručního nahrávání způsobí zahájení záznamu (s možností uložení předpoplachového záznamu, pokud je nastaven). Pokud kamera zaznamenává nízkou či střední snímkovou frekvencí (viz tvorba pravidel záznamu) a je-li povoleno zvýšení snímkové frekvence během událostí, způsobí zahájení události ručního nahrávání zvýšení snímkové frekvence záznamu.

POZOR

Z toho vyplývá, že pro fungování této funkce je nezbytné, aby kamera měla přiřazeno záznamové pravidlo, které povoluje záznam při událostech nebo alespoň zvýšení snímkové frekvence záznamu při události.

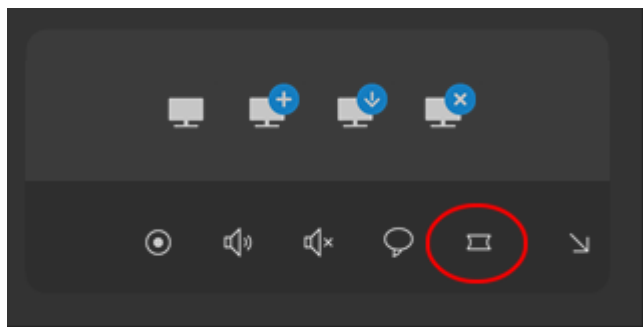
Ovládací prvek ručních událostí umožňuje dále také nastavit délku trvání události, za tuto dobu (určenou v minutách) bude událost automaticky ukončena. Událost je rovněž možné ukončit ještě před vypršením této doby pomocí příslušného tlačítka.

POZNÁMKA

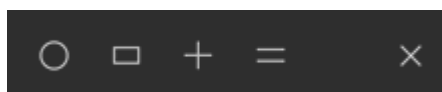
Vícenásobné zahájení události ručního nahrávání není možné, předchozí událost musí být vždy nejdříve ukončena (uplynutím doby jejího trvání nebo ručně), než bude možné zahájit událost novou.

4.4.13. Korekce obrazu typu rybí oko

Pokud administrátor systému konfiguroval vybranou kameru jako zdroj videa typu rybí oko (tzv. fish-eye kamery se speciálním objektivem pokrývajícím 360 stupňů), je možné pomocí tlačítka Korekce obrazu aktivovat výběr režimů pro korekci obrazu. Tato korekce se provádí proto, že základní obraz typu rybí oko zobrazený v obdélníkové oblasti ve Vašem pohledu je přirozeně deformován.



Po stisknutí tlačítka se symbolem obrazu typu rybí oko se objeví nová sada tlačítek pro aktivaci režimů korekce obrazu.



Pomocí těchto tlačítek je možné aktivovat následující režimy korekce obrazu:

- obraz 360 stupňů (bez korekce),
- jednoduchý PTZ pohled (korekce v jeden pohled s možností ovládání jako u otočné kamery),
- „quad“ pohled (korekce do čtyř pohledů do různých sekcí také s možností ovládání),
- panorama pohled (jednoduchý nebo dvojité panorama pohled).

POZNÁMKA

U režimu jednoduchého pohledu lze obraz oddálit až do úrovně celkového přehledu (360 stupňů), korekce je aplikována plynulým způsobem dle potřeby.

Tlačítka pro přepínání režimů korekce obrazu lze skrýt pomocí symbolu bílého křížku.

Režimy, které umožňují PTZ ovládání, je možné ovládat stejným způsobem jako v případě skutečných PTZ kamer přímo pomocí klikání do obrazu kamery.

POZNÁMKA

Jednoduchý nebo dvojitý panorama pohled je automaticky zvolen pohled toho, jakou orientaci pro kameru nastavil administrátor systému. Více viz kapitola o základním nastavení kamery.

Libovolný zvolený režim korekce obrazu nastavený pro vybranou pozici v pohledu je vždy uložen spolu s aktuálním pohledem. To znamená, že při otevření tohoto pohledu a samozřejmě také při jeho sdílení je režim korekce obrazu aktivován automaticky.

POZNÁMKA

V rámci pohledu je uložena nejen informace o zvoleném režimu korekce, ale také informace o jeho PTZ nastavení. Pokud je tedy jednoduchý PTZ pohled či quad pohled dodatečně otočen do jiné pozice, tato informace bude uložena spolu s pohledem. Samotné otočení však na rozdíl od změny režimu korekce obrazu nevyvolá při opuštění pohledu bez uložení změn dialog, kterým lze změny uložit.

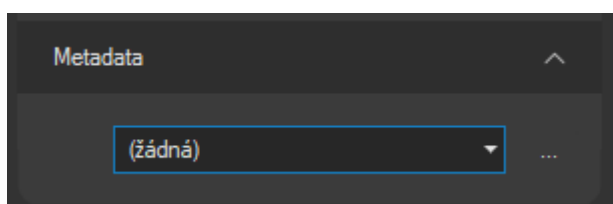
POZNÁMKA

Zvolený režim korekce a otočení se také automaticky přenáší, pokud je zobrazen detailní pohled kamery ve stejném či samostatném okně.

Změnu režimu korekce obrazu typu rybí oko lze provádět v živém zobrazení i při přehrávání záznamu. Pokud máme tedy v systému uložený plný obraz typu rybí oko (360 stupňů), můžeme k němu kdykoliv přistupovat např. jako k otočné kameře s tím, že se můžeme zcela volně rozhlížet po zaznamenané scéně.

4.4.14. Zobrazení metadat

Pokud administrátor systému připojil ke kameře metadata neuronových sítí anebo externí zdroje analytických dat, budou se jejich názvy zobrazovat po výběru příslušné kamery.



Po výběru zdroje dat se budou analytická metadata ihned vykreslovat ve videu kamery nezávisle na tom, zdali došlo či nedošlo k události. Vykreslování např. výsledků objektové analýzy má přidanou hodnotu i v situaci, kdy ještě nedošlo ke vzniku události dle nastavených pravidel.

POZNÁMKA

Zvolený zdroj metadat pro danou kameru je uložen spolu s pohledem včetně sdíleného pohledu.

POZNÁMKA

Pokud je aktivováno ukládání metadat neuronových sítí, bude možné metadata po výběru ze seznamu také přehrávat spolu s videem kamery.

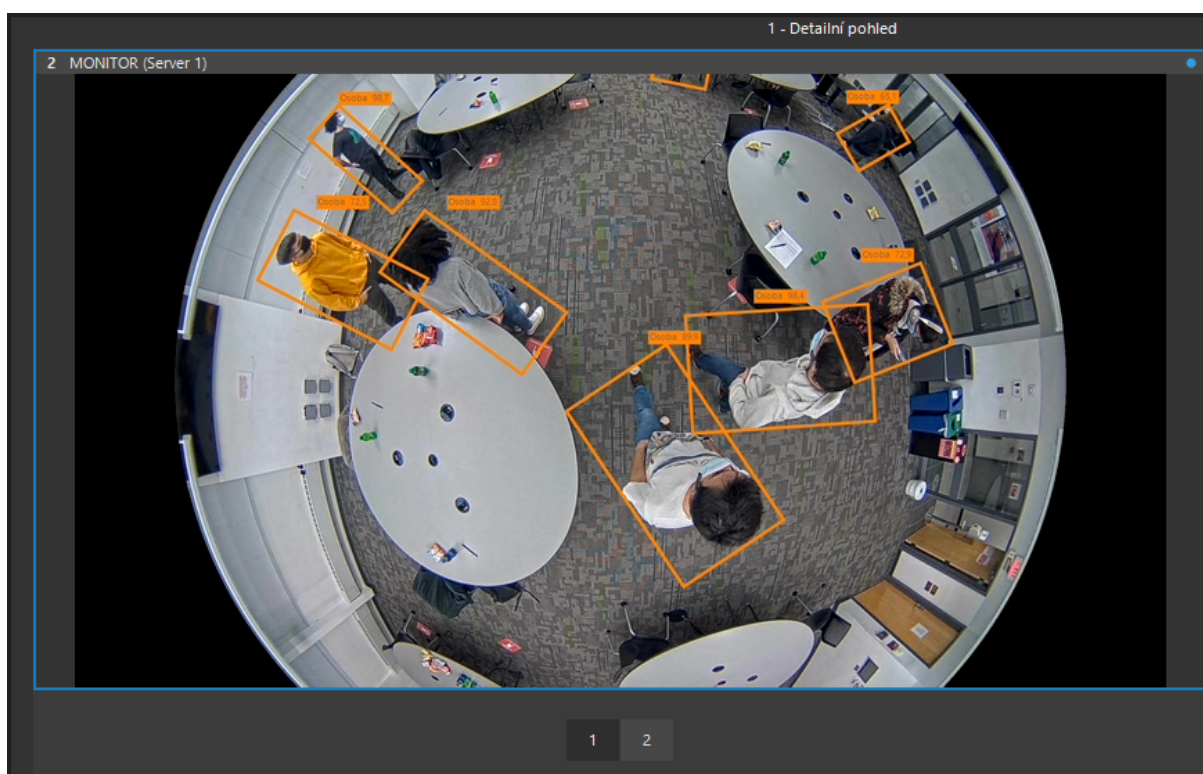
POZNÁMKA

Šířku pera pro vykreslování metadat lze určit v lokálním nastavení klienta. Tato šířka zůstává neměnná i při digitálním přiblížení kamery (narozdíl od situace, kdy vykreslování provádí přímo kamera).

Sítě, které umí predikovat další atributy objektů anebo rozšířené informace o poloze objektů, mohou zobrazovat i další vizuální informace. Např. model WD dokáže díky predikci úhlu zobrazit natočené umístění objektů.

POZNÁMKA

Pro zobrazení natočených objektů je nutné aktivovat akceleraci zobrazování metadat.



4.4.15. Konfigurace detekce pohybu a analýzy uživatelem

Tlačítko před rozbalovacím seznamem skupin metadat (viz předchozí subkapitola) může být oprávněným uživatelem, kterému bylo administrátorem přiděleno příslušné oprávnění, použito ke konfiguraci detekce pohybu na serveru a konfiguraci analytických zdrojů událostí. To se týká úpravy parametrů detekce pohybu jako citlivost, úpravy stávajících či přidání nových detekčních zón neuronové sítě či změny parametrů událostních zdrojů.

POZNÁMKA

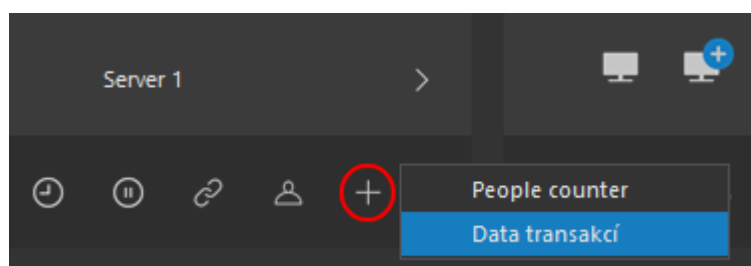
Na rozdíl od vyvolání tohoto nastavení z administrační sekce, nelze přidávat zcela nové zdroje událostí, což je dáno tím, že uživatel nemá přístup k plánovači zdrojů událostí a k vytvoření událostního scénáře.

Postupy konfigurace všech těchto nastavení jsou podrobně popsány v příslušných kapitolách o administraci systému, jedná se vždy o totožné uživatelské rozhraní a logiku nastavení.

4.5. Práce s transakčními daty

4.5.1. Živý náhled

Pokud administrátor systému svázal některé kamery s transakčními daty (např. s daty pokladního systému), je možné zobrazit tato transakční data živě i ze záznamu přímo v dohledovém okně. Zobrazení transakčních dat pro vybranou kameru lze provést z nabídky možností dodatečných dat kamery.



Příjem transakčních dat z kamer je pak standardní součástí kamerových pohledů (lokálních i sdílených). V rámci jednoho pohledu lze kombinovat příjem videa z kamery, příjem přidružených transakčních dat a příjem obrazovky pokladního terminálu pomocí aplikace ATEAS Screen Recorder.

POZNÁMKA

Kombinací funkcí video dohledu, zapojení obrazovek pokladních terminálů do kamerového systému a integrace transakčních dat lze vytvořit kompletní systém pro obchody všeho druhu s vysokou přidanou hodnotou.

POZNÁMKA

Výskyt nějaké konkrétní položky kdekoli v transakci také může být důvodem pro vznik události. Více viz kapitola o vlastních událostech kamer.

4.5.2. Přehrávání transakcí

Přehrávání transakcí se svým ovládáním nijak neliší od přehrávání videa jednotlivých kamer. Transakční data jedné či více kamer jsou automaticky synchronizována během přehrávání i při posouvání časové osy. Během přehrávání se v rámci aktuálně zobrazené transakce vždy označuje aktuální řádek dané transakce vzhledem k času přehrávání.

1 Axis P1344 (Server 1)

ATEAS transakce

549780	Oranges	15.20
005890	Milk	19.90
479055	Potatoes	49.00
789475	Eggs	25.00
497528	Bread	16.50
210591	Whiskey	764.50

Nepřipojeno

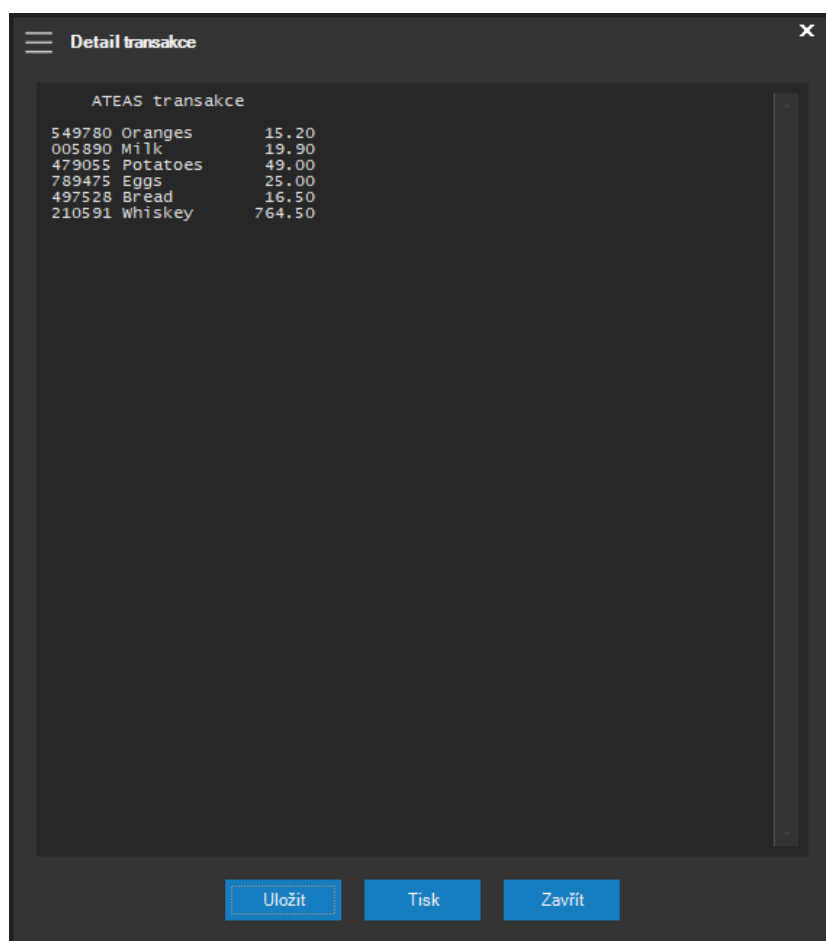
POZOR

Aby mohl automatický výběr řádku a jeho posun fungovat, musí být transakční data přijímána v reálném čase. Příjem celých transakcí v jeden časový okamžik tuto funkci pochopitelně neumožní.

Zobrazená transakce nabízí také nový způsob synchronizace času záznamu v dohledovém okně. Kliknutím na vybranou položku v transakci je přehrávání posunuto na časový okamžik vzniku této položky transakce. Dojde tedy k synchronizaci videa či transakcí na všech ostatních pozicích dohledového okna.

4.5.3. Uložení transakce

Pomocí tlačítka, které běžně používáme pro uložení aktuálního snímku v okně, lze provést uložení transakce.



V tomto okně lze transakci uložit do textového souboru nebo rovnou vytisknout na Vámi zvolené tiskárně.

4.6. Spolupráce s mapovým oknem

4.6.1. Synchronizace při výběru kamer či prvků

Pokud je v lokálním nastavení nastavena automatická synchronizace mapy na plnou, bude při výběru kamery či prvku synchronizována mapová scéna (automatický výběr mapové úrovně – patra, centrování a přiblížení či oddálení dle nastavení a aktuálního přiblížení).

K automatické synchronizaci bude také docházet, pokud je kamera automaticky přepnuta do detailu a nebo také při aktivaci automatického režimu přepínání kamer (automat). Pokud bude okno s aktivovaným automatem vybráno, bude při přepnutí kamery synchronizována mapa. Je tedy možné provádět virtuální procházky objektem i s automatickou synchronizací mapy.

POZOR

Pokud není mapové okno otevřeno, nebude možné automatickou synchronizaci provést. Jinými slovy, automatická synchronizace neotevře mapové okno, pokud je zavřené. To musí být vždy nejprve otevřeno ručně pomocí příslušného tlačítka.

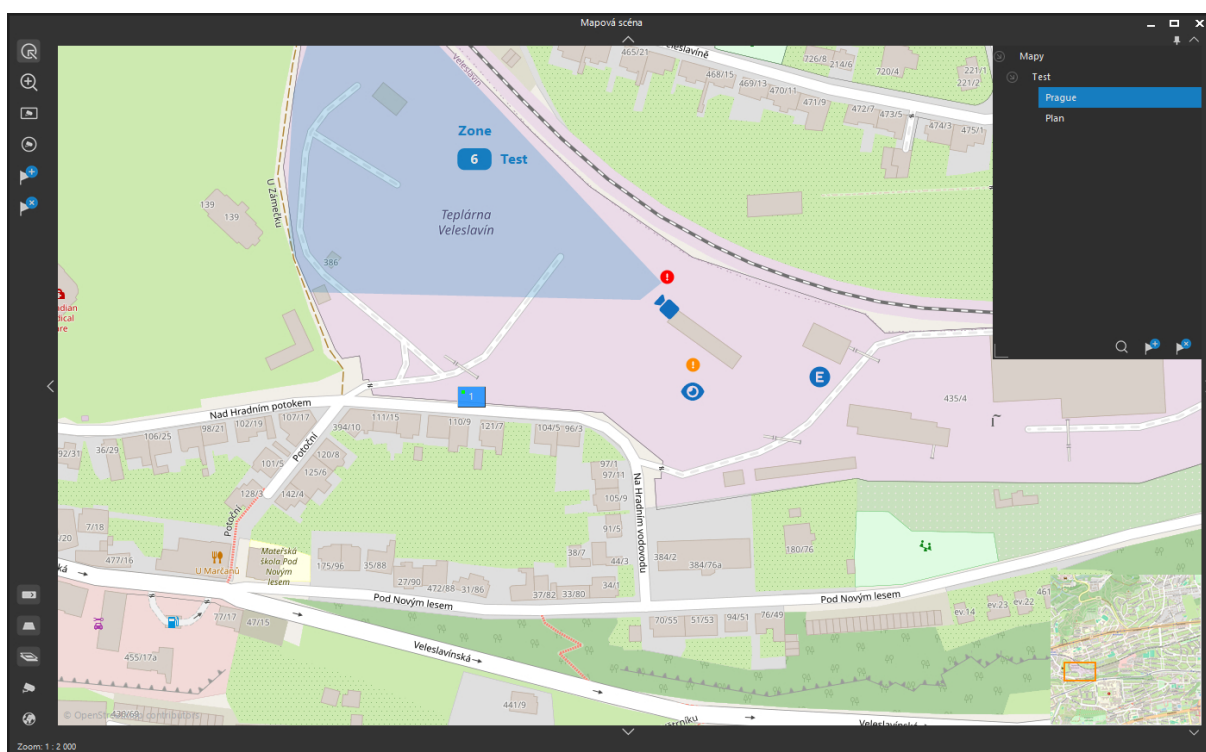
POZNÁMKA

Pro lepší názornost bude symbol kamery v mapě po jejím výběru vždy na pár vteřin zvýrazněn.

4.6.2. Synchronizace při události

Pokud je v lokálním nastavení nastavena automatická synchronizace mapy na plnou nebo událostní, bude při výskytu události synchronizována mapová scéna stejně jako v předchozím případě. To znamená, že při události dojde k vycentrování a volitelnému mapovému přiblížení místa jejího výskytu. K automatické synchronizaci mapy na událost dojde vždy (i když zároveň nedojde k přepnutí do událostního pohledu z důvodu dvou příliš rychle po sobě se vyskytujících událostech nebo přepnutí událostního pohledu, které by bylo vyhodnoceno jako přetěžující pro operátora). V takovém případě detekovaného přetížení více událostmi sice nebude automaticky přepnut událostní pohled, bude však automaticky synchronizována mapa (samozřejmě pouze pokud je výskyt události lokalizovatelný – kamera detekující pohyb má určeny souřadnice) a bude také přidán řádek do seznamu aktivních událostí.

Události jsou indikovány dodatečným symbolem vykřičníku u kamer v poplachu. V závislosti na jejich stáří se mění barvy událostí až do jejich úplného zmizení z mapové scény. Na obrázku jsou vidět události s různým stářím. Časové prodlevy mezi jednotlivými fázemi jsou nastavitelné v části lokální nastavení.



K automatické synchronizaci také dojde (je-li zapnuta alespoň událostní automatická synchronizace) při výběru řádku s událostí. V takovém případě dojde také k přepnutí do událostního pohledu.

POZOR

Zde není prováděna synchronizace na kamery událostního pohledu, ale na kameru či prvek, které událost vyvolaly, což může být zcela jiná kamera, než jaké jsou zařazeny do událostního pohledu.

POZNÁMKA

Pokud vznikne externí událost, která není lokalizována, bude mapa synchronizována alespoň podle první kamery v událostním scénáři, která je lokalizována. Tím uživatel získá přehled o místě výskytu externí události.

4.6.3. Výběry z mapy

Do dohledových oken (dle lokálního nastavení) lze promítat kamery vybrané pomocí výběrových funkcí mapového okna popsanych v samostatné kapitole o ovládání mapového okna. Vybrané kamery jsou v mapě vyznačeny odlišnou barvou a nově vytvořený pohled nese název Výběr mapy.

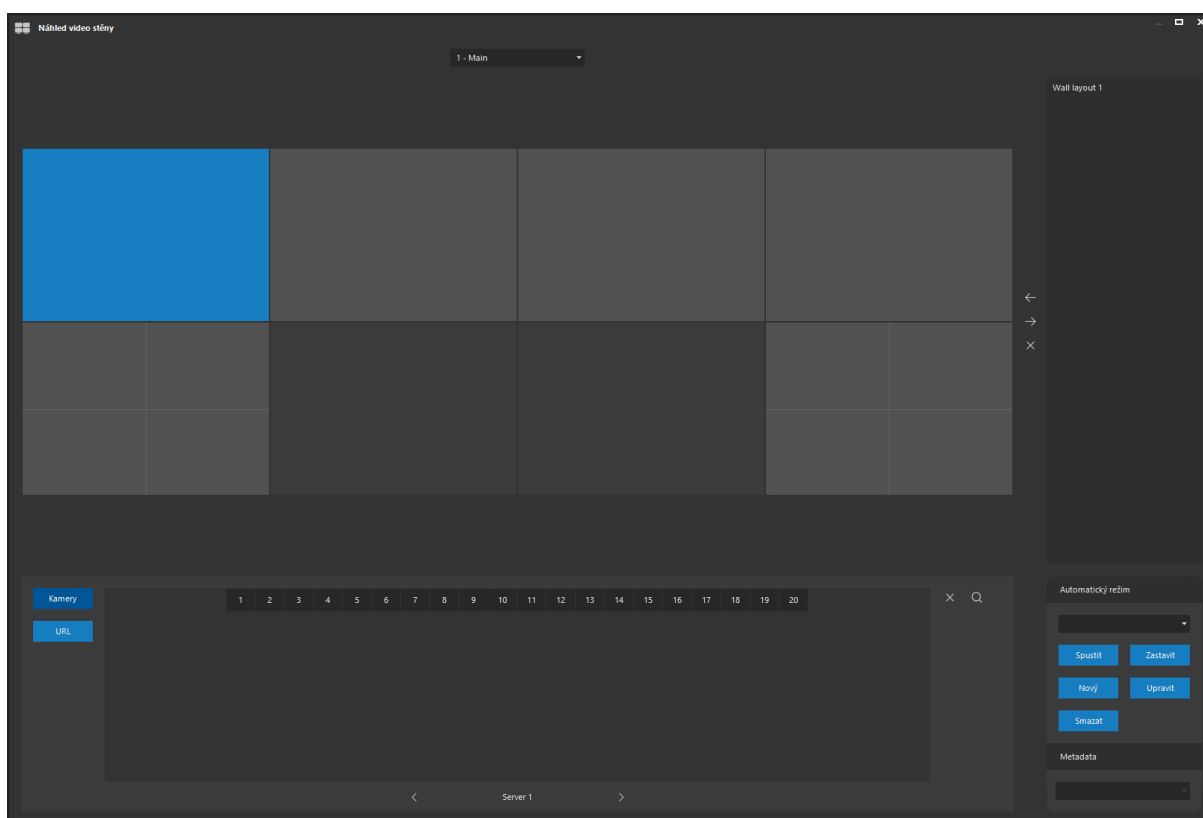
4.7. Práce s video stěnou

4.7.1. Přepínání kamer

Video stěna představuje fyzicky nebo virtuálně uskupené monitory připojené k podřízeným stanicím v systému, které mohou být ovládány z jiných klientských pracovišť, která k tomu mají oprávnění. Pokud máte v hlavní nabídce položku Video stěna a pokud máte oprávnění ji spustit a ovládat, budete mít také přístup ke všem vzdáleným monitorům, které byly administrátorem konfigurovány.

POZNÁMKA

Konfigurace a principy fungování video stěny jsou popsány v administrační části v sekci administrace pohledů, subkapitola o video stěně.



V rozbalovacím seznamu v horní části okna lze vybrat video stěnu, kterou chceme používat. Jejich počet není v podstatě omezen a mohou představovat nezávislé skupiny externích monitorů na různých místech.

Pomocí tohoto okna má uživatel k dispozici video stěny, tak jak je vytvořil a nakonfiguroval administrátor systému. Na libovolný aktivní (světlý) monitor lze přepnout libovolnou kameru v systému (ke které má uživatel přístup). Přepnutí se provede velmi jednoduše tak, že nejprve kliknutím vybereme některý z aktivních monitorů video stěny (výběr je indikován modrým pozadím) a poté v ovládacím prvku ve spodní části okna klikneme na příslušnou kameru libovolného serveru. Výběr serveru listováním nebo ze seznamu funguje stejně jako v případě přepínání v dohledových oknech nebo při tvorbě událostních scénářů. Pokud dojde k úspěšnému přepnutí kamery na vzdálený monitor, v symbolu monitoru se objeví nad sebou identifikace serveru a identifikace kamery. Vypnutí kamery z monitoru se provede tlačítkem se symbolem křížku vedle ovládacího prvku se servery a kamerami.

Náhled video stěny je samozřejmě aktualizován v závislosti na činnosti všech uživatelů s přístupem k video stěně (a také v důsledku výskytu poplachových událostí). Pokud tedy jiný uživatel (či sám systém) provede přepnutí kamery na vzdálený monitor, informaci ihned uvidíte také ve svém náhledu video stěny.

Monitory označené symbolem bílé tečky patří do skupiny událostních monitorů a systém na ně automaticky umísťuje a posouvá kamery, které zobrazují poplachové události systému (které jsou v událostním scénáři opatřeny příznakem Zařadit do pohledu).

Monitory s viditelným rozdělením na 4, 9, nebo 16 částí jsou monitory typu Quad, Triple a Šestnáct, které zobrazují až 4, 9, nebo 16 kamer. Pokud je vybraný monitor typu Quad, Triple, nebo Šestnáct, je kromě celého monitoru vybrána vždy také jedna z jeho částí, na kterou bude provedeno ruční přepnutí kamery.

Pomocí tlačítka pro vyhledání zařízení lze stejným způsobem jako v dohledovém okně rychle vyhledat kameru dle čísla či názvu a přepnout ji na video stěnu.

POZNÁMKA

Video stěna má implementovány všechny mechanismy obnovy spojení jako standardní klient (výpadek kamery, výpadek spojení s kamerovým serverem). Navíc je vybavena i možností obnovy spojení s administračním serverem. Po restartu samotné video stěny (počítače či klientské software) dojde k automatické obnově do předchozího stavu.

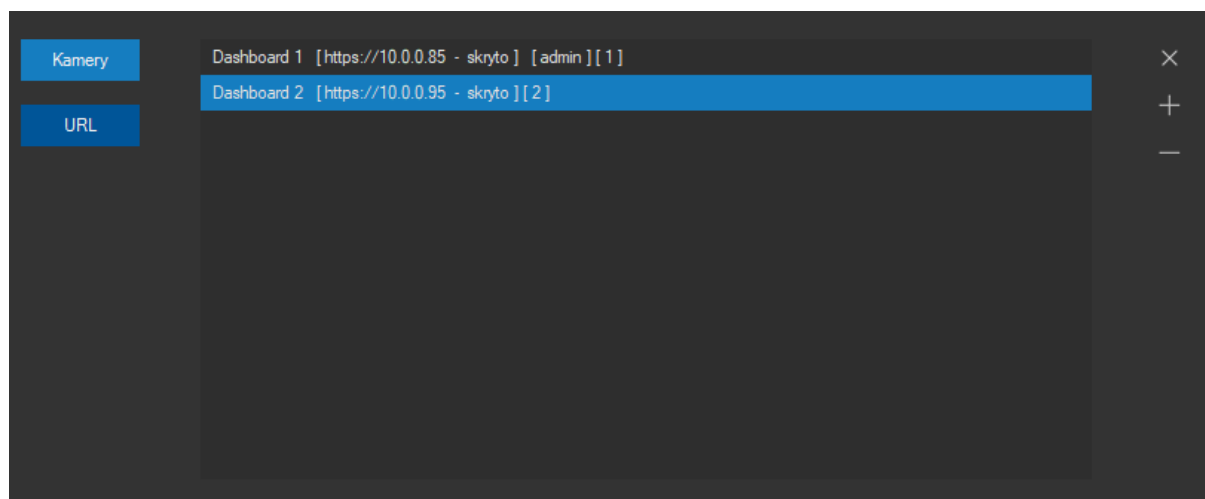
4.7.2. Zobrazení metadat

Obdobně jako v lokálních či sdílených pohledech lze na video stěně aktivovat zobrazování analytických metadat pocházejících z neuronové sítě ATEAS anebo přímo z kamer. Pro přepnutí na vybranou pozici video stěny lze použít rozbalovací seznam Metadata v pravé dolní části okna.

Při zobrazení většího počtu kamer ve vysokých snímkových frekvencích na jednom počítači video stěny je vhodné aktivovat v lokálním nastavení klienta video stěny GPU akceleraci pro zobrazení videa a při větších počtech detekovaných objektů také GPU akceleraci vykreslování metadat.

4.7.3. Přepínání URL

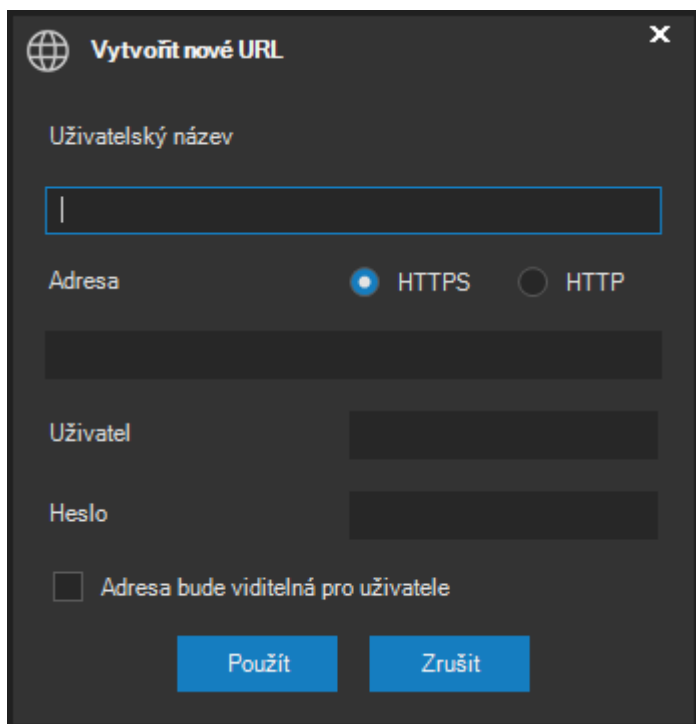
Video stěna podporuje také zobrazení webového obsahu v moderním provedení HTML 5, CSS atd. Na libovolné místo ve video stěně je možné stejným způsobem jako kameru provést také přepnutí URL, které do systému vložil oprávněný uživatel. Výběr URL je možné aktivovat tlačítkem **URL**.



V seznamu URL jsou zobrazeny uživatelské názvy URL a taktéž adresa URL, pokud je její zobrazení uživatelům povoleno. Pokud je zobrazení skryto, uživatel může URL přepnout na video stěnu, nevidí ale jeho skutečnou adresu. Pokud uživatel má oprávnění k tvorbě URL, adresu vidí vždy. Pokud je nastavená jako skrytá, vidí tuto informaci za adresou.

Na konci URL je oprávněným uživatelům zobrazen jeho číselný identifikátor pro použití s ATEAS API.

URL lze přidat kliknutím na tlačítko se symbolem plus. Poté je potřeba vyplnit následující dialog.



Je nutné vyplnit uživatelský název a adresu (spolu s protokolem http nebo https). Pokud dané URL vyžaduje autentizaci, je možné vyplnit uživatelské jméno a heslo. Video stěna pak bude schopná se sama k dané adrese přihlásit a zobrazit webový obsah.

Pomocí příslušné volby lze také ovlivnit, zdali uživatelé bez oprávnění k tvorbě nových URL budou moci vidět adresu konkrétního URL.

Tlačítkem se symbolem minus lze vybrané URL odstranit ze seznamu.

Stejně jako v případě webového obsahu zobrazeného přímo v dohledovém okně klienta, lze i do webového obsahu zobrazeného na video stěně vložit aktuální hodnoty čítačů. Více viz tvorba komplexních událostí a čítačů.

4.7.4. Zobrazení detailu

Zajímavou a důležitou funkcí je možnost rychlého přístupu k vybrané kameře video stěny. Pomocí dvojitého kliknutí na aktivní monitor s přepnutou kamerou lze ihned zobrazit standardní lokální pohled v detailním pohledu na vybranou kameru. Funkci lze samozřejmě použít pro monitory všech typů včetně Quad monitorů.

POZNÁMKA

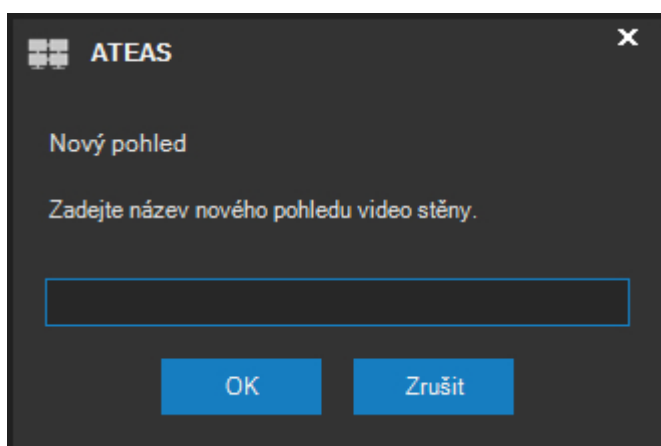
Tuto funkci využijete, jakmile budete u vybrané kamery potřebovat provádět další funkce. To se týká např. ovládání kamery, přepnutí do prepozice, poslechu zvuku, aktivace výstupů, náhledu či stažení záznamu apod.

4.7.5. Pohledy video stěny

Přepínání kamer na video stěnu je zcela analogické přepínání kamer na lokální dohledová okna. Velmi podobný princip má také ukládání lokálních pohledů a ukládání pohledů video stěny. Pro ovládání pohledů video stěny slouží skupina tlačítek mezi náhledem video stěny a seznamem pohledů video stěny.



Pomocí prostředního tlačítka lze aktuální stav video stěny (čili rozmístění kamer na monitorech) uložit jako pohled video stěny. Před uložením postačí pouze zadat název.



Uložené pohledy video stěny se zobrazují v seznamu v pravé části okna. Libovolný pohled video stěny lze kdykoliv opět vyvolat tak, že příslušný pohled vybereme v seznamu a použijeme horní tlačítko se symbolem šipky směřující vlevo. Tímto způsobem lze tak provést rozmístění libovolného počtu kamer na video stěnu jedním kliknutím.

POZNÁMKA

Pohledy video stěny jsou pro každého uživatele lokální a nelze je sdílet.

Spodním tlačítkem ve skupině tlačítek ovládání pohledů video stěny se symbolem křížku lze libovolný lokálně uložený pohled video stěny smazat.

I přes zjevnou analogii mezi lokálními pohledy a pohledy video stěny existuje při jejich přepínání jeden významný rozdíl. Přepínání pohledů video stěny není invazivní. Tím se rozumí následující chování. Pokud jsou součástí lokálního pohledu prázdné pozice, budou při přepnutí lokálního pohledu tyto prázdné pozice vytvořeny (tj. na příslušných pozicích budou vypnuty kamery). Při přepínání pohledů video stěny však na neobsazených (volných) monitorech zůstávají původní kamery. To znamená, že si můžete vytvořit pohledy, které budou měnit např. pouze horní či spodní řadu video stěny nebo pouze nějaké konkrétní vybrané monitory.

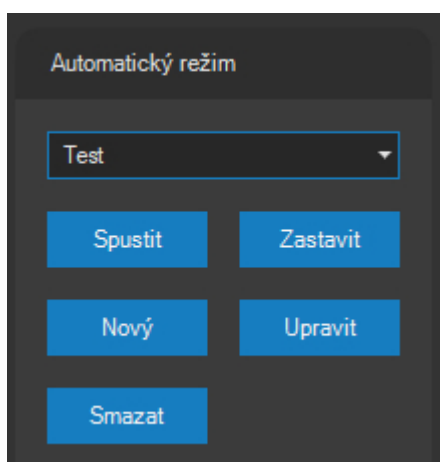
4.7.6. Automatický režim

Pokud máte vytvořeny pohledy video stěny, je možné je využít k vytvoření automatického režimu (automatické střídání pohledů video stěny).

POZNÁMKA

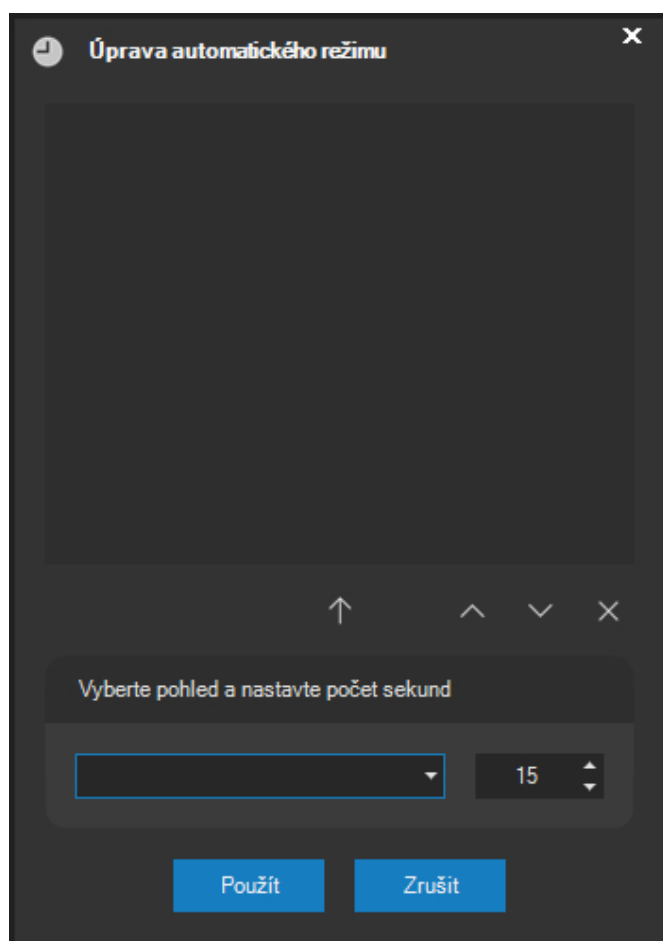
Stejně jako jsou pohledy video stěny analogické lokálním pohledům uživatele, je automatický režim video stěny podobný lokálním automatickým režimům (automatům) v dohledových oknech, pouze s tím rozdílem, že automatický režim video stěny je sestaven z jednotlivých pohledů, zatímco automat v dohledovém okně je sestaven pro libovolnou pozici v dohledovém okně přímo z jednotlivých kamer na jednom či více serverech.

Pro vytvoření a správu automatických režimů a pro jejich spouštění slouží skupina ovládacích prvků v pravé spodní části okna.



V rozbalovacím seznamu je zobrazen seznam všech vytvořených automatických režimů. Stejně jako v případě pohledů video stěny, jsou i automatické režimy video stěny uloženy na konkrétní stanici a není možné je sdílet.

Tlačítkem **NOVÝ** lze vytvořit nový automatický režim. Po zadání názvu pro automatický režim je zobrazen dialog, ve kterém je možné automatický režim upravit. Jedná se o stejný dialog, který je pro vybraný automatický režim zobrazen i při jeho budoucích úpravách po stisku tlačítka **ÚPRAVY**.



Ve spodní části je třeba vybrat libovolný pohled video stěny a prodlevu v sekundách. Stiskem zelené šipky je pohled přidán na konec automatického režimu do seznamu Pohledy video stěny. Prodlevu (setrvání daného pohledu na video stěně) lze nastavit v rozmezí od 5 sekund do 10 hodin. Po uplynutí této doby bude přepnut následující pohled v seznamu (nebo první, pokud je dosaženo konce seznamu). Pomocí tlačítek vpravo od seznamu pohledů lze měnit pořadí pohledů nebo vybraný pohled odstranit. Jeden pohled může být samozřejmě součástí automatického režimu vícekrát, celkový počet pohledů není v podstatě omezen.

POZNÁMKA

V důsledku neinvazivního přepínání pohledů video stěny lze jednoduše vytvářet automatické režimy, které budou měnit například pouze určitou část video stěny.

Vybraný automatický režim lze odstranit tlačítkem **SMAZAT**.

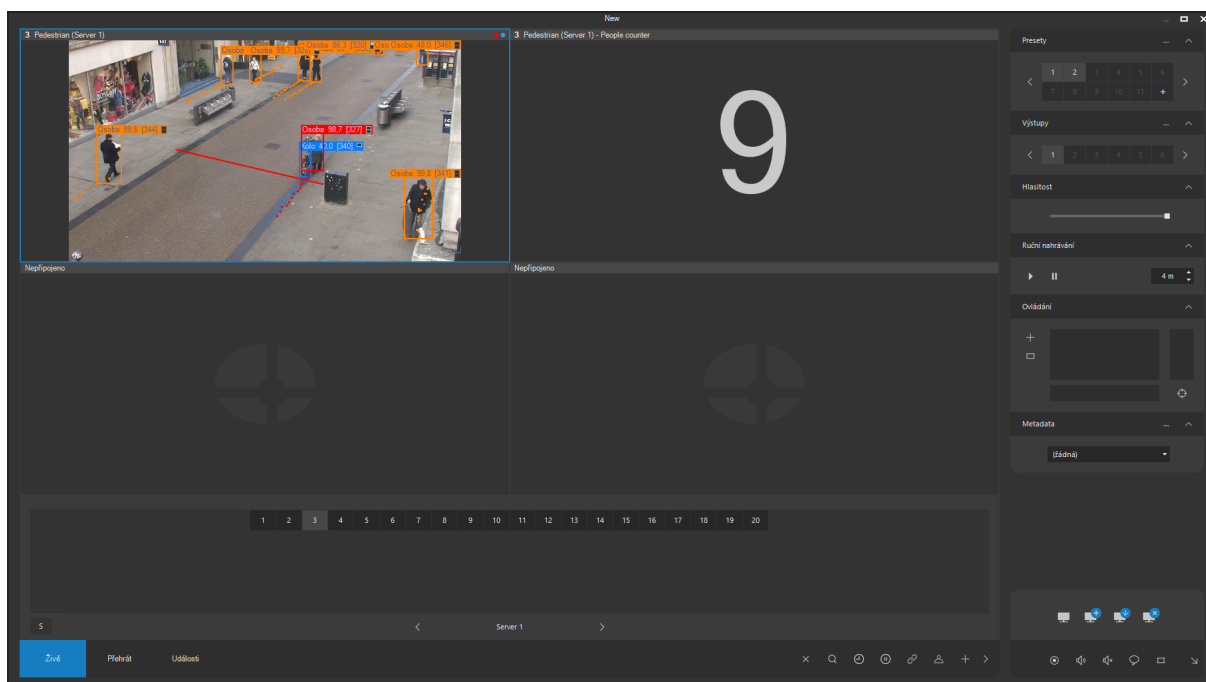
Libovolný automatický režim lze spustit a případně zastavit pomocí tlačítek **SPUSTIT** a **ZASTAVIT**. Použitím tlačítka **SPUSTIT** lze aktivovat zvolený automatický režim, aktuálně spuštěný je vždy ukončen. Pokud je zvolený režim již spuštěn, je restartován. Tento způsob restartování automatického režimu je také zapotřebí použít, pokud je automatický režim upraven za běhu a chceme aplikovat provedené změny. Pokud jiný oprávněný uživatel spustí jiný automatický režim, je aktuální režim nahrazen novým.

POZNÁMKA

Automatický režim je po spuštění uložen na serveru a bude aktivní do doby, než je opět deaktivován oprávněným uživatelem. Automatický režim tedy běží i po zavření okna video stěny či odhlášení uživatele.

4.8. Práce s čítači

Pomocí čítačů lze přímo v dohledovém okně zobrazovat počet výskytů libovolné události nebo jejich kombinace. Budeme-li např. kombinovat událost přechodu osoby přes čáru ve všech vchodech a ve východech, bude čítač ukazovat aktuální počet lidí v budově nebo areálu. Pokud je vchod zároveň i východ, lze vytvořit dva událostní zdroje podle směru překročení čáry.



POZNÁMKA

Pro statistické zobrazení počtů událostních zdrojů slouží grafický modul analýzy metadat. Čítač naproti tomu je okamžitou hodnotou dané kombinace zdrojů.

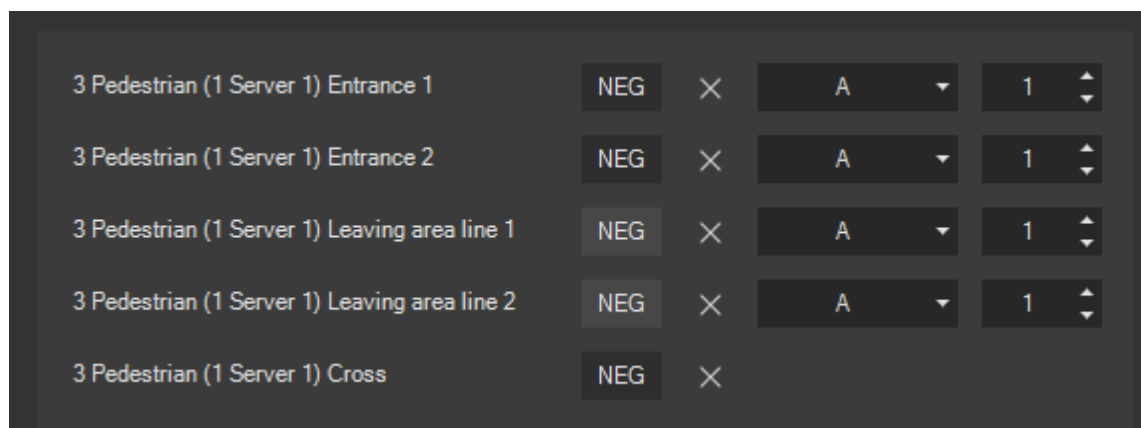
4.8.1. Zónové čítače

Zónové čítače jsou v systému vytvořené automaticky a odpovídají vytvořeným analytickým událostním zdrojům navázaným na uzavřené zóny. Hodnota zónového čítače tak odpovídá aktuálnímu celkovému počtu objektů všech typů, jaké jsou v rámci zdroje vybrány.

4.8.2. Komplexní čítače

Pro libovolnou kameru lze čítač vytvořit jako komplexní událost. Komplexní čítač je v systému ekvivalentní právě složenému zdroji události. Nezajímá nás zde sice logický výsledek celé události, ale využíváme možnost propojení zdrojů mezi sebou napříč kamerami či servery.

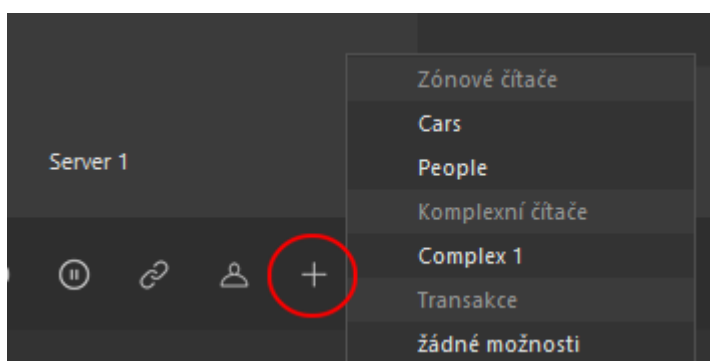
Při tvorbě čítače (komplexní události) budou všechny událostní zdroje jeho hodnotu zvyšovat, pokud nebudou opatřeny logickou negací. Logická negace bude hodnotu čítače snižovat, jak ilustruje následující obrázek.



Do hodnoty čítače lze samozřejmě zkombinovat události z mnoha různých kamer připojených k různým serverům, včetně externích událostí.

4.8.3. Zobrazení hodnoty čítače

Zobrazení hodnoty čítače pro vybranou kameru lze provést z nabídky možností dodatečných dat kamery, kde jsou automaticky zahrnuty všechny zónové i komplexní čítače.



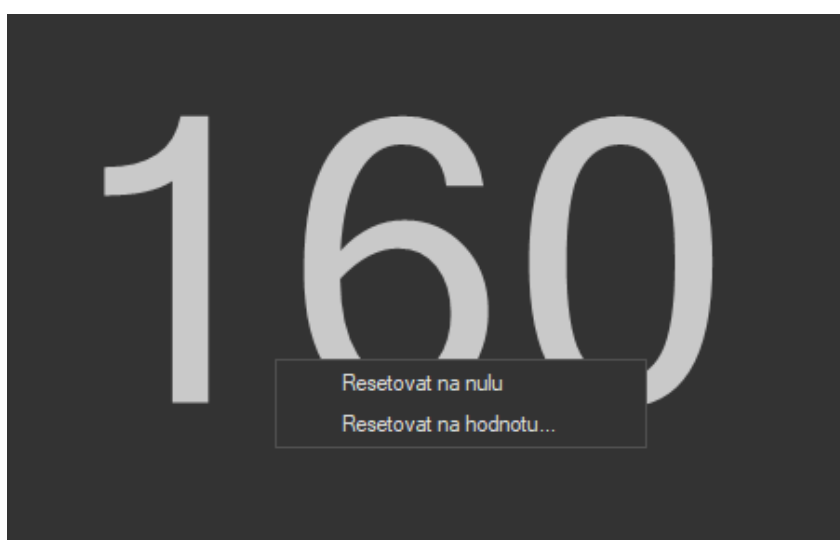
Seznam čítačů je zobrazen vždy pro vybranou kameru, obsah vybrané pozice je poté nahrazen hodnotou čítače. Pokud je okno v režimu živého náhledu, čítače budou zobrazovat hodnoty v reálném čase. V režimu přehrávání budou čítače zobrazovat hodnoty platné v čase určeném časovou osou při přehrávání.

4.8.4. Ruční reset hodnoty čítače

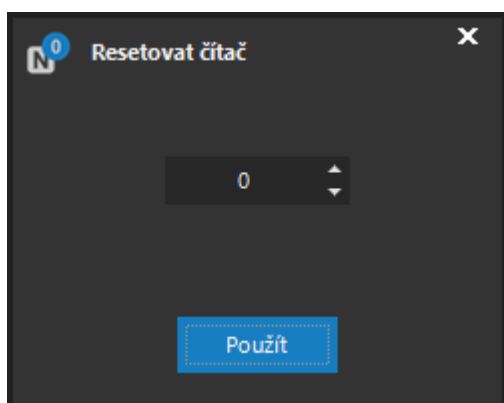
Oprávnění uživatelé mohou kdykoliv provést reset hodnoty čítače na nulu nebo jinou celočíselnou hodnotu. Oprávnění potřebné pro tuto funkci ke administrátorovi k dispozici pod názvem Rozšířené událostní funkce. Reset se provádí pomocí kontextového menu na daném čítači.

POZNÁMKA

Reset hodnoty je možné provádět pouze pro komplexní čítače, nikoliv pro automatické zónové.



Při volbě druhé položky je zobrazen dialog, ve kterém je možné zvolit hodnotu.

**TIP**

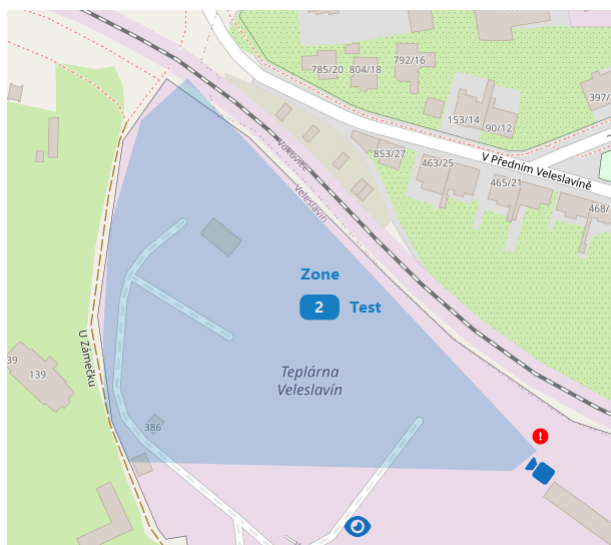
Stejným způsobem je možné provést ruční reset i v případě čítače vloženého do webové stránky, která je zobrazena v rámci klienta ATEAS.

4.8.5. Událostní reset hodnoty čítače

Čítač lze dále resetovat na nulu či libovolnou hodnotu v reakci na libovolnou událost v systému pomocí nastavení v událostním scénáři. Lze tedy hodnotu resetovat pravidelně v určitém čase (na základě časové události) anebo pomocí jakékoliv jiné události včetně externí. Více viz správa událostí v systému.

4.8.6. Zónové čítače v mapě

Automatické zónové čítače jsou také automaticky zobrazeny v mapových podkladech, a to jakmile je lokalizována příslušná zóna, na kterou jsou čítače navázány.



4.8.7. Hodnota čítače ve webové stránce

Aktuální hodnoty čítačů mohou být zobrazeny také jako součást aktivního webového obsahu. V tomto případě je možné v rámci jedné webové stránky v jednom místě pohledu zobrazit i více různých čítačů. Čítač je do webové stránky vložen pomocí libovolné html značky s příslušným ID parametrem. Více viz tvorba komplexních událostí a čítačů. Hodnoty čítačů zobrazených ve webové stránce jsou však vždy hodnotami čítače v reálném čase včetně situace, kdy je okno přepnuto do režimu přehrávání.

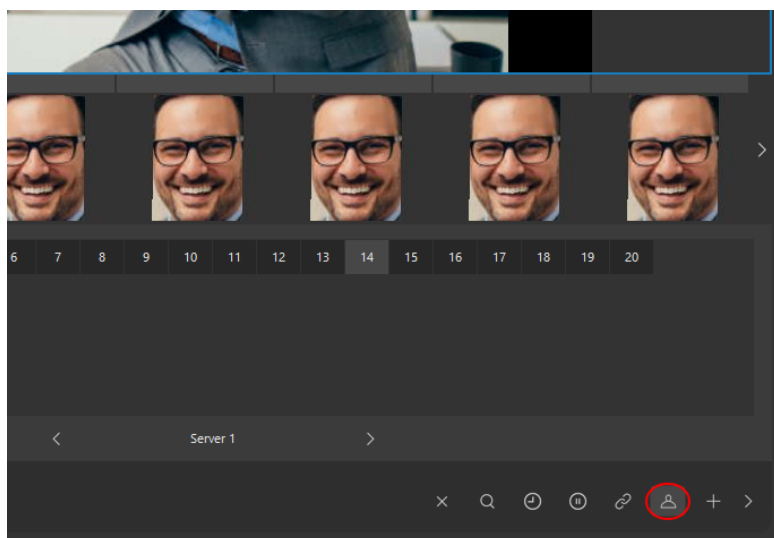
POZNÁMKA

Historické hodnoty čítačů lze zobrazit tak, že čítač zobrazíme v pohledu přímo.

4.9. Práce s databází obličejů

4.9.1. Náhled obličejů

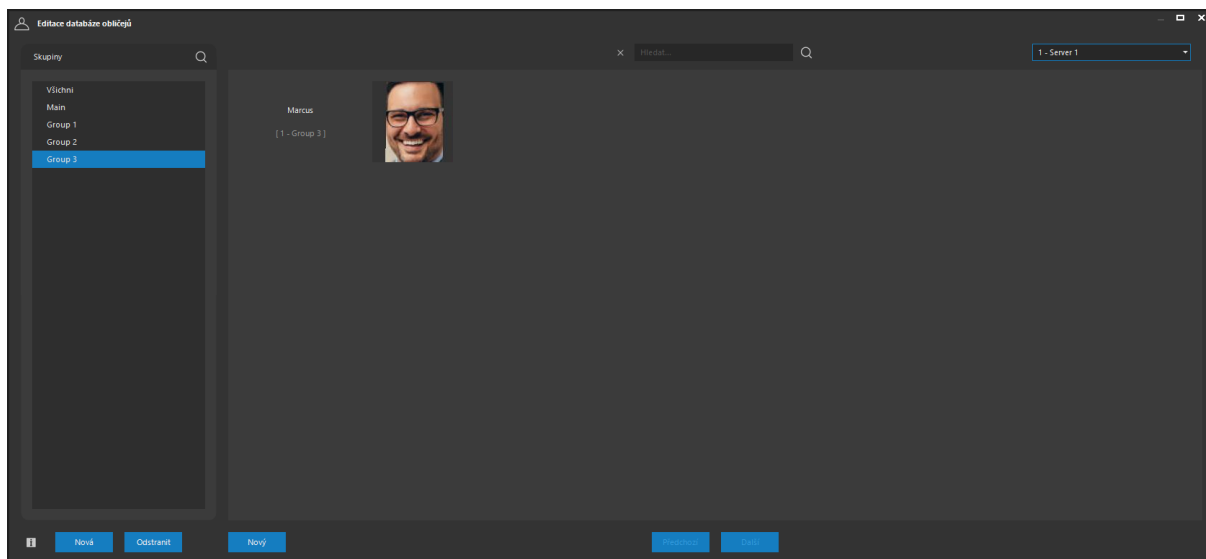
Pokud pro vybranou kameru probíhá analýza typem sítě Rozpoznávání obličejů, je možné zobrazit náhled obličejů v kanonickém (základním) tvaru živě v reálném čase nebo ze záznamu. K tomu slouží tlačítko se symbolem obličeje.



Pokud je daný obličej přiřazen konkrétní osobě, bude nad náhledový obrázek automaticky doplněno jméno a skupina. K zobrazení obličejů je nutné mít příslušné oprávnění pro zobrazení metadat.

4.9.2. Databáze obličejů

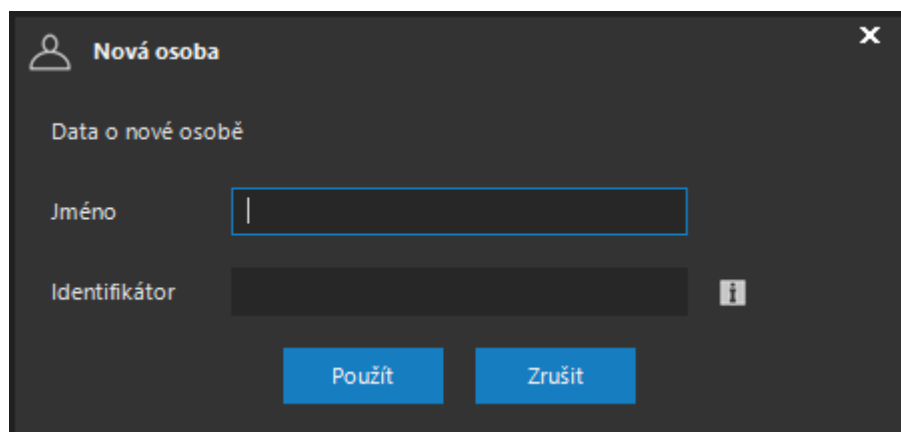
Uživatelé s oprávněním pro editaci databáze obličejů mohou pravým tlačítkem v oblasti zobrazených obličejů vyvolat nabídku, ve které je možné vybraný obličej kopírovat nebo vstoupit do databáze obličejů. Databázi lze také rychle otevřít v hlavní nabídce ve skupině Nástroje.



Detekované obličeje jsou v reálném čase porovnávány s databází a obličejům jsou přiřazovány dle nastavení parametru podobnosti pro neuronovou síť konkrétní jména a skupiny. Všechny osoby musí být zařazeny do nějaké skupiny, které je možné tvořit či mazat v levé části okna pomocí tlačítek **NOVÁ** a **ODSTRANIT**. Nový záznam osoby lze po výběru skupiny přidat stiskem tlačítka **NOVÝ**. Jak mezi

skupinami, tak mezi všemi osobami v databázi či ve skupinách lze pohodlně vyhledávat pomocí vyhledávacích polí v horní části okna. Tlačítka **PŘEDCHOZÍ** a **DALŠÍ** slouží ke stránkování osob v databázi.

Při vytváření nové osoby lze kromě celého jména zadat také volitelný identifikátor, který slouží k integračním účelům a může být součástí událostních notifikací zasílaných pomocí ATEAS API.



Osobu lze z databáze odstranit kliknutím na symbol křížku, který se objeví po najetí myši na jméno osoby. Přejmenovat skupinu či osobu lze dvojitým kliknutím na její současný název. Přesun osoby do jiné skupiny se provede jednoduše jejím přetažením.

4.9.3. Vkládání obrázků

Ke každé osobě lze přiřadit až 10 obrázků v kanonickém (základním) tvaru obličeje, přičemž na jejich pořadí nezáleží. To lze provést několika způsoby:

- zkopírováním obličeje v dohledovém okně a vložení na vybranou pozici v databázi pomocí kontextové nabídky po stisku pravého tlačítka myši,
- jednoduše přetažením obrázku do databáze z dohledového okna,
- přímým vložení obrázku ve formátu jpeg.

V případě přímého vložení obrázku však musí proběhnout jeho konverze do základního tvaru a k tomu je nutné vybrat kamerový server se spuštěným typem neuronové sítě Rozpoznávání obličejů. Pokud je to možné, kamerový server bude vybrán automaticky.

POZNÁMKA

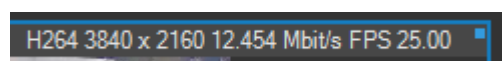
Pokud není na obrázku nalezen obličej v požadované spolehlivosti či jich bude nalezeno více, přímé vložení nebude možné.

Obrázky lze přesouvat jednoduše přetažením na jinou pozici. Pomocí symbolu křížku lze obrázek z databáze odstranit.

System je díky pokročilým technologiím na běžném hardware schopný v reálném čase provádět porovnávání detekovaných obličejů v databázi čítající milióny vložených obrázků. Tyto počty ovšem vyžadují zvýšenou rezervu operační paměti na administračním serveru ATEAS, zhruba 1GB RAM na 100 tisíc osob.

4.10. Informace o videu

V praxi velmi často potřebujeme získat přesné informace o tom, v jakém video formátu či v jakém rozlišení aktuálně klient přijímá video z kamery. K tomu slouží funkce zobrazení základních diagnostických informací, kterou lze aktivovat pro libovolný pohled. Aktivace funkce pro celý pohled se provede pomocí stisku kombinace kláves SHIFT – S (statistika). Následně se v pravých horních rozích jednotlivých kamerových oken budou pravidelně aktualizovat základní informace.



Informace obsahují údaje o video formátu, rozlišení, aktuálním datovém toku a snímkové frekvenci. Pomocí těchto údajů tak lze velmi rychle ověřit nastavení kamer, schopnost kamer produkovat deklarovanou snímkovou frekvenci či zátěž sítě.

POZNÁMKA

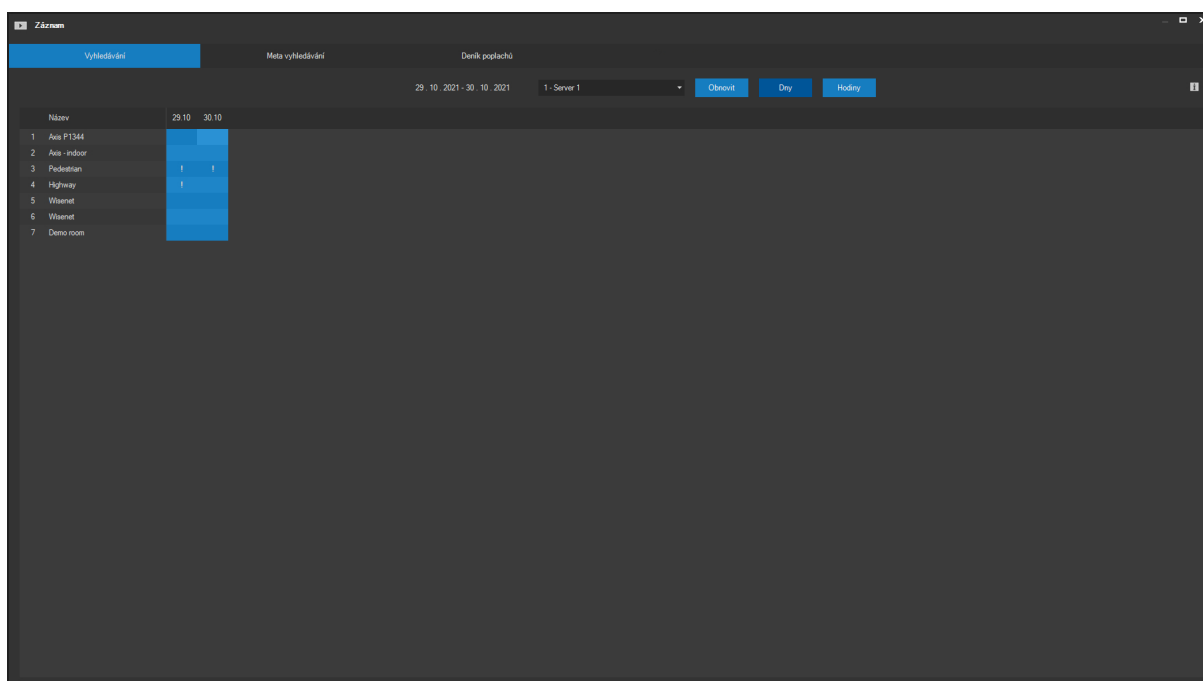
Data jsou získávána z videa, které je přenášeno mezi kamerovým serverem a klientem. Výsledky jsou tedy ovlivněny i nastavením videa na straně výstupu serveru (např. primární a sekundární snímková frekvence).

Kapitola 5 - Práce se záznamem

5.1. Vyhledávání záznamu

5.1.1. Přehled záznamu

Vedle přehrávání pohledu přímo v dohledových oknech je přístup k záznamu v systému možný přes volbu Záznam z hlavní nabídky aplikace. Pomocí časové tabulky po výběru kamerového serveru je možné jedním pohledem dostat informaci o čase a všech kamerách v záznamu včetně toho, kdy se vyskytly události či poplachové situace. Tato tabulka se objeví po výběru serveru z rozbalovacího seznamu a může být aktualizována stiskem tlačítka vedle rozbalovacího seznamu kamerových serverů, vše na kartě **Vyhledávání**.



Název	29. 10.	30. 10.
1. Asa P1344		
2. Asa - indoor		
3. Pedestrian		
4. Highway		
5. Wiseret		
6. Wiseret		
7. Demo room		

Sloupce tabulky jsou tvořeny jednotlivými dny (či hodinami), které jsou v záznamové databázi, řádky jsou tvořeny kamerami vybraného kamerového serveru opatřenými číslem a názvem. Pokud je buňka tabulky odpovídající určité kameře a určitému dni (či hodině) bez výplně, nejsou v tomto intervalu pro kameru k dispozici žádná zaznamenaná data. Pokud má buňka barevnou výplň, je pro celý nebo část dne (či hodiny) záznam kamery k dispozici. Pokud se navíc na barevném pozadí objevuje symbol vykřičníku, jsou pro tento interval k dispozici události či poplachové situace.

	Název	29.10	30.10
1	Axis P1344		
2	Axis - indoor		
3	Pedestrian	!	!
4	Highway	!	
5	Wisenet		
6	Wisenet		
7	Demo room		

Implicitně je tabulka zobrazena nejprve v režimu rozdělení do dní (sloupce tabulky jsou tvořeny dny). Přepínání mezi režimem Dny a Hodiny lze pomocí příslušných dvou tlačítek, vedle kterých se zobrazuje aktuální rozsah dní (v režimu Dny) nebo vybraný den (v režimu Hodiny).

29. 10. 2021 - 30. 10. 2021
1 - Server 1
Obnovit
Dny
Hodiny

Tlačítko **HODINY** však bude moci být úspěšně použito pouze tehdy, pokud je v tabulce vybrán příslušný den (je označena libovolná buňka ve sloupci daného dne). V opačném případě není možné do režimu Hodiny přepnout. Do režimu Hodiny lze jednoduše přepnout také dvojitém kliknutím do libovolné buňky tabulky s barevným pozadím indikujícím dostupnost záznamu. Dojde k přetvoření tabulky, po kterém budou jednotlivé sloupce představovat hodiny vybraného dne, řádky a údaje v tabulce mají nadále stejný význam.

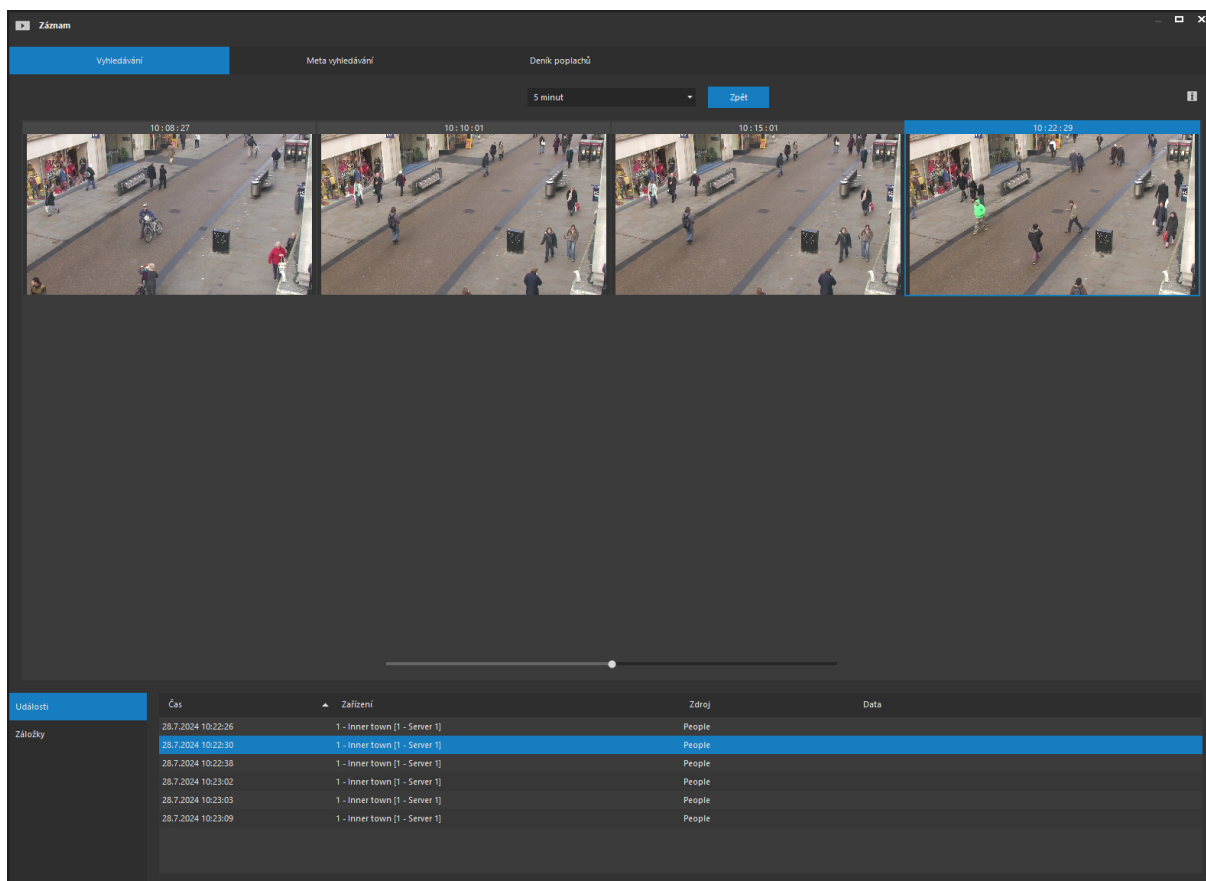
POZNÁMKA

Zatímco při zobrazení denního přehledu bude počet sloupců odpovídat počtu dnů obsažených v záznamové databázi vybraného serveru, hodinový přehled bude mít vždy 24 sloupců (rozdělení do hodin).

Pokud má buňka v režimu Dny barevné pozadí (resp. je navíc opatřena symbolem vykřičníku), musí po přepnutí do režimu Hodiny být pro danou kameru k dispozici alespoň jedna buňka (hodina) s barevným pozadím (resp. se symbolem vykřičníku).

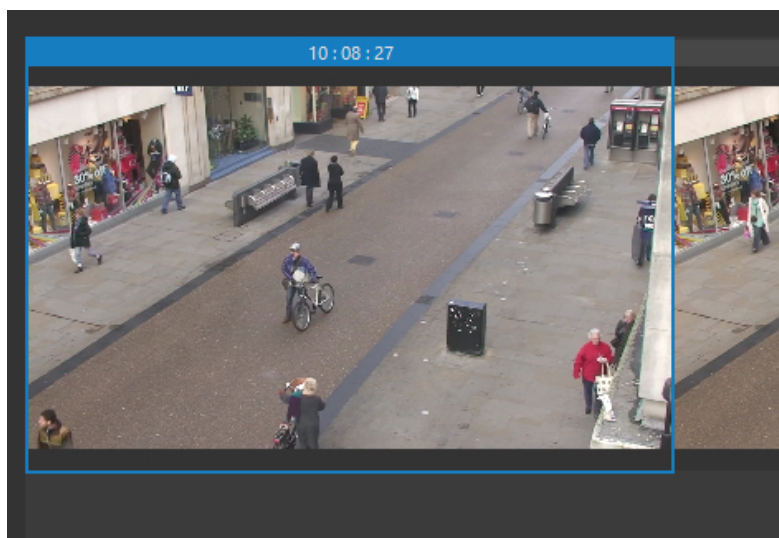
5.1.2. Zobrazení video přehledů

Záznam vybrané hodiny lze pro maximálně rychlou orientaci v zaznamenaných datech zobrazovat v náhledovém zobrazení. Dvojitě kliknutí na buňku s barevným pozadím v režimu Hodiny vede k zobrazení video přehledu pro vybranou hodinu. Při hledání lze tak velmi rychle identifikovat cílový časový úsek, který uživatele v dané chvíli zajímá.



Události	Čas	Zařízení	Zdroj	Data
Záložky	28.7.2024 10:22:26	1 - Inner town [1 - Server 1]	People	
	28.7.2024 10:22:30	1 - Inner town [1 - Server 1]	People	
	28.7.2024 10:22:38	1 - Inner town [1 - Server 1]	People	
	28.7.2024 10:23:02	1 - Inner town [1 - Server 1]	People	
	28.7.2024 10:23:03	1 - Inner town [1 - Server 1]	People	
	28.7.2024 10:23:09	1 - Inner town [1 - Server 1]	People	

Tlačítkem **ZPĚT** je možné se vrátit k hodinovému přehledu a zobrazit jinou hodinu případně tutéž hodinu jiné kamery. Standardně je video přehled zobrazen s rozlišením pět minut, tj. bude zobrazeno až dvanáct přehledových snímků za hodinu. Toto rozlišení je však možné změnit a klient pokaždé upraví rozvržení pro optimální náhled videa. Ve video přehledu je v záhlaví každého začátku intervalu uveden přesný čas.



Jednotlivé intervaly lze vybírat pomocí levého tlačítka myši. Kolem vybraného intervalu je zobrazen modrý rámeček. Vybraný interval lze dále zobrazovat v náhledu či provést jeho stažení (export ze záznamové oblasti kamerového serveru na lokální disk).

POZNÁMKA

U vybraného okna lze pro lepší náhled pomocí kolečka myši a klikáním do obrazu provádět operace digitálního přiblížení a posunu.

Pokud vybraná hodina obsahuje události či poplachové situace (buňka byla opatřena symbolem vykřičníku), bude pod video přehled automaticky doplněn seznam událostí.

Událost	Čas	Zařízení	Zdroj	Data
Zálohy	29.10.2021 17:14:02	server 1 (Server 1) kamera 3 (Pedestrian)	Cross	278
	29.10.2021 17:14:02	server 1 (Server 1) kamera 3 (Pedestrian)	Cross	273
	29.10.2021 17:14:05	server 1 (Server 1) kamera 3 (Pedestrian)	Cross	317
	29.10.2021 17:14:07	server 1 (Server 1) kamera 3 (Pedestrian)	Cross	304
	29.10.2021 17:14:11	server 1 (Server 1) kamera 3 (Pedestrian)	Cross	316
	29.10.2021 17:14:15	server 1 (Server 1) kamera 3 (Pedestrian)	Cross	331
	29.10.2021 17:14:15	server 1 (Server 1) kamera 3 (Pedestrian)	Cross	330
	29.10.2021 17:14:19	server 1 (Server 1) kamera 3 (Pedestrian)	Cross	340
	29.10.2021 17:14:19	server 1 (Server 1) kamera 3 (Pedestrian)	Cross	340

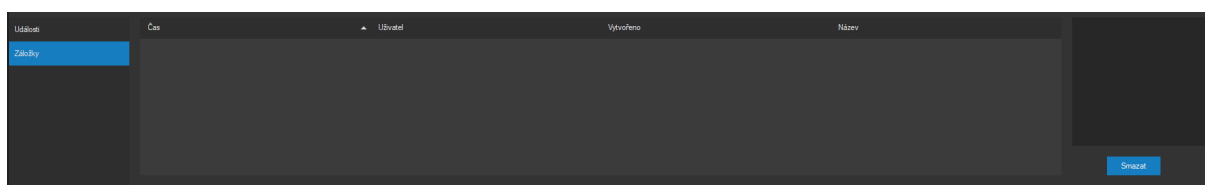
Tento přehled obsahuje přesné datum a čas události, zařízení, které událost vyvolalo, zdroj události na daném zařízení (detekce pohybu, poplachový vstup atd.) a doplňující informaci či upřesnění zdroje události (např. RZ vozidla).

POZOR

Zobrazené události pod video přehledem jsou událostmi, na které vybraná kamera reagovala událostním záznamem (může být doprovázeno zahájením záznamu či zvýšením jeho snímkové frekvence dle nastavení). Zařízení, které událost vyvolalo, tak nemusí být shodné s kamerou, jejíž záznam právě prohlížíte.

Kliknutím na libovolnou událost v seznamu dojde k automatickému vybrání příslušného časového intervalu ve video přehledu (vytvoří se modrý rámeček) a také k synchronizaci času na začátek události přes ovládací prvek rychlého náhledu (viz dále).

Pokud vybraná hodina obsahuje záložky (buňka byla opatřena symbolem trojúhelníku indukujícím komentář), bude pod video přehled automaticky doplněn seznam záložek.



Tento přehled obsahuje přesné datum a čas záložky, jméno uživatele, který ji vytvořil, čas vytvoření a nadpis záložky.

Kliknutím na libovolnou záložku v seznamu dojde k automatickému vybrání příslušného časového intervalu ve video přehledu (vytvoří se modrý rámeček) a také k synchronizaci času na začátek záložky přes ovládací prvek rychlého náhledu (viz dále). Zároveň se také zobrazí plný text záložky v textovém poli vedle seznamu.

POZNÁMKA

Ve výchozím nastavení je jako první zobrazen seznam událostí a poplachů. Mezi seznamem událostí a poplachů a seznamem záložek lze přepínat pomocí rozbalovacího seznamu.

Odstranění záložky lze provést pomocí tlačítka **SMAZAT** vedle seznamu záložek. K tomu, aby uživatel mohl vkládat záložky do záznamu a provádět jejich výmaz, musí mít přiděleno příslušné oprávnění.

POZNÁMKA

I pokud má uživatel přiděleno oprávnění vkládat a mazat záložky, může vždy odstranit jen záložku, kterou vytvořil on sám, ledaže by byl administrátorem systému. V takovém případě by mohl mazat záložky všech uživatelů.

5.1.3. Náhled a uložení záznamu

Jednotlivé intervaly je možné stáhnout na lokální počítač. Jedině tak je možné tyto záznamové sekvence ochránit před přepisem na záznamovém serveru. Základní strategií při záznamu je cyklický přepis záznamových oblastí, a i když mohou být např. poplachové situace umístěny ve zvláštních oblastech, které nejsou při naplnění kapacity ihned přepisovány, je stažení sekvence jedinou možností, jak natrvalo záznam uložit.



Pro rychlý náhled intervalu je možné použít tento posuvník. Jeho levý a pravý doraz reprezentují začátek a konec právě vybraného intervalu video přehledu a pohybem posuvníku je synchronizováno video. Při náhledu intervalu tak můžete sekvenci přehrát v podstatě libovolnou rychlostí.

POZNÁMKA

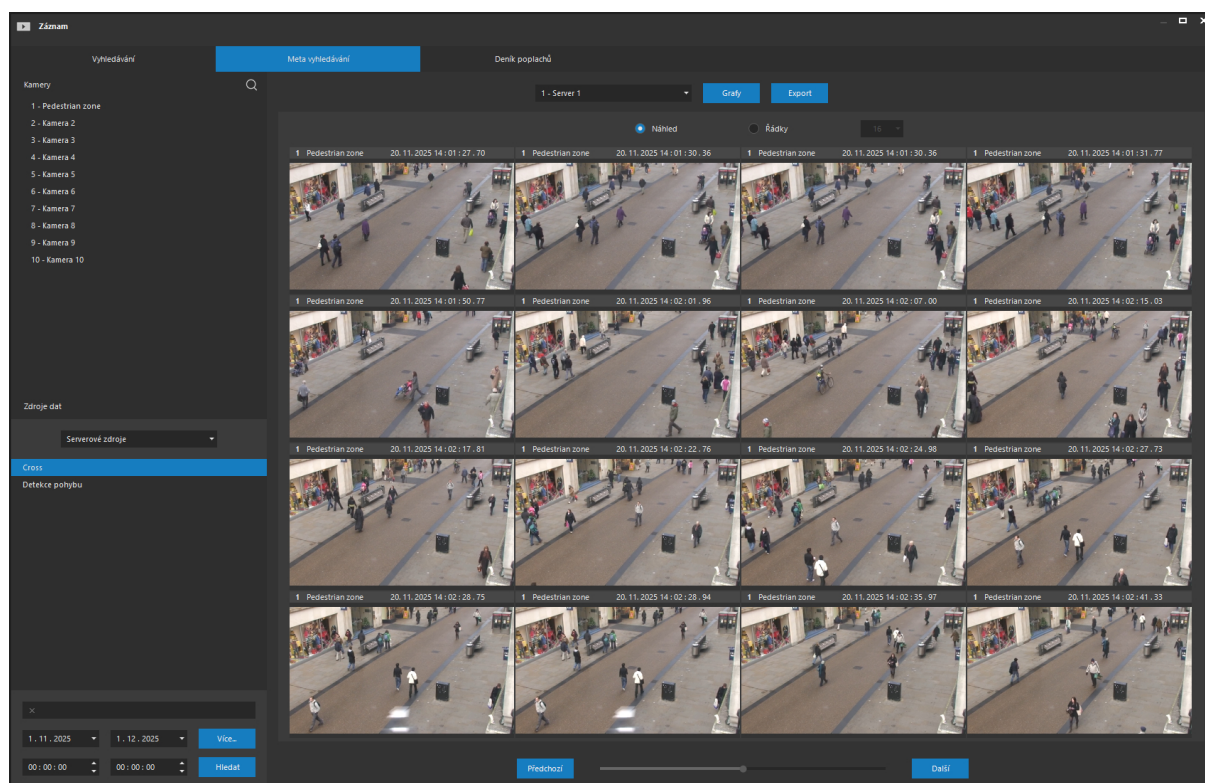
V okně s náhledem videa kamery nebo v seznamu položek je kdykoliv možné dvojitým kliknutím na jeho záhlaví či na položku v seznamu provést automatické otevření dohledového okna a jeho nastavení pro přehrávání zvoleného časového okamžiku.

Stažení intervalu lze provést dvojitým kliknutím na jeho náhled.

Stahování dat ze záznamových oblastí jednotlivých kamerových serverů je prováděno pomocí inteligentního manažera stahování, který je popsán v samostatné kapitole. Manažer stahování eviduje požadavky na stažení sekvencí jako své úkoly, které postupně či paralelně provádí. Dvojitým kliknutím lze do manažera stahování přiřadit nový úkol.

5.2. Meta vyhledávání

Meta vyhledávání slouží pro rychlé vyhledání na základě výběru zdroje událostí či dodatečných dat.



POZNÁMKA

Kromě kamerových zdrojů dat lze pomocí meta vyhledávání hledat také externí zdroje událostí, a to výběrem položky Externí objekty.

5.2.1. Zadání kritérií

Nejprve je nutné provést výběr kamerového serveru, jehož kamery budou následně zobrazeny v seznamu kamer. V seznamu se nachází také položka Externí objekty pro vyhledávání mezi externími zdroji událostí z objektů a jejich prvků.

POZNÁMKA

Pokud je v systému aktivována centralizace metadat, bude možné vybrat také položku Všechny servery.

V seznamu kamer je možné vybrat libovolný počet kamer. Pokud vyhledáváme v centralizovaných metadatech, bude možné vybírat kamerové servery. Vícenásobný výběr je možný např. pomocí klávesy CTRL.

TIP

Pokud není vybrána žádná kamera, budou do vyhledávání zahrnuty automaticky všechny kamery.

V části Zdroje dat je dále nutné vybrat minimálně jeden zdroj, a zahrnout ho tak do vyhledávání. Opět je možné označit více různých zdrojů. V případě, že chceme vybrat zdroje napříč skupinami, v rozbalovacím seznamu zvolíme Zobrazit vše.

Kamery

1 - Pedestrian zone

2 - Kamera 2

3 - Kamera 3

4 - Kamera 4

5 - Kamera 5

6 - Kamera 6

7 - Kamera 7

8 - Kamera 8

9 - Kamera 9

10 - Kamera 10

Zdroje dat

Poznávací značky

SPZ - neregistrovaná

SPZ - povolená

SPZ - zakázaná

SPZ - uživatelská 1

SPZ - uživatelská 2

×

1. 11. 2025

1. 12. 2025

Více...

00 : 00 : 00

00 : 00 : 00

Hledat

POZNÁMKA

Dynamické zdroje zahrnují všechny zdroje nabízené přímo konkrétní kamerou a to včetně kamer připojených přes rozhraní ONVIF.

POZNÁMKA

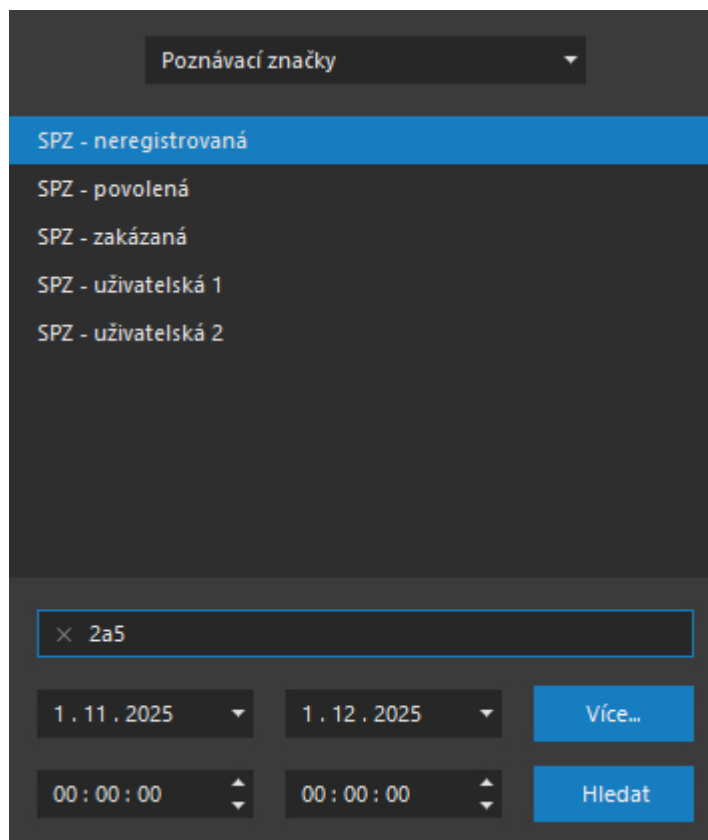
Při výběru více kamer jsou pro skupiny serverových, dynamických či komplexních zdrojů jednotlivé zdroje automaticky sdružovány podle jejich názvu.

Externí objekty

Pokud prohledáváme externí objekty, máme k dispozici přímo prvky vybraného objektu, které již nejsou rozděleny do skupin. Vyhledávání můžeme provést pro konkrétní objekt a jeden či více jeho prvků anebo také pro více objektů současně. V případě výběru objektů probíhá vyhledávání vždy pro všechny prvky vybraných objektů.

Dodatečná data

Pro většinu zdrojů je možné zadat dodatečná data pro vyhledávání do příslušného textového pole pod seznamem zdrojů.



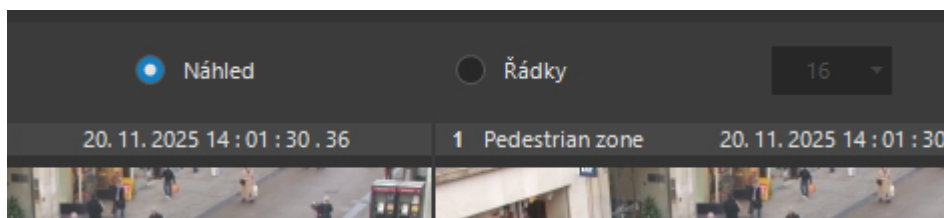
The screenshot shows a search interface with a dark theme. At the top, there is a dropdown menu labeled "Poznávací značky" with a downward arrow. Below the menu, a list of options is displayed: "SPZ - neregistrovaná" (highlighted in blue), "SPZ - povolená", "SPZ - zakázaná", "SPZ - uživatelská 1", and "SPZ - uživatelská 2". Below the list, there is a search input field containing the text "2a5" with a clear button (X) on the left. Under the input field, there are two date pickers: "1. 11. 2025" and "1. 12. 2025", each with a downward arrow. To the right of the date pickers are two buttons: "Více..." and "Hledat". Below the date pickers, there are two time pickers: "00 : 00 : 00" and "00 : 00 : 00", each with up and down arrows. To the right of the time pickers is another "Hledat" button.

Při jednoduchém zadání slova či více slov budou vyhledány výsledky, které obsahují všechny zadané skupiny znaků nezávisle na jejich pořadí. Pomocí tlačítka **VÍCE** lze provádět pokročilejší způsoby vyhledávání, jak je popsáno níže v samostatné subkapitole.

Pro vyhledávání je automaticky nastaven aktuální měsíc. Pomocí intuitivního kalendáře a prvků pro zadání času je možné vybrat jiný začátek a konec vyhledávání až do celkové délky intervalu jeden rok.

5.2.2. Zobrazení výsledků

Po zadání vyhledávacích kritérií stiskneme tlačítko **HLEDAT**. Výchozí podoba zobrazení výsledků nabízí náhled videa přesně synchronizovaného na konkrétní časový okamžik.



Výsledky lze přepnout do řádkového zobrazení, ve kterém je možné volit počet řádků zobrazených na jedné stránce. V obou režimech zobrazení výsledků je možné používat tlačítka **PŘEDCHOZÍ** a **DALŠÍ** pro přesun mezi stránkami. V režimu zobrazení náhledu videa je také možné pro vybraný výsledek pomocí posuvníku pod výsledky zobrazit video před časem a po času výsledku v celkové délce intervalu jedné minuty.

Dvojitým kliknutím na video či řádek lze zobrazit přidružený událostní pohled, pokud existuje.

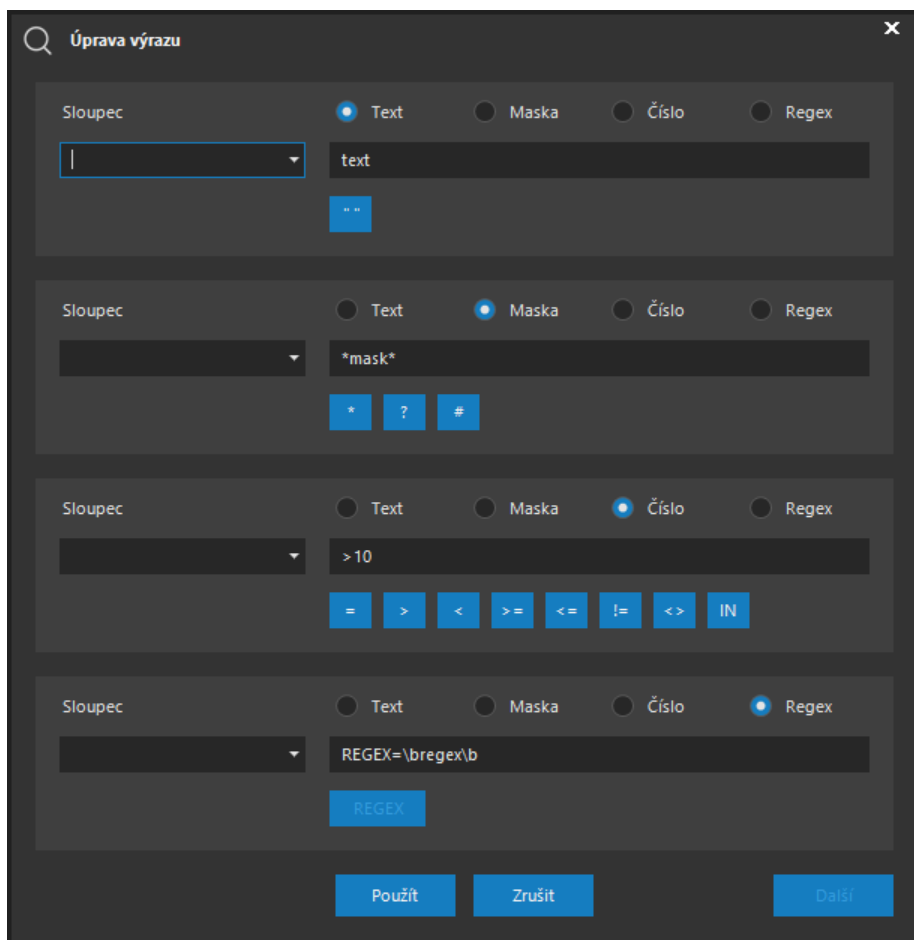
TIP

Událostní pohled obsahovat i další kamery, které chceme automaticky zobrazit.

Pokud bychom chtěli vynutit zobrazení pouze konkrétní kamery zobrazené ve výsledku, použijeme namísto dvojitého kliknutí na oblast videa dvojité kliknutí na záhlaví výsledku.

5.2.3. Rozšířené textové vyhledávání

Základní textové vyhledávání funguje tak, že ve výsledku musí být nalezeny všechny skupiny znaků nezávisle na jejich pořadí. Pomocí tlačítka **VÍCE** však lze tyto možnosti významně rozšířit.



V tomto dialogu je možné zvolit následující způsoby vyhledávání, pro každý z nich jsou zobrazena pomocná tlačítka sloužící k rychlému vložení dané funkce do pole pro vyhledávání.

POZNÁMKA

Všechny tyto způsoby lze využít i přímo ručním zadáním do textového pole vyhledávání. Dialog je pouze pomocníkem při tvorbě vyhledávacího výrazu.

Text: Vyhledání textu umožňuje vyhledat všechny skupiny znaků oddělených mezerami nezávisle na jejich pořadí. Pokud chceme vyhledat skupinu znaků obsahující mezeru, můžeme použít uvozovky.

Maska: Výchozí textové vyhledávání v podstatě nabízí režim masky, kdy jsou vyhledány i skupiny znaků, i když se nacházejí na začátku, uprostřed či konci slova. V režimu masky však můžeme toto chování ovlivnit použitím zástupných znaků * (zastupuje libovolné množství znaků včetně žádného), ? (zastupuje právě jeden znak) a # (zastupuje právě jednu číslici).

Číslo: Tento způsob umožňuje číselné porovnání hodnoty dle všech operátorů, které jsou zobrazeny pod textovým polem. Jedná se vyšetření rovnosti či nerovnosti, případně příslušnosti k intervalu.

POZNÁMKA

Číselné porovnávání podporuje desetinná čísla se symbolem tečky i čárky.

TIP

Systém dokáže zpracovat i číselné hodnoty, za kterými následuje text. To je zejména vhodné při definici podmínek u číselných údajů doplněných jednotkou, např. 50 km/h apod.

Regex: Tento způsob podporuje velmi rychlé vyhledávání pomocí regulárního výrazu se všemi možnostmi, které regulární výrazy nabízejí.

Nejsou-li data organizována ve sloupcích, je vyhledávací výraz použit vždy na kompletní datovou větu. Pokud však data obsahují více položek (např. RZ vozidla, typ vozidla, rychlost), je možné kombinovat více sloupců a více podmínek tak, že podmínku uvedeme názvem sloupce následovaným dvojtečkou. Např.

plate: 2A5 speed: > 50

Při použití této syntaxe musí výsledky vyhovovat vždy všem kritériím. Dynamické zdroje událostí, které poskytují dodatečná data, velmi často zahrnují více datových položek (sloupců), které mohou být přidány a ukládány s tím, že na ně lze později uplatnit tyto pokročilé metody vyhledávání.

Zahrnutí více sloupců lze provést opakovaným stiskem tlačítka **DALŠÍ**.

POZNÁMKA

Přestože v dialogu je počet sloupců omezen na čtyři, ruční zadání jich může obsahovat více.

TIP

Po provedeném meta vyhledávání systém analyzuje výsledky a v dialogu bude automaticky nabízet zjištěné sloupce, což velmi zjednoduší zadávání.

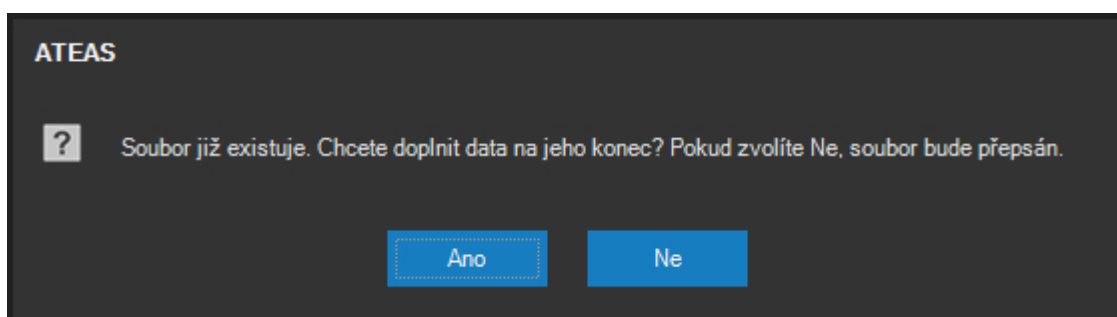
V průběhu editace podmínek v textových polích dialogu jsou výrazy průběžně analyzovány a je automaticky aktivován přepínač pro právě aktivní způsob vyhledávání. Po stisku tlačítka **POUŽÍT** je výraz přepsán do vyhledávacího pole a spuštěno vyhledávání. Symbolem křížku ve vyhledávacím textovém poli lze provést jeho reset.

POZNÁMKA

Sloupcová notace používá znak dvojtečky. Pokud bychom chtěli tento znak vyhledat v datové položce, pak musíme zvolit únikovou sekvenci \: potlačující speciální význam dvojtečky.

5.2.4. Exportní funkce

Tlačítkem **EXPORT** je možné provést uložení metadat do textového souboru. Jako výstupní soubor lze vybrat libovolný nový i již existující soubor s koncovkou txt. Pokud vybraný soubor již existuje, aplikace zobrazí následující zprávu:



V tomto případě je tedy možné soubor buď přepsat nebo doplnit výpis na konec existujícího souboru.

Použitý textový výstupní formát je CSV (comma-separated values), což je jednoduchý formát pro export a možný import do libovolných databázových formátů, ve kterém je na každé řádce jeden záznam a jednotlivé položky jsou odděleny čárkou.

Tímto způsobem tak lze exportovat data pro celé dny či měsíce a pro libovolný počet kamer najednou.

5.2.5. Grafy

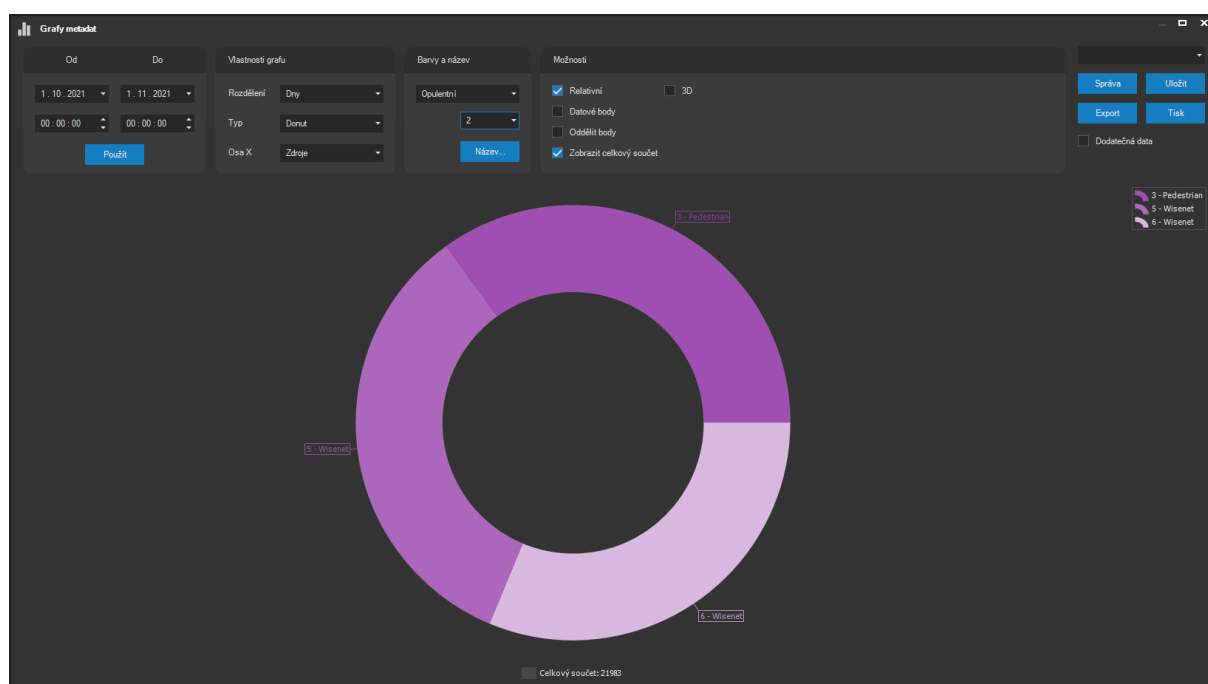
Aktuální výběr metadat dle nastaveného filtru může být vyjádřen také v podobě grafu. Graf je statistickou vizuální reprezentací metadatového výběru a slouží jako nejlepší možný nástroj pro prezentaci dat v systému v podobě výstižných reportů.

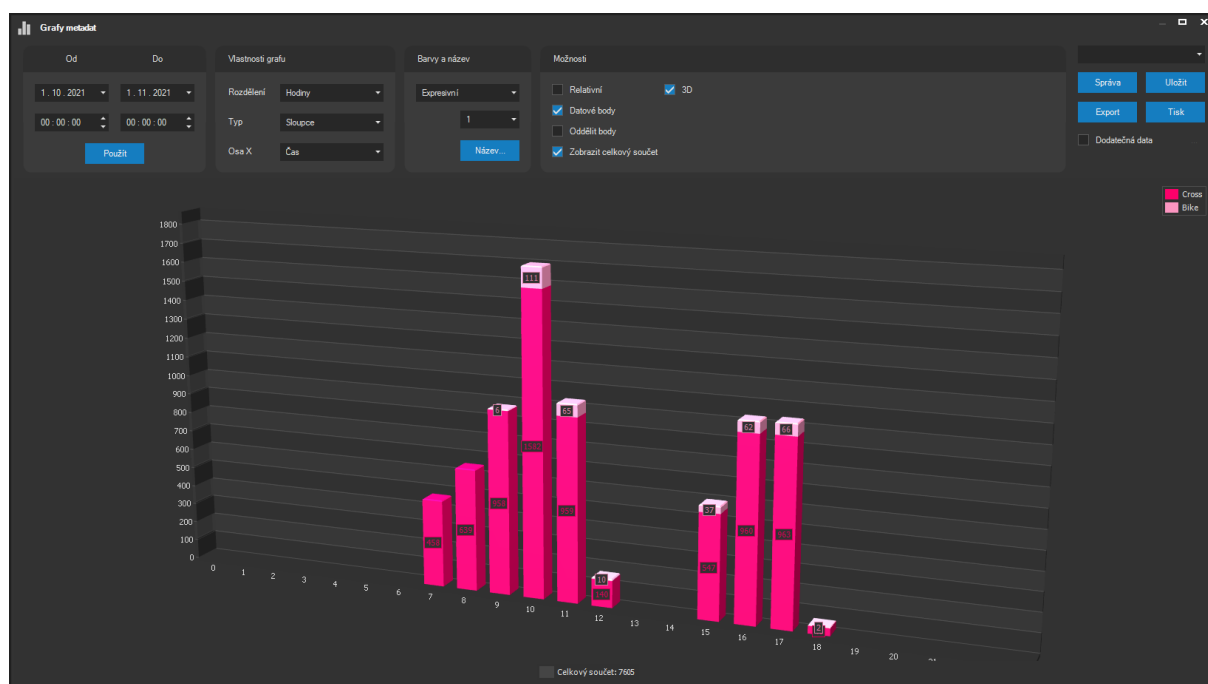
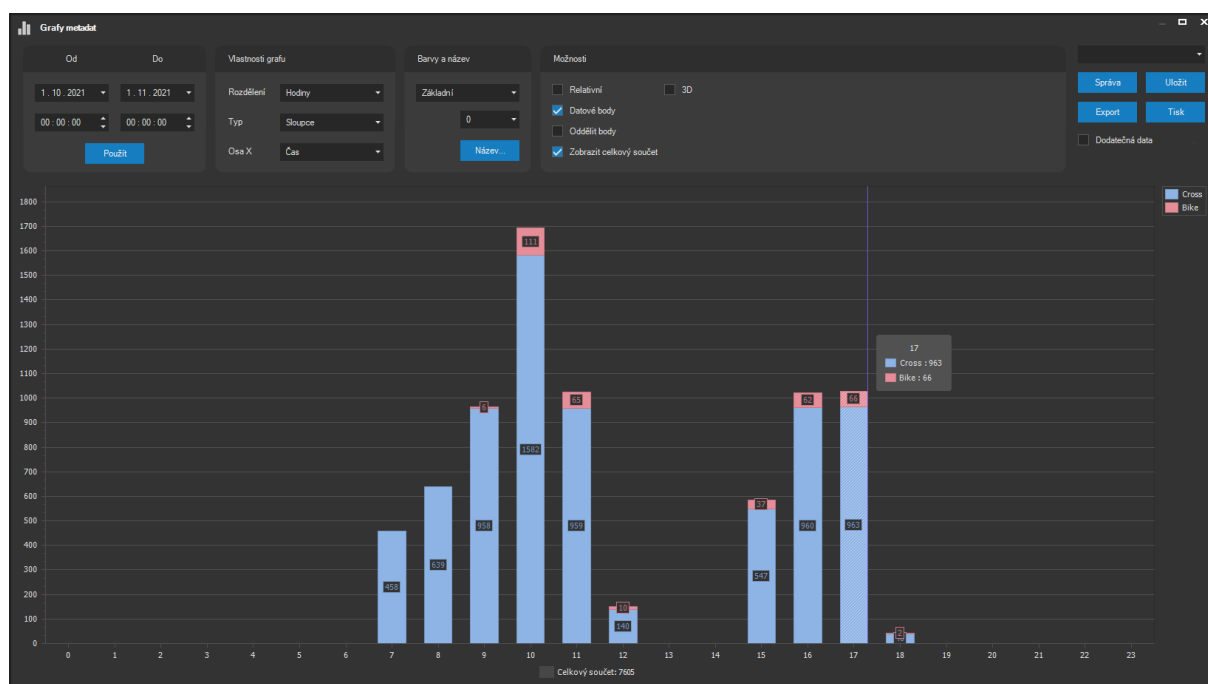
Grafy aktivujeme pomocí tlačítka se symbolem grafu v pravém horním rohu okna.

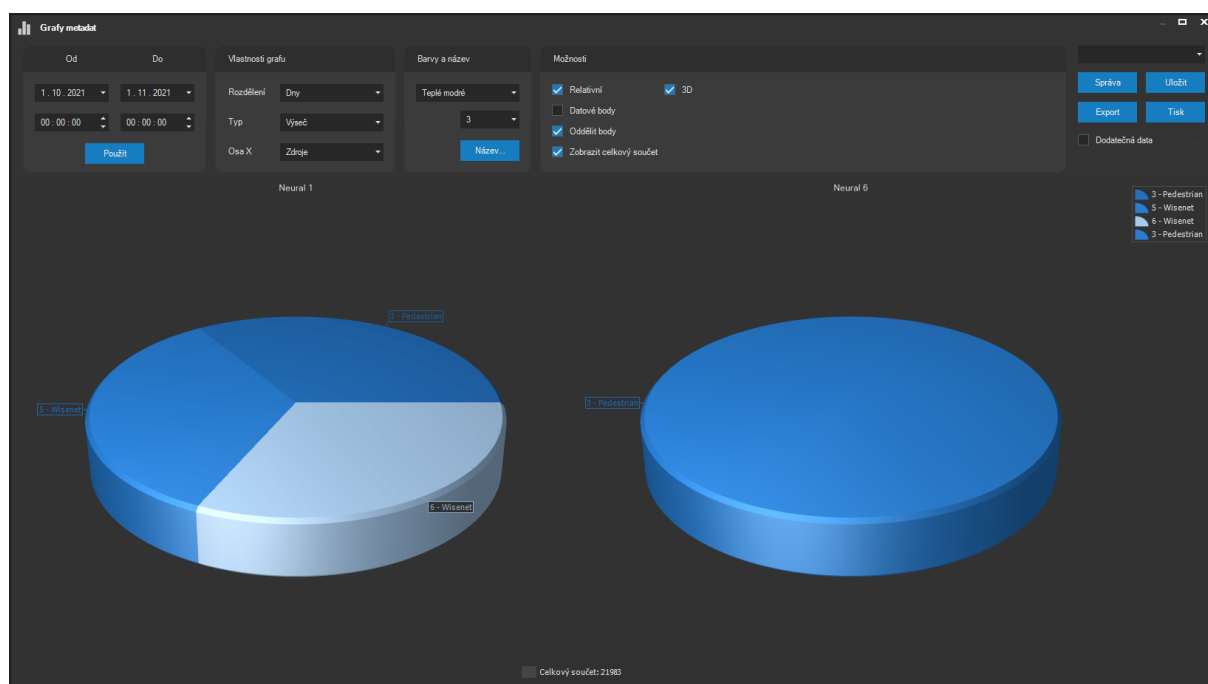
POZNÁMKA

Stejně jako v případě exportu musí být nejdříve vybrán alespoň měsíční časový interval.

Pomocí sloupcových, výsečových a dalších grafů tak můžete analyzovat všechny druhy metadat od četnosti RZ vozidel v průběhu měsíce v jednotlivých hodinách, výpadků kamer, počítání a statistiky osob či vozidel dle událostí z neuronové sítě a mnoho dalších. Zde uvádíme některé ukázky grafů.







Význam položek pro volbu typu a nastavení grafu je následující.

V nastavení Od Do lze zvolit dny a přesné časy, ze kterých bude vytvořen graf. Maximální délka intervalu pro graf je 90 dní, rozsah lze v okně grafů upravovat nezávisle na původně vybraném intervalu ve vyhledávání metadat.

Položka Rozdělení určuje, zdali bude vytvořen graf denní anebo hodinový.

POZNÁMKA

Rozdělení má smysl pouze pro sloupcové grafy.

Pokud byl před otevřením okna grafu vybrán delší než denní interval, bude automaticky použit denní graf, v opačném případě graf hodinový.

POZNÁMKA

Hodinový graf má však zásadní význam i pro delší než denní období, může např. ukázat měsíční statistiku průjezdů vozidel podle hodin.

V nastavení Typ grafu je možné volit mezi sloupcovým anebo výsečovým typem grafu s případnými dalšími modifikacemi těchto základních typů. Označením volby Zobrazit celkový součet lze ve spodní části grafu zobrazit celkový součet přes všechny datové body.

V nastavení Osa X lze zvolit, jakým způsobem budou data prezentována. U sloupcového grafu je vždy základním rozdělením čas. Poté však můžeme volit (pro jednotlivé časové body sloupcového grafu anebo pro jednotlivé výseče), zdali mají být rozděleny podle kamer a poté podle typu metadat anebo nejprve podle typu metadat a až poté podle kamer. V obou případech vždy získáme jiný náhled na metadata v systému.

V části Barevné schéma lze vybrat z mnoha předdefinovaných barevných schémat grafu a dále také jeho podtyp. Celkem tedy lze vytvořit přibližně 100 různých barevných prezentací grafu.

Volba Relativní má tento účinek:

- u sloupcových grafů přepne graf do relativního zobrazení (vyrovná výšky sloupců a zobrazí procenta),
- u výsečového grafu, který již je relativním vyjádřením dat, provádí přepínání zobrazení absolutních a relativních hodnot datových bodů.

Volba Datové body ukáže číselné hodnoty datových bodů přímo v grafu.

Volba Oddělit body provede oddělení datových bodů v rámci jednoho sloupce anebo výseče do podbodů (dle nastavení osy x). Budou tedy vytvořeny samostatné podbody kamer anebo metadat.

POZNÁMKA

Pokud byla vybrána pouze jedna kamera, bude se oddělení datových bodů vztahovat na jednotlivé událostní zdroje, což je typ zobrazení, který by u více kamer ve výběru nebyl možný.

Volba 3D aktivuje trojrozměrné zobrazení grafu beze změny barevného schématu.

Název grafu

Pomocí tlačítka **NÁZEV** je možné vytvořit vlastní název pro graf, který bude zobrazen nad ním. Zadáání názvu grafu podporuje základní HTML formátování jako je tučné či podtržené písmo (, <u>) anebo změna barvy (<color=red>).

Ovládání grafu

Jakýkoliv 3D graf anebo 2D sloupcový graf lze přiblížit či oddálit kolečkem myši.

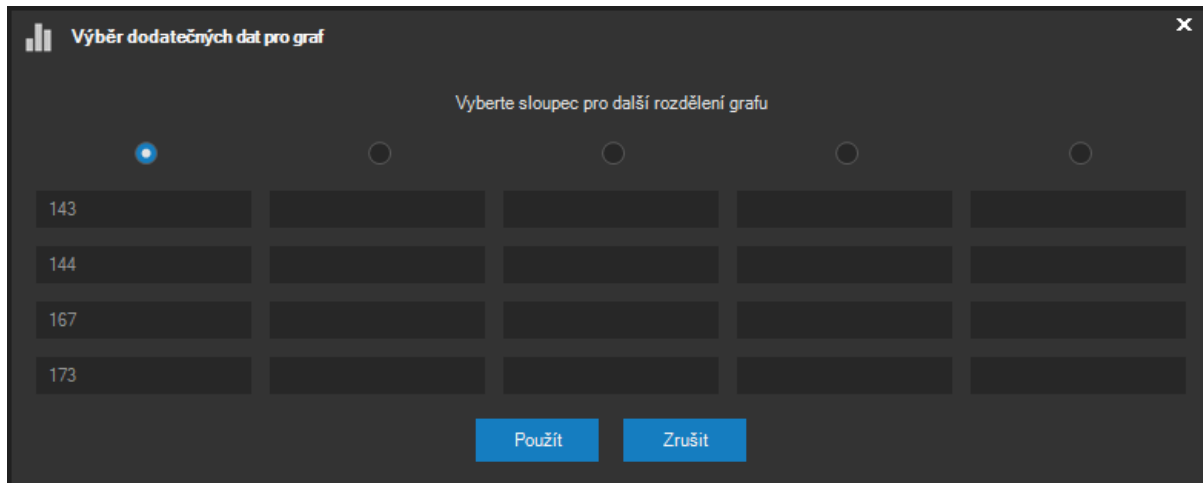
Při přiblížení 2D grafu je možné ho posouvat pomocí posuvníků anebo přetažením myši.

Při přiblížení 3D grafu je možné ho posouvat pomocí přetažení myši při současně stisknutém kolečku myši. Běžným přetažením pomocí myši je možné měnit natočení 3D grafu.

Další rozdělení grafu dle datových položek

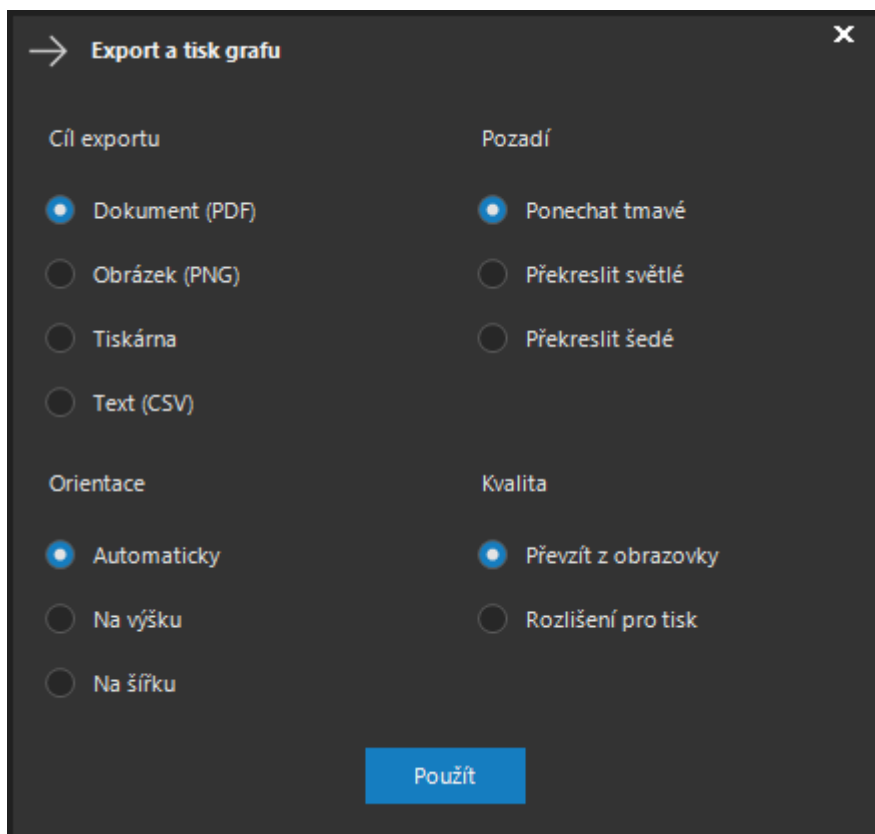
Obvykle jsou grafy vytvářeny přímo z metadatových zdrojů vybraných kamer. Pokud je však daný typ metadat doplněn o dodatečná data, je možné tato data použít k dalšímu zjemnění tvorby grafu. Např. je možné graficky analyzovat RZ vozidel dle státní příslušnosti anebo (pokud jsou data k dispozici) podle typu či modelu vozidla. Stejně tak je možné graficky oddělit jakákoliv data, která lze kategorizovat, tj. vyskytují se jako výčet hodnot (typy identifikačních karet, kategorie balíků apod.).

Pro aktivaci tohoto rozdělení je nutné aktivovat volbu Dodatečná data a v následujícím dialogu vybrat příslušný sloupec, podle kterého bude rozdělení vytvořeno.



Export grafu

Stisknutím tlačítka EXPORT je možné zahájit export zobrazeného grafu.



Graf je možné exportovat do dokumentu PDF, obrázku PNG anebo přímo na tiskárnu. Orientace může být zvolena na výšku anebo na šířku. Při ponechání automatické volby se orientace bude řídit aktuálním rozměrem grafu.

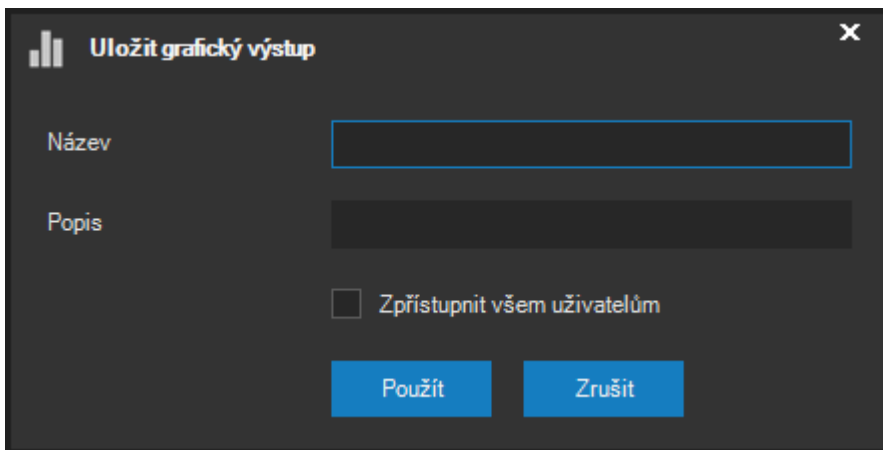
Jelikož grafy mají v aplikaci tmavé pozadí, je možné je při exportu překreslit na světlé či šedé pozadí. V části Kvalita je možné zvýšit rozlišení grafu pro tisk.

Data lze v agregované podobě exportovat také do textového souboru ve formátu CSV. Tento formát lze přímo importovat např. do programu Excel, kde z nich lze vytvořit obdobné typy grafů a případně je dále podrobněji upravovat.

Při použití tlačítka **TISK** se exportní dialog automaticky otevře s volbami vhodnými pro běžný tisk – cíl exportu bude nastaven na tiskárnu, aktivováno bude světlé překreslení a zvýšení rozlišení.

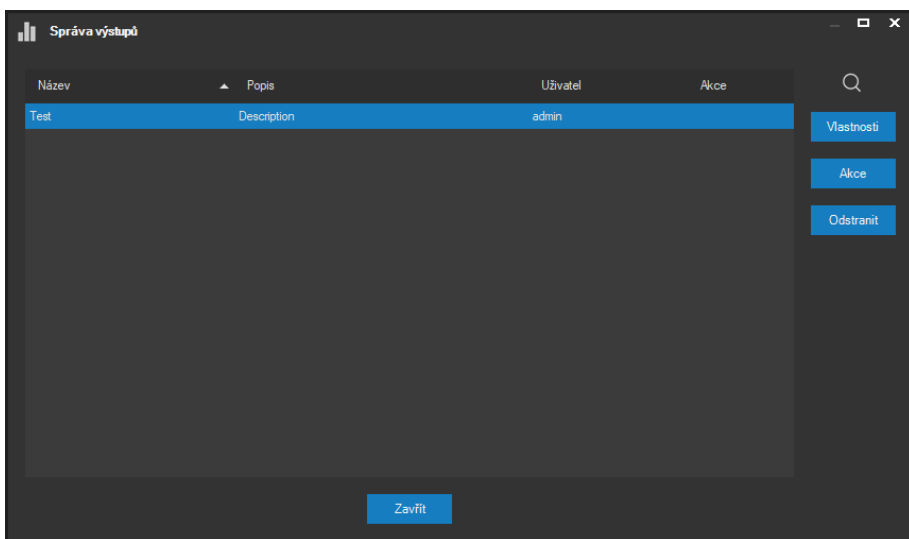
5.2.6. Automatický reporting

Libovolný graf se všemi nastaveními lze uložit pro pozdější použití pod vhodným názvem doplněným o základní popis. Uložení lze provést pomocí tlačítka **ULOŽIT**.



Administrátor může zaškrtnutím příslušné volby graf uložit tak, že ho uvidí všichni uživatelé. Běžní uživatelé tuto možnost nemají a vidí vždy pouze své grafy a ty, které vytvořil administrátor jako sdílené. Uložené grafické výstupy pak mohou být kdykoliv opět vyvolány jedním kliknutím – výběrem ze seznamu uložených výstupů v pravé horní části okna grafů.

Tlačítkem **SPRÁVA** lze otevřít okno se seznamem všech uživateli dostupných uložených grafů.



Master administrátor systému zde vidí také uložené výstupy ostatních uživatelů. V tomto okně je možné uložené výstupy také kdykoliv odstranit. V seznamu je kromě názvu a popisu uveden též uživatel, který graf vytvořil, a aktuální automatická akce, pokud je nastavena.

Administrátoři systému pak mají dále možnost použít tlačítka **VLASTNOSTI** a **AKCE** pro nastavení automatického generování grafů a jejich zasílání. Prvním z těchto tlačítek lze nastavit shodné parametry jako v případě výše popsaného exportu grafu, tj. formát, pozadí či orientaci na stránce. Druhé tlačítko pak otevírá dialog s možnostmi automatického vytváření a zasílání.

Vytvoření výstupu

Nastavení času

Kdy vytvořit: 26. 7. 2024 13:00:00

Opakování: Žádné

Počet: 1

Jak poslat:

Nastavení akce

Adresy komu: @

SMTP server:

Název souboru:

Vytvoření výstupu

Nastavení času

Kdy vytvořit: 26. 7. 2024 13:00:00

Opakování: Žádné

Počet: 1

Jak poslat:

Nastavení akce

FTP server:

Vzdálená složka:

Přihlášení:

Název souboru:

Zabezpečení: ☐ Použít TLS

Vytvoření výstupu

Nastavení času

Kdy vytvořit: 26. 7. 2024 13:00:00

Opakování: Žádné

Počet: 1

Jak poslat:

Nastavení akce

Cesta k souboru:

Název souboru:

V horní části okna je možné zadat přesný čas, kdy má být graf systémem vytvořen, a režim opakování. V případě nastaveného opakování dochází také k posunu časového úseku, ze kterého byla získána podkladová data.

POZNÁMKA

Tímto způsobem tak lze automaticky obdržet graf vždy z aktuálních dat.

Zasílání je možné buď zcela vypnout anebo nastavit na e-mail, ftp nebo soubor. Ve všech případech je vždy nutné vyplnit potřebné údaje pro vybraný komunikační kanál včetně možnosti komunikaci zabezpečit. Při odeslání pomocí e-mailu je možné zadat více příjemců oddělených čárkami či středníkem.

V případě uložení sestavy do souboru je možné použít lokální či síťovou cestu na administračním serveru. V případě použití síťové cesty však musí být služba administračního serveru přihlášena pod jiným uživatelským účtem.

Graf je vždy vytvořen přímo administračním serverem systému z dat, která jsou uložena buď přímo v jeho databázích (externí objekty, centralizovaná metadata kamerových serverů) anebo stažena z příslušných kamerových serverů při vytváření grafu. Pokud je nutné stáhnout data z kamerového severu, který je offline, systém se pokusí o stažení několikrát než je pokus o vytvoření grafu nakonec zastaven.

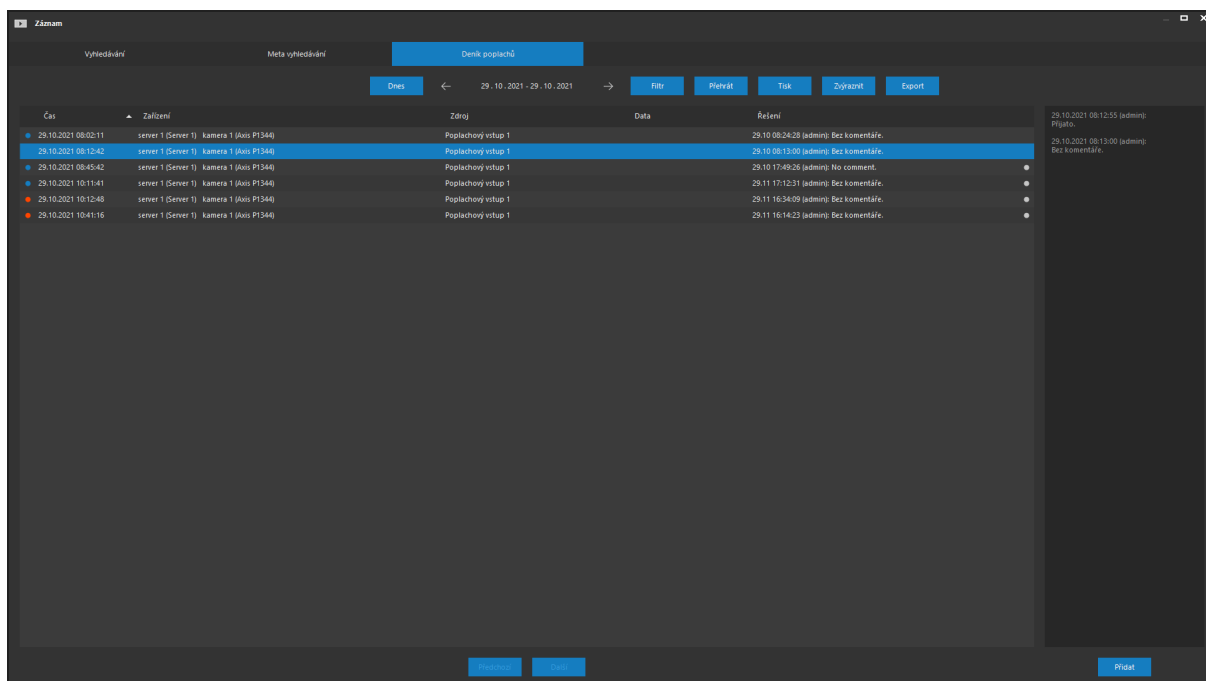
5.3. Deník poplachů

5.3.1. Prohlížení deníku poplachů

Do deníku poplachů jsou automaticky ukládány všechny poplasy, u kterých administrátor systému aktivoval režim řešení a to včetně událostí doručených v režimu funkce ATEAS Interlogin. Deník událostí lze zobrazit výběrem karty Deník poplachů v hlavním okně Záznam.

POZNÁMKA

Pro přístup k deníku poplachů je nutné, aby Vám administrátor systému přidělil příslušné oprávnění.



Čas	Zařízení	Zdroj	Data	Řešení
29.10.2021 08:02:11	server 1 (Server 1) kamera 1 (Ais P1344)	Poplachový vstup 1	29.10.08:24:28 (admin): Bez komentáře.	29.10.2021 08:12:55 (admin): Přijato.
29.10.2021 08:12:42	server 1 (Server 1) kamera 1 (Ais P1344)	Poplachový vstup 1	29.10.08:13:00 (admin): Bez komentáře.	29.10.2021 08:13:00 (admin): Bez komentáře.
29.10.2021 08:45:42	server 1 (Server 1) kamera 1 (Ais P1344)	Poplachový vstup 1	29.10.17:49:26 (admin): No comment.	
29.10.2021 10:11:41	server 1 (Server 1) kamera 1 (Ais P1344)	Poplachový vstup 1	29.11.17:12:31 (admin): Bez komentáře.	
29.10.2021 10:12:48	server 1 (Server 1) kamera 1 (Ais P1344)	Poplachový vstup 1	29.11.16:34:09 (admin): Bez komentáře.	
29.10.2021 10:41:16	server 1 (Server 1) kamera 1 (Ais P1344)	Poplachový vstup 1	29.11.16:14:23 (admin): Bez komentáře.	

Po vstupu do deníku poplachů se automaticky zobrazí všechny poplachy s aktivovaným režimem řešení (vyřešené i nevyřešené) pro aktuální den. K dnešnímu dni se lze kdykoliv jednoduše vrátit tlačítkem **DNES**. Pokud není zvolen jiný časový interval, posouvají směrové šipky deník poplachů vždy o jeden den.

Po stisknutí tlačítka **FILTR** se zobrazí dodatečné možnosti pro vyhledání poplachů. Tlačítkem **DNY** lze zobrazit kalendář a vybrat libovolný časový úsek pro zobrazení poplachů. Pokud je nalezených poplachů příliš mnoho, je možné seznamem listovat pomocí tlačítek vpravo dole pod seznamem. Po nastavení intervalu na určitý počet dní pak šipky nad seznamem provádějí posun o nový počet dní, nikoliv pouze o výchozí hodnotu jednoho dne. Lze tak snadno přejít na další týden či měsíc.

Vyhledávání je také možné omezit zadáním textu do polí nad jednotlivými sloupci. Vyhledávání bude automaticky aktualizováno s tím, jak zadáváte hodnotu do textového pole. Pro více zadaných slov platí, že jsou vyhledány všechny výskyty, nikoliv jejich přesná fráze. Ve vyhledávání je také možné použít zástupné znaky * a ? pro libovolnou část slova resp. libovolný jeden znak.

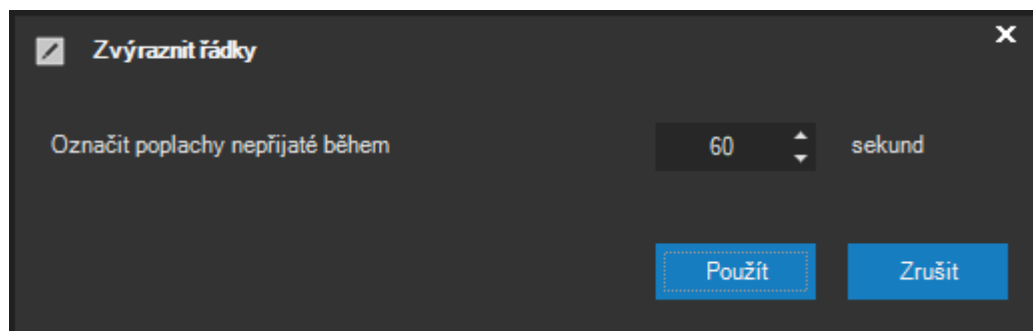
POZNÁMKA

Stejně jako jinde v systému lze i v tomto seznamu dále lokálně vyhledávat i pomocí zkratky CTRL-F.

Opětovným stiskem tlačítka **FILTR** se seznam obnoví do stavu se všemi poplachu pro zadaný časový interval.

V seznamu poplachů jsou zobrazeny informace o aktuálním stavu poplachu, zařízení, které poplach vyvolalo, zdroj události, dodatečná data a poslední komentář k řešení tohoto poplachu. Neuzavřené poplachu jsou vyznačeny červenou výstražnou ikonou, uzavřené poplachu mají tuto ikonu zbarvenou modře.

Poplachu, které nebyly přijaty operátorem během nastaveného limitu, jsou automaticky v seznamu označeny. Tento limit lze změnit pomocí tlačítka **ZVÝRAZNIT**, nově nastavený limit bude ihned aplikován na seznam poplachů. Označeny jsou poplachu nepřijaté žádným z operátorů, přičemž není rozhodující, kdy byly vyřešeny a uzavřeny, což může být ovlivněno povahou poplachu.



Libovolný poplach v seznamu lze přehrát dvojitým kliknutím na řádek poplachu anebo stiskem tlačítka **PŘEHRÁT**.

POZNÁMKA

Přehrání poplachu otevře událostní pohled pro tento poplach. To znamená, že může být automaticky přehrán pohled z více kamer současně, pokud administrátor systému v nastavení událostního scénáře aktivoval volbu Zařadit do pohledu pro více než jednu kameru.

Po výběru libovolného poplachu v seznamu se v pravé části okna zobrazí kompletní postup řešení daného poplachu. První záznam vždy odpovídá uzavření poplachu z dohledového okna, další komentáře mohou již být vkládány přímo v deníku poplachů pomocí tlačítka **PŘIDAT**. U každého komentáře jsou samozřejmě zobrazeny údaje o přesném čase vložení, uživatelské jméno a text komentáře.

29.10.2021 17:49:26 (admin):
No comment.

5.3.2. Export a tisk deníku

Deník poplachů lze vytisknout na libovolné tiskárně (včetně např. PDF tiskárny) stiskem tlačítka **TISK**. Deník je vytisknut přesně v podobě a se všemi údaji tak, jak ho vidíte na obrazovce počítače v seznamu poplachů.

Tisk
Zavřít



Deník poplachů: 29.10.2021 - 29.10.2021

29.10.2021 08:02:11	1 - Server 1	1 - Axis P1344	Poplachový vstup 1	29.10.08:24:28 (admin): Bez komentáře.
29.10.2021 08:12:42	1 - Server 1	1 - Axis P1344	Poplachový vstup 1	29.10.08:13:00 (admin): Bez komentáře.
29.10.2021 08:45:42	1 - Server 1	1 - Axis P1344	Poplachový vstup 1	29.10.17:49:26 (admin): No comment.
29.10.2021 10:11:41	1 - Server 1	1 - Axis P1344	Poplachový vstup 1	
29.10.2021 10:12:48	1 - Server 1	1 - Axis P1344	Poplachový vstup 1	
29.10.2021 10:41:16	1 - Server 1	1 - Axis P1344	Poplachový vstup 1	

1 Printed: 30.10.2021 10:49
Printed by: admin

Pro potřeby automatizovaného či dávkového zpracování či jako podklad pro výrobu vlastních uživatelských tiskových sestav, statistik či přehledů lze využít exportní funkce do formátu XML. Tlačítko pro export do XML se nachází hned vedle tlačítka **TISK**.

POZNÁMKA

Součástí výsledného XML dokumentu je též kompletní postup řešení každého poplachu včetně všech komentářů.

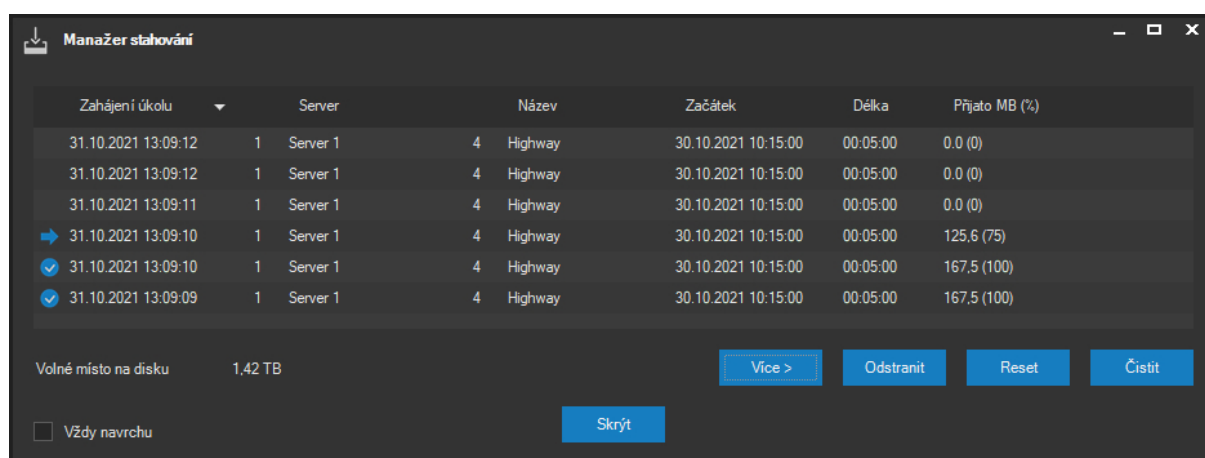
POZNÁMKA

Pokud je na seznam poplachů aplikován filtr pomocí zadání nějakého vyhledávacího výrazu, vztahují se funkce tisku a exportu pouze na zobrazené (filtrované) záznamy.

Kapitola 6 - Práce s manažerem stahování

6.1. Základní popis

Manažer stahování je inteligentní nástroj pro stahování ze záznamových oblastí jednotlivých kamerových serverů, který eviduje a postupně či paralelně vyřizuje všechny uživatelem vytvořené úkoly. Okno manažera stahování lze otevřít z hlavní nabídky aplikace ze skupiny Nástroje nebo automaticky také vytvořením nového úkolu v dohledovém okně či okně záznamu.



Zahájení úkolu	Server	Název	Začátek	Délka	Přijato MB (%)
31.10.2021 13:09:12	1 Server 1	4 Highway	30.10.2021 10:15:00	00:05:00	0.0 (0)
31.10.2021 13:09:12	1 Server 1	4 Highway	30.10.2021 10:15:00	00:05:00	0.0 (0)
31.10.2021 13:09:11	1 Server 1	4 Highway	30.10.2021 10:15:00	00:05:00	0.0 (0)
→ 31.10.2021 13:09:10	1 Server 1	4 Highway	30.10.2021 10:15:00	00:05:00	125,6 (75)
✓ 31.10.2021 13:09:10	1 Server 1	4 Highway	30.10.2021 10:15:00	00:05:00	167,5 (100)
✓ 31.10.2021 13:09:09	1 Server 1	4 Highway	30.10.2021 10:15:00	00:05:00	167,5 (100)

Volné místo na disku: 1.42 TB

☐ Vždy navrchu

Více > Odstranit Reset Čistit

Skrýt

POZOR

Zavřením okna manažera stahování nedojde k přerušení či pozastavení úkolů. Manažer v takovém případě běží na pozadí aplikace a nadále postupně vyřizuje jednotlivé úkoly.

Veškerá stahování jsou prováděna do kontejnerů ve formátu ATS, který umožňuje maximální zabezpečení pomocí přístupového hesla, ochranu digitálním podpisem a podporuje všechny další podstatné funkce jako je dynamická změna rozlišení videa či snímkové frekvence. Samozřejmostí je podpora všech hlavních video a audio kodeků.

Na rozdíl od běžného stahování dat ze záznamových oblastí je manažer stahování vybaven mnoha inteligentními funkcemi, které pomáhají uživatelům se stahováním dat:

- Automatické varování při nedostatku volného místa na disku.
- Automatické přerušení stahování před vyčerpáním veškerého volného místa na disku a jeho znovu obnovení při uvolnění místa.

- Možnost vytvořit neomezené množství úkolů stahování, které budou postupně vyřizovány.
- Náhled stavu jednotlivých úkolů a automatický postupný restart úkolů, které nebyly úspěšně vyřízeny.
- Současné stahování dat z různých kamerových serverů.
- Možnost automatického a ručního vytváření úkolů.
- Při ručním vytváření možnost odloženého startu úkolu (např. v noci při nižší zátěži sítě apod.).

6.2. Správa úkolů

6.2.1. Automatické přidávání úkolů

Pro jednotlivé úkoly jsou v seznamu manažera stahování evidovány a zobrazeny všechny podstatné položky jako je datum a čas zahájení úkolu, číslo a název serveru, číslo a název kamery, začátek stahované sekvence, délka stahované sekvence a množství stažených dat v jednotkách MB a také v procentuelním vyjádření ve vztahu k celkové délce intervalu pro stažení.

Nejnovější úkoly jsou vždy zobrazeny v úvodu seznamu, nicméně řazení úkolů lze libovolně měnit pomocí kliknutí na záhlaví jednotlivých sloupců (opětovné kliknutí na záhlaví mění způsob třídění mezi sestupným a vzestupným).

U každého úkolu je zobrazen jeho aktuální stav. Mezi základní stavy patří následující: úkol čeká na spuštění (není zobrazena žádná ikona), úkol je právě vyřizován (je zobrazena ikona modré šipky) a úkol byl úspěšně vyřízen (je zobrazena zelená ikona potvrzení).

POZNÁMKA

Úkoly lze samozřejmě třídit či seskupit také pomocí záhlaví prvního sloupce, tedy podle jejich stavu.

POZNÁMKA

Úkoly, které nejsou úspěšně vyřízeny, není nutné znovu vytvářet, neboť budou manažerem stahování restartovány po nějaké době automaticky.

Do seznamu úkolů lze automaticky přidat nový úkol, pokud na dohledovém okně či v okně záznamu označíme či vybereme příslušnou kameru a sekvenci pro stažení dat. Tyto postupy jsou popsány

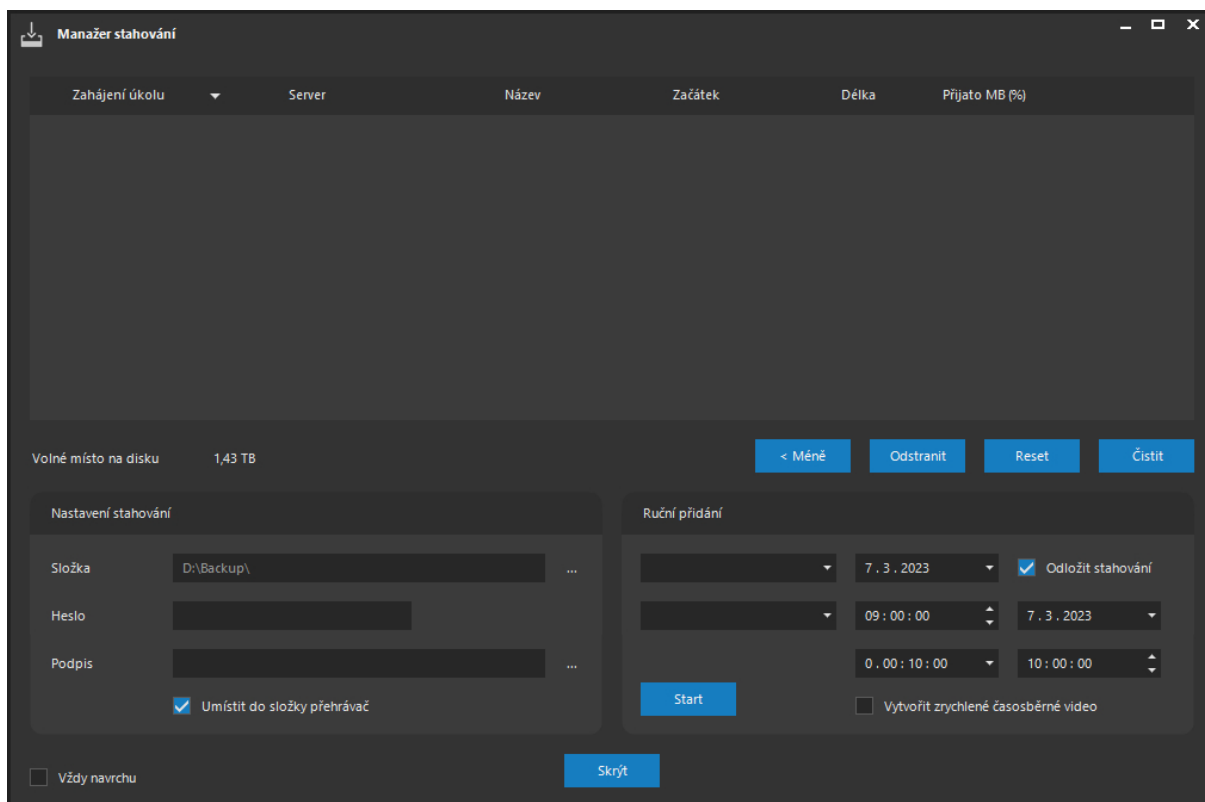
v kapitolách o ovládání jednotlivých částí aplikace. Pro přidání úkolu bude datum a čas jeho zahájení nastaveno automaticky na právě aktuální datum a čas nebo na přednastavenou hodnotu v části rozšířených nastavení.

POZNÁMKA

To však ještě nemusí znamenat, že úkol bude zahájen ihned za každých okolností. Pokud je stále vyřizován (na stejném serveru) jiný úkol, zahájení tohoto úkolu bude odloženo až na dobu po ukončení právě zpracovávaného úkolu.

6.2.2. Ruční přidávání úkolů

Kromě automatizovaných možností přidávání úkolů do manažera stahování existuje také možnost ručního vytvoření nového úkolu. Pro tuto možnost je nutné zobrazit rozšířené nastavení a dodatečné ovládací prvky manažera stahování pomocí tlačítka **VÍCE**. Zpětné přepnutí lze pak samozřejmě provést kdykoliv pomocí tlačítka **MÉNĚ**.



The screenshot shows the 'Manažer stahování' (Download Manager) application window. The main area displays a table with columns: 'Zahájení úkolu' (Task start), 'Server', 'Název' (Name), 'Začátek' (Start), 'Délka' (Length), and 'Přijato MB (%)' (Received MB (%)). Below the table, it shows 'Volné místo na disku' (Free space on disk) as 1,43 TB. On the right, there are buttons: '< Méně' (Less), 'Odstranit' (Remove), 'Reset', and 'Čistit' (Clean).

The 'Nastavení stahování' (Download settings) panel on the left includes:

- Složka** (Folder): D:\Backup\
- Heslo** (Password): [Redacted]
- Podpis** (Signature): [Redacted]
- ☒ **Umístit do složky přehrávač** (Place in playback folder)

The 'Ruční přidání' (Manual addition) panel on the right includes:

- Server**: [Dropdown menu]
- Start**: 7. 3. 2023
- End**: 09 : 00 : 00
- Interval**: 0. 00 : 10 : 00
- ☒ **Odložit stahování** (Delay download)
- ☐ **Vytvořit zrychlené časosběrné video** (Create accelerated time-lapse video)
- Start** button

At the bottom left, there is a checkbox ☐ **Vždy navrchu** (Always on top) and a **Skrýt** (Hide) button.

V části Ruční lze provést ruční definici a přidání nového úkolu do seznamu. Při ručním přidání je nutné vybrat server a kameru (případně všechny), datum a čas záznamu a délku intervalu pro stažení. Pomocí volby Odložit stahování je možné úkol naplánovat na pozdější dobu.

POZNÁMKA

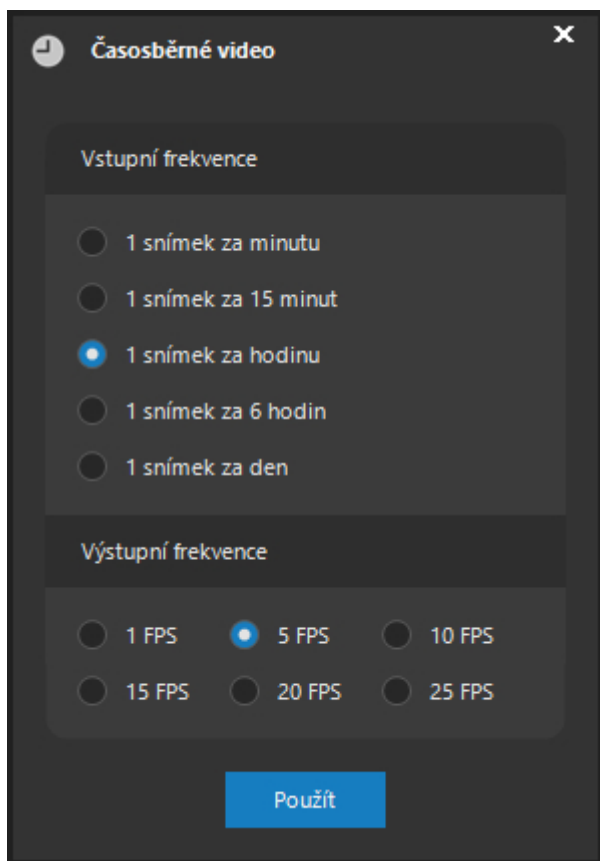
Odloženým startem zahájení úkolu lze naplánovat stažení většího množství dat a delších intervalů např. na noční hodiny, kdy bude provoz na síti nižší.

Je-li interval pro stažení delší než 30 minut, bude provedeno automatické rozdělení intervalu pro snazší manipulaci se staženými daty.

6.2.3. Časosběrná videa

Je-li v manažeru stahování zobrazeno rozšířené nastavení pomocí tlačítka **VÍCE**, je k dispozici také volba Vytvořit zrychlené časosběrné video. Pomocí této volby je možné při stahování videa provést náležité úpravy v časování jednotlivých snímků tak, aby výsledkem bylo zrychlené časosběrné video. Časosběrné video typicky zobrazuje delší časový úsek (týdny, měsíce či roky) ve zrychleném režimu v řádu několika minut či desítek vteřin. Výsledkem je efektní zobrazení pomalu plynoucích jevů (např. stavby apod.).

Pro vytvoření časosběrného videa postačí zaškrtnout příslušnou volbu v okně manažera stahování. Pro optimální výsledek je možné upravit vstupní a výstupní snímkovou frekvenci.



V části Vstupní frekvence lze určit frekvenci snímků, které budou načteny z databáze snímků pro vytvoření zrychleného videa. V části Výstupní frekvence lze určit frekvenci snímků po stažení, která je nepřímou úměrnou výsledné době trvání video souboru.

POZNÁMKA

Zrychlené časoběrné video nikdy nebude obsahovat zvukovou stopu, i když je v záznamu na serveru k dispozici.

POZNÁMKA

Pokud je zvolený typ úložiště, ze kterého bude provedeno stažení, nastaven na hodnotu Kamera, nelze zrychlené časoběrné video vytvořit. Aplikace bude v takovém případě reagovat varovnou zprávou.

POZNÁMKA

Pokud provádíte záznam kamery pouze pro účely vytvoření časosběrného videa, můžete použít minimální snímkovou frekvenci pro záznam, což je jeden snímek za minutu. Pokud by i tato frekvence byla ve Vašem případě zbytečně vysoká, lze záznam provádět pomocí časové události s nastavenou periodou ještě s výrazně nižší frekvencí.

POZNÁMKA

Možnost generování časosběrných videí je dostupná až od edice ATEAS Security PROFESSIONAL.

6.2.4. Ovládání seznamu úkolů

Pod seznamem úkolů jsou k dispozici tlačítka pro ovládání vybraných úkolů či celého seznamu. Níže uvádíme jejich stručný význam.

Tlačítko **ODSTRANIT**: Pomocí tohoto tlačítka lze ze seznamu odstranit vybraný úkol. Pokud se nejedná o úspěšně dokončený úkol, tento úkol bude ihned předčasně přerušen (a nebude již restartován). Neúplně stažená sekvence nebude dostupná v seznamu stažených sekvencí a její data budou odstraněna z lokálního počítače.

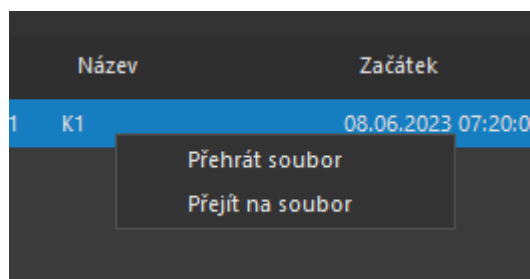
POZNÁMKA

V seznamu úkolů je možné vybrat libovolný počet položek pomocí standardních metod systému Windows (pomocí myši, pomocí kláves CTRL anebo SHIFT, klávesovou zkratkou CTRL-A). Lze tedy provést odstranění více položek najednou.

Tlačítko **RESET**: Pomocí tohoto tlačítka lze provést kompletní reset a odstranění všech úkolů ze seznamu. Funkce tlačítka je stejná jako funkce tlačítka **ODSTRANIT**, je ovšem použito na všechny úkoly v seznamu. Před provedením resetu bude nutné potvrdit zprávu.

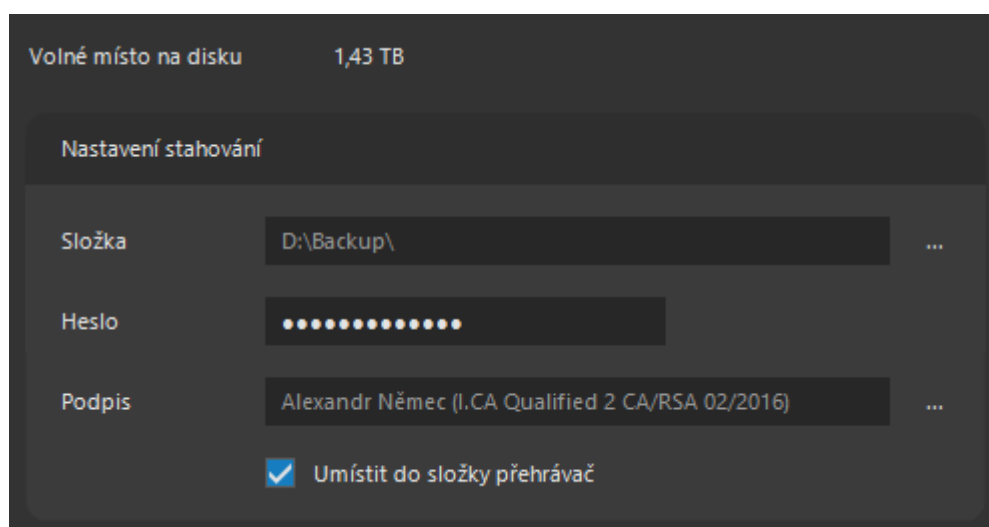
Tlačítko **ČISTIT**: Pomocí tohoto tlačítka lze provést vyčištění seznamu úkolů. To znamená, že ze seznamu budou odebrány všechny úspěšně ukončené úkoly a budou ponechány všechny právě probíhající úkoly a úkoly ukončené s chybou, čekající na restart.

U každého stahování je možné pomocí kontextové nabídky provést rychlé přehrání staženého souboru anebo rychlý přechod do složky se souborem.



6.3. Nastavení stahování

V části Nastavení stahování v rozšířené části manažera je možné určit cílovou složku pro stažený záznam ve formátu ATS, heslo pro automatickou ochranu stažených dat a digitální podpis, který bude automaticky po stažení aplikován.



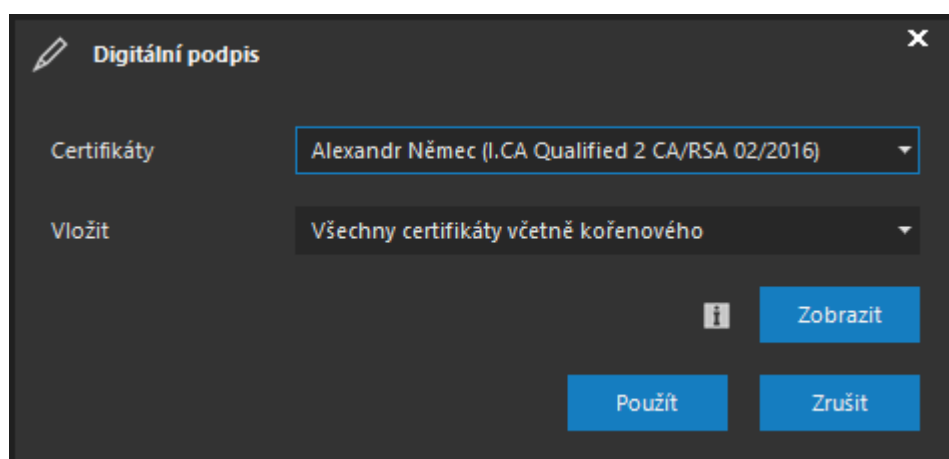
V cílové složce pro stažení záznamu bude podobně jako v případě záloh dat kamerovým serverem automaticky vytvořena přehledná struktura serverů (případně pohledů), kamer a jednotlivých dnů. Soubory nesou označení času.

Možnost zápisu hesla nemusí být dostupná, pokud administrátor systému ochránil všechna stahovaná data heslem na ochranu stahování a pokud zároveň nemáte přiděleno oprávnění pro export dat mimo systém.

POZNÁMKA

Možnost šifrování ATS souborů je dostupná až od edice ATEAS Security PROFESSIONAL.

Pokud chceme stažená data automaticky digitálně podepsat, vybereme příslušný podpis z dialogu všech certifikátů podpisu.



Do určené složky je také možné automaticky přidat samostatný přehrávač ATEAS souborů, který lze na cílovém počítači spustit bez instalace klienta ATEAS. Pokud zaškrtnete příslušnou volbu, bude přehrávač exportován přímo do cílové složky.

POZOR

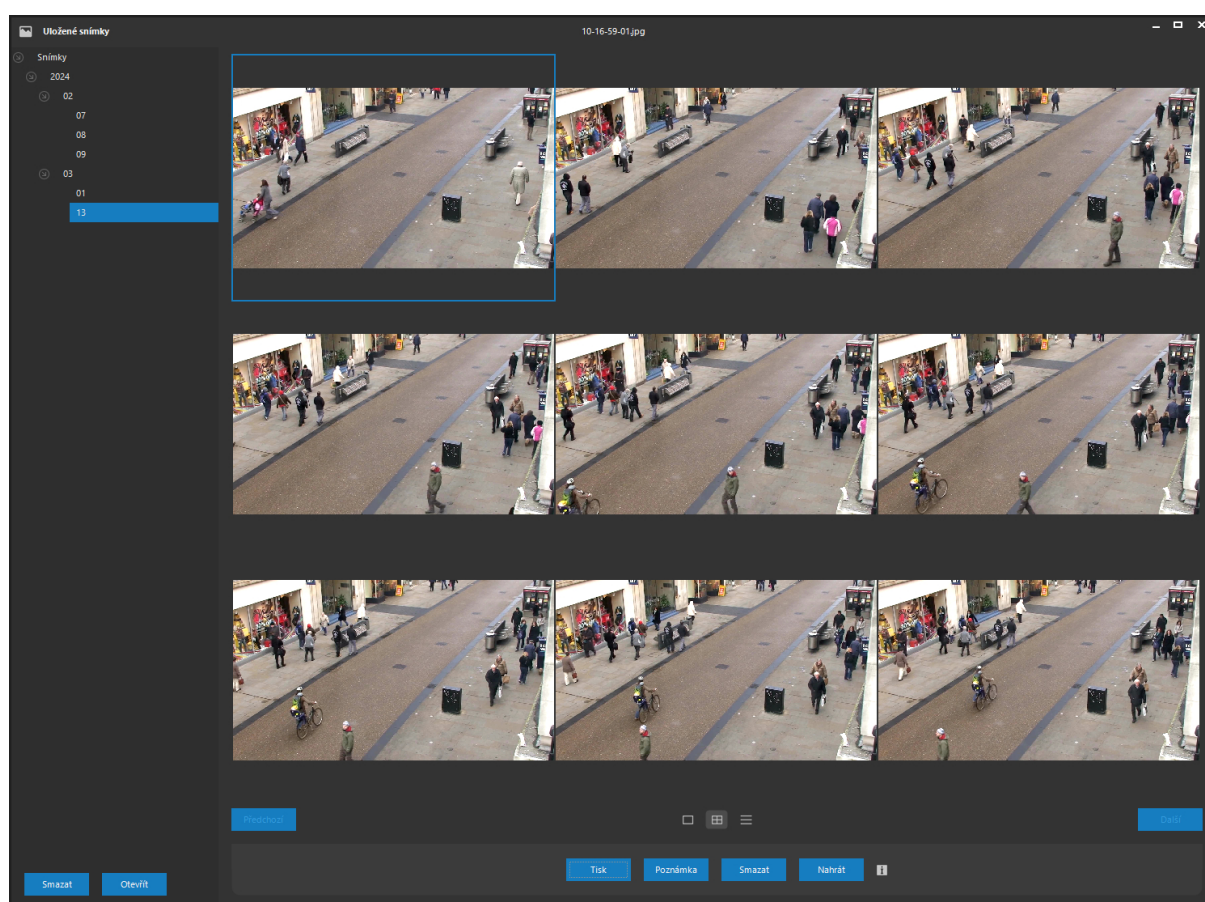
Aby bylo možné exportovat přehrávač spolu s daty, Váš klient si nejprve přehrávač stáhne z administračního serveru ATEAS. Jakmile ho má stažený, nové stahování již není při opakovaných exportech potřeba. Pro první stažení je však nutné, aby Váš administrační server měl dostupný svůj http port.

Kapitola 7 - Práce se snímky

7.1. Správa snímků

7.1.1. Přehled snímků

Po uložení snímku z vybrané kamery u živého nebo zaznamenaného videa dojde k otevření samostatného okna pro správu snímků a zobrazení snímků v náhledu.

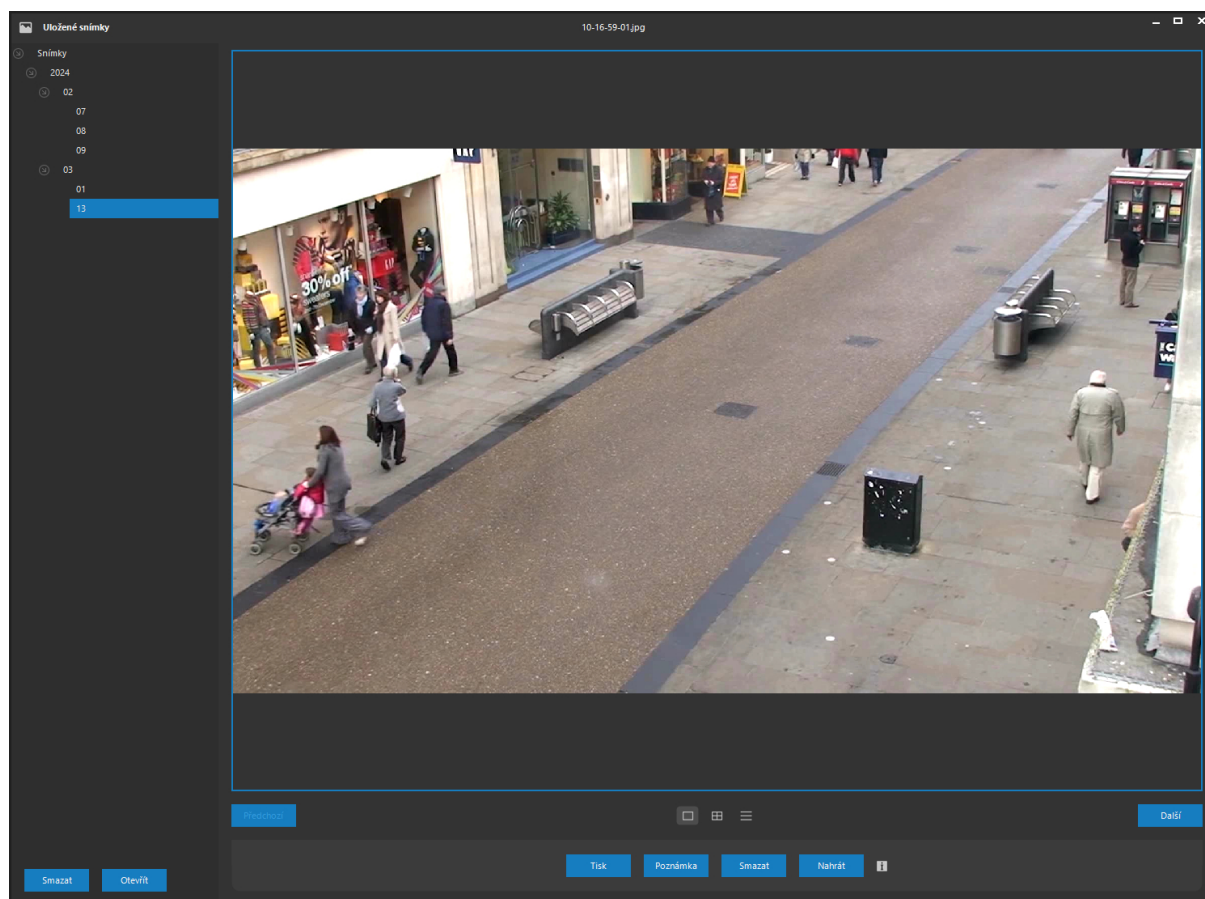


Jednotlivé snímky ve vybraném dni lze zobrazit v různých velikostech, režim zobrazení lze vybrat ze skupiny třech tlačítek ve spodní části okna. Pokud v daném režimu zobrazení překročí počet snímků hodnotu umožňující pohodlné prohlížení, budou automaticky doplněna tlačítka Předchozí a Další pro plynulé přecházení mezi více stránkami.



Jednotlivé snímky jsou k dispozici ve formátu JPEG ve složce Shots v instalačním adresáři aplikace. Tam mohou být také prohlíženy libovolným externím prohlížečem. Metadata jsou k nim připojena v podobě JSON souborů se stejným názvem.

Dvojitým kliknutím lze vybraný snímek přepnout do detailního zobrazení.



POZNÁMKA

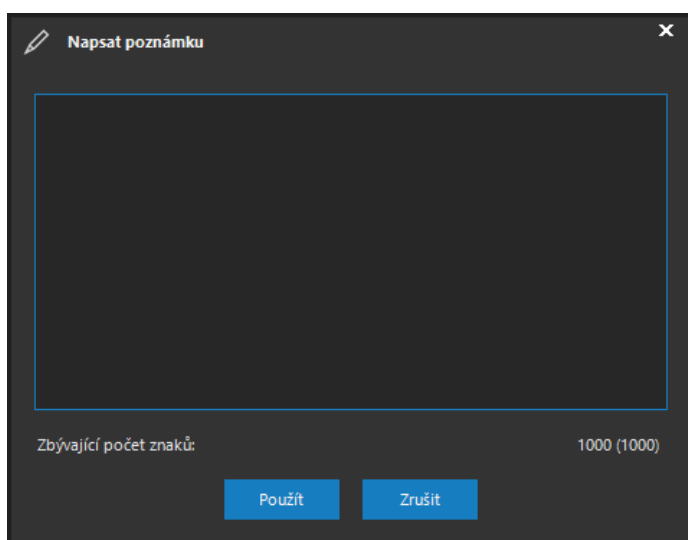
U vybraného snímku lze pro lepší náhled pomocí kolečka myši a klikáním do obrazu provádět operace digitálního přiblížení a posunu.

Zobrazení snímků je možné filtrovat podle času a to výběrem skupiny ze seznamu v levé části okna. Tento ovládací prvek automaticky vytváří časové složky ve stromové struktuře. Na první úrovni jsou roky, druhou úroveň tvoří měsíce, třetí úroveň je tvořena dny.

Libovolný snímek lze odstranit kliknutím na tlačítko **SMAZAT** ve spodní části okna. Pokud chcete smazat všechny snímky v dané časové složce (rok, měsíc či den), je možné po výběru složky použít tlačítko **SMAZAT** pod přehledem časových složek. Tlačítko **OTEVŘÍT** umožňuje rychlý přechod přímo do vybrané složky snímků.

7.1.2. Doplnění údajů

Ke každému snímku je možné uložit jeho bližší popis, který vystihuje např. jednání zachycené na snímku. Tento popis je poté automaticky též vytištěn spolu se snímkem. Popis je možné doplnit po stisku tlačítka **POZNÁMKA**.

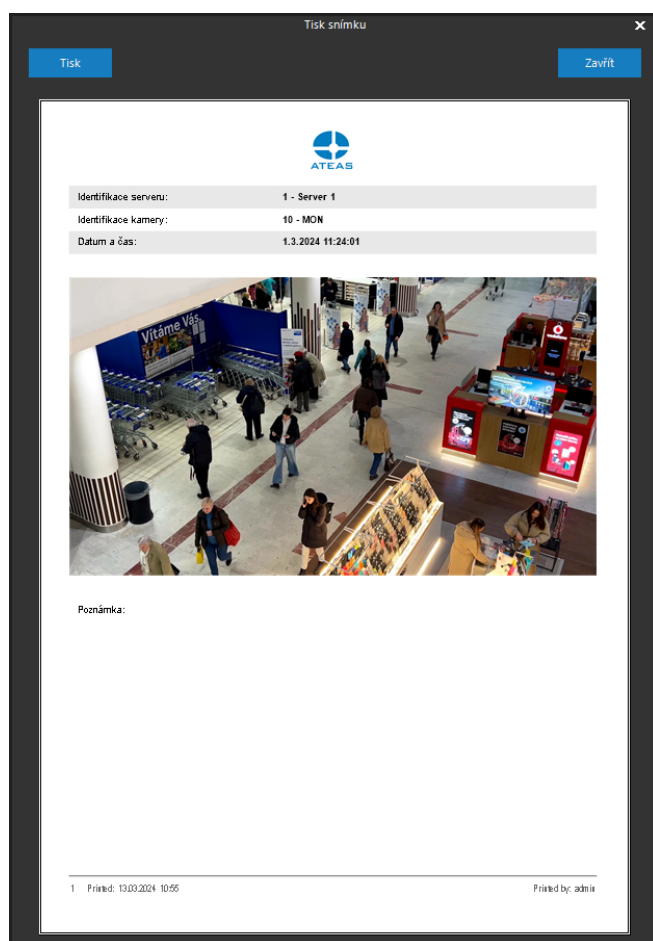


7.1.3. Tisk snímků

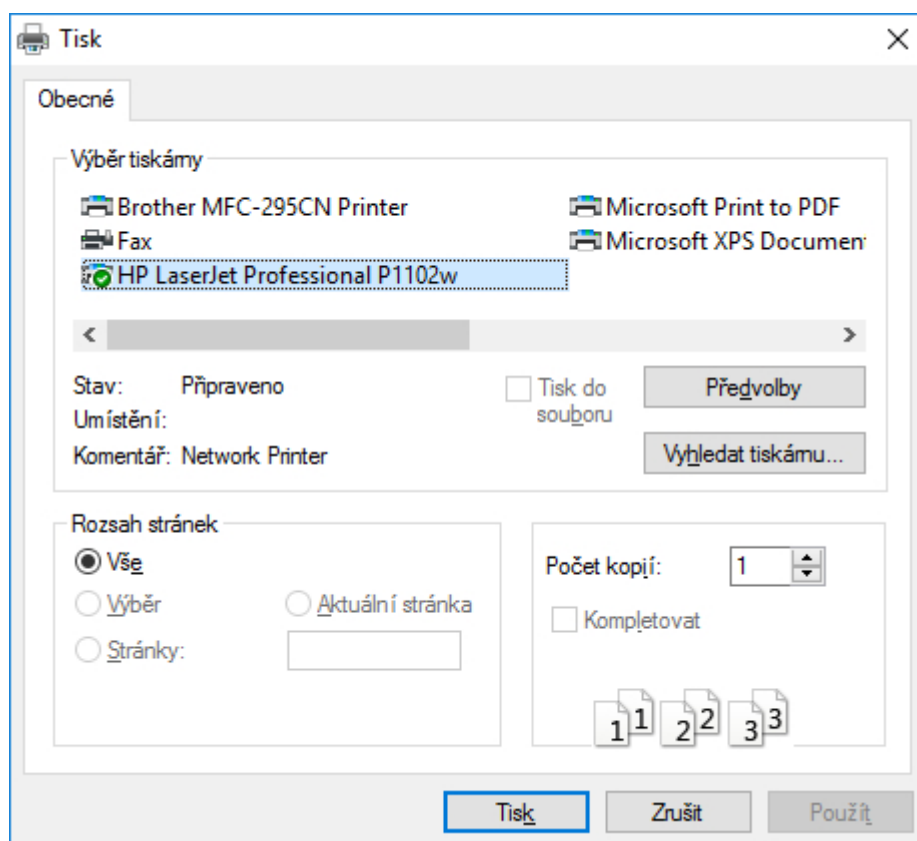
Libovolný vybraný snímek lze vytisknout na libovolnou v systému přidanou lokální či síťovou tiskárnu. Export nebo tisk se provádí stisknutím tlačítka **TISK**.



Pro tisk snímku použijte tlačítko **TISK**. Pokud není v systému nainstalována žádná tiskárna, aplikace zobrazí varovnou zprávu a v tisku nebude možné pokračovat. V první fázi je zobrazen náhled výsledného dokumentu, který obsahuje údaje o kameře, serveru, přesném času snímku a také doplňující popis přidáný uživatelem.



Po vytvoření náhledu je k dispozici tlačítko **ZAVŘÍT** pro návrat zpět. V levém horním rohu tiskového okna je tlačítko tisku, které již vyvolá konkrétní tiskový dialog. Jedná se o standardní tiskový dialog systému Windows s možností vybrat tiskárnu, upravit její vlastnosti či nastavit počet kopií. Tisk je zahájen po stisku tlačítka **TISK**.



7.1.4. Vytvoření náhledu na serveru

Pomocí tlačítka **NAHRÁT** může administrátor systému nahrát vybraný snímek na server, kde bude použit pro statický náhled videa z kamery.

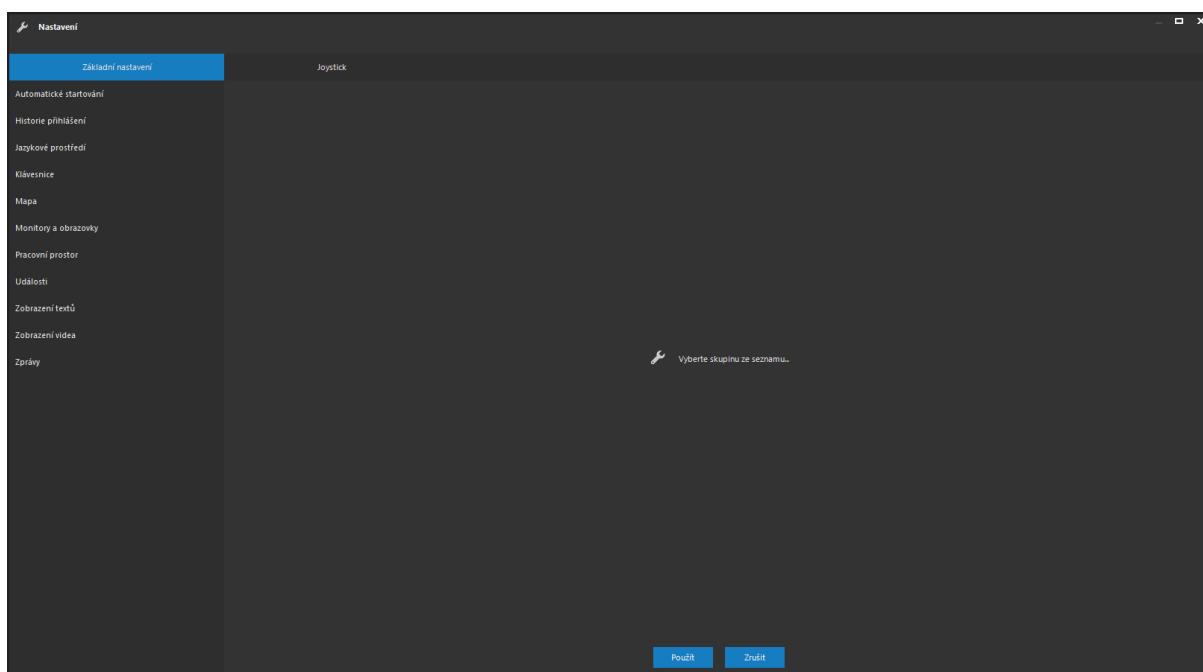
POZNÁMKA

Tyto náhledy mohou být využity např. aplikací ATEAS pro Android TV.

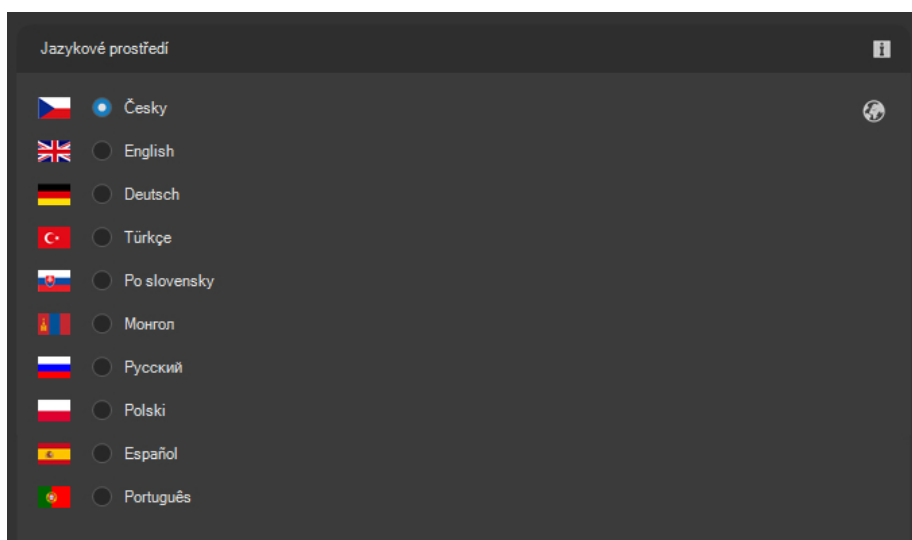
Kapitola 8 - Lokální nastavení

8.1. Základní nastavení

Okno s nastavením lokální stanice je dostupné přes volbu Nastavení z hlavní nabídky aplikace. Na kartě **Základní nastavení** je možné provést lokální nastavení týkající se chování Vaší aplikace. Jednotlivé skupiny nastavení jsou zobrazeny v seznamu v levé části této karty v abecedním pořadí. Po výběru některé z položek jsou nastavení pro danou položku zobrazena vždy v pravé části karty. Veškerá nastavení provedená ve všech částech se uloží až po stisku tlačítka **POUŽÍT**.



8.1.1. Jazykové prostředí



Základní nastavení prostředí včetně volby jazyka také probíhá pomocí interaktivních dialogů při prvním spuštění aplikace na dané stanici.

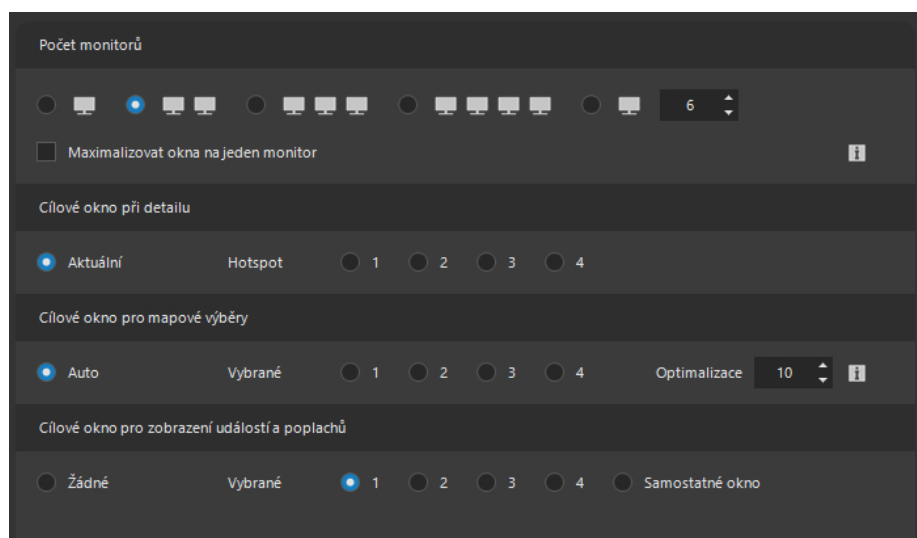
POZOR

Změna jazyka se projeví až po restartování aplikace.

POZNÁMKA

Administrátor systému může aktivovat uživatelskou politiku, při které bude systém ukládat jazyky všech uživatelů a provede jejich automatické přepnutí na libovolné stanici. Takovéto nastavení má vyšší prioritu než nastavení jazyka v lokálním nastavení stanice.

8.1.2. Monitory a obrazovky



Zde je možné nastavit počet aktuálně připojených monitorů k počítači (dohledové stanici). Podporováno je až 16 monitorů, aplikace automaticky detekuje použitý režim vícemonitorového systému (monitory v závislém režimu s jednou plochou – horizontal span, monitory v nezávislém režimu s více plochami – dual či multi head) a bude vždy fungovat optimálně v dané konfiguraci.

POZOR

Z hlediska výkonu při zobrazení lze doporučit konfiguraci v závislém režimu (tj. s jednou plochou – hlavní panel systému Windows je roztažen přes všechny monitory).

Pokud je větší počet monitorů sjednocen do jedné plochy, můžete aktivací volby Maximalizovat okna na jeden monitor docílit lepšího chování okna aplikace při maximalizaci. Okna budou maximalizována pouze v rámci jednoho monitoru, nikoliv celé plochy.

POZNÁMKA

K počítači může být připojeno až 16 monitorů, standardní klient může otevřít nejvýše 16 dohledových oken. Monitory lze využít pro zobrazení mapy, prohlížení záznamu, náhled snímků atd. Klient podřízený video stěně také může zobrazovat video na 16 monitorech. Více v kapitole o video stěně.

Položka Cílové okno při detailu určuje, v jakém dohledovém okně bude zobrazen detail vybrané kamery (po dvojitém kliknutí na její záhlaví). Implicitně je zvolen přepínač Aktuální, při kterém detailní zobrazení nahradí aktuální pohled v daném dohledovém okně. Pokud chceme detaily kamer odesílat na jiný monitor, lze tak učinit zvolením přepínače s konkrétním dohledovým oknem.

Podobnou funkci má i položka Cílové okno pro mapové výběry. Kamery lze pomocí mapových funkcí vybírat také v mapě. Mapový výběr kamer je poté zobrazen v některém z dohledových oken. Cílové okno je možné určit přímo pomocí symbolů monitorů očíslovaných jedna až čtyři. Implicitně je zvolena volba Auto, která mapový výběr umístí do posledního aktivního dohledového okna nebo do okna primárního (pokud není primární okno otevřeno). Přestože je možné pomocí výběrových nástrojů v mapovém okně vybrat najednou libovolné množství kamer (prvků) bude v cílovém okně zobrazeno maximálně 100 kamer v rozvržení 10 x 10.

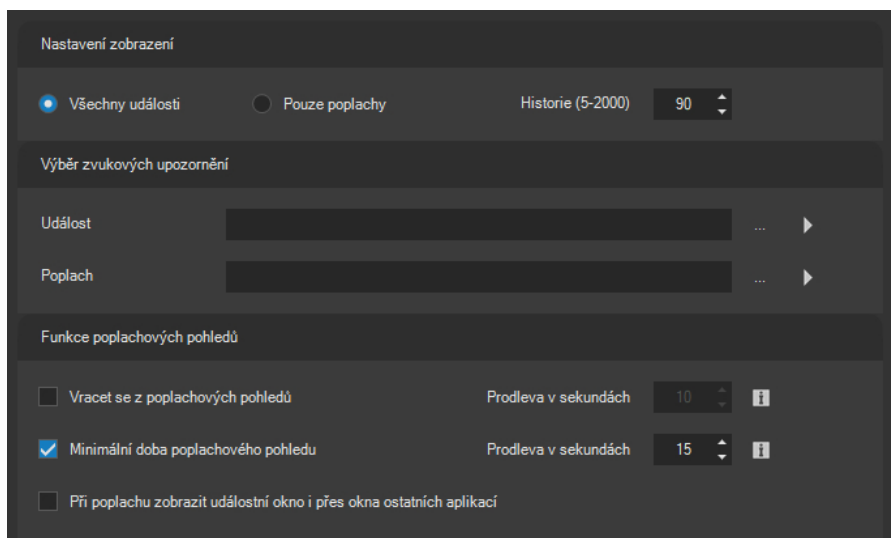
Nastavením hodnoty Optimalizace je možné určit počet vybraných kamer v mapě, od kterého budou použity sekundární streamy kamer, pokud jsou konfigurovány.

TIP

Tím lze snížit zátěž klienta po otevření mapového pohledu.

Nastavení cílového dohledového okna pro příjem událostí je možné učinit pomocí položky Cílové okno pro zobrazení událostí a poplachů. Pokud je příjem vypnut (nastavení na Žádné), aplikace nebude signalizovat příchozí události a poplachy. Volba Samostatné okno aktivuje příjem událostí do samostatného okna namísto do vybraného dohledového okna.

8.1.3. Události



K dispozici jsou tato nastavení:

- Nastavení filtru na běžné události. Uživatel má možnost odfiltrovat běžné události od poplachových stavů, běžné události nebudou v jeho okně zobrazovány.
- Nastavení maximálního počtu událostí a poplachů udržovaného v seznamu událostí v dohledovém okně. Délka historie je implicitně nastavena na 20 událostí a poplachů. Touto hodnotou však nelze omezit počet zobrazených nevyřešených poplachů s aktivovaným režimem řešení.
- Nastavení zvuků pro přehrání při příjmu události. Aby mohl být při příjmu události nebo poplachu přehráván zvuk, je nutné vyplnit cestu nebo nalistovat platný zvukový soubor. Výběr lze zahájit tlačítkem pro procházení složek. Zvukové soubory pro událost a událost ze statutem poplachu se mohou lišit. Jejich vypnutí se provede výmazem obsahu příslušného textového pole.

Pomocí standardního dialogu Windows lze poté vybrat libovolný zvukový soubor ve formátu WAV. Několik vhodných zvukových souborů je i součástí instalace klientské aplikace. Vybraný zvuk, jehož cesta se objeví v textovém poli, je možné otestovat (přehrát) pomocí tlačítka s bílou šipkou.

V části Funkce poplachových pohledů jsou dále k dispozici některé funkce pro nastavení vhodné ergonomie při příjmu poplachů.

Pokud je aktivována volba návratu z poplachových pohledů, bude v dohledovém okně, které přijímá poplachy, po uplynutí nastaveného intervalu automaticky vrácen původní lokální nebo sdílený pohled,

který byl zobrazen před poplachem. To významně zlepšuje práci operátora v situaci, kdy nemá jedno dohledové okno vyhrazeno pouze pro poplachy, ale sleduje na něm i jiné kamerové pohledy.

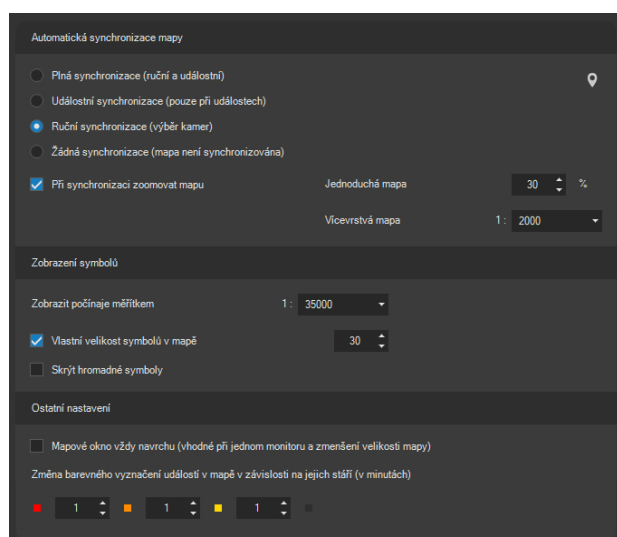
Pokud je aktivována funkce minimální doby poplachového pohledu, nebude v dohledovém okně přepnut žádný další poplachový pohled, pokud od přepnutí posledního poplachového pohledu neuplynul alespoň nastavený časový interval. Tato funkce se využívá proto, aby se zlepšila situace operátora a jeho schopnost reakce při výskytu více poplachů v krátkém časovém intervalu.

POZNÁMKA

Pokud není následkem předchozí funkce provedeno automatické přepnutí do poplachového pohledu, nemá to samozřejmě žádný vliv na zobrazení tohoto poplachu v seznamu událostí ve spodní části dohledového okna.

Pokud pracujete s více okny či aplikacemi zároveň, při příjmu poplachu nedochází automaticky k přepnutí událostního okna do popředí, abyste mohli plynule pokračovat v práci v jiném okně či aplikaci. Na příchozí poplach tak můžete být upozorněni např. pomocí zvukové notifikace. Pokud si však přejete, aby se okno s událostním pohledem automaticky přeneslo do popředí před ostatní okna i aplikace, aktivujte příslušnou volbu.

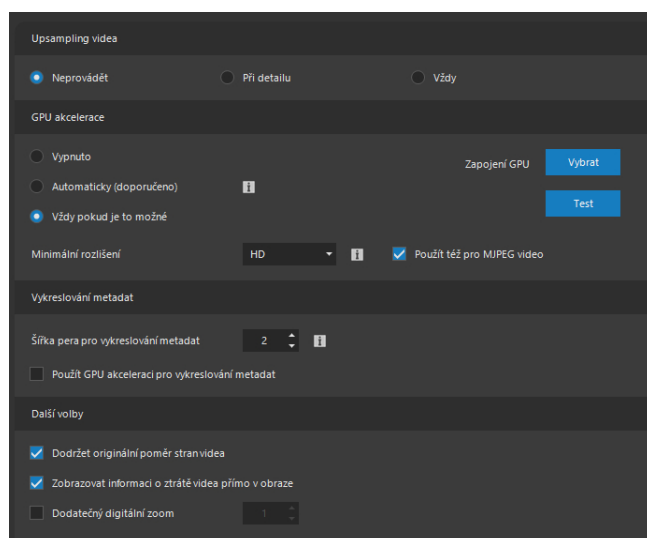
8.1.4. Mapa



V této části nastavení je možné s lokální platností (pro danou stanici) nastavit chování mapové okna. K dispozici jsou následující nastavení:

- Automatická synchronizaci mapy. Mapa je inteligentní integrovanou komponentou, která může být při nejružnějších činnostech synchronizována (automatická lokalizace událostí, kamer a objektů včetně úpravy zoomu). Při nastavení plné synchronizace bude mapa synchronizována vždy, když to bude vhodné, včetně událostí a ručního výběru kamer lokalizovaných v mapě. Při událostní synchronizaci bude mapa synchronizována pouze při výskytu události u lokalizovaného objektu, nikoliv již však při ručních výběrech. Pomocí volby Ruční synchronizace lze naopak způsobit, aby se mapa synchronizovala pouze při ručních výběrech kamer, nikoliv při událostech v systému. Automatickou synchronizaci mapy lze vypnout označením přepínače Žádná synchronizace.
- Určení zoomu. Při automatické synchronizaci je mapa automaticky centrována na vybraný prvek či událost. Dodatečně lze vyvolat také operaci mapového zoomu. Tuto hodnotu lze pro jednoduché mapy nastavit v procentech původní velikosti mapové úrovně, pro vícevrstvé mapy ji lze zadat jako reálné mapové měřítko.
- Zobrazení symbolů v mapě. Pro vícevrstvé mapy lze nastavením maximálního měřítko, při kterém budou ještě zobrazeny symboly v mapě (kamery, uživatelská tlačítka), zabránit vykreslování kamer či tlačítek při velkém oddálení mapy, což může ztížit orientaci v mapě. Mapa je pro tento případ vybavena funkcí inteligentního sdružování prvků mapy stejného typu, které zůstávají dále zobrazeny. Jejich skrytí spolu s jednotlivými symboly prvků je však možné zapnout pomocí volby Skrýt hromadné symboly.
- Vlastní velikost symbolů v mapě. Implicitně je velikost všech administrátorem definovaných mapových symbolů kamer nastavena na 24 bodů. Na každé stanici lze však tuto velikost upravit vzhledem k rozlišení monitorů či subjektivnímu vnímání uživatelů.
- Volba mapové okno vždy navrchu umožňuje mapové okno přepnout do režimu, kdy nebude nikdy překryto jiným oknem aplikace. To je vhodné pro jednomonitorové dohledové stanice, na kterých je možné mapové okno zmenšit a nechat zobrazené vždy navrchu, což vede k usnadnění orientace a odstranění nutnosti přepínání oken.
- Změna barevného označení událostí v mapě. Při zobrazování událostí v mapě je možné jejich vzhled měnit v závislosti na jejich stáří, což umožňuje operátorovi jedním pohledem na mapu zhodnotit stav událostí a poplachů. Událost je vždy zobrazena orámováním symbolu, který událost vyvolal. Ihned po výskytu události je tento rámeček červený, po nějaké době je změněn na oranžovou, poté na žlutou než je v dalším kroku z mapy zcela odstraněn. Časové prodlevy mezi těmito změnami je možné definovat pomocí zde dostupných ovládacích prvků. Při obnovení nějaké události v daném místě je samozřejmě celý proces restartován a událost označena jako aktivní.

8.1.5. Zobrazení videa



V části Upsampling videa je možné nastavit, zdali bude použita technika dopočítávání obrazových bodů, pokud je rozlišení cílového místa pro zobrazení kamery na monitoru v daném okně vyšší než nativní rozlišení videa kamery (upsampling). Implicitně se dopočet (zvětšení obrazu) neprovádí, lze ho však zapnout pro režim detailu (při jediné kameře v pohledu) nebo i pro veškeré živé zobrazení videa.

V části GPU akcelerace je možné aktivovat využití procesoru grafické karty nebo dedikovaného grafického čipu (GPU). Pokud je tato funkce aktivována, je dekomprese videa akcelerována pomocí GPU a není tedy výhradně zatížen pouze centrální procesor klienta (CPU).

POZNÁMKA

Zapojení GPU tak může být zejména vhodné u náročných aplikací, kde se využívá video ve vysokých snímkových frekvencích (60 FPS) nebo video s velmi vysokým rozlišením (4K).

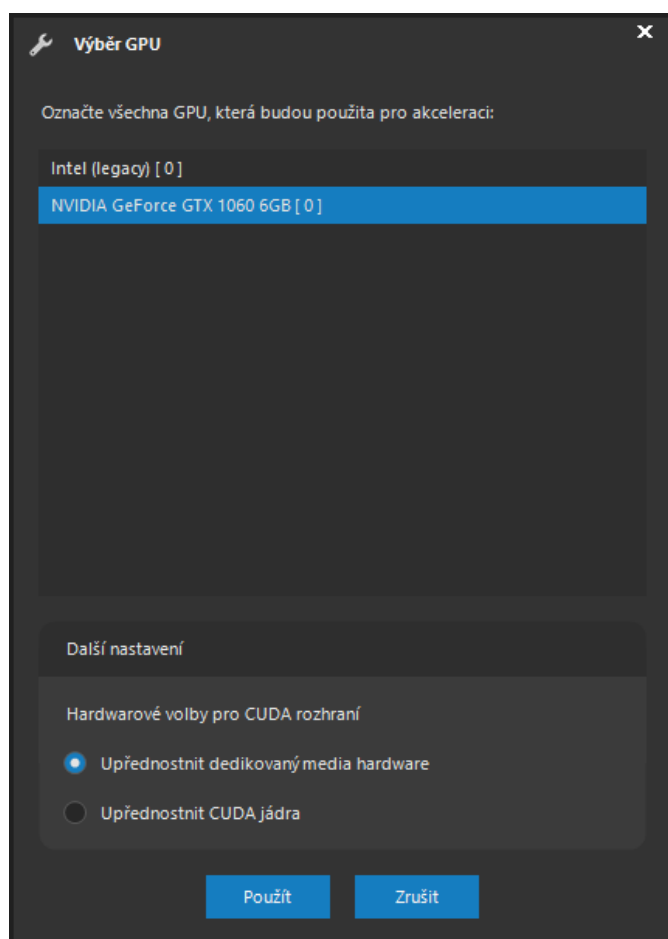
Pomocí přepínačů můžeme zvolit, zdali bude grafický procesor využíván jen při zobrazení plynulého videa nebo i při omezené snímkové frekvenci. Pro většinu instalací bude dostačovat doporučená volba, tj. využití GPU při zobrazení plynulého videa. Pro H265 video je však GPU akcelerace použita vždy.

V části nastavení GPU akcelerace můžeme dále určit minimální rozlišení videa, při kterém bude GPU akcelerace využita (pokud alespoň jeden z rozměrů videa vyrovná anebo překoná nastavenou hodnotu). Také je možné z akcelerace vyloučit formát MJPEG nezávisle na rozlišení videa.

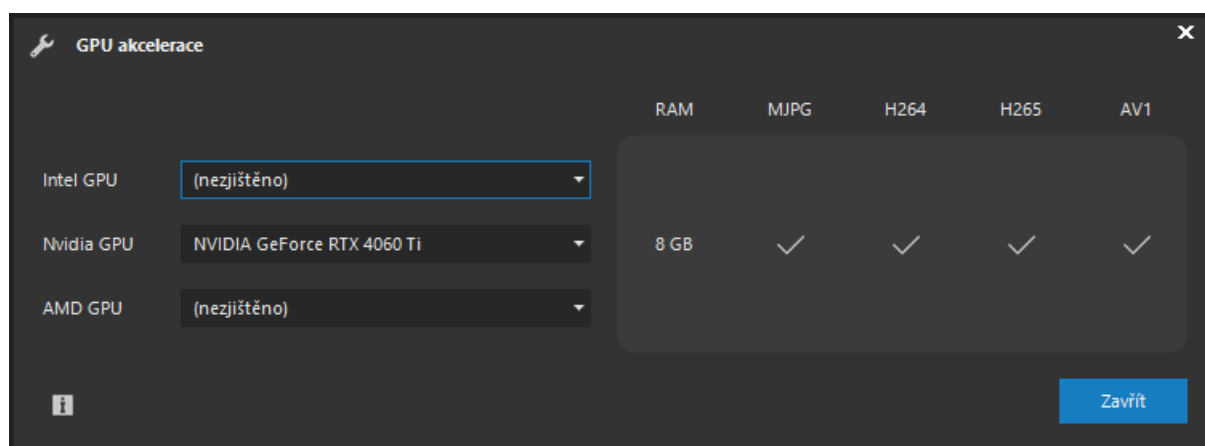
Tlačítko **VYBRAT** zobrazí dialog se seznamem všech grafických karet. Ze seznamu je nutné zvolit jednu anebo více grafických karet, které budou použity pro akceleraci videa. Klient je tedy schopen využít různé technologie GPU akcelerace a více GPU i v rámci jedné aplikace pro dosažení maximálního výkonu.

POZNÁMKA

Pro rozhraní CUDA je navíc možné i učit některé hardwarové preference, zejména je možné určit, jestli pro akceleraci budou použita CUDA jádra anebo bude využit dedikovaný hardware pro dekompresi videa.



Pomocí tlačítka **TEST** můžeme ověřit, zdali bude možné na daném počítači používat akcelerovanou dekompresi videa. Následující dialog zobrazuje výsledky testu grafické akcelerace zpracování videa pro formáty MJPEG, H264, H265 a AV1. Podporováno je akcelerační rozhraní pro všechny hlavní výrobce GPU.



POZNÁMKA

Pokud je spuštěn přehrávač bez přihlášení do systému, bude využití GPU akcelerace automatické.

V části Vykreslování metadat je možné určit šířku pera v bodech, která bude použita pro vykreslování metadat získaných z neuronové sítě či externích zdrojů analytických dat. Šířku je možné nastavit v intervalu jedna až pět, výchozí hodnota je dva body.

POZNÁMKA

Tato šířka zůstává shodná nezávisle na digitálním přiblížení videa, což velmi zvyšuje uživatelský komfort při vnímání vykreslovaných metadat.

Vykreslování metadat do videa může být při větších počtech detekovaných objektů v obraze, vysoké snímkové frekvenci videa a větších počtech kamer v pohledu náročné na spotřebu CPU. Pokud vykreslovaná metadata již nejsou zcela synchronní s videem, je možné aktivovat volbu GPU akcelerace vykreslování metadat, která zátěž přenesení přímo na GPU.

POZNÁMKA

Při GPU akcelerovaném vykreslování metadat jsou metadata již přímo součástí video vrstvy a některé funkce CPU vykreslování (šířka kresby nezávislá na digitálním přiblížení nebo automatická optimalizace pozice textových rámečků) již nebudou dostupné.

GPU akcelerované vykreslování metadat je zejména vhodné při použití s video stěnou. Předpokladem je vždy aktivace GPU akcelerovaného vykreslování videa přes Nvidia GPU, které je popsáno výše v textu.

V části Další volby jsou k dispozici doplňkové volby pro tuto část nastavení, např. volbu týkající se dodržování originálního poměru stran videa. Tato volba je implicitně zapnuta. V praxi je poté při zobrazení kamerového obrazu použito tmavých vertikálně či horizontálně orientovaných pruhů, které kompenzují rozdíl v poměrech stran videa a okna pro zobrazení. Toto chování lze vypnout zrušením zaškrtnutí této volby. Poté bude pro zobrazení videa použita maximální možná plocha okna, může být však narušen poměr stran videa.

Dále je možné aktivovat možnost zobrazení informace o ztrátě videa přímo v obraze. Tato informace se zobrazuje v podobě červeného textu s nápisem Není video.

POZNÁMKA

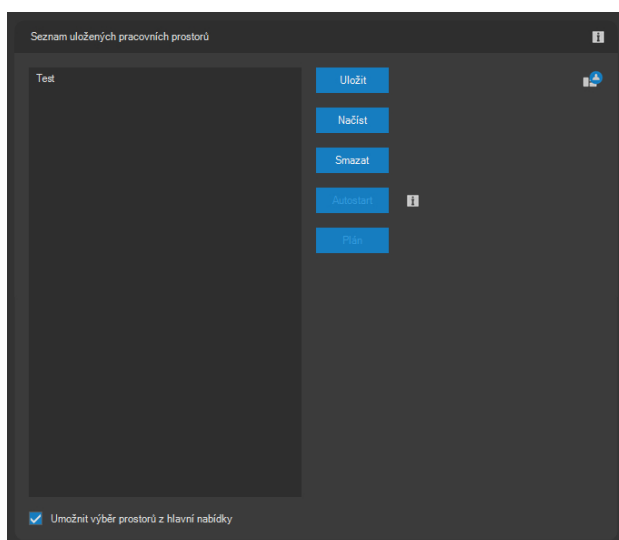
Stejnou funkci má i jeden z indikátorů synchronizace, nicméně použití této funkce může sloužit k výraznějšímu upozornění operátora na nedostupný obraz kamery při jejím výpadku. Funkce je pro dohledová okna implicitně vypnuta.

Ve výchozím nastavení je vypnuta možnost provádění digitálního zoomu nad úroveň nativního rozlišení videa. Pomocí volby Dodatečný digitální zoom je možné docílit situace, kdy bude možné vybranou kameru digitálně přiblížit i na několikanásobek původní velikosti obrazu. Hodnotu tohoto násobku je možné nastavit v rozmezí od 1 do 10.

POZNÁMKA

Nastavení Zobrazení videa se týká pouze lokálních dohledových oken. V části administrace video stěny existují analogická nastavení pro video zobrazované na monitorech, které jsou součástí virtuální video stěny. U podřízených stanic (po přihlášení pod účtem podřízeným video stěně) se tedy toto nastavení při zobrazení videa na monitorech nebere v úvahu.

8.1.6. Pracovní prostor



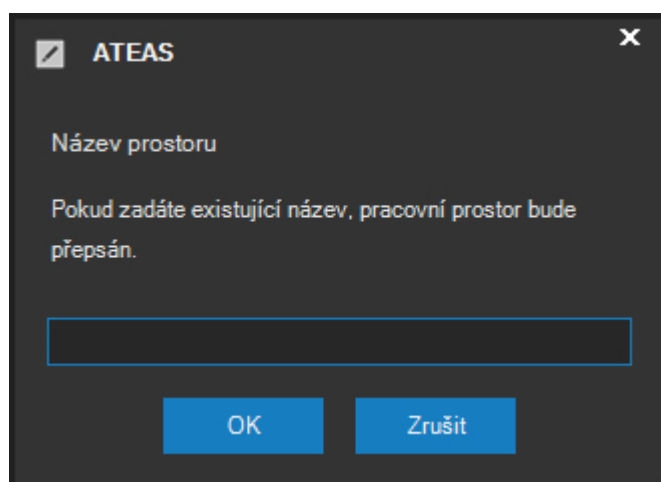
Většina uživatelů na pracovních stanicích přistupujících ke kamerovému systému používá vždy určité rozložení dohledových oken na svých monitorech, určité umístění a velikost mapového okna. Aby nebylo nutné tuto rozložení nastavovat vždy znovu, podporuje klientská aplikace jejich uložení v podobě pracovních prostorů (workspace). V rámci uloženého pracovního prostoru si tedy aplikace zapamatuje:

- počet a umístění všech (tj. maximálně 16) dohledových oken,
- umístění a velikost dalších oken (záznam, mapová scéna, okno s hlavní nabídkou),
- lokálně uložené či sdílené pohledy přepnuté v dohledových oknech,
- stav dohledových oken (maximalizace pomocí F12),
- poslední vybrané pozice v dohledových oknech,
- okno pro příjem událostí (dohledové či samostatné) a zobrazené sloupce včetně jejich pořadí a rozměrů.

TIP

Uložení vybrané pozice umožňuje po otevření prostoru automaticky připojit zvuk vybrané kamery.

Takto vytvořený pracovní prostor lze uložit pomocí tlačítka **ULOŽIT**. Před uložením bude ještě nutné zadat pro pracovní prostor nějaký název.



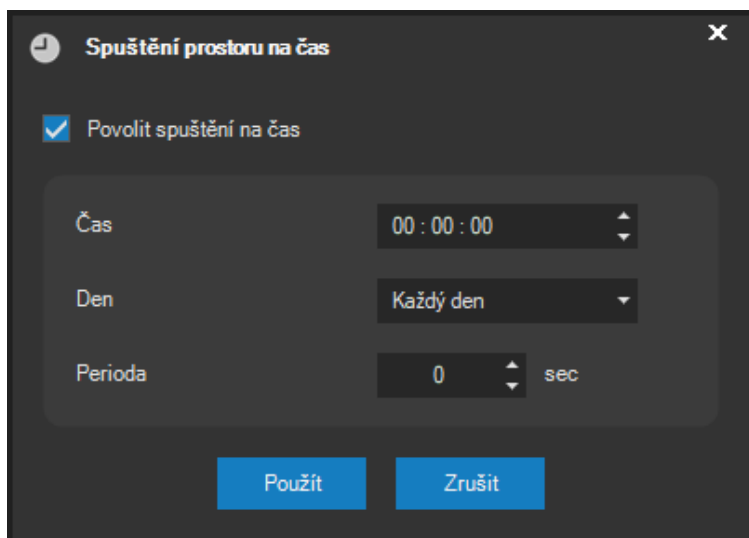
Po uložení se prostor objeví v seznamu. Pracovních prostorů může být uloženo libovolné množství, kterýkoliv vybraný prostor lze načíst pomocí tlačítka **NAČÍST**, výmaz prostoru včetně všech jeho uložených informací se provede tlačítkem **SMAZAT**.

Pomocí přepínacího tlačítka **AUTOSTART** lze jeden prostor označit za automatický. To znamená, že po úspěšném přihlášení bude tento prostor automaticky po několika vteřinách načten. Aplikace tedy po přihlášení automaticky rozmístí všechna dohledová okna na Vaše monitory, na příslušném místě otevře mapu a přepne lokální či sdílené pohledy.

POZNÁMKA

Pomocí klávesy SHIFT lze zablokovat automatické otevření pracovního prostoru po startu aplikace.

Pomocí tlačítka **PLÁN** je možné spuštění prostoru vyvolat namísto ruční akce výběru z nabídky anebo ze seznamu prostorů zadáním doby, kdy k aktivaci prostoru dojde automaticky.

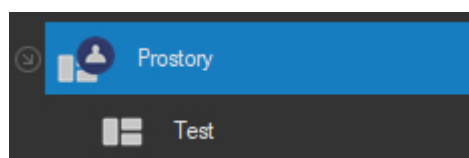


Aktivací volby Povolit spuštění na čas a nastavením času dojde k aktivaci prostoru automaticky v konkrétní časový okamžik. Dále je možné nastavit, zdali bude k aktivaci docházet denně anebo jen v určité dny v týdnu a také periodu. Je-li nastavena perioda (hodnota vyšší než nula), bude prostor aktivován vždy v určený čas a poté pokaždé po uplynutí periody.

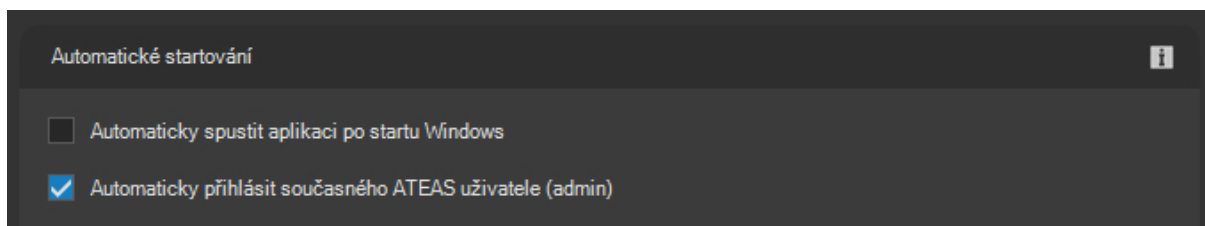
POZNÁMKA

V určený čas v nejbližší nastavený den je prostor automaticky aktivován a perioda restartována.

Pomocí zaškrtnutí políčka pod seznamem prostorů lze také pro jejich snadnější načítání provést jejich zobrazení v hlavní nabídce aplikace.



8.1.7. Automatické startování



-  Pro potlačení auto loginu podržte při startu aplikace klávesu SHIFT.
-  Pro automatické otevření pohledů po přihlášení přejděte na nastavení prostorů.

V části Automatické startování je možné aktivovat možnost automatického spuštění klientské aplikace po startu Windows a také možnost automaticky přihlásit konkrétního uživatele. Aktivovat automatické přihlášení může uživatel vždy pouze sám pro sebe. Automatické přihlášení může být potenciálně nebezpečné, pokud jsou jeho oprávnění vysoká, neboť může dojít k jejich zneužití. Nejlepší variantou je použití automatického přihlášení pro univerzální uživatele např. Obsluha s nízkým oprávněním.

Pokud je na jednom počítači vytvořeno více uživatelských účtů, může si každý uživatel aktivovat volbu automatického přihlášení. Tím lze docílit situace, kdy bude automaticky přihlášen aktuální uživatel Windows.

POZNÁMKA

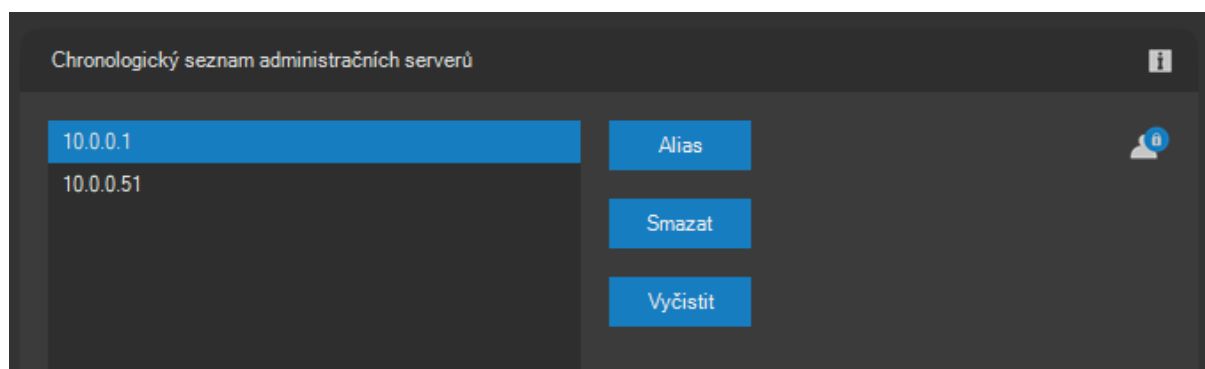
Automatický start aplikace po startu Windows může úspěšně aktivovat či deaktivovat pouze uživatel, který má ve Windows oprávnění zápisu do registru Windows. Poté je toto nastavení již platné pro libovolný uživatelský účet operačního systému.

POZNÁMKA

Pokud je automatické přihlášení uživatele neúspěšné z důvodu nedostupnosti administračního jádra systému, aplikace automaticky pokus o přihlášení opakuje v určitých kratších časových intervalech až do vyčerpání přednastaveného počtu pokusů. Tento proces lze přerušit ručním pokusem o přihlášení mezi pokusy o automatické přihlášení.

Spojením voleb automatického spuštění aplikace po startu Windows, automatického přihlášení a automatického otevření pracovního prostoru (viz nastavení Pracovní prostor) lze docílit maximální automatizace startu a obnovení klientské aplikace až po otevření všech dohledových oken či mapy.

8.1.8. Historie přihlášení



V části Historie přihlášení jsou zobrazeny všechny kamerové systémy (adresy jejich administračních serverů), kam se daný klient úspěšně přihlásil. Stejný chronologicky řazený seznam se zobrazuje také v rozbalovacím seznamu v poli serverů při přihlášení do systému.

Pokud je nějaká položka v seznamu považována za citlivou, tj. nechcete, aby se v seznamu při přihlášení příštího uživatele znovu objevovala, je možné ji odstranit pomocí tlačítka **SMAZAT**. Celou historii je možné odstranit pomocí tlačítka **VYČISTIT**.

Pomocí tlačítka **ALIAS** lze pro vybranou položku v seznamu historie definovat vlastní název pro adresu či síťový název serveru. Pomocí tohoto alias názvu se bude možné přihlásit do systému zcela stejně jako při použití jeho skutečné adresy.

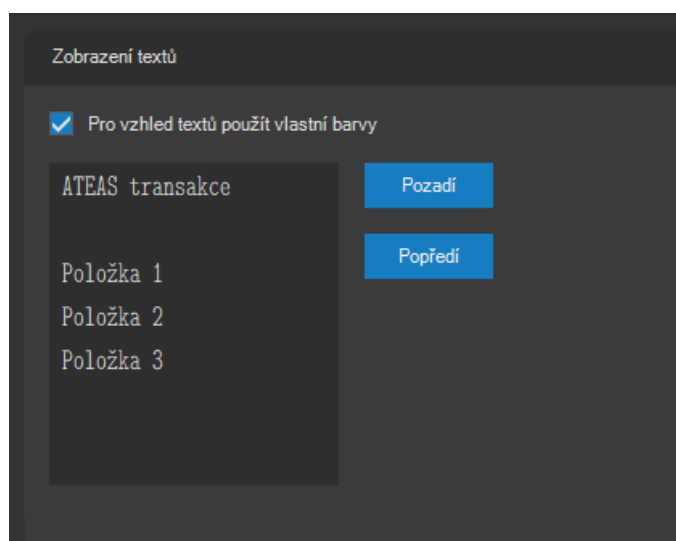
Vlastní název pro server (alias) lze vložit také automaticky již při přihlašování, pokud alias název uvedete za adresu serveru do kulatých závorek. Tento postup je také popsán v úvodní kapitole u přihlašování do systému.

POZOR

Pokud je definován alias název, který může být zároveň vyhodnocen jako síťový název, alias název má při vyhodnocování přednost.

8.1.9. Zobrazení textů

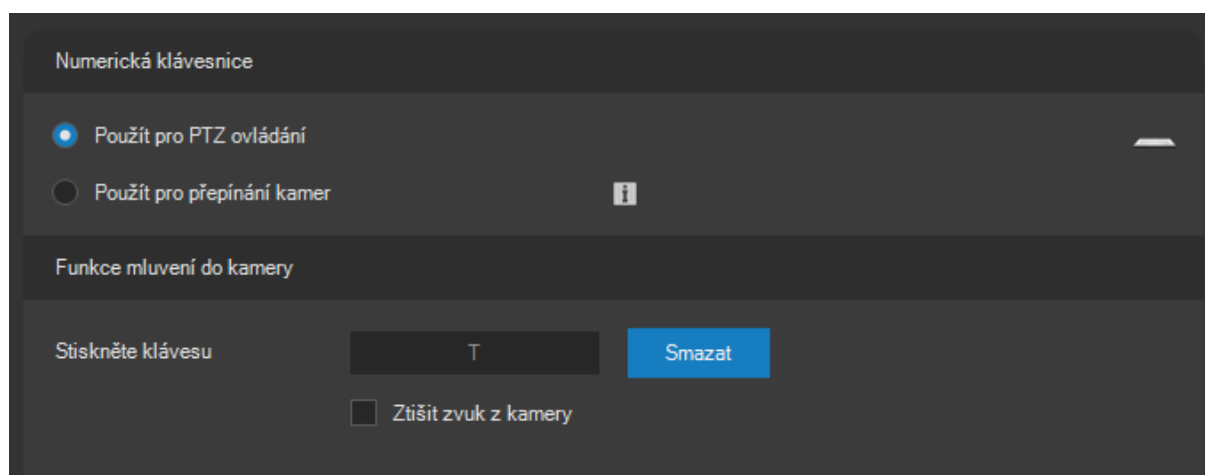
V části Zobrazení textů je možné změnit implicitní barevné schéma zobrazovaných textových dat – např. transakčních dat nebo čítačů přímo v dohledových oknech.



Pomocí tlačítek **POZADÍ** a **POPŘEDÍ** lze samostatně nastavit libovolnou barvu pro pozadí textového okna a písmo (popředí).

8.1.10. Klávesnice

Numerická klávesnice je implicitně používána jako jeden ze způsobů PTZ ovládání kamer. Alternativně však může být použita také pro výběr kamer (více viz kapitola Funkce vybrané kamery).



V dohledovém okně je k dispozici tlačítko pro aktivaci funkce mluvení do kamery. Namísto stisknutí a uvolnění tlačítka pro zahájení resp. ukončení vysílání zvuku do kamery je možné v části Funkce mluvení do kamery přiřadit této funkci libovolnou klávesu. Při jejím stisku bude zahájeno vysílání zvuku do kamery, při jejím uvolnění bude vysílání přerušeno.

Aktivací volby Ztišit zvuk z kamery lze zároveň na dobu vysílání zvuku ztlumit příchozí zvuk z důvodu zamezení zpětné zvukové vazby.

POZNÁMKA

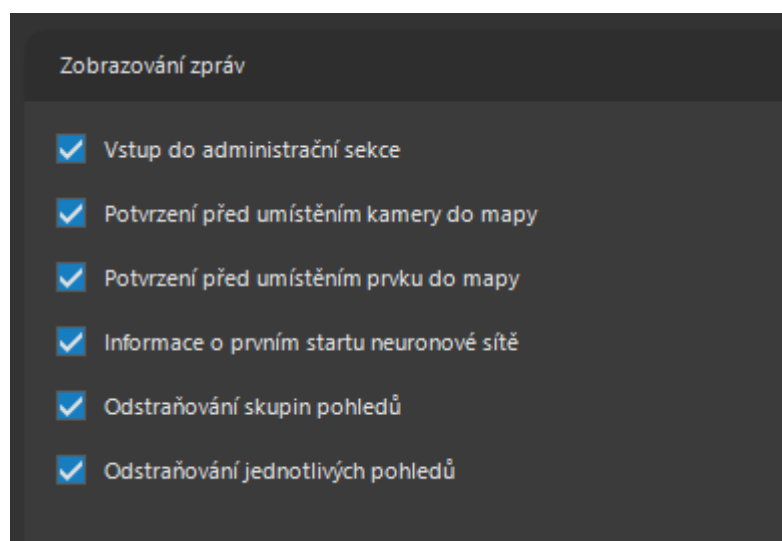
Stejnou funkci má dvojité kliknutí na tlačítko vysílání zvuku do kamery v dohledovém okně.

POZNÁMKA

Klávesnici nelze použít pro současné vysílání zvuku do všech kamer v pohledu. To lze provést pouze pravým tlačítkem myši na tlačítku pro vysílání zvuku do kamery.

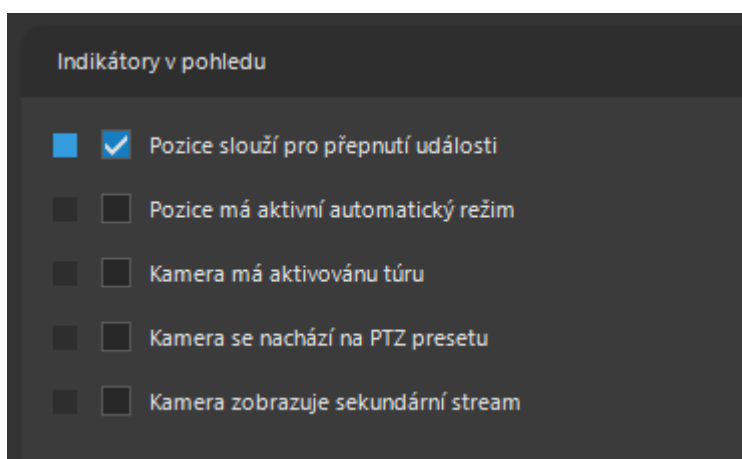
8.1.11. Zprávy

Vybrané zprávy, které zobrazuje klientská aplikace při Vaší práci se systémem, lze aktivací volby Příště již nezobrazovat vypnout. Tato část lokálního nastavení zobrazuje aktuální stav zobrazování jednotlivých zpráv a také možnost je znovu aktivovat.



8.1.12. Vlastní indikátory

Vlastní indikátory jsou zobrazeny v dohledových oknech vždy za označením kamery, systémové indikátory jsou zobrazeny při pravém okraji. Vlastní indikátory mohou vhodně poskytovat vizuální zpětnou vazbu o některých stavech kamery či konkrétní pozice v pohledu, které nemusí být na první pohled zřejmé.



Kliknutím na barevný symbol lze u aktivního indikátoru změnit jeho barvu.

TIP

Systémové i vlastní indikátory nabízejí kromě barevného odlišení při setrvání kurzorem myši na jejich pozici také textový popis.

POZNÁMKA

Událostní pozice v pohledu určené pro příjem událostí lze vytvořit v editoru pohledů.

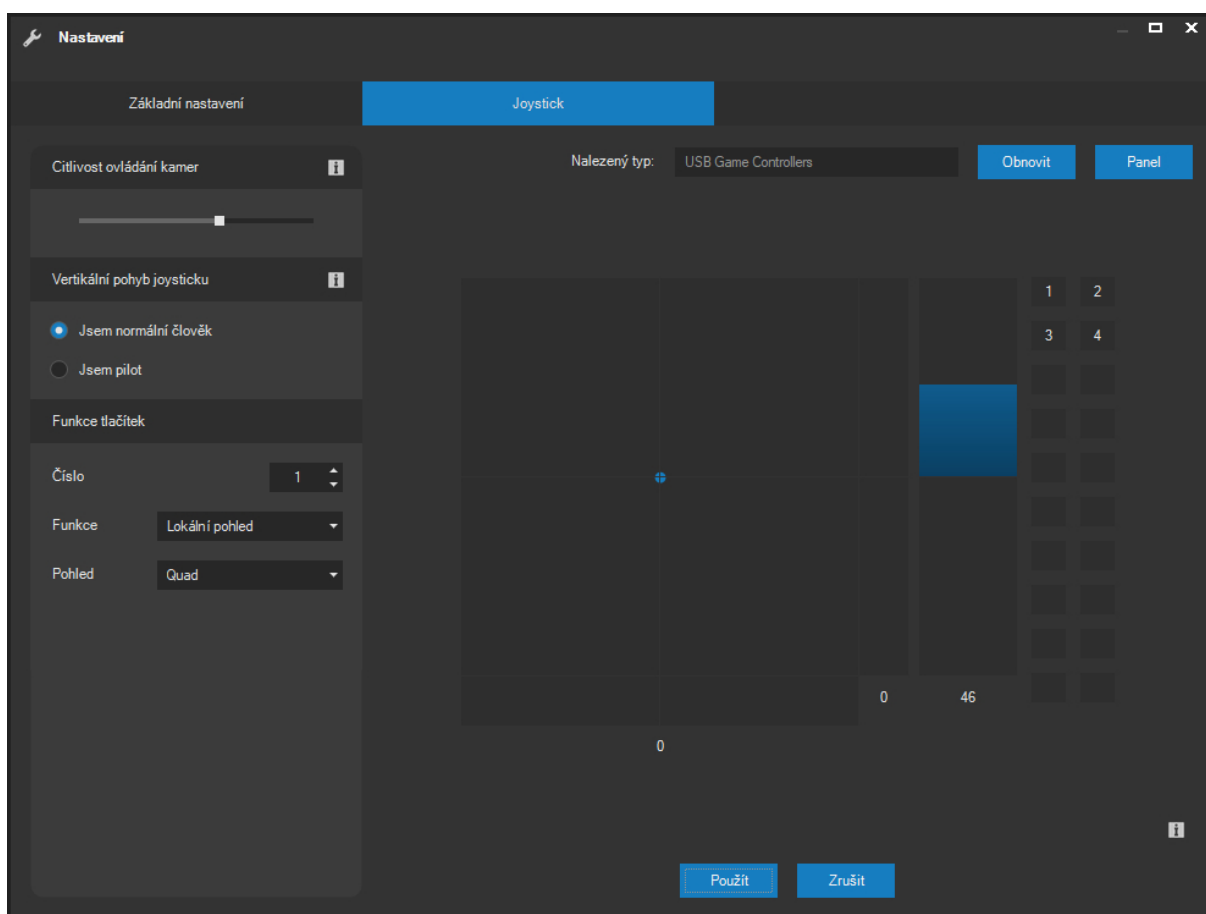
TIP

Indikátor PTZ presetu je vhodný, pokud používáte analytické funkce navázané na PTZ preset.

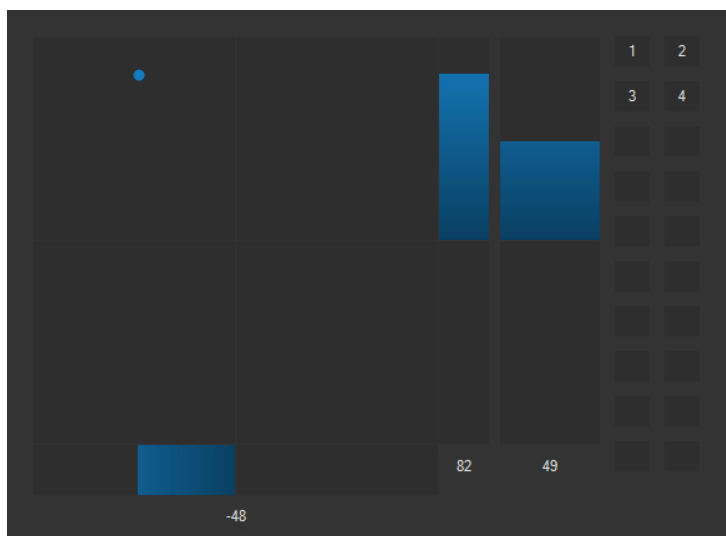
8.2. Nastavení joysticku

8.2.1. Základní nastavení

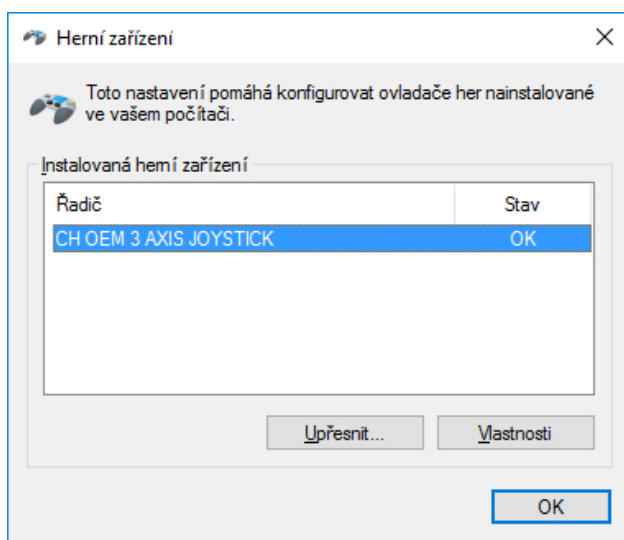
Na kartě **Joystick** je možné provést některá nastavení týkající se chování joysticku.



Na velkém ovládacím prvku s černým pozadím lze testovat pohyb joysticku ve všech osách, název joysticku se zobrazuje nad tímto ovládacím prvkem. Pokud je joystick vyměněn nebo doplněn při otevření okna nastavení, je možné název zařízení (joysticku) získat tlačítkem **OBNOVIT**. K dispozici je také náhled stisku všech tlačítek. Ta budou použita pro ovládání zoomu otočné kamery, pokud joystick není vybaven třetí osou (osou Z).



Pokud není možné joystick plynule pohybovat po celém obvodu čtverce (osy X a Y) nebo v celém rozsahu sloupce pro osu Z, bude nutné joystick kalibrovat. To se provede standardním způsobem vestavěným do operačního systému Windows. Po stisknutí tlačítka **PANEL**, se zobrazí seznam zařízení typu joystick.



Po stisku tlačítka **VLASTNOSTI** se objeví další dialog, který obsahuje kartu **Nastavení**, ze které je již možné spustit kalibrační proces.

V pravé části okna je možné nastavit citlivost joysticku, která roste s pohybem posuvníku k pravému dorazu. Změny citlivosti se projevují na ovládání kamer okamžitě bez uložení změn v okně nastavení. Dále je k dispozici přepínač, který určuje chování ovládané kamery při pohybu páky joysticku v ose Y. Při nastavení Jsem normální člověk dochází při pohybu páky joysticku směrem dopředu k pohybu kamery nahoru, při nastavení na Jsem pilot k pohybu dolů.

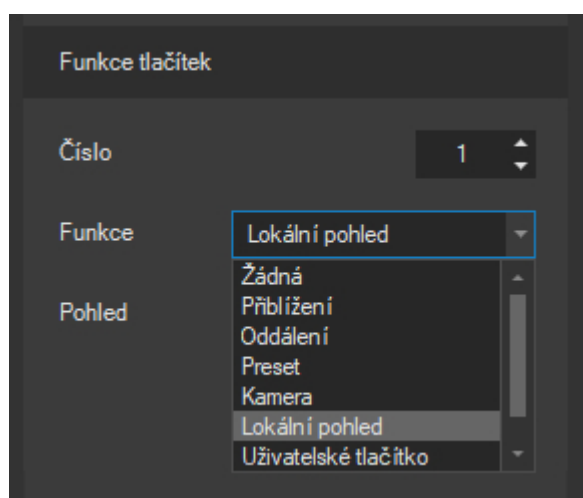
Veškerá nastavení učiněná v okně Nastavení mohou být uložena stiskem tlačítka **POUŽÍT**.

8.2.2. Funkce tlačítek

Pokud je k počítači připojen joystick s tlačítky, je jejich počet aplikací automaticky rozpoznán. Náhled stisku jednotlivých tlačítek se zobrazuje na příslušném místě ovládacího prvku joysticku.



Každému tlačítku joysticku lze přiřadit některou z předdefinovaných funkcí, které se vztahují k ovládání právě aktivního dohledového okna. Na výběr máte z několika možností, jak ukazuje i následující obrázek.

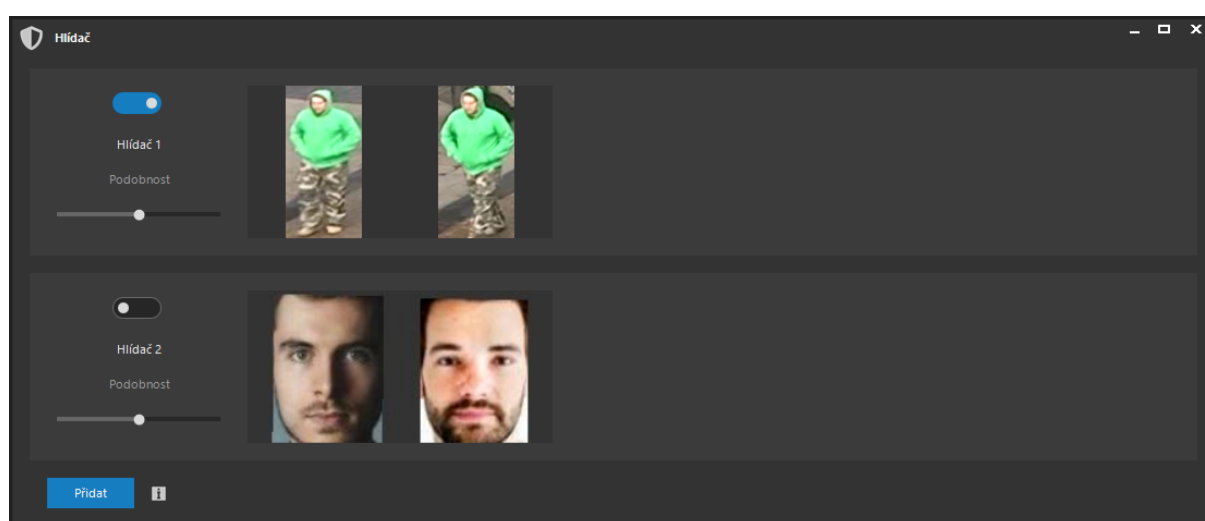


- Při nastavení na Žádná nebude mít příslušné tlačítko joysticku žádnou funkci.
- Funkce Přiblížení a Oddálení ovládají zoom otočných kamer. Přiřazení funkcí přiblížení a oddálení k tlačítkům joysticku může být nutné zejména tehdy, pokud Váš joystick nemá třetí osu pro ovládání zoomu.
- Nastavením na Preset bude tlačítko fungovat jako rychlá volba pro zvolení prepozice otočné kamery. Při tomto nastavení se vždy shoduje číslo tlačítka s číslem presetu. Tlačítko joysticku číslo 2 tedy provede přepnutí vybrané kamery do presetu číslo 2 atd.
- Volba Kamera provede rychlé vyvolání detailu vybrané kamery v aktuální dohledovém okně. Kameru je zapotřebí vybrat přes volbu kamerového serveru a volbu konkrétní kamery.
- Volba Lokální pohled je podobná jako volba kamera, lze však pomocí ní provést rychlé přepnutí nikoliv jedné vybrané kamery, ale celého lokálního pohledu sestávajícího z libovolného počtu kamer. Příslušný lokální pohled je třeba vybrat ze seznamu.
- Volba Uživatelské tlačítko umožňuje přiřadit vybranému tlačítku joysticku libovolné uživatelské tlačítko. Tlačítko joysticku pak bude mít stejnou funkci jako spárované uživatelské tlačítko.
- Volba Přepnout zoom / fokus umožňuje uživateli pomocí tlačítka joysticku ovlivnit funkci jeho třetí osy (Z), která bude použita buď pro zoom nebo fokus vybrané kamery.

Kapitola 9 - Další nástroje

9.1. Osobní hlídač

Funkce Osobní hlídač umožňuje automatické hlídání poplachových situací a vytváří upozornění pro uživatele, pokud k nim dojde. Může se jednat např. o poplach při zjištěné vizuální podobnosti některých objektů jako je obličej či osoba na základě analýzy příslušných neuronových sítí. Funkce je dostupná z hlavní nabídky aplikace ze skupiny Nástroje.



Tlačítkem **PŘIDAT** lze tvořit nové hlídače až do jejich maximálního počtu. Na libovolnou pozici v každém hlídači je možné vložit objekt pomocí kontextové nabídky a volby Vložit. Zkopírovat objekt je možné v liště obličejů v dohledovém okně nebo v nástroji inteligentního vyhledávání.

Hlídač se aktivuje přepnutím přepínače nad názvem hlídače do aktivní polohy.

POZNÁMKA

Na rozdíl od událostí v systému, jsou upozornění tvořená hlídači zobrazována jen uživateli, který hlídače vytvořil.

Hlídače je možné přejmenovat dvojitým kliknutím na jeho název a může být odstraněn pomocí symbolu křížku po najetí myši na hlídače.

Pomocí ovládacího prvku Podobnost je možné zvýšit či snížit požadovanou podobnost nalezených objektů v živém videu z kamer. Čím nižší podobnost bude nastavena, tím více planých upozornění hlídače může vznikat.

9.2. Uživatelská tlačítka

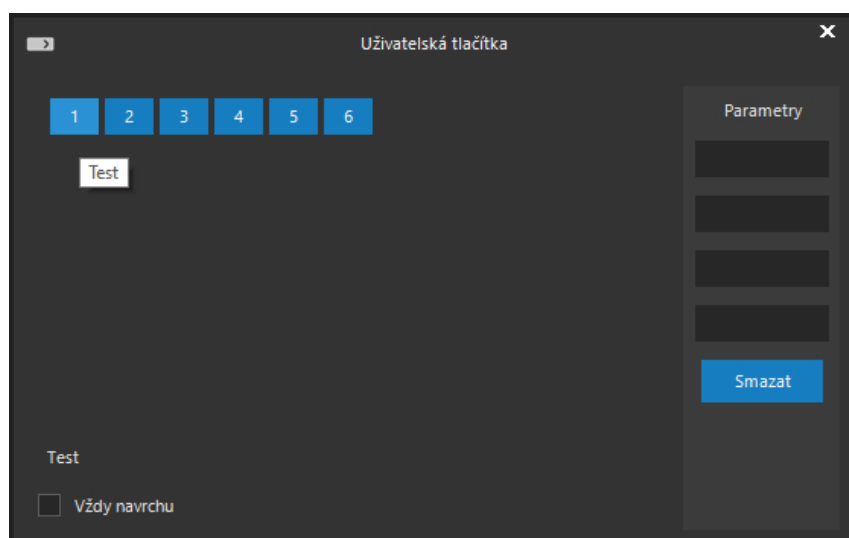
Administrátor má možnost v systému definovat uživatelská tlačítka. Uživatelská tlačítka jsou nástrojem pro spouštění vlastních akcí a příkazů přes protokol http nebo https a mohou sloužit k aktivaci rozšířených funkcí kamer či k obsluze celé řady externích zařízení. Okno s uživatelskými tlačítky je možné otevřít z hlavní nabídky aplikace ze skupiny Nástroje.

POZNÁMKA

Pokud administrátor v systému nevytvořil žádná uživatelská tlačítka, aplikace bude reagovat varovnou zprávou a další postup nebude možný.

POZNÁMKA

Pokud nemáte oprávnění k používání uživatelských tlačítek, aplikace bude reagovat varovnou zprávou a další postup nebude možný.



Tlačítka mohou být nastavena tak, že jsou zobrazena jejich čísla a popis v bublinách nad nimi anebo mohou zobrazovat popis přímo, v takovém případě budou tlačítka automaticky zvětšena.

Kliknutím na libovolné tlačítko bude automaticky spuštěna přednastavená akce. Uživatelé nemají přímý přístup ke tvaru http příkazu svázaného s danou akcí ani k přihlašovacím údajům, které mohou být pro vykonání příkazu potřeba. Při pohybu myši nad jednotlivými tlačítky se však uživatelům zobrazuje administrátorem definovaný popis akce, který by měl danou akci dostatečně charakterizovat. Popis se zobrazuje jednak v textovém řádku s názvem Popis, jednak také jako text v bublině nad tlačítkem.

POZNÁMKA

Pokud administrátor systému konfiguroval některá uživatelská tlačítka jako přepínače, zůstanou tato tlačítka po prvním stisku stisknutá a při dalším stisku budou opět uvolněna. Při stisknutí a uvolnění tlačítka se mohou spouštět různé akce.

POZNÁMKA

Při prvním otevření okna uživatelských tlačítek anebo v průběhu práce s ním je možné, že některá tlačítka konfigurovaná jako přepínače se automaticky přepnou do stisknutého stavu, protože jiní uživatelé tlačítko aktivovali.

Pokud administrátor vložil do tvaru příkazu speciální znaky pro podporu parametrů (blíže viz kapitoly o správě systému), může uživatel výsledný příkaz dodatečně upravit pomocí zápisu konkrétních hodnot do textových polí označených textem Parametry.

Pomocí zaškrtávacího políčka Vždy navrchu je možné okno přepnout do stavu, ve kterém nebude překryto žádnými jinými okny v systému, a uživatelé ho tak budou mít stále na očích.

POZNÁMKA

Pokud administrátorem vytvořený příkaz neobsahuje parametry, jejich uvedení v tomto okně nemá žádný efekt.

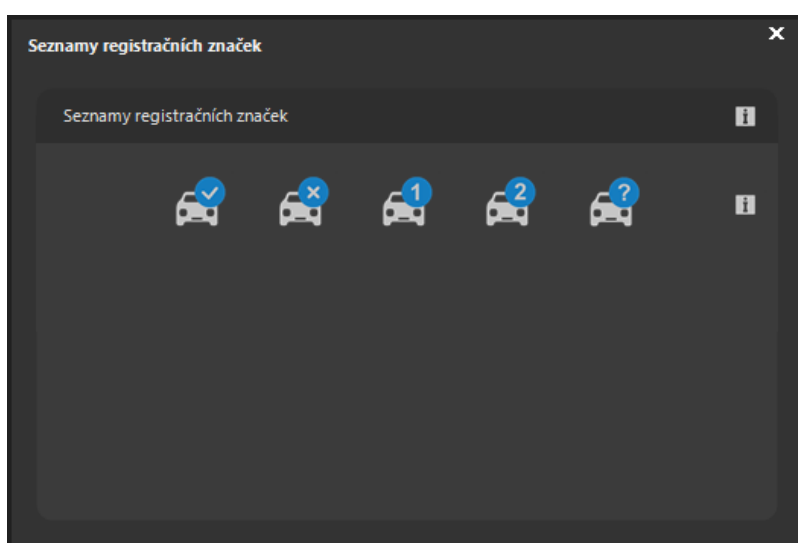
POZNÁMKA

Okno s uživatelskými tlačítky může být uloženo spolu s pracovním prostorem a při jeho načtení automaticky otevřeno v určeném místě.

9.3. Seznamy značek

Pokud má uživatel oprávnění Rozšířené funkce událostí, může z hlavní nabídky aplikace ze skupiny Nástroje otevřít okno pro práci se seznamy registračních značek vozidel.

Jednotlivá tlačítka umožňují pracovat se všemi seznamy registračních značek vozidel, přidávat či odebírat značky či testovat jejich zařazení do seznamu. Ovládání oken a práce se seznamy jsou zcela shodné, pokud jsou prováděny z části administrace systému, kde jsou tyto činnosti popsány v subkapitole Práce se seznamy RZ.



Kapitola 10 - Webový přístup

10.1. Spuštění a přihlášení do systému

Pro přístup k Vaším kamerám je možné také použít webový prohlížeč, který plně podporuje HTML 5. Pro správné fungování je nutné, aby prohlížeč bezchybně podporoval i všechna poslední rozšíření HTML 5 a související standardy až např. pro video v H265 formátu.

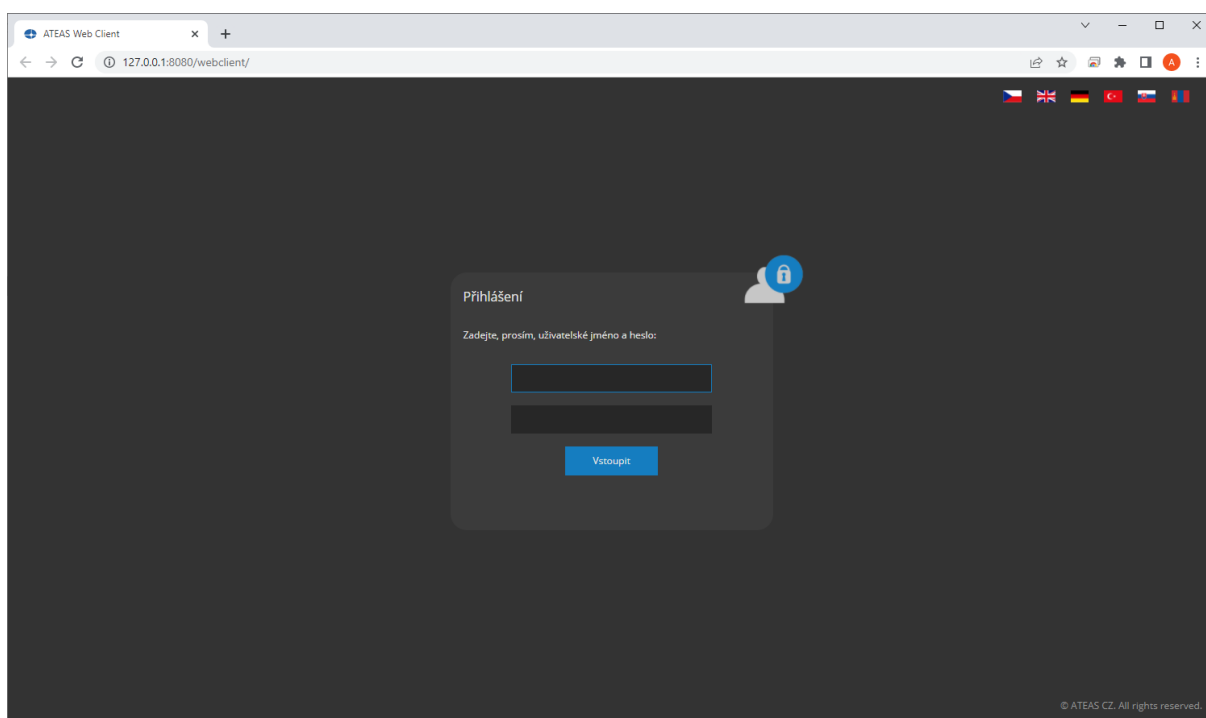
POZNÁMKA

Webový přístup do ATEAS Security je založen na standardu HTML 5, a pro jeho fungování tak není zapotřebí instalace jakýchkoliv doplňků a technologií jako je Flash, Silverlight nebo ActiveX.

Webového klienta je možné spustit pomocí odkazu přímo na webové stránce Vašeho administračního serveru anebo přímým zadáním jeho adresy do Vašeho prohlížeče. Tato adresa obsahuje adresu Vašeho administračního serveru doplněnou o /webclient/, tedy např. <http://127.0.0.1/webclient/>.

POZNÁMKA

Podle konfigurace, jakou zvolil administrátor systému, můžete být automaticky přesměrováni tak, aby byla použita zabezpečená verze protokolu http. Adresa tak bude začínat <https://>.



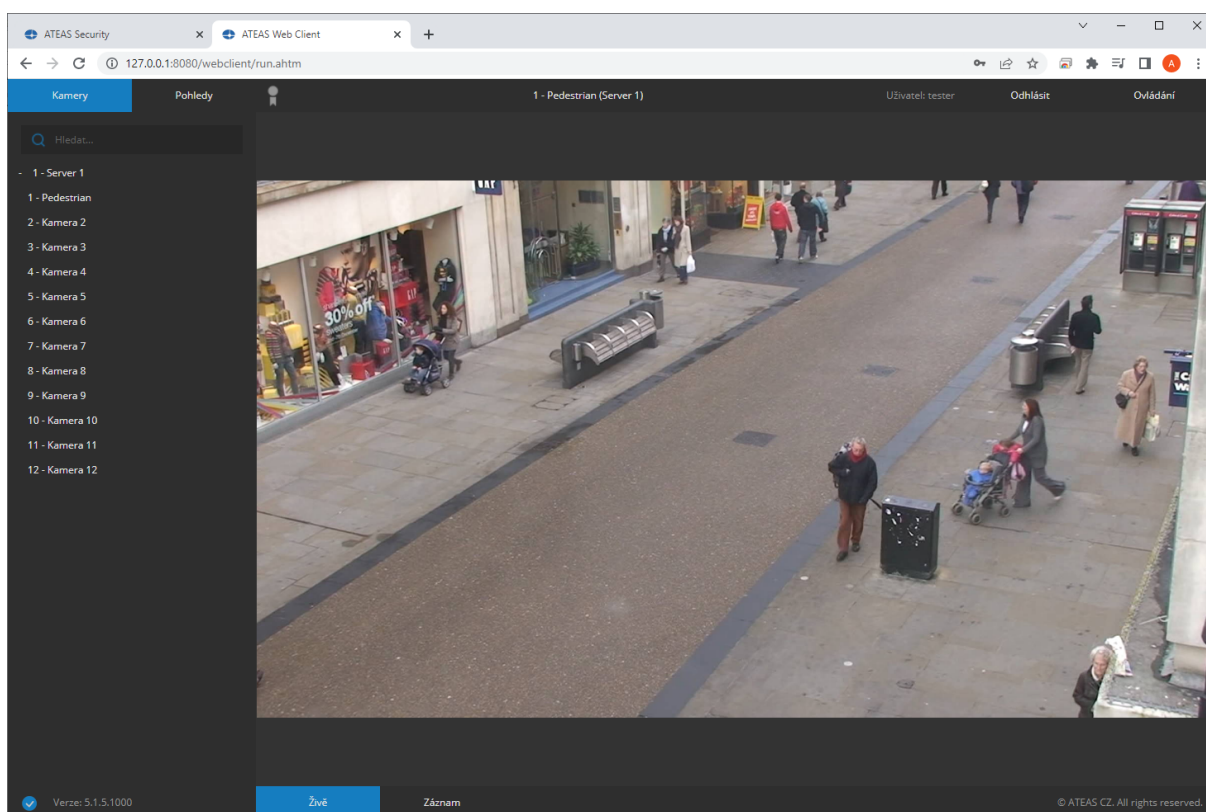
Na úvodní stránce je možné se přihlásit do systému. Pro zadání uživatelského jména a hesla platí shodná pravidla jako při přihlašování pomocí standardního ATEAS klienta. Pro změnu jazykového prostředí je možné použít ikony vlajek v pravém horním rohu okna.

POZNÁMKA

Pokud se pomocí uživatelského účtu přihlašujete poprvé nebo bylo Vaše heslo resetováno anebo vypršela jeho platnost, budete stejně jako v případě standardního klienta vyzváni ke změně Vašeho hesla. Nároky na délku a sílu hesla určuje administrátor systému.

10.2. Živý dohled

Po přihlášení do systému budete automaticky připojeni ke všem kamerovým serverům, ke kterým Vám byl zřízen přístup, a budete mít k dispozici všechny kamery (a pohledy kamer) v souladu s Vašimi oprávněními v systému.



V levé části okna je zobrazena stromová struktura kamerových serverů a k nim přiřazeným kamer. Pomocí odkazů Kamery a Pohledy se lze přepínat mezi stromovou strukturou serverů a pohledů. Pohledy mohou být administrátorem organizovány do skupin a mohou sestávat z mnoha kamer. Výběrem libovolné položky ze stromové struktury je možné přejít na zobrazení živého videa vybrané kamery či skupiny kamer v pohledu.

Pomocí vyhledávacího pole nad seznamem serverů a kamer lze provádět vyhledávání jak mezi servery, tak mezi kamerami. Je možné zadat více skupin znaků, vyhledávání fráze s mezerami je možné provést s použitím uvozovek.

POZNÁMKA

Stejně jako při práci v prostředí standardního klienta je pro náhled videa v pohledu více kamer použita sekundární snímková frekvence a pro náhled jedné kamery primární snímková frekvence. Tyto frekvence může zcela libovolně určit administrátor systému pro každou kameru.

POZNÁMKA

Přestože v průběhu práce v prostředí webového klienta zůstáváte na adrese Vašeho administračního serveru (např. na centrále), jednotlivá připojení ke kamerovým serverům vedou vždy nejkratší cestou a video data k Vám budou proudit přímo z kamerového serveru (např. přímo z Vaší pobočky).

Horní ovládací panel obsahuje odkaz Menu, pomocí kterého je možné stromovou strukturu ukrýt či znovu zobrazit pro zvětšení zobrazované plochy videa. Podobně funguje odkaz Ovládání, který zobrazuje a skrývá panel s dalšími funkcemi v pravé části okna.

Kromě těchto odkazů obsahuje horní ovládací panel také šedou či výraznou ikonu certifikátu. Po kliknutí na tuto ikonu se zobrazí informace o koncovém uživateli a partnerovi, který provedl instalaci. V případě certifikovaného partnera bude mít ikona výraznou barvu. Tyto informace jsou shodné s informacemi, které zobrazuje též standardní ATEAS klient. Bližší informace jsou uvedeny v kapitole Certifikované instalace.

Dále obsahuje název aktuálně zobrazené kamery či pohledu, jméno přihlášeného uživatele a odkaz pro odhlášení ze systému.

Spodní ovládací panel indikuje stav připojení k administračnímu serveru, zobrazuje verzi systému a obsahuje odkazy pro přepnutí mezi živým náhledem a prohlížením záznamu.

10.3. Funkce vybrané kamery

V režimu zobrazení jedné kamery, kterého docílíme buď přímým výběrem názvu kamery ze stromové struktury serverů a kamer anebo kliknutím do videa libovolné kamery v pohledu více kamer, je možné provádět další funkce pro aktuálně vybranou kameru.

POZNÁMKA

Při přepnutí z pohledu více kamer dojde automaticky k použití primární snímkové frekvence a může také automaticky dojít k úpravě rozlišení (v závislosti na nastavené hodnotě posunu kamery při zobrazení detailu).

PTZ ovládání a presety

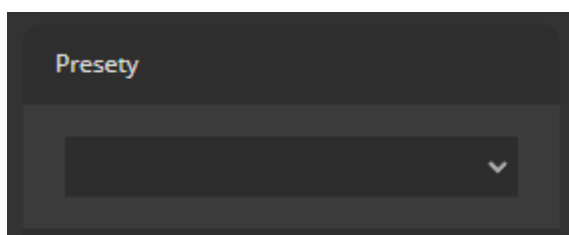
Pokud se jedná o otočnou kameru a máte-li příslušná oprávnění pro její ovládání, je možné dotykem či stisknutím a přidržením tlačítka myši kameru ovládat. Směr natáčení kamery je dán směrem od středu videa do aktuální pozice kurzoru myši. Rychlost pohybu je daná vzdáleností těchto bodů.

Ovládání zoomu kamery je možné jednoduše provádět pomocí kolečka myši.

POZNÁMKA

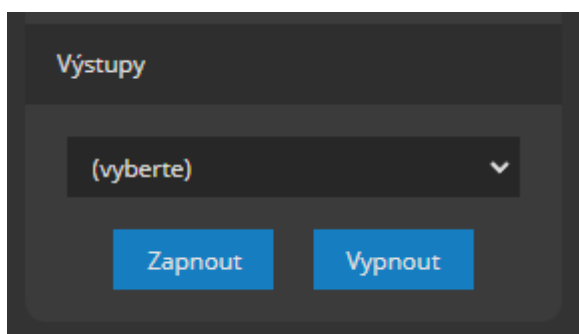
Možnost ovládat kameru v daném čase je samozřejmě také dána Vaší PTZ prioritou nastavenou pro vybranou kameru. Uživatelé s vyšší PTZ prioritou mohou kdykoliv ovládání kamery převzít nebo zamknout.

Pohyb kamery na předdefinovaný bod (preset) je možné provést zvolením presetu z rozbalovacího seznamu v ovládacím panelu v pravé části okna, který lze zobrazit či schovat pomocí odkazu Ovládání.



Aktivace výstupů

Má-li vybraná kamera výstupy připojeny na nejrůznější externí zařízení, je možné je prostřednictvím webového klienta aktivovat či deaktivovat pomocí tlačítek v ovládacím panelu v pravé části okna.



Po výběru daného výstupu z rozbalovacího seznamu je možné použít tlačítka **ZAPNOUT** a **VYPNOUT** pro jeho aktivaci či deaktivaci.

Uložení snímku

Pomocí ikony Sejmout snímek umístěné ve spodní části ovládacího panelu v pravé části okna je možné povést uložení snímku ve formátu JPEG z aktuálně zobrazovaného živého nebo zaznamenaného videa.

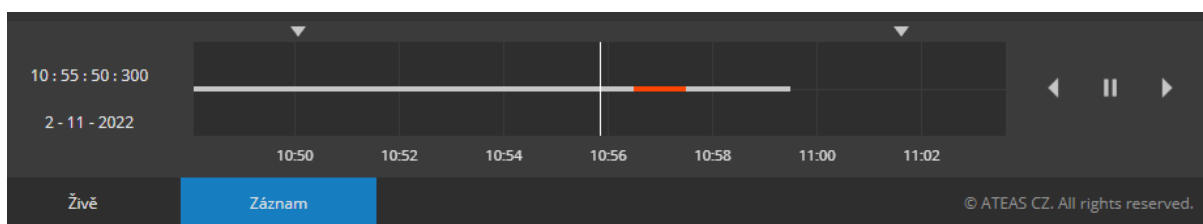
POZNÁMKA

Uložení snímku se může dle podpory této funkce Vaším prohlížečem projevit různě. Např. se může objevit nová karta prohlížeče se zobrazeným uloženým snímkem, který můžete následně ručně uložit, nebo se provede automatické stažení snímku do předdefinované složky prohlížeče.

10.4. Práce se záznamem

10.4.1. Přehrávání záznamu

Pomocí odkazů Živě a Záznam je možné provést přepínání mezi živým a videem a videem uloženým v záznamových oblastech serveru. Pro vybranou kameru se po přepnutí do přehrávání záznamu objeví pod videem náhled časové osy, která přehledně zobrazuje dostupné časové úseky, ve kterých probíhal běžný záznam (bílá barva), probíhal událostní záznam (červená barva) anebo neprobíhal žádný záznam (bez barvy).



Časovou osu lze intuitivně posouvat pomocí přetažení dotykem či myší. Při posouvání časové osy dochází k okamžité a plynulé synchronizaci video obsahu. Aktuální datum a čas přehrávání záznamu je zobrazen vlevo od časové osy. Vpravo jsou zobrazena tlačítka pro spuštění přehrávání směrem vzad, vpřed a pro zastavení přehrávání.

Rozlišení časové osy je možné měnit od zobrazení týdnů až po půlminutové úseky pomocí kolečka myši.

10.4.2. Export záznamu

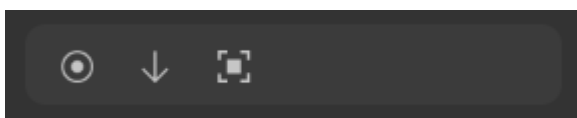
Pomocí pohyblivých šipek nad časovou osou přehrávání záznamu lze určit interval pro export. Vybraný úsek bude na kamerovém serveru exportován a připraven pro stažení a poté bude zahájeno stahování souboru ve formátu mp4 s podporou pro video i zvuk.

POZNÁMKA

Interval pro export musí být v rozmezí pěti vteřin až půl hodiny.

10.5. Nastavení klienta

Ve spodní části webového klienta je k dispozici panel s dodatečným nastavením pro práci s živým videem i záznamem, který obsahuje následující funkce.



Vedle základních funkcí je možné aktivovat upsampling videa, tedy jeho zobrazení ve větší velikosti než je nativní rozlišení videa v případě, že k tomu má webový klient prostor.

POZNÁMKA

Toto nastavení může být vhodné na monitorech s velmi jemným rozlišením (např. displeje Retina), kdy by se video v nativním rozlišení mohlo jevit malé.

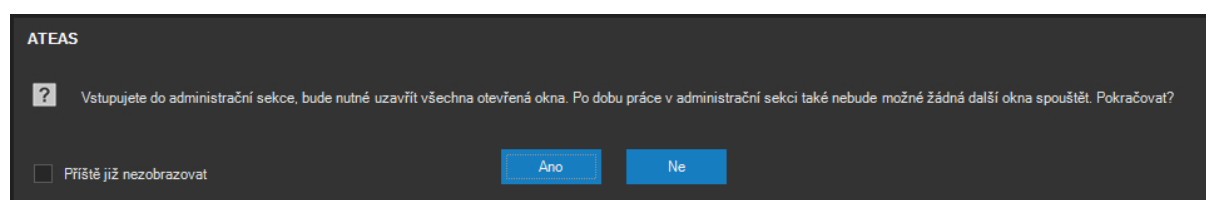
POZNÁMKA

I při aktivovaném upsamplingu videa však vždy zůstává zachován správný poměr jeho stran.

Kapitola 11 - Administrace systému

11.1. Vstup do administrační sekce

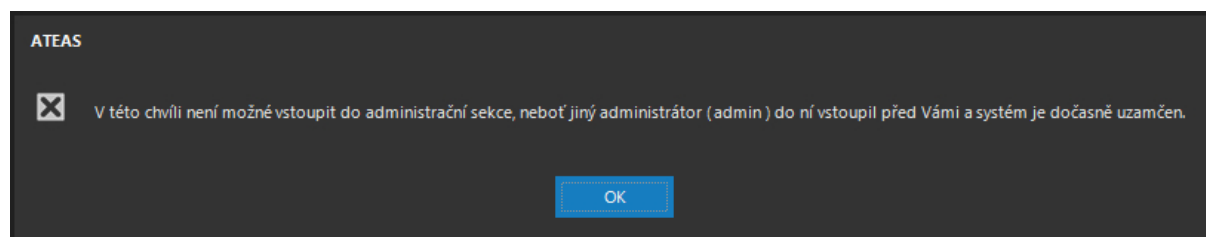
Do části aplikace, kde se provádí administrace systému, tj. do všech položek hlavní nabídky Administrace má přístup pouze uživatel zařazený ve skupině administrátorů. Uživatel ve skupině běžných uživatelů nemá administrační část přístupnou. Při vstupu do administrační sekce je nutné potvrdit následující zprávu.



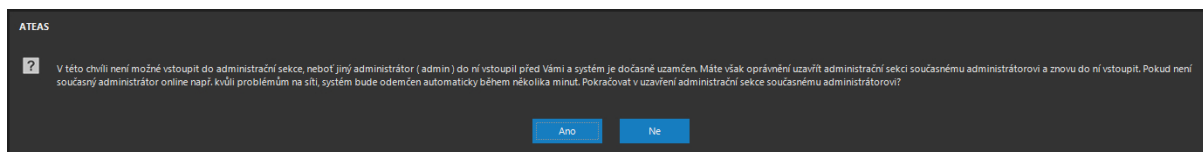
POZNÁMKA

Pokud nechcete, aby klient zobrazoval tuto zprávu při každém vstupu do administrační sekce, aktivujte volbu v levém spodním rohu okna. Znovu povolit zobrazování zpráv lze v lokálním nastavení klienta.

Po dobu práce s administračními panely nemohou být otevřena žádná jiná okna aplikace s výjimkou mapového ona. Do systému může být přihlášeno libovolné množství uživatelů a libovolné množství administrátorů (dle licenčního čísla). V jeden moment však může být v administrační sekci pouze jeden administrátor, pokud se do administrační sekce pokusí vstoupit jiný administrátor, systém mu přístup nedovolí a bude reagovat varovnou zprávou.



Výjimku tvoří master administrátor, tedy administrátorský účet s číslem 1, jehož specifika jsou blíže popsána v subkapitole o správě uživatelů. Master administrátor má oprávnění si vynutit vstup do administrační sekce i přesto, že v dané chvíli se v ní nachází jiný administrátor.



Po potvrzení zprávy na předchozím obrázku bude administrační sekce jiného administrátora automaticky uzavřena a bude mu několik sekund blokován opětovný vstup, tak aby master administrátor mohl administrační sekci získat pro sebe.

V obou předchozích případech je součástí zprávy i uživatelské jméno administrátora, který má aktuálně otevřenu administrační sekci systému.

Přestože v administrační sekci systému může být v jeden čas pouze jeden administrátor, privilegovaní uživatelé s příslušným oprávněním mohou současně provádět některá nastavení a konfiguraci systému počínaje např. nastavováním presetů kamer až po komplexní záležitosti typu úpravy pohybové detekce či analytických zdrojů událostí.

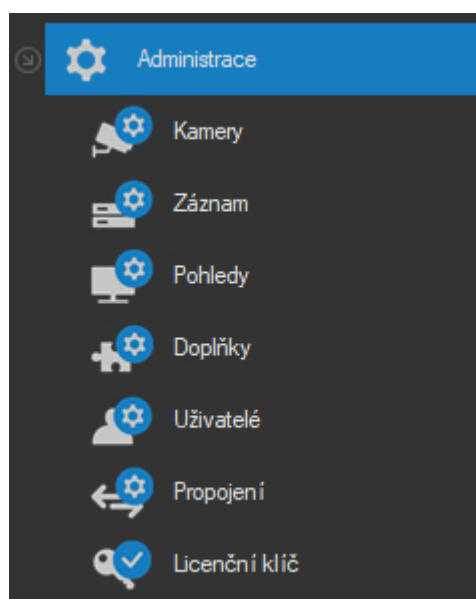
POZNÁMKA

Během administrace systému mohou ostatní klienti systému pokračovat v práci bez omezení. Některé změny, jako je přidávání či odebrání kamer, jsou jim online promítány.

POZOR

Systém umožňuje vzdálenou správu, pokud při vzdálené správě systému dojde např. k problémům na síti a aplikace je odpojena, bude možné do administrační části znovu vstoupit až po uplynutí ochranné doby (několik minut).

V administrační části se může administrátor pohybovat mezi jednotlivými částmi administrace systému přímo pomocí položek hlavní nabídky.



11.2. Správa kamer

11.2.1. Automatické vyhledání kamer na síti

Po volbě Kamery je administrační okno přepnuto do stavu, ve kterém je možné přidávat a odebírat kamery a video servery do či ze systému. Všechny kamery jsou do systému vždy připojeny prostřednictvím kamerového serveru (ATEAS Server), který je zodpovědný za záznam či vyhodnocování událostí. Na úvod přidávání či odebírání kamer je tak nutné vybrat z rozbalovacího seznamu Kamerové servery příslušný server, kterého se operace bude týkat.

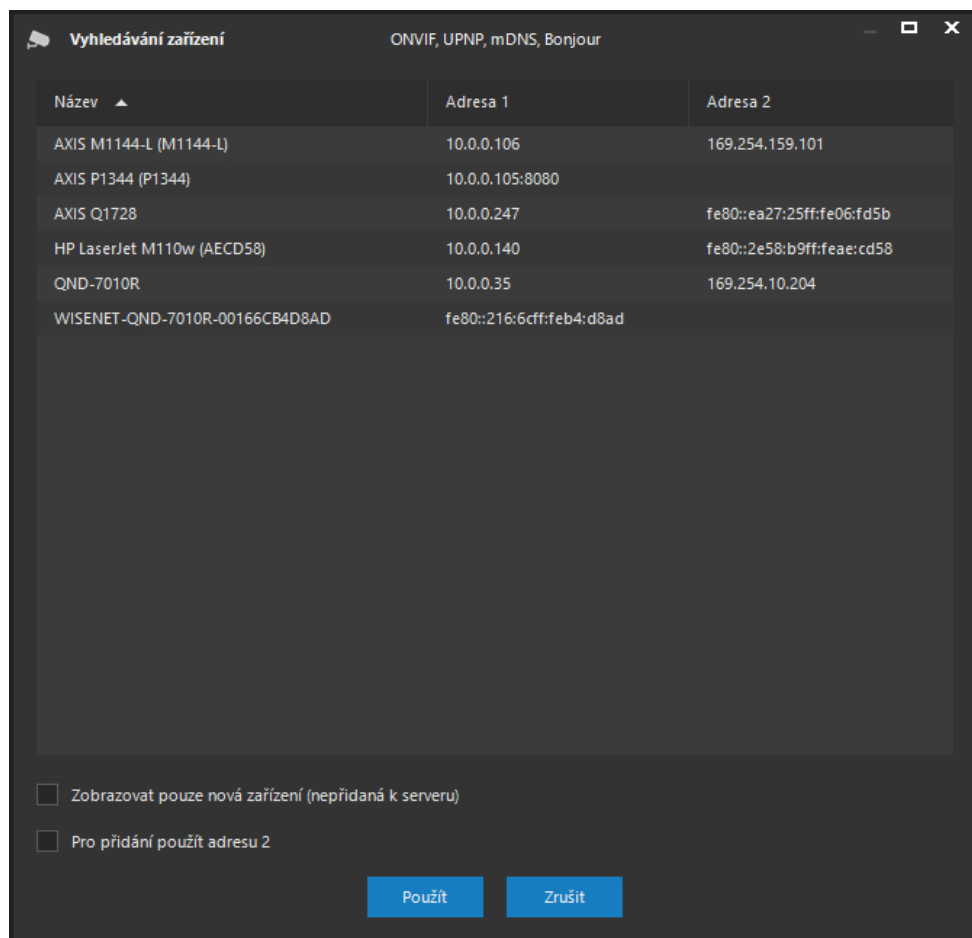
POZOR

Ve všech edicích ATEAS Security je nutné nejprve do systému vložit alespoň jeden kamerový server, ke kterému se budou vztahovat operace s kamerami. Přidávání kamerových serverů a určování profilu uživatele ke kamerovým serverům se provádí v části Uživatelé, která je popsána dále v této kapitole.

Přidání kamer do systému je velmi rychlé a jednoduché, lze ho navíc provádět hromadně a v automatickém režimu. Jednotlivé adresy či názvy kamer lze zadat ručně anebo je možné je vyhledat. Pro vyhledání slouží tlačítko **HLEDAT**, které je umístěno v části Přidat kamery. Po stisku tlačítka se zobrazí okno s vyhledanými kamerami.

POZNÁMKA

Automatické vyhledávání kamer v lokální síti je dostupné pro všechny typy kamer, které podporují standardy ONVIF (WS Discovery), UPNP (Universal Plug and Play), nebo mDNS (multicast DNS, Bonjour).



Seznam nalezených kamer obsahuje označení výrobce a modelu kamery a jejich adresu na síti. Seznam je automaticky a nepřetržitě aktualizován a doplňován o nově nalezené kamery. Pro některé kamery mohou být zobrazeny dvě různé adresy (může se např. jednat o IP adresu získanou pomocí DHCP serveru a adresu APIPA).

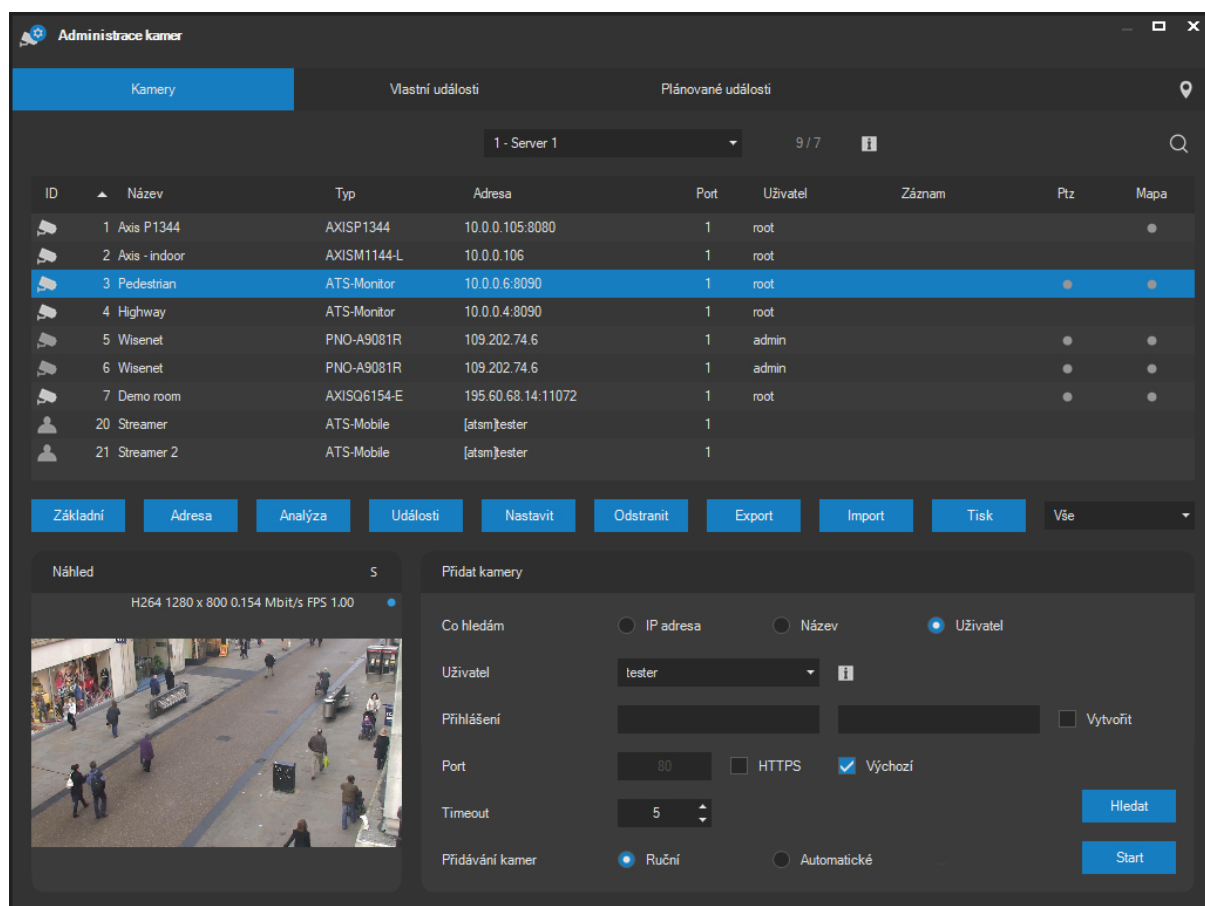
V seznamu kamer lze označit kamery, které mohou být v dalším kroku přidány ke kamerovému serveru. Pomocí tlačítka **POUŽÍT** jsou poté adresy všech vybraných kamer oddělené středníkem převzaty do pole Název v části Přidat kamery v základním administračním okně, kde lze pomocí tlačítka **START** kamery ihned přidat do systému.

Seznam kamer lze velmi efektivně zúžit pouze na kamery dosud nepřidané k aktuálně vybranému kamerovému serveru zaškrtnutím volby Zobrazovat pouze nová zařízení. To může být velká úspora při doplňování nově osazených kamer do systému.

POZOR

Aby mohlo správně fungovat vyhledávání přes UPNP, musí být při startu služby ATEAS Server v systému povolena služba SSDP vyhledávání (SSDP Discovery). Pro vyhledávání Onvif by měla být naopak zakázána služba Publikování prostředků rozpoznávání funkcí - Function Discovery Resource Publication, se kterou může být Onvif vyhledávání v kolizi.

11.2.2. Přidávání a odebírání kamer v systému



ID	Název	Typ	Adresa	Port	Uživatel	Záznam	Ptz	Mapa
1	Axis P1344	AXISP1344	10.0.0.105:8080	1	root			
2	Axis - indoor	AXISM1144-L	10.0.0.106	1	root			
3	Pedestrian	ATS-Monitor	10.0.0.6:8090	1	root			
4	Highway	ATS-Monitor	10.0.0.4:8090	1	root			
5	Wisenet	PNO-A9081R	109.202.74.6	1	admin			
6	Wisenet	PNO-A9081R	109.202.74.6	1	admin			
7	Demo room	AXISQ6154-E	195.60.68.14:11072	1	root			
20	Streamer	ATS-Mobile	[atasm]tester	1				
21	Streamer 2	ATS-Mobile	[atasm]tester	1				

Pod rozbalovacím seznamem se nachází seznam kamer aktuálně přiřazených vybranému kamerovému serveru. V části Přidat kamery je možné provést přidání nových kamer do systému. Pro každou kameru v seznamu jsou zobrazovány tyto údaje:

- identifikační číslo kamery (unikátní pro daný server),
- název kamery,
- typ kamery (či video serveru),
- IP adresa,
- port (implicitně 1, pro víceportové video servery může být vyšší),
- jméno uživatele pro přihlášení ke kameře,
- aktuálně přiřazené záznamové pravidlo,
- informace o tom, zdali je možné kameru ovládat,
- informace o tom, zdali je kamera lokalizována v mapě.

Seznam kamer je možné filtrovat podle typu připojení pomocí rozbalovacího seznamu vedle seznamu serverů. Vyhledávání v seznamu lze provést standardně pomocí klávesové zkratky CTRL-F anebo příslušným tlačítkem vpravo nad seznamem kamer.

Nad seznamem kamer se zobrazuje počet aktuálně přiřazených kamer k vybranému kamerovému serveru. V závorce je s předponou „lic“ uveden počet kamer, pro který je započtena kamerová licence. Tyto počty se mohou lišit, pokud je některá kamera přidána ke kamerovému serveru vícenásobně, více o této konfiguraci uvádíme dále v textu.

ATEAS uplatňuje systém licencování kamer per IP adresní bod, to znamená, že zařízení s jednou IP adresou spotřebují vždy jednu kamerovou licenci (včetně jejich vícenásobného přidání). To se vztahuje i na speciálních kamery s více objektivy nebo enkodérů s více video porty.

POZNÁMKA

Pokud však dvě různá zařízení sdílejí jednu IP adresu (a používají tak více síťových portů), je započteno více kamerových licencí.

Pro vybranou kameru se navíc ve spodní části okna zobrazuje náhled videa. Všechny sloupce v seznamu kamer mohou být použity pro rychlé seřazení kamer. Kliknutím do záhlaví sloupce lze seznam kamer seřadit vzestupně podle hodnot ve sloupci, opakovaným kliknutím se provede sestupné seřazení.

U náhledu videa jsou automaticky zobrazeny statistické údaje o formátu, rozlišení, snímkové frekvenci a šířce pásma videa. Náhled sekundárního streamu, pokud je konfigurován, lze provést aktivací symbolu S u náhledu videa.

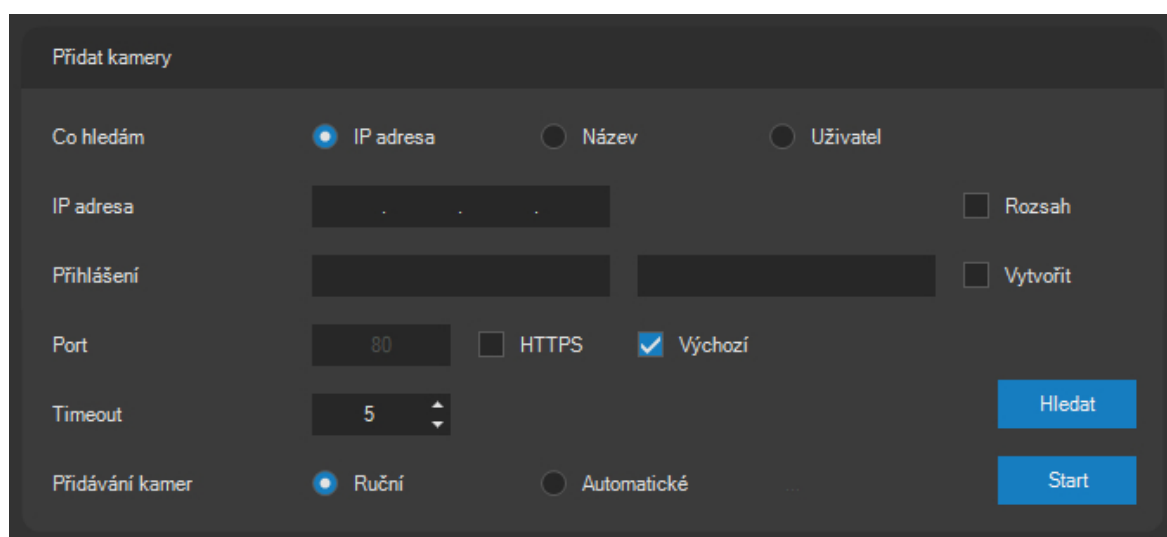
TIP

Tyto údaje lze také zobrazit přímo v dohledovém okně pro všechny kamery pomocí klávesové zkratky SHIFT-S.

První sloupec v seznamu kamer, který obsahuje číslo kamery, obsahuje také symbol kamery barevně odstupňovaný podle způsobu připojení kamery k serveru (nativní rozhraní výrobce, Onvif, pouze RTSP protokol). Zdroje videa jako jsou mobilní zařízení (např. chytré telefony s operačním systémem Android nebo iOS) anebo nositelné kamery (body worn) používají symbol uživatele.

Přidání kamer k vybranému kamerovému serveru

V části Přidat kamery je zapotřebí vyplnit potřebné údaje.



The screenshot shows a dark-themed dialog box titled "Přidat kamery". It has several sections:

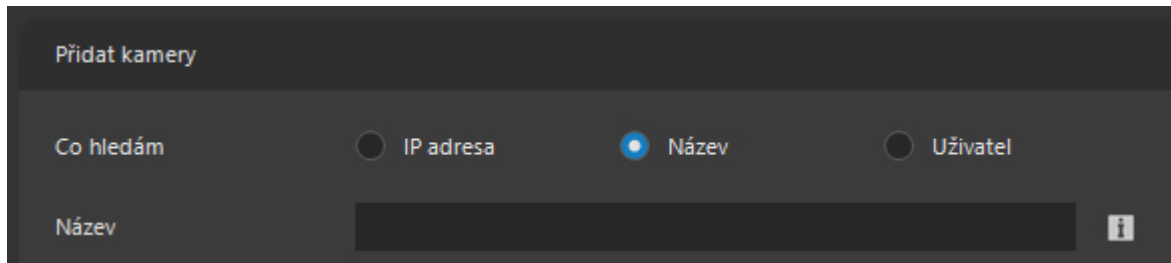
- Co hledám**: Three radio buttons: "IP adresa" (selected), "Název", and "Uživatel".
- IP adresa**: A text input field.
- Přihlášení**: A text input field.
- Port**: A text input field with "80" and a "HTTPS" checkbox.
- Timeout**: A spinner box with "5".
- Přidávání kamer**: Two radio buttons: "Ruční" (selected) and "Automatické".
- Buttons**: "Rozsah" checkbox, "Vytvořit" checkbox, "Hledat" button, and "Start" button.

V poli IP adresa je zapotřebí vyplnit IP adresu přidávaného zařízení. Pokud chcete najednou přidat více kamer, je možné zaškrtnout políčko Zadat rozsah. Tím se zobrazí ještě jedno pole pro zadání IP adresy a při přidávání kamer budou detekovány IP adresy v daném rozsahu od nižší po vyšší adresu.

POZNÁMKA

Pokud bude prohledáván daný rozsah IP adres vymezený dvěma adresami, smí se tyto adresy lišit pouze v koncovém čísle, jinak nebude přidávání spuštěno.

Alternativně lze k vybranému kamerovému serveru přidat také kameru pomocí názvu. Při zaškrtnutí volby Název se namísto vstupního pole pro IP adresu zobrazí textové pole pro zadání názvu kamery.



Zadávaný název nesmí obsahovat určení protokolu (http). Kamerový server podporuje též vyhledání názvu v systému DNS (Domain Name System) a přeloží ho na IP adresu. V databázi serveru však zůstává uložen vždy název zařízení. Pomocí názvů tak systém podporuje dynamické přidělování adres koncovým zařízením. Pokud jsou přidávána zařízení pomocí IP adres, lze provádět hromadné přidávání kamer pomocí určení rozsahu IP adres. Pokud je použita metoda přidávání kamer pomocí názvu, lze přidat více kamer současně tak, že mezi jejich názvy či IP adresy napíšete středník.

Při přidávání kamery pomocí názvu je také možné zadat adresu začínající protokolem rtsp://. V takovém případě bude přidán přímo RTSP video a audio stream na dané adrese, u kterého není vyžadována nativní ani Onvif podpora v zařízení.

Dalším protokolem, který je možné použít při přidávání pomocí názvu, je protokol file. Tímto způsobem lze přidat složku dostupnou pro kamerový server (např. na jeho lokálním disku). Pokud tato složka obsahuje soubory typu ats nebo mp4, bude automaticky přehráván jejich obsah, jako kdyby se jednalo o zdroj živého videa a zvuku. Soubory budou přehrávány v abecedním pořadí a po dosažení posledního souboru opět od začátku.

Každá kamera přidaná s protokolem file bude mít také automaticky vytvořeny výstupy pro ovládání přehrávání, zejména akce zpět a vpřed pro posun mezi soubory spolu s možností pozastavit a spustit přehrávání.

POZNÁMKA

Některé typy ats a mp4 souborů nemohou být přehrávány. Týká se to zejména ats souborů obsahující více kamer či mp4 souborů využívající fragmentaci či atomy typu ctts.

TIP

Pokud je ats soubor ochráněn heslem, lze ho otevřít tak, že složku přidáme s konkrétním heslem nebo ho dodatečně změníme.

Do polí Uživatel a heslo je zapotřebí zadat platné uživatelské jméno a heslo pro přihlášení ke kameře či video serveru, pokud je nutná autentizace. Tyto přístupové údaje bude kamerový server používat při přístupu ke kameře, pro uživatele nebudou tyto přihlašovací údaje viditelné. Pro zařízení Onvif je k dispozici také možnost zřízení administrátorského uživatelského účtu v kameře při prvním přidání kamery do systému.

POZNÁMKA

Je vhodné použít přístupové údaje na úrovni administrátora, aby byl zajištěn přístup kamerového serveru ke všem funkcím kamery či video serveru.

V poli HTTP port je možné zadat jiné číslo portu než je implicitní (80), pokud je takto kamera nastavena, nebo pokud bude kamerový server ke kameře přistupovat přes směrovač s aktivovaným NAT.

POZNÁMKA

Pokud přidáváte kamery podle názvu a součástí názvu je i označení portu, port v názvu bude mít přednost před portem zvoleným v poli HTTP port.

Pokud aktivujeme volbu https, bude kamera přidána rovnou pomocí zabezpečeného připojení. V takovém případě musí být pochopitelně kamera schopna komunikace pomocí protokolu https.

POZNÁMKA

Pokud je kamera přidána s aktivovanou volbou https, bude v jejím nastavení automaticky aktivována volba Používat HTTPS a zároveň také bude zvoleno preferované RTSP schéma RTP (HTTP, TCP), neboť použití protokolu https automaticky předpokládá využití protokolu http.

Poslední volbou v řádku Co hledám je volba Uživatel. Pokud do systému přidáme kameru pomocí jména uživatele, bude mít tento uživatel možnost vysílat do systému video ze svého mobilního zařízení, pokud je zařízení (telefon, tablet) vybaveno kamerou. Tuto funkci je možné vhodně využít k archivaci video dat z mobilních zařízení používaných bezpečnostními pracovníky v terénu a na podporu rozhodování operátorského pracoviště. Více informací k této funkci naleznete v kapitolách o jednotlivých mobilních klientech.

POZNÁMKA

Při přidávání této mobilní kamery není nutné zadávat údaje pro přihlášení, podmínkou pro autentizaci bude přímo přihlášení uživatele z mobilního zařízení do systému.

POZNÁMKA

Po přidání mobilní kamery je možné s ní zacházet stejně jako s jinými kamerami v systému. Můžete tedy např. měnit její rozlišení, nastavit jinou než výchozí hodnotu komprese videa anebo aktivovat zvuk (v takovém případě bude spolu s videem přenášen též zvuk z mikrofону mobilního zařízení).

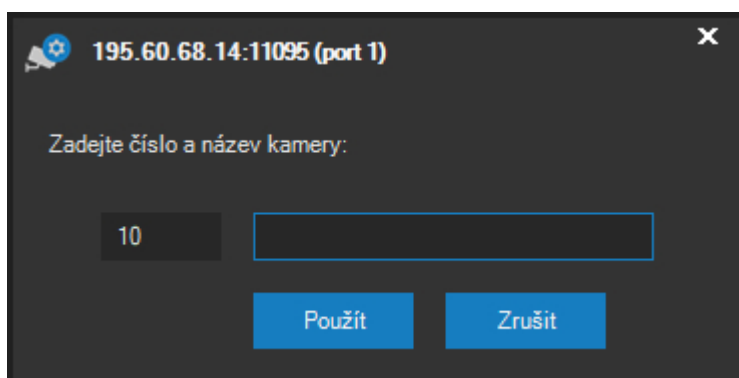
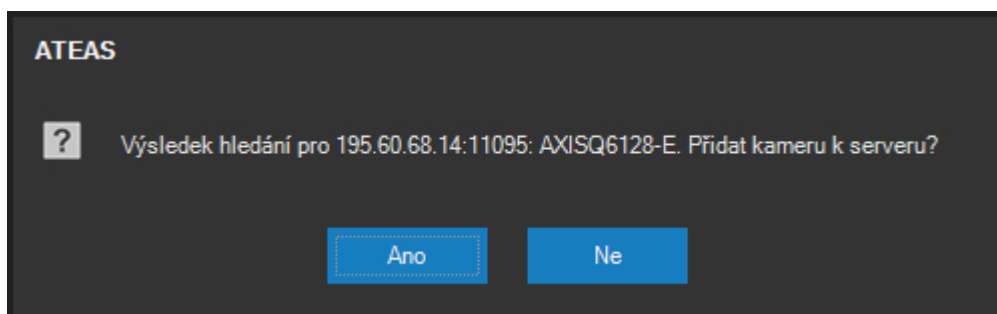
Operátor může současně sledovat video z více kamer mobilních zařízení. V praxi je ovšem důležitý okamžik, kdy uživatel mobilního zařízení vysílání zahájí, neboť to může znamenat důležitou okolnost. Zahájení vysílání je možné velmi jednoduchým způsobem propojit s událostním řízením tak, že na daném kamerovém serveru vytvoříte vlastní událost s názvem MOBILECAMERA a pro danou kameru aktivujete v plánovači sledování této události. Při zahájení vysílání se poté jako obvykle přehraje nastavený událostní scénář. V nejjednodušším případě se tedy např. zobrazí video z této kamery automaticky na monitoru operátora.

POZNÁMKA

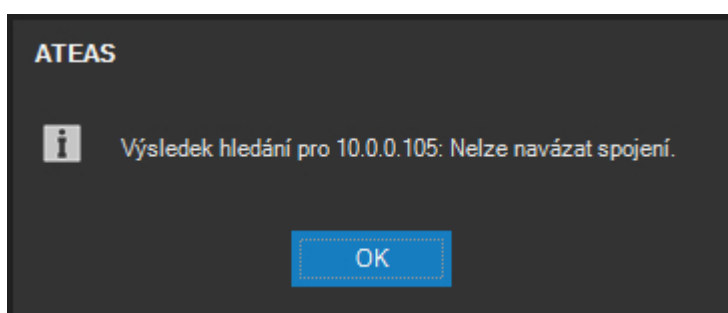
Možnost využití kamer mobilních zařízení je dostupná až od edice ATEAS Security PROFESSIONAL.

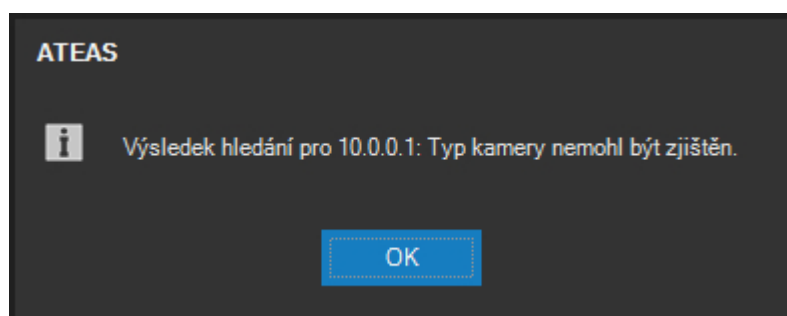
Při ručním přidávání bude pro každou detekovanou IP adresu zobrazena zpráva s výsledkem detekce s otázkou, zdali si uživatel přeje kameru do systému přidat, dále dotaz na číslo a název kamery a také zpráva o výsledku přidání kamery do systému. Při ručním přidávání je vždy navrženo první volné číslo kamery rovné nebo vyšší než 1 nebo nastavené počáteční číslo kamery v dialogu možností přidávání.

Proces přidávání kamer je nutné zahájit tlačítkem **START**. Tlačítkem **RESET** lze všechny parametry přidávání kamer vrátit na výchozí hodnoty. Kdykoliv během prohledávání segmentu sítě a přidávání nalezených kamer lze stisknout tlačítko **STOP**, které ukončí prohledávání.



Při detekci IP adresy může také dojít k situacím, kdy nebude možné během nastaveného času v poli Timeout (ve vteřinách) navázat spojení, nebo nebude možné rozpoznat typ kamery. V takovém případě je nutné prověřit dostupnost zařízení na dané adrese.





Při ručním přidávání kamer je vždy prováděna kontrola, aby zadané číslo kamery nebylo duplicitní, aplikace neakceptuje zadání již existujícího čísla kamery.

POZNÁMKA

Čísla kamer mohou být přidělována v rozsahu 1 – 999 s celkovým maximálním počtem 999 kamer na jednom serveru.

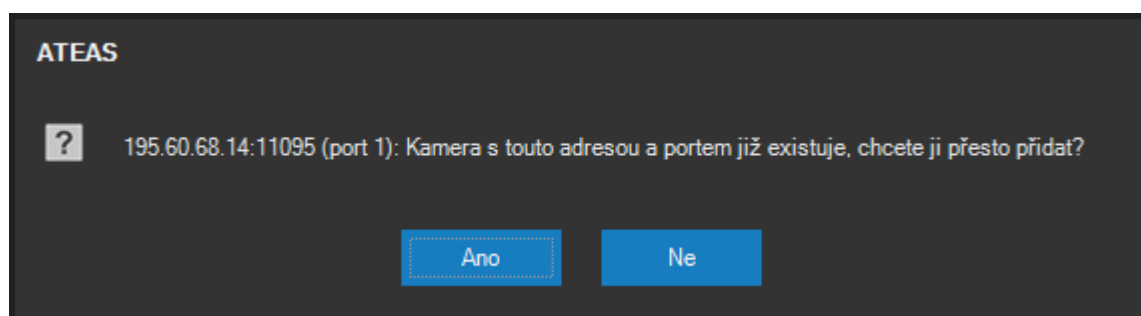
POZNÁMKA

Po dokončení procesu přidávání kamer jsou všechny nově přidané kamery automaticky vybrány, a je tak možné ihned pokračovat v jejich nastavení.

Díky vlastnostem ATEAS Security jako je flexibilní adaptace datových toků na podmínky v síti si lze v drtivé většině případů vystačit s definicí jednoho formátu videa a jeho nastavením pro každou kameru s tím, že ATEAS servery dále modifikují snímkovou frekvenci videa při distribuci klientům (viz koncept primární a sekundární snímkové frekvence) včetně multicastového vysílání. Pro další flexibility lze kamery k serveru přidat vícekrát.

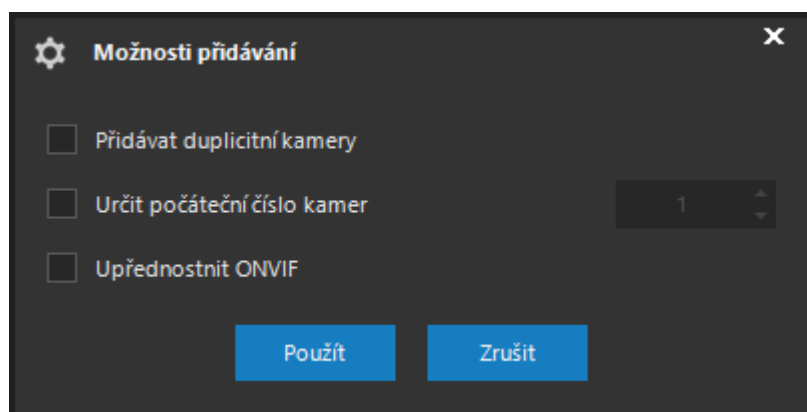
Při využití vícenásobného přidání jedné kamery či video serveru k jednomu kamerovému serveru nedochází k čerpání více kamerových licencí. Pokud je tedy do systému přidáno zařízení se stejnou adresou či názvem vícekrát, bude obsazena pouze jediná kamerová licence.

Výše popsané konfigurace lze docílit tak, že vybrané kamery jsou ke kamerovému serveru přidány vícekrát (počet není omezen) a každá kamera je poté jinak nastavena. Při ručním přidání kamery, která je již ke kamerovému serveru připojena, je zobrazena varovná zpráva, aby k této skutečnosti nedocházelo nedopatřením.



Pokud je na dané IP adrese detekován víceportový video server, interaktivní přidání kamery proběhne pro daný video server v počtu odpovídajícím všem portům, tj. u čtyřportového video serveru bude možné přidat až čtyři nové kamery do systému. Toto se však týká pouze víceportových video serverů, které pracují na jedné IP adrese.

Při automatickém přidávání kamer do systému neprobíhá žádná interaktivní komunikace s administrátorem. Daná IP adresa (případně celý rozsah) je prohledán a v případě úspěšné detekce kamery je tato automaticky přidána do systému s prvním volným číslem kamery a s implicitním názvem. Název je možné kdykoli později změnit. Implicitně nejsou v automatickém režimu přidány kamery vícenásobně, což umožňuje flexibilně prohledávat celé segmenty sítě a přidat vždy jen nové kamery. V mnoha případech však budeme chtít v automatickém režimu přidat kamery též duplicitně (např. při párování kamer) a také určit počátek, od kterého má začít automatické číslování. To vše můžeme nastavit v dialogu možností přidávání, který lze aktivovat pomocí tlačítka se symbolem tří teček.



Pomocí volby Přidávat duplicitní kamery můžeme určit, zdali budou v režimu automatického přidávání kamer přidány kamery vícenásobně. Dále lze také určit počátek pro automatické číslování kamer.

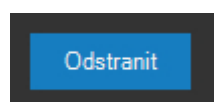
POZNÁMKA

Pokud se při automatickém číslování narazí na již obsazené číslo kamery, je vždy zvoleno nejbližší vyšší volné číslo. Pokud by takové číslo přesáhlo nejvyšší povolenou hodnotu 999, kamera nebude přidána.

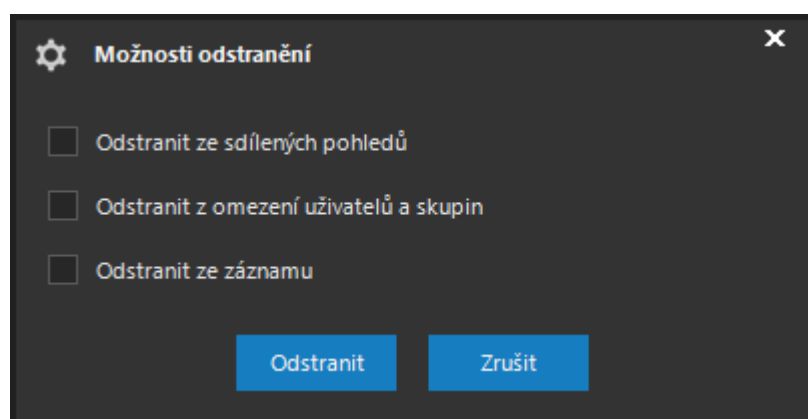
Dialog také obsahuje volbu, pomocí které je možné upřednostnit přidání kamery pomocí rozhraní ONVIF, pakliže by kamera byla jinak přidána přednostně pomocí nativního rozhraní výrobce kamery.

Odebrání kamery

Libovolnou kameru lze od serveru odebrat pomocí tlačítka **ODSTRANIT**.



Při odstranění jsou kamery odstraněny kompletně tedy včetně např. jejich akcí v událostních scénářích apod. Při odstranění je možné dále zvolit rozsah, v jakém bude odstranění provedeno.

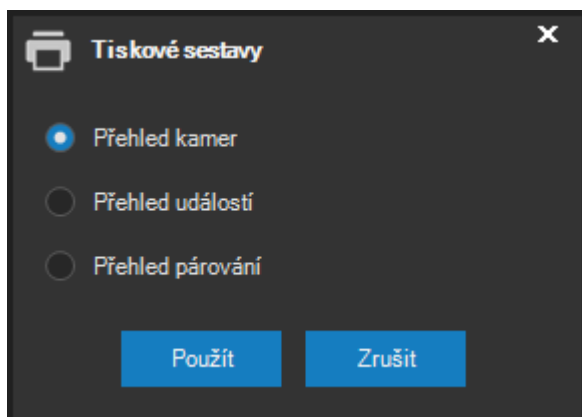


POZOR

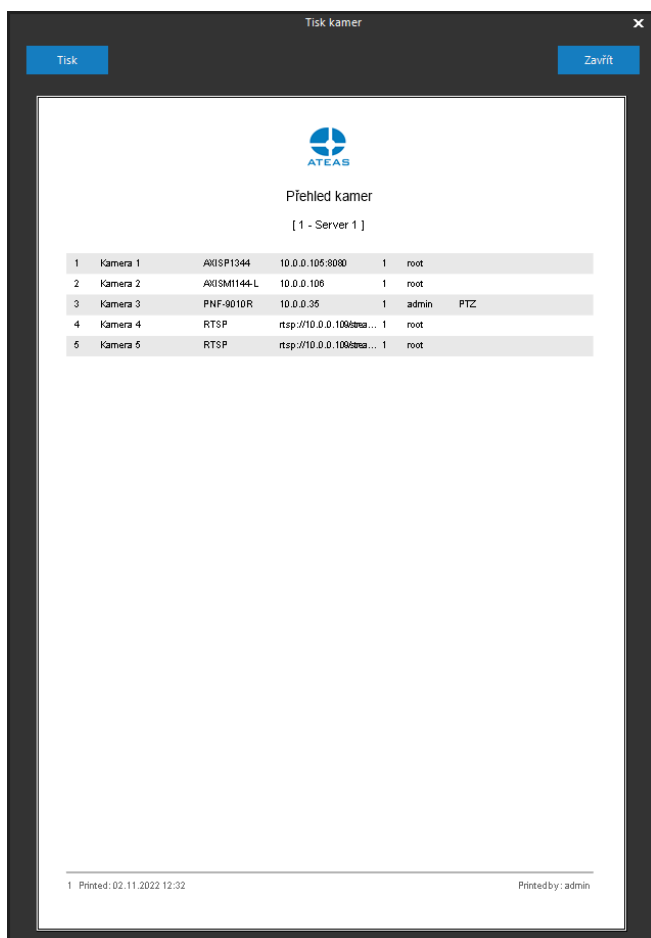
Odstranění ze záznamu je pouze metadatovou operací. Data odstraněných kamer lze obnovit připojením existující záznamové oblasti.

Tiskové sestavy kamer

Pomocí tlačítka **TISK** lze pro vybraný kamerový server vytisknout aktuální seznam všech kamer včetně základních parametrů, které jsou zobrazeny v seznamu na obrazovce. K dispozici jsou i další tiskové sestavy.



Tisková sestava Přehled kamer vytiskne výše zmíněný přehled všech kamer připojených k aktuálně vybranému kamerovému serveru.



Sestava Přehled událostí obsahuje seznam všech aktivních zdrojů událostí a událostních scénářů, které jsou při vzniku události spuštěny.

Sestava Přehled párování obsahuje informace o párování vícenásobně přidáných kamer mezi sebou, tj. informace o nastavení posunu čísla kamery při zobrazení detailu a zobrazení záznamu. Pro záznam jsou zobrazeny jednak posuny pro samotné zobrazení záznamu, jednak pro generování video náhledu (např. v dohledovém okně). Chybně nastavené posuny jsou navíc automaticky barevně zvýrazněny.

POZNÁMKA

Pomocí sestav Přehled událostí a Přehled párování lze velmi efektivně provádět kontrolu nastavení zejména větších systémů.

11.2.3. Podpora grabovacích karet

Pomocí speciálního schématu protokolu CAPT lze k serveru připojit i kamery v podobě vstupů některých grabovacích karet umístěných v počítači s nainstalovaným kamerovým serverem. Důvodem pro využití karet může být minimální latence při digitalizaci analogových anebo HDMI video vstupů. Pro přidání takové kamery se použije přidání pomocí názvu ve formátu:

```
capt://device:port[:gpu]
```

kde

device je číslo zařízení v počítači, je dáno pořadovým číslem anebo výrobcem,
port je číslo vstupu na grabovací kartě, je dáno pořadovým číslem vstupu,
gpu je index GPU od nuly výše, které bude použito pro kódování videa.

Parametr GPU není povinný a při jeho vynechání bude GPU přiřazeno automaticky.

POZNÁMKA

Bez GPU, jehož akcelerace bude použita pro kódování videa, nebude možné grabovací kartu využívat. Pomocí GPU akcelerace bude video kódováno do formátu H264 s nastavením pro minimální latenci.

Pro grabovací karty je v části administrace kamer v nastavení videa možné ovlivnit některé parametry jako je snímková frekvence nebo maximální datový tok, který ovlivňuje kvalitu videa při kódování.

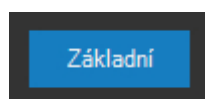
11.2.4. Základní nastavení kamery

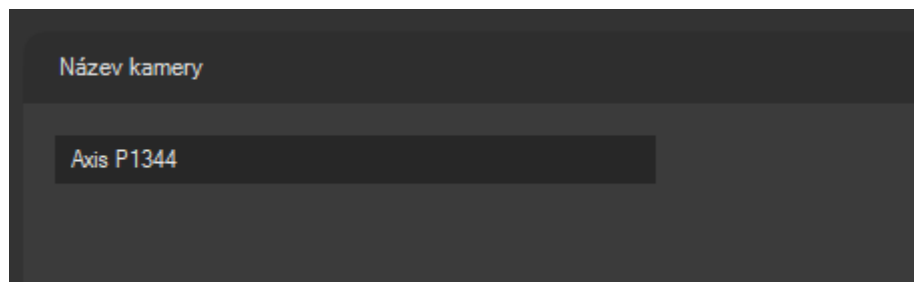
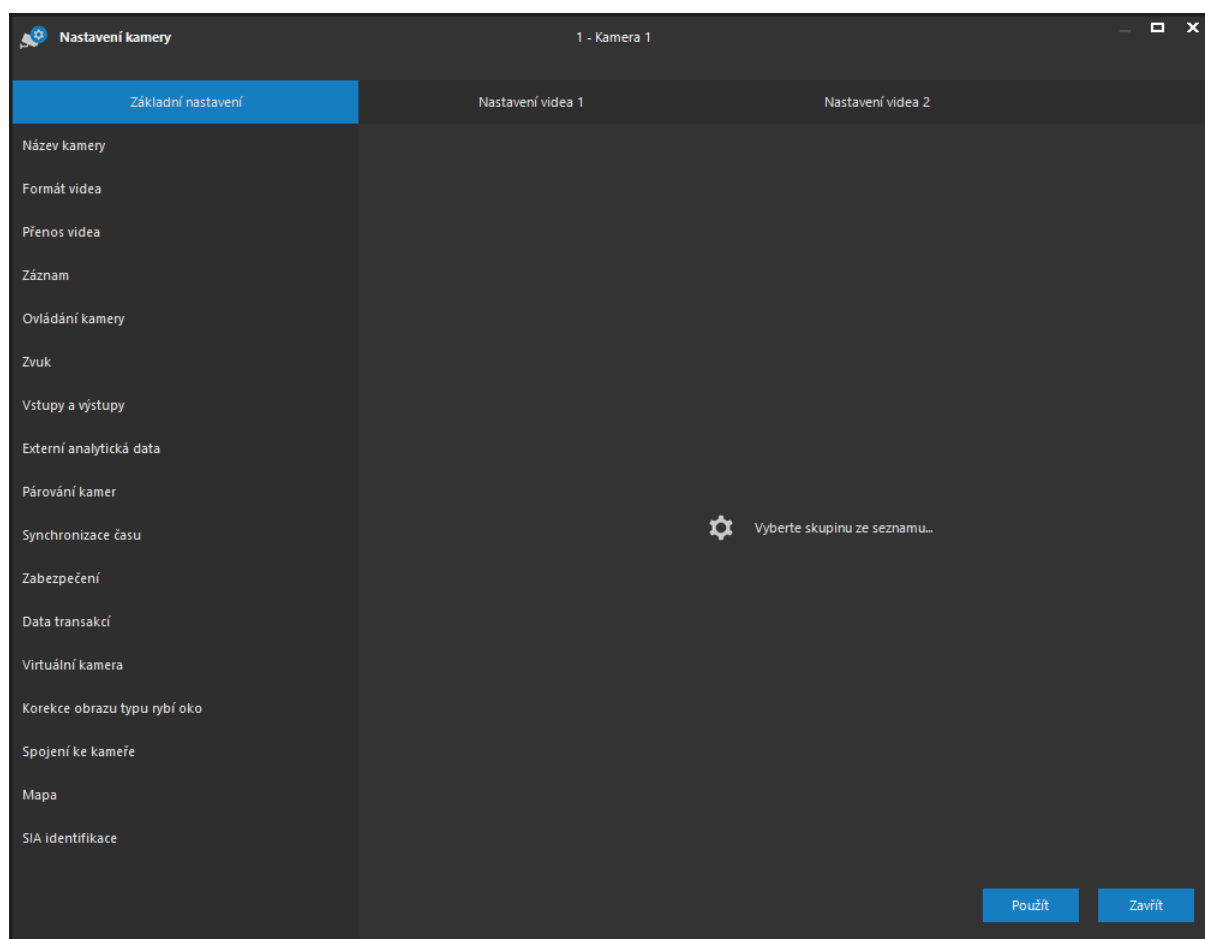
U vybrané kamery lze provádět rozsáhlá nastavení. Do sekce nastavení kamery lze vstoupit po stisku některého tlačítka ze skupiny tlačítek Nastavení.



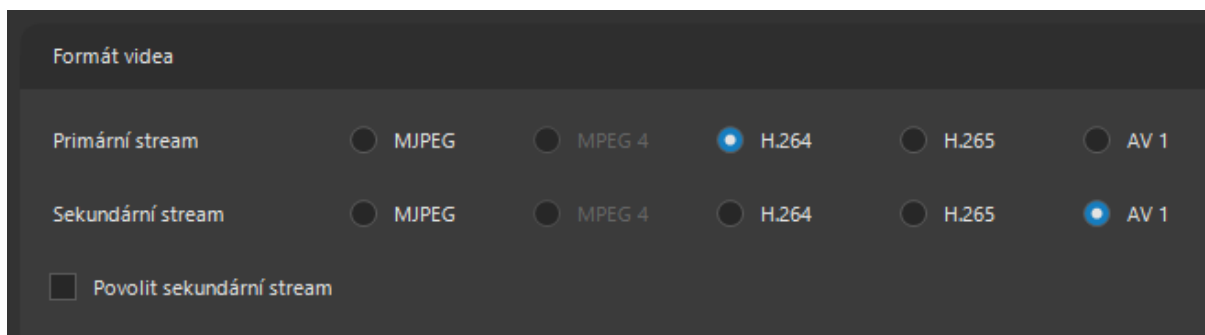
Základní nastavení kamery je vždy uloženo na aktuálním kamerovém serveru, nastavení detekce pohybu je ukládáno kombinovaně na kamerovém serveru či přímo v zařízení. Nastavení událostního řízení je poté uloženo jak na kamerovém serveru (nastavení událostních zdrojů), tak na administračním serveru (událostní scénář). V každém případě je nastavení velmi snadné a intuitivní, ukládání nastavení v dané části systému je automatické. Veškerá nastavení se provádí v samostatných oknech, tomu odpovídají i jednotlivé subkapitoly.

Do základního nastavení lze vstoupit stiskem tlačítka **ZÁKLADNÍ**. Při opakovaném otevření tohoto okna bude automaticky aktivována naposledy používaná sekce.





V části **Název kamery** lze upravit název vybrané kamery zápisem do textového pole. Limit pro název je až 60 znaků, nicméně příliš dlouhé názvy nemusí být při určitých rozvrženích pohledů a v jiných částech aplikace zobrazeny celé, skrytá část může být nahrazena tečkami.

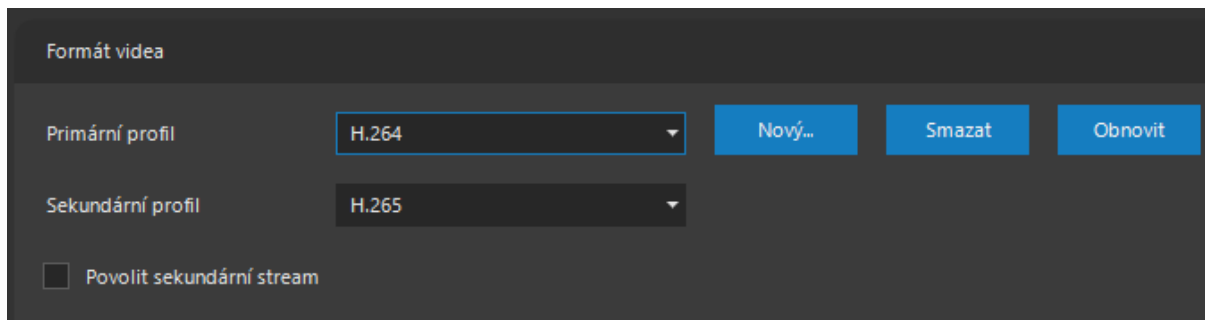


Formát videa lze podle možností kamery nastavit na formát MJPEG, MPEG4, H264, H265 nebo AV1 pro primární a sekundární stream. Sekundární stream není po přidání kamery aktivní, jeho aktivaci je nutné provést pomocí volby Povolit sekundární stream.

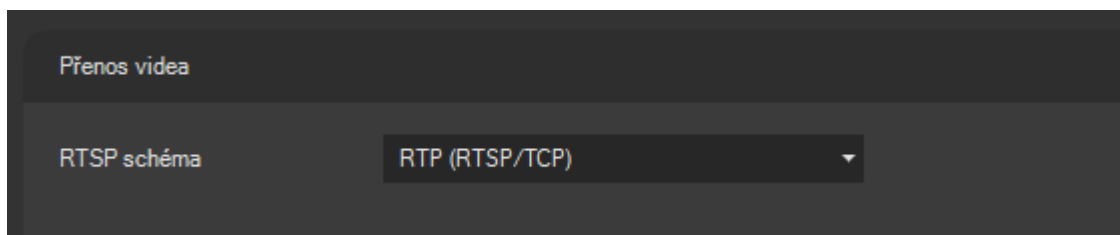
TIP

Sekundární stream lze použít např. pro pohledy s více kamerami, záznam, pokud není aktivní událost, anebo pro video analýzu.

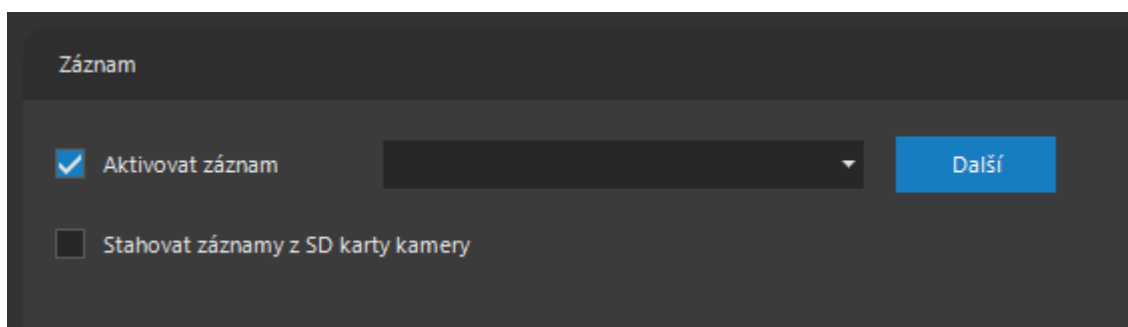
Část nastavení Formát videa je však odlišná, pokud je právě nastavovaná kamera (či výběr kamer) připojena namísto proprietárního rozhraní pomocí Onvif.



Namísto volby video formátu je k dispozici rozbalovací seznam profilů, které jsou načteny přímo ze zařízení a které obsahují veškerá nastavení video a audio formátu. Zařízení podle specifikace Onvif nabízí přednastavené profily připravené pro nejčastější situace a využití. Pomocí tlačítka **OBNOVIT** vedle seznamů profilů je možné kdykoliv provést aktualizaci profilů přímo ze zařízení. Je možné vybrat různé profily pro primární a sekundární stream. Tlačítka **NOVÝ** a **SMAZAT** slouží k vytvoření nového či odstranění profilu. Jejich změny lze provést v částech nastavení videa.

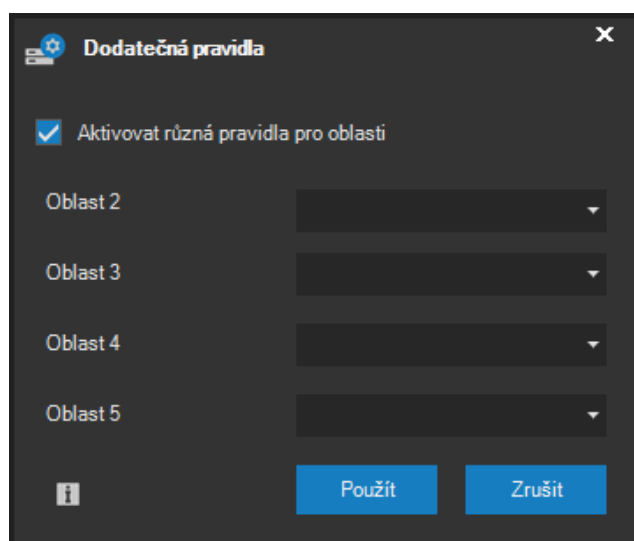


V části **Přenos videa** je možné nastavit preferované schéma pro přenos dat pomocí protokolu RTSP a RTP. Ve všech případech se jedná o přenosy typu unicast, neboť multicastové vysílání je schopen pro všechny formáty provádět sám kamerový server s výhodami z toho vyplývajícími. Více viz kapitola o správě uživatelů a nastavení profilu uživatele ke kamerovému serveru, který může využítí multicast vysílání automaticky iniciovat.



V části **Záznam** je možné kameře přiřadit určitý záznamový profil, který obsahuje veškeré informace o tom, jak bude obraz či zvuk dané kamery zaznamenáván. Záznamové profily se tvoří v části administrace záznamu (kde je jejich vytváření také popsáno) a jsou způsobem, jak velmi jednoduše nastavit pro kameru všechna pravidla nahrávání. Kamery mohou záznamové profily sdílet nebo mohou mít své vlastní profily.

Pokud je pro vybrané kamery aktivován záznam do více oblastí současně, můžete pomocí tlačítka vedle seznamu pravidel záznamu zobrazit dialog, ve kterém lze pro každou záznamovou oblast zvolit jiné pravidlo záznamu. Tímto způsobem lze např. pořizovat záznam ve vyšší kvalitě, který bude k dispozici několik dní a současně záznam v nižší kvalitě, který bude k dispozici výrazně delší dobu.



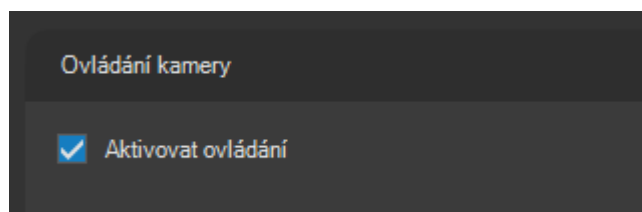
POZNÁMKA

Pokud je pro vybrané kamery aktivován záznam do více oblastí současně a nejsou specifikována různá pravidla pro záznam, bude pro záznam do všech oblastí použito výchozí pravidlo zvolené v okně Základní nastavení kamery.

POZNÁMKA

Pokud pro daný časový úsek existuje záznam ve více oblastech, je klientům poskytnut vždy záznam z oblastí s nižším číslem. Nižší čísla záznamových oblastí tedy mají prioritu, měly by tudíž vždy obsahovat záznam ve vyšší kvalitě než oblasti s vyšším číselným označením.

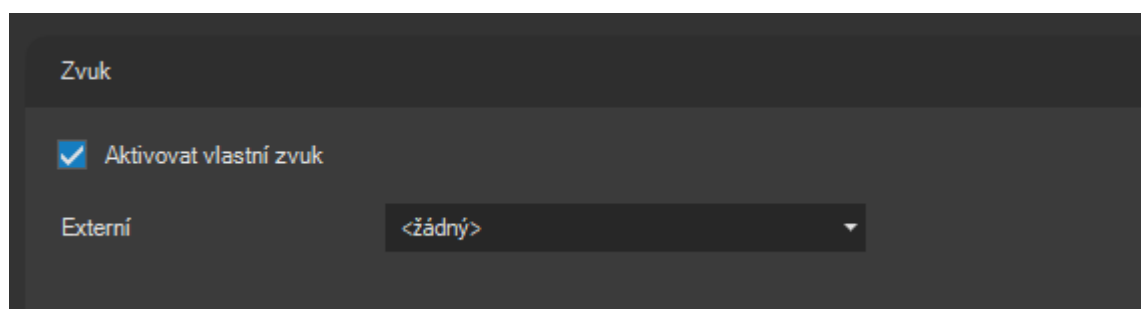
Pomocí volby Stahovat záznamy z SD karty kamery je možné synchronizovat záznam uložený na SD kartě kamery přímo se záznamovými oblastmi kamerového serveru, a doplnit je tak v případě výpadku síťového spojení či restartu serveru o chybějící data. Nastavení záznamu v kameře musí být vždy provedeno přímo na webu kamery. Pro synchronizaci je použito nativní rozhraní kamery anebo rozhraní Onvif profil G.



V části **Ovládání kamery** je možné pomocí zaškrtnutí políčka aktivovat či deaktivovat ovládání kamery.

POZNÁMKA

U otočných kamer je ovládání automaticky aktivováno již při přidání kamery do systému. Pokud je například připojena otočná kamera k video serveru, je nutné provést aktivaci ovládání ručně.



V části **Zvuk** je možné aktivovat pro danou kameru zvuk. Zvuk není automaticky aktivován při přidání kamery do systému a zaškrtnutí políčka Vlastní je dostupné pouze v případě, když daná kamera zvuk podporuje. Bez zaškrtnutí tohoto políčka není možný poslech živého zvuku ani jeho záznam. Úspěšné získání zvuku z kamery může u některých typů záviset také na nastavení přímo v kameře, kde může být zvuk implicitně blokován. U víceportových zařízení s několika video vstupy může být zvuk aktivován u libovolné kombinace video vstupů, a to i tehdy, pokud má zařízení s více video vstupy pouze jeden audio vstup.

Dále je v části nastavení zvuku k dispozici také rozbalovací seznam s názvem Externí. Z tohoto seznamu je možné aktuálně vybrané kameře přiřadit externí zdroj zvuku. Se zvukem získávaným z externího zdroje je zacházeno stejně jako s vlastním zdrojem zvuku. Zvuk je automaticky přehráván při výběru kamery v živém náhledu a může být také přehráván při prohlížení záznamu a exportován spolu s videem. Jako zdroj externího zvuku mohou sloužit zvukové IP moduly, zařízení, které nejsou kamerou ani video serverem (nepředstavují zdroj videa), mohou však být vybaveny dalšími funkcemi jako jsou vstupy a výstupy.

POZNÁMKA

Zvuk ze zařízení, které nepředstavují současně také zdroj videa, je možné získávat též samostatně, tyto zvukové moduly mohou být do systému přidány jako běžné kamery.

POZNÁMKA

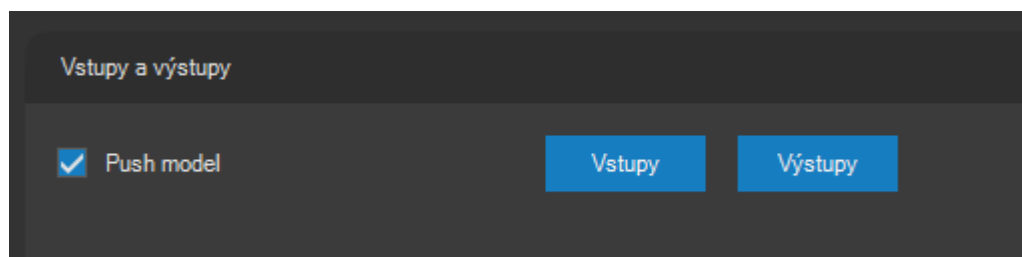
Externí zvuk může být přiřazen kameře, která nemá vlastní zdroj zvuku, ale také kameře, která vlastní zdroj zvuku má. Pokud je vlastní zdroj zvuku aktivní (je zaškrtnuta volba Aktivovat zvuk), má vlastní zdroj zvuku přednost před externím zdrojem, pokud by byl současně také nastaven.

POZNÁMKA

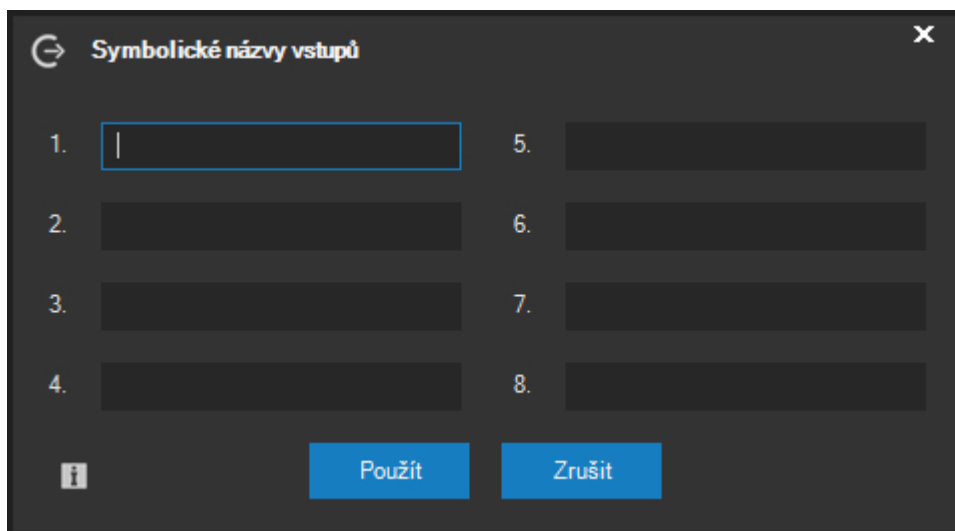
Funkce přiřazení zařízení jako externího zvukového zdroje se týká též funkce vysílání zvuku (push-to-talk). Pro externí zvukové zařízení je tedy podporována funkce obousměrného přenosu zvuku.

Podporovány jsou tyto zvukové kodeky:

- G711 (64 kbit), varianta u a A,
- G726 (24 – 32 kbit)
- AAC (8 – 48 kHz, 8 – 128 kbit)
- DVI 4 (IMA ADPCM)



V části **Vstupy a výstupy** je možné definovat symbolické názvy pro poplachové vstupy a výstupy kamer. Standardně jsou vstupy a výstupy v systému pojmenovány slovem Vstup či Výstup doplněným o číslo. Pro lepší orientaci uživatelů (při manuální aktivaci výstupů nebo při příjmu události) je možné změnit názvy vstupů a výstupů. Tlačítka nebudou dostupná, pokud na daném zařízení nejsou k dispozici poplachové vstupy či výstupy.



V této části okna je také možné aktivovat pro vstupy tzv. „push“ komunikační model. Pokud je ovládací prvek dostupný a kamera má instalován poslední firmware s podporou této funkce, je možné pro poplachové vstupy docílit kratší odezvy na změny jejich stavu.



V části **Externí analytická data** je možné aktivovat příjem externích analytických dat z kamer pomocí Onvif, nativních rozhraní kamer anebo i z jiných externích zdrojů.

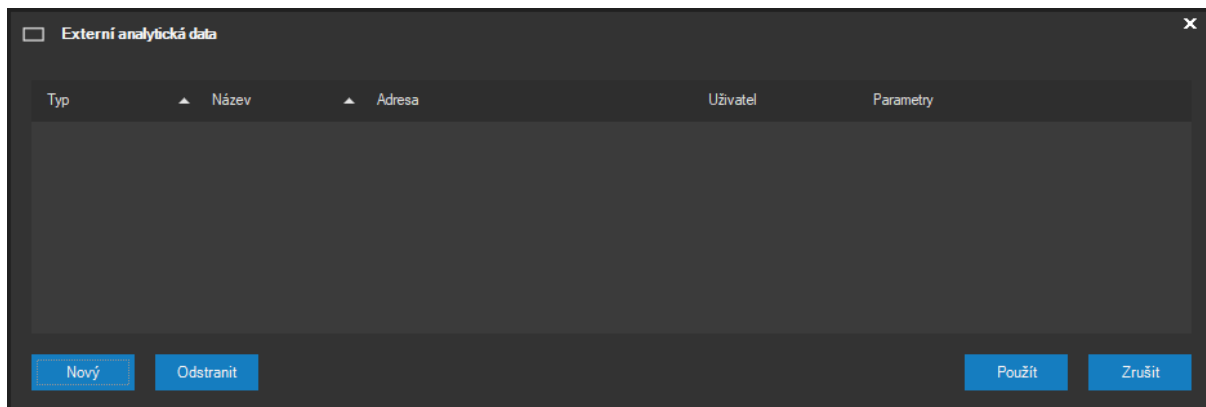
POZNÁMKA

Možnost využití externích analytických dat je dostupná až od edice ATEAS Security PROFESSIONAL.

Pro Onvif analytické zdroje je dále nutné, aby vybraný profil kamery měl přiřazenou konfiguraci analýzy a metadat. Je-li pak aktivována volba Aktivovat příjem dat, mohou být v závislosti na možnostech kamery přijímána data o rozpoznaných objektech, jejich typu, pozici či úrovni spolehlivosti rozpoznání.

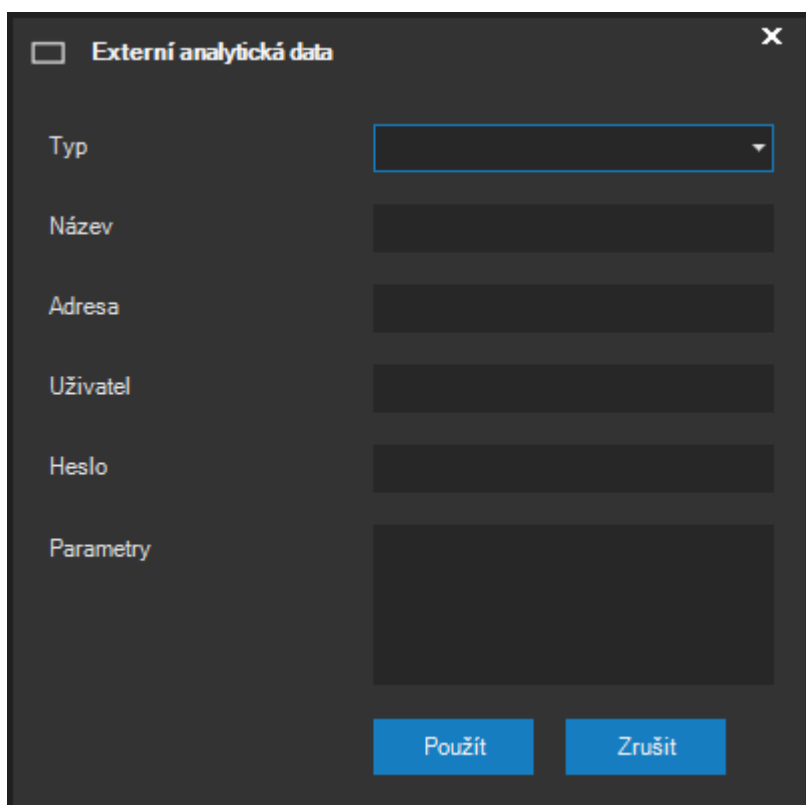
Tato metadata jsou poté zobrazována stejným způsobem jako data z ATEAS neuronových sítí a mohou být využita pro událostní management a forenzní vyhledávání.

Seznam dalších externích zdrojů analytických dat se zobrazí po stisku tlačítka **DALŠÍ**.



The screenshot shows a dialog box titled "Externí analytická data" with a close button (X) in the top right corner. Below the title bar is a table with five columns: "Typ", "Název", "Adresa", "Uživatel", and "Parametry". The table is currently empty. At the bottom of the dialog, there are four buttons: "Nový" (New), "Odstranit" (Remove), "Použít" (Use), and "Zrušit" (Cancel).

Nový externí zdroj je možné přidat pomocí tlačítka **NOVÝ**. Později je možné libovolný externí zdroj kdykoliv odstranit.



The screenshot shows the same dialog box, but now it is in the "Add New" mode. The "Typ" field is a dropdown menu. Below it are text input fields for "Název", "Adresa", "Uživatel", and "Heslo". The "Parametry" field is a larger text area. At the bottom, there are two buttons: "Použít" (Use) and "Zrušit" (Cancel).

V tomto dialogu je možné vybrat typ zdroje, určit jeho název a zadat jeho adresu (např. IP adresu). Volitelně je dále možné zadat uživatelské jméno a heslo, pokud zdroj vyžaduje autentizaci. Pokud zdroj vyžaduje ještě nějakou konkrétní parametrizaci nad rámec určení adresy, je možné využít pole Parametry.

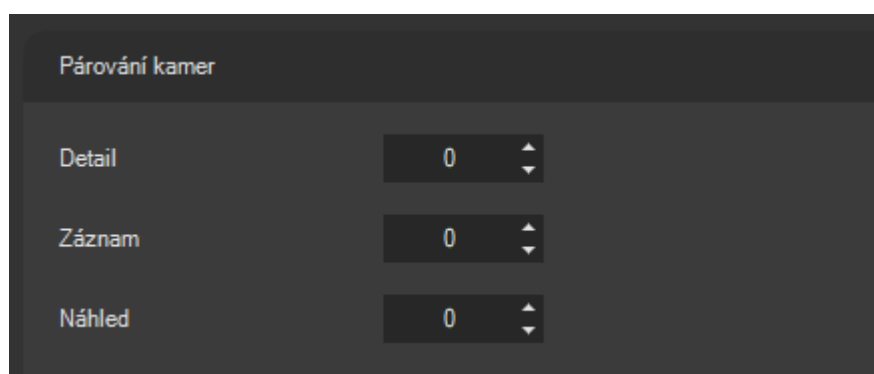
POZNÁMKA

Jednotlivé integrované externí zdroje analytických dat jsou samostatně zdokumentovány v příloze dokumentace s názvem Externí analytická data.

Po přidání jednoho či více externích zdrojů analytických dat budou moci oprávnění uživatelé sledovat výsledky externí videoanalýzy přímo v dohledovém okně po výběru příslušného zdroje, mezi kterými mohou přepínat.

POZNÁMKA

Z externího zdroje analytických dat je možné velmi často také získat informaci, kdy došlo k události. S těmito událostmi lze zacházet stejným způsobem jako s vlastními událostmi kamer. V případě výskytu události pak ATEAS automaticky vybere též příslušný externí zdroj analytických dat v dohledovém okně.



V části **Párování kamer** je možné určit, která kamera bude zobrazena v detailu po dvojitém kliknutí na záhlaví okna s kamerou a také, která kamera bude zobrazena při přepnutí živého pohledu do režimu přehrávání záznamu. Tyto funkce se využívají zejména tehdy, pokud je v systému jedna kamera přidána vícekrát s různými parametry videa a chcete-li při detailu nebo v záznamu zobrazit jiný video stream téže kamery např. s vyšším rozlišením.

Pomocí nastavení hodnoty pro Náhled lze určit, jaký video stream bude zobrazen pro danou kameru při využití funkce video náhledu v dohledovém okně při přehrávání záznamu. Tím lze načítání video náhledu zrychlit, neboť pro video náhled není potřeba video ve vysokém rozlišení.

POZNÁMKA

Často je možné např. využít stejných hodnot pro streamy vyhrazené pro náhled více kamer současně na mobilních klientech a pro video náhled záznamu, neboť v obou případech lze upřednostnit nižší rozlišení videa.

Nastavení se provádí pomocí relativních hodnot posunu na jiné číslo kamery. Máme-li tedy v systému vhodně uspořádané kamery s nižším a vyšším rozlišením, nastavení lze provádět hromadně pro všechny kamery. Při detailu nebo při přepnutí do režimu přehrávání pak každá kamera zobrazí kameru posunutou o nastavenou hodnotu.

Implicitně jsou tyto hodnoty nastaveny na nula, což znamená, že kamera se při detailu ani při přehrávání nezmění. Přestože nedojde ke změně kamery (přepnutí na jiný video stream), bude při detailu automaticky změněna snímková frekvence ze sekundární na primární.

POZNÁMKA

Pokud výsledná kamera určená posunem podle nastavené hodnoty neexistuje nebo k ní uživatel nemá přístup, uvidí v detailu či v záznamu kameru beze změny.

POZNÁMKA

Je možné používat jak pozitivní, tak negativní hodnoty.

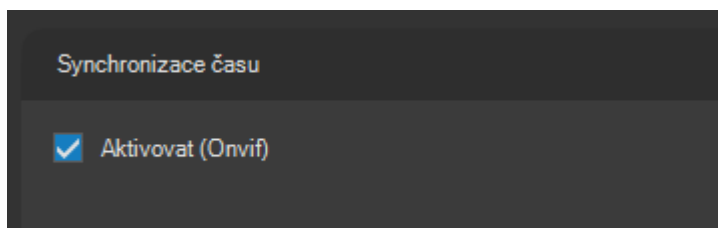
Pokud jsou kamery spárovány pomocí hodnoty Detail, bude automaticky spárováno též jejich PTZ ovládání. Na kameru s nastaveným offsetem je nahlíženo jako na PTZ podřízenou kameru a na kameru s nenastaveným offsetem jako na PTZ nadřízenou. PTZ zámek a informace v logu pak budou vždy vztaheny k nadřízené kameře nezávisle na tom, zdali se PTZ ovládání vztahuje k podřízené či nadřízené kameře. Kamery budou též sdílet své presety.

POZNÁMKA

Pro podřízenou kameru nejsou dostupné některé funkce jako jsou ovládání tůr a speciální PTZ funkce. Ty je možné nastavit jen po přepnutí na nadřízenou kameru.

POZNÁMKA

Pro vícenásobně přidané kamery ke kamerovému serveru lze uživatelům odebrat speciální oprávnění k zobrazení jejich čísla v přehledovém zobrazení čísel kamer v dohledovém okně a tím vytvořit přehlednější podobu čísel kamer.



V části **Synchronizace času** je možné pro vybrané kamery aktivovat automatickou synchronizaci času s kamerovým serverem. Přestože čas kamery není pro systém určující (určují čas je čas administračního serveru, který automaticky synchronizuje připojené kamerové servery), může mít v systému význam v těchto případech:

- Při komunikaci s kamerou přes Onvif může zařízení pro úspěšnou autentizaci vyžadovat kromě správného uživatelského jména a hesla také synchronizovaný čas, jinak může být přihlášení neúspěšné.
- Pokud využíváte funkci kamery, kdy je datum a čas vykreslen přímo ve videu, pak je tento čas získán přímo z kamery.
- Pokud využíváte ukládání dat na paměťové médium v kameře (např. SDHC karta) a přistupujete k těmto datům prostřednictvím ATEAS klienta, data na kartě jsou určena časem kamery.

POZNÁMKA

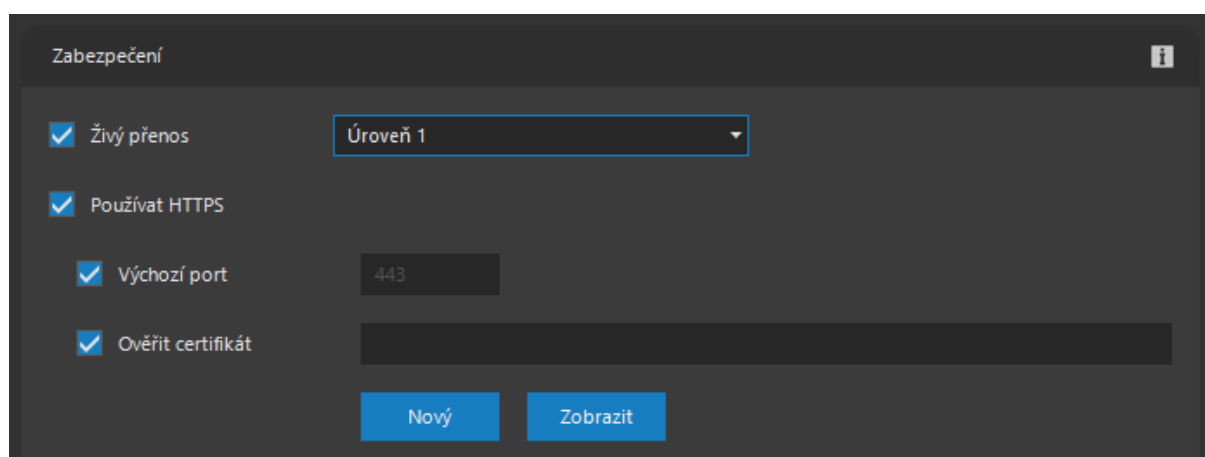
V souladu s výše uvedenou poznámkou ohledně časové synchronizace, která může být vyžadována pro autentizaci operací přes Onvif, může být nutné kameru před prvním přidáním do systému časově synchronizovat s počítačem kamerového serveru, aby mohlo dojít k úspěšné autentizaci.

POZNÁMKA

Funkce synchronizace času je k dispozici pouze pro Onvif kamery.

POZNÁMKA

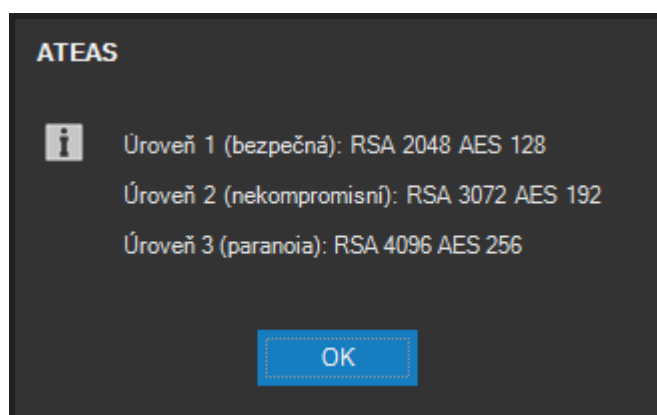
Pokud je aktivována funkce časové synchronizace kamery a zároveň je v kameře aktivována synchronizace času pomocí NTP serveru, NTP server bude mít přednost a kamerový server nebude čas kamery synchronizovat.



Část **Zabezpečení** obsahuje možnost aktivovat komunikaci na zabezpečeném kanále, a to jednak pro komunikaci mezi serverem a klienty, jednak mezi kamerou a serverem.

Pro zabezpečení živé komunikace mezi serverem a klienty systému (redistribuce videa a zvuku) je možné aktivovat pokročilé šifrování AES. Tím je zajištěno, že jakýkoliv odposlech sítě a přenášených paketů není možné převést do čitelné datové podoby a zobrazit tak video či přehrát zvuk, než dorazí ke klientovi ATEAS Security systému. Šifrování bude aplikováno na přenosy typu unicast i multicast (pokud mají uživatelé nastaven profil LOCAL). Více viz kapitola o nastavení profilů uživatelů.

Úroveň šifrování je možné nastavit v rozmezí 1 až 3. Přestože i první úroveň nabízí ochranu neprolomitelnou současnými prostředky, je možné za ceny vyšší spotřeby výkonu zvolit i vyšší úroveň zabezpečení spočívající zejména v délce použitých kryptografických klíčů. Jejich parametry zobrazuje pomocný dialog.



POZNÁMKA

Možnost šifrování komunikace mezi serverem a klienty je dostupná až od edice ATEAS Security PROFESSIONAL.

Pro zabezpečení komunikace s kamerou je použita technologie TLS (Transport Layer Security), pokud tuto technologii kamera podporuje. Při zabezpečené komunikaci s kamerou pomocí TLS je použit protokol https s možností změny portu.

POZOR

Předpokladem je použití protokolu http, tudíž rtsp schéma kamer musí být přepnuto do režimu tunelování přes protokol http.

Volba Ověřit certifikát umožňuje vložení certifikátu zařízení, který musí být úspěšně ověřen, aby mohlo být zařízení vpuštěno do systému.

POZNÁMKA

Možnost použití a ověřování certifikátů je dostupná až od edice ATEAS Security PROFESSIONAL.

Je-li zároveň aktivována volba ověřování certifikátů na úrovni serveru, bude mít certifikát zařízení a výsledek jeho ověření přednost před certifikáty na úrovni celého systému. Zatímco u certifikátů na úrovni celého systému je při ověření zkoumána celá hierarchie certifikátu zařízení, zde si musí

certifikáty odpovídat přímo. Podporovány jsou všechny hlavní formáty pro uložení certifikátů včetně formátu cer, crt, pfx nebo p12.

POZNÁMKA

Některé formáty budou vyžadovat heslo pro otevření souboru.

Tlačítkem **ZOBRAZIT** lze otevřít okno s podrobnostmi o vybraném certifikátu. Certifikát pochopitelně nemusí obsahovat soukromý klíč, ale pouze veřejný klíč nutný pro ověření.



V části **Data transakcí** je možné aktivovat volbu Příjem dat, která umožní integraci libovolných externích transakčních dat s Vaším kamerovým systémem.

POZNÁMKA

Možnost příjmu transakčních dat je dostupná až od edice ATEAS Security PROFESSIONAL.

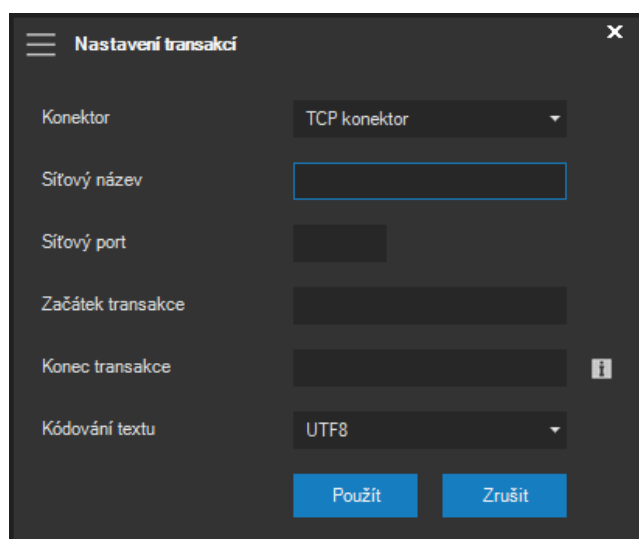
POZNÁMKA

Transakční data jsou jakákoliv textová data poskytována systémem třetí strany, která mohou být rozdělena do transakcí podle řídících či opakujících se znaků v datech. Data jsou poté přidružena ke kameře a mohou být sledována online, ze záznamu nebo podle nich lze vyhledávat.

POZNÁMKA

Typickým příkladem pro příjem transakčních dat jsou pokladní systémy (POS).

Po aktivaci příjmu dat je nutné provést nastavení příjmu dat pomocí tlačítka **NASTAVIT**.



Příjem dat může být realizován pomocí síťového protokolu UDP nebo TCP. Pro oba protokoly je třeba vyplnit pole Síťový port. Pro protokol TCP je navíc nutné vyplnit i pole Síťový název.

POZNÁMKA

Zatímco u protokolu UDP určuje číslo portu lokální port, na kterém jsou přijímána data, u protokolu TCP se jedná o vzdálený port na adrese či počítači určeném v poli Síťový název, ke kterému se ATEAS připojuje.

Do polí Začátek a Konec transakce je možné zadat textové řetězce, které ohraničují transakci. Textové informace mezi začátkem a koncem transakce jsou daty jedné transakce. Jednotlivé řádky transakcí jsou pak automaticky vytvářeny dle výskytu znaků pro oddělení řádků přímo v textu transakce.

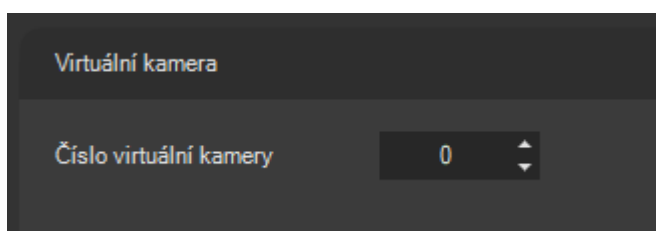
POZNÁMKA

Zadání konce transakce není povinné. Pokud není zadán, je transakce automaticky ukončena při detekci začátku následující transakce.

POZOR

Transakční data musí být formátována tak, že řetězce začátku a konce transakce jsou unikátní a nevyskytují se v rámci transakce. To by vedlo k chybné tvorbě transakcí.

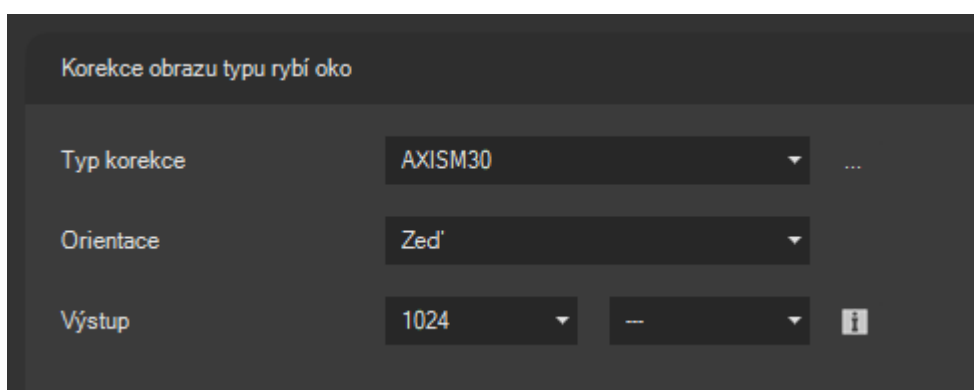
V seznamu Kódování textu zvolte vždy správné kódování textu transakčních dat. Jen tak bude možné správně interpretovat např. diakritické znaky nebo speciální znaky v různých jazycích.



V části **Virtuální kamera** lze pro některé typy zařízení provádět nastavení virtuálních kamer. Virtuální kamery jsou technologií, kterou používají zejména kamery s vysokým rozlišením a která spočívá v tom, že kamera je schopna samostatně vysílat několik různě umístěných výseků celého obrazu. Některé typy kamer jsou schopny virtuální kamery zprovoznit na samostatné IP adrese. V tomto případě jsou virtuální kamery podporovány nativně, neboť je lze připojit k serveru pomocí jejich vlastních IP adres stejným způsobem jako reálné kamery. Některé typy kamer však mají podporu virtuálních kamer řešenu v rámci své IP adresy a může tedy být nutné nastavit konkrétní číslo virtuální kamery v této části nastavení.

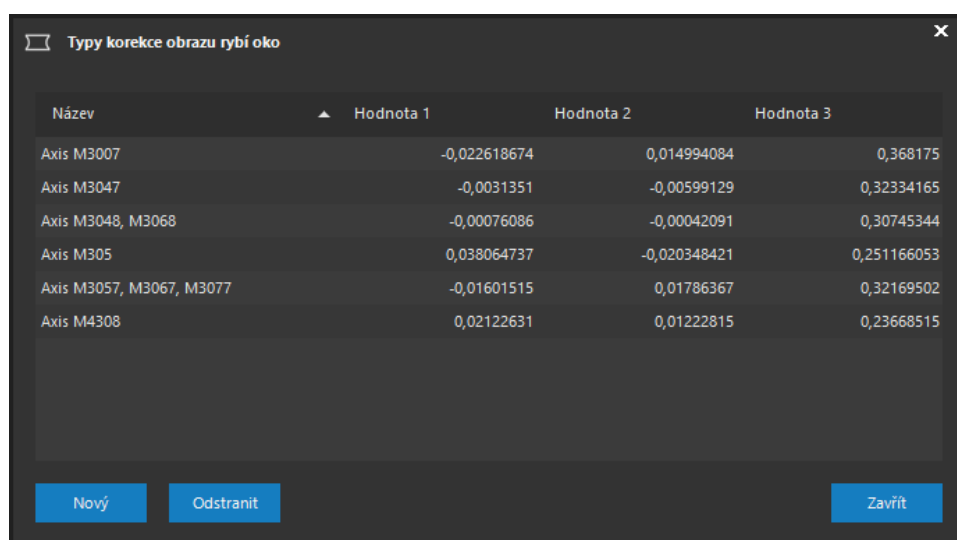
POZNÁMKA

Ovládací prvek pro nastavení čísla virtuální kamery bude dostupný pouze u kamer, které virtuální kamery podporují a zároveň pro ně nevytvářejí samostatné IP adresy.



V části **Korekce obrazu typu rybí oko** lze pro vybrané kamery umožnit, aby uživatelé v pohledu mohli pro obraz z těchto kamer použít některý z režimů korekce pro obraz typu rybí oko, který je v základním zobrazení deformován kvůli svému záběru 360 stupňů. Aby bylo možné v dohledovém okně provádět korekci, musí být pro vybrané kamery zvolen typ korekce, orientace kamery a výsledné rozměry videa.

Typ korekce lze vybrat z předdefinovaných typů anebo je možné vytvořit typ vlastní. Jelikož se jednotlivé typy objektivů typu rybí oko liší ve svých fyzikálních parametrech (funkce zakřivení), může být nutné do systému přidat svůj vlastní typ objektivu pro daného výrobce. Seznam všech typů je možné zobrazit pomocí tlačítka vedle rozbalovacího seznamu typů.



Název	Hodnota 1	Hodnota 2	Hodnota 3
Axis M3007	-0,022618674	0,014994084	0,368175
Axis M3047	-0,0031351	-0,00599129	0,32334165
Axis M3048, M3068	-0,00076086	-0,00042091	0,30745344
Axis M305	0,038064737	-0,020348421	0,251166053
Axis M3057, M3067, M3077	-0,01601515	0,01786367	0,32169502
Axis M4308	0,02122631	0,01222815	0,23668515

Tlačítkem **NOVÝ** je možné do seznamu přidat nový typ korekce, kde jednotlivé tři hodnoty vyjadřují koeficienty polynomu, pomocí kterého lze vypočítat vzdálenost bodu od optického středu v cílovém obraze ze vzdálenosti bodu od optického středu ve zdrojovém obraze.

Tlačítkem **ODSTRANIT** je možné Vámi přidaný typ korekce odstranit ze systému.

POZNÁMKA

Předdefinované typy korekce, které jsou součástí instalace a nebyly ručně přidány, nemohou být odstraněny.

V rozbalovacím seznamu Orientace je nutné určit, jakým způsobem je kamera namontována, protože její orientace v prostoru je důležitou vstupní informací pro algoritmus korekce, aby jeho výsledek byl

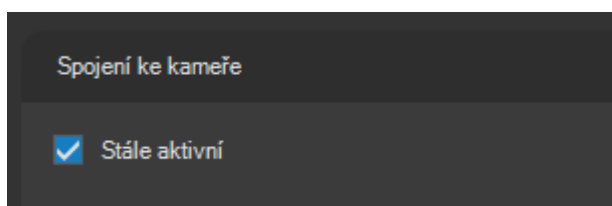
správně orientovaný v prostoru. U varianty montáže na zeď se navíc v dohledovém okně při aktivaci panoramatického režimu korekce automaticky použije jednoduchý panorama pohled namísto dvojitého.

Dle vstupního rozlišení obrazu typu rybí oko a požadované úrovně detailu po aplikaci algoritmů korekce je třeba určit výslednou šířku videa po přepočtení.

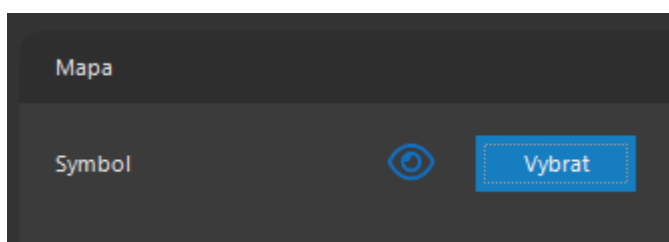
POZNÁMKA

Nastavená hodnota platí pro korekci do jednoduchého PTZ pohledu, režimy korekce do pohledu typu panorama nebo quad budou automaticky vytvářet video s dvakrát vyšším rozlišením.

V rozbalovacím seznamu Poměr stran lze určit požadovaný poměr stran obrazu po korekci. Ten je implicitně odvozen od původních rozměrů videa, nicméně např. při poměru stran nekorigovaného videa 1:1 (čtverec) je vhodné ho uzpůsobit.



V části **Spojení ke kameře** je k dispozici zaškrťovací políčko pro udržování permanentního spojení ke kameře. Toto políčko je implicitně zapnuto. V některých případech je velmi vhodné zaškrtnutí zrušit a monitorovat např. poplachové stavy i bez datově náročného toku videa.

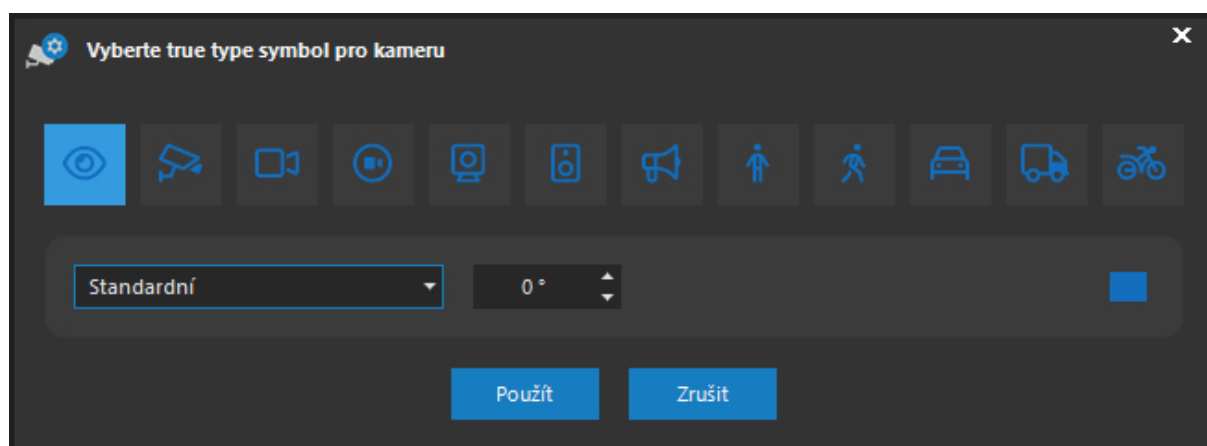


V části **Mapa** je možné definovat podobu symbolu, který bude použit při zobrazení kamery v mapě.

POZNÁMKA

Velikost symbolů, která bude při zobrazení použita, nenastavuje administrátor, ale každý uživatel ve vztahu ke svému monitoru, rozlišení obrazu a vnímání v části lokální nastavení.

Po kliknutí na tlačítko **VYBRAT** se zobrazí okno s možností výběru nového symbolu (každá kamera má při přidání do systému přiřazen implicitní symbol a barvu).



TIP

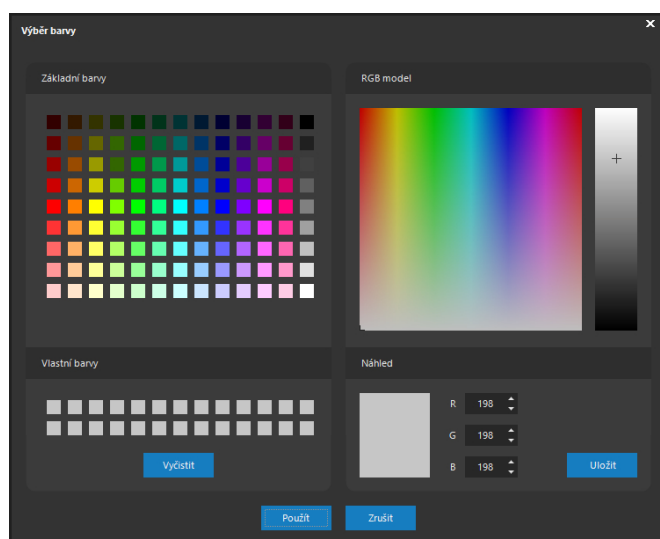
Již lokalizovaným kamerám lze rychleji změnit symbol pomocí kontextové nabídky symbolu kamery v mapě.

Vybírat je možné z různých symbolů a jejich provedení. Symboly je také možné volně otáčet, což umožní např. nastavit směrově orientované symboly fixních kamer přesně podle skutečného stavu.

POZNÁMKA

Mobilní symboly jako je symbol osoby nebo vozidel lze použít např. pro kamery mobilních zařízení, které (pokud mají vytvořenu výchozí lokalizaci v mapě) jsou při vysílání videa automaticky zobrazovány v mapě dle jejich GPS lokalizace v reálném čase či ze záznamu.

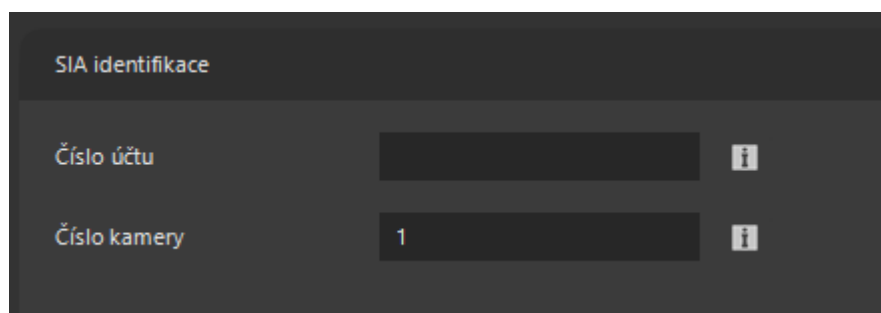
Tlačítkem s barvou je možné změnit barvu použitou pro zobrazení symbolu.



TIP

U dvoutónového provedení symbolů je možné nastavit kombinaci dvou barev. Nejlépe bude vypadat kombinace barev stejného odstínu s různou světlostí, tj. volba z jednoho sloupce.

Po stisku tlačítka **POUŽÍT** v okně pro výběr symbolu kamery je původní symbol v náhledu nahrazen nově definovaným. Aby však tento symbol byl použit i pro zobrazení v mapě, je nutné potvrdit všechny změny provedené v okně nastavení kamery (viz dále).



V části SIA identifikace je možné upravit identifikaci kamery pro protokol SIA. Číslo účtu (objektu) má stejný význam jako v případě otevření SIA kanálu, možnost ho změnit pro každou kameru může být nutná tehdy, pokud jsou v jednom systému ATEAS sdruženy kamery, které patří k více SIA objektům (účtům).

TIP

Hodnotu pro účet lze zadat také v hexadecimálním tvaru pomocí prefixu 0x.

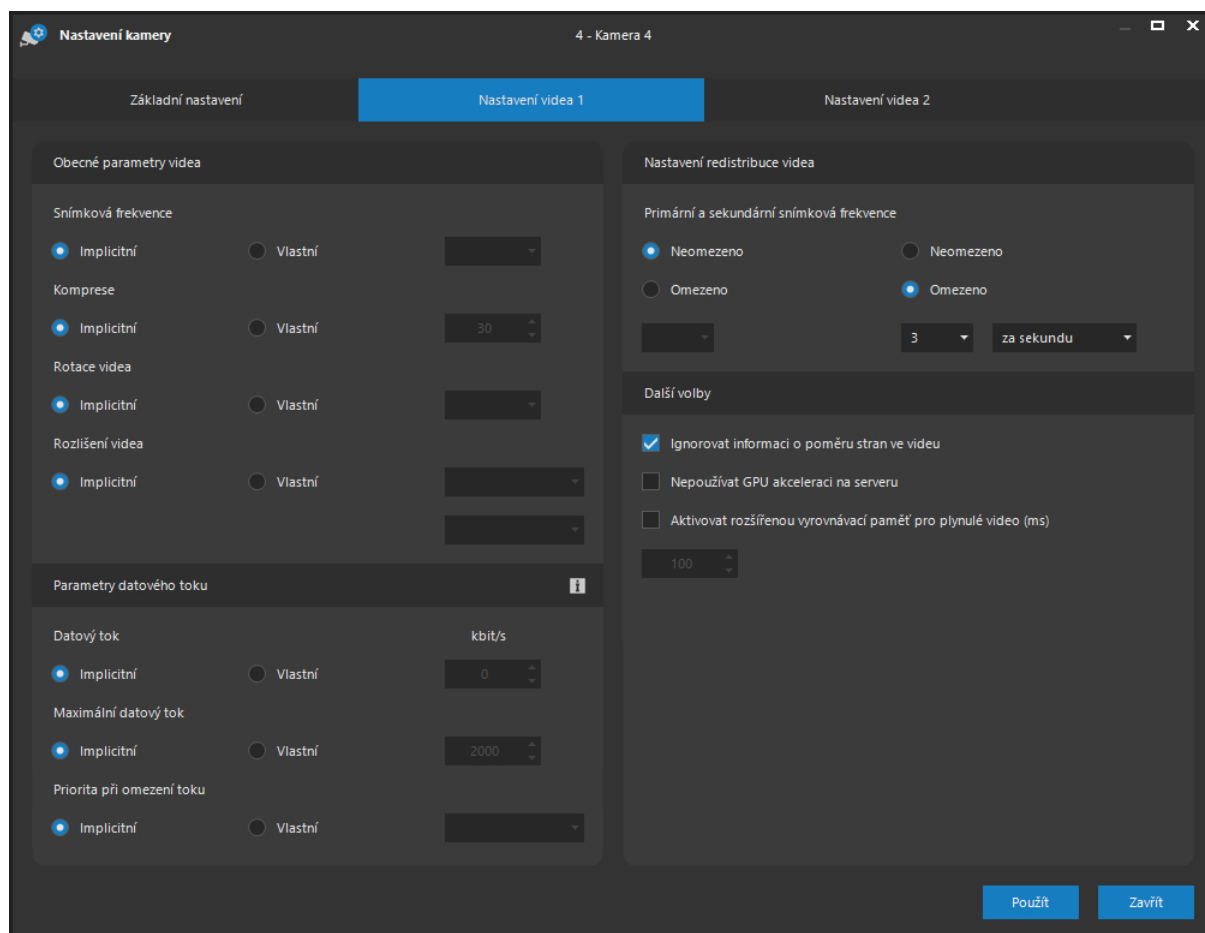
Číslo kamery je implicitně nastaveno na skutečné číslo kamery, může však být upraveno na jinou hodnotu v rozsahu 2 bytů.

11.2.5. Nastavení videa

Obsah na kartě Nastavení videa se liší podle způsobu připojení kamery k serveru. Ve všech případech je možné odděleně a na samostatných kartách nastavit primární a sekundární stream videa.

Nastavení na kartě Video pro nativní rozhraní kamer

Karta Video obsahuje základní nastavení videa nastavované kamery nebo kamer.



V části Obecné parametry videa (vstup serveru) je možné nastavit vstupní snímkovou frekvenci, stupeň komprese videa a jeho rozlišení. Při volbě rozlišení je nejprve nutné vybrat poměr stran. Při volbě Implicitní budou pro dané nastavení použity hodnoty aktuálně nastavené přímo v kameře. Poměr stran nesouvisí s výsledným počtem obrazových bodů, pro konkrétní poměr stran tak lze zvolit více výsledných rozlišení až do maximálního rozlišení pro konkrétní kameru (včetně rozlišení N megapixelů). Speciálním případem je varianta SCALE, pomocí které nelze zadat konkrétní rozlišení, ale pouze faktor redukce maximálního či výchozího rozlišení dané kamery (pouze u některých zařízeních).

V této části lze také nastavit parametr rotace videa. Pokud je nastaven na hodnotu implicitní, bude použita rotace nastavená přímo v kameře, jinak je možné zadat rotaci videa 0, 90, 180 a 270 stupňů. Nastavení rotace videa může být důležité v souvislosti s nastavením detekce pohybu.

POZNÁMKA

Některé typy kamer nepodporují rotaci videa nebo nepodporují všechny hodnoty.

V části Nastavení redistribuce videa (výstup serveru) je možné nastavit primární a sekundární snímkovou frekvenci pro video. Primární snímková frekvence je použita, pokud uživatel má danou kameru zobrazenou v detailu, sekundární snímková frekvence je použita při zobrazení dané kamery v pohledu s více než jednou kamerou. U sekundární snímkové frekvence je navíc možné provést nastavení počtu snímků buď za vteřinu, nebo za minutu. To je z důvodu, aby mohla být snímková frekvence snížena pod hranici 1 FPS, což může být nutné zejména při více otevřených pohledech obsahujících mnoho desítek kamer (maximálně $4 * 100$, tj. 400 současně zobrazených kamer na jedné stanici).

POZNÁMKA

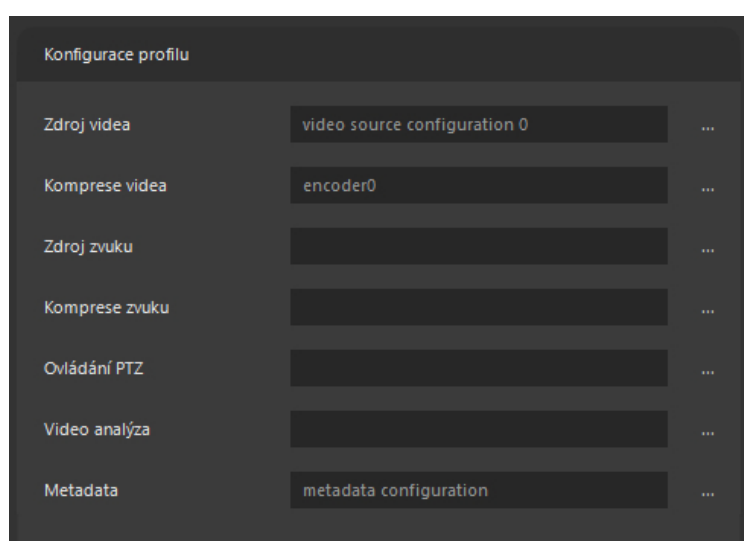
Při použití formátu videa jiného než MJPEG se omezená snímková frekvence počítá pouze z kompletních snímků bez závislosti na ostatních.

V části Parametry datového toku lze nastavit parametry datového toku. Při použití volby Implicitní opět platí, že bude použito aktuální nastavení přímo v kameře. Datový tok může být nastaven na variabilní (VBR) nebo na konstantní (CBR) v jednotkách kilobitů za sekundu. Dále je také možno omezit maximální datový tok (vhodné zejména pro VBR). Pokud nastane situace, kdy by z hlediska snímání scény bylo nutné generovat významně vyšší než konstantní nebo vyšší než maximálně povolený datový tok, bude muset dojít k omezení kvality videa nebo jeho snímkové frekvence. Pro tento případ

je možné nastavit prioritu při omezování toku. Při nastavení na Snímky se bude kamera snažit udržet snímkovou frekvenci na úkor kvality videa, při nastavení na Kvalita se bude naopak snažit udržet kvalitu videa na úkor snímkové frekvence. Při nastavení na Žádná budou obě veličiny sníženy zhruba rovnocenně.

Nastavení na kartě Video pro rozhraní kamer Onvif

Část nastavení Obecné parametry videa (vstup serveru) je však odlišná, pokud je právě nastavovaná kamera (či výběr kamer) připojena namísto proprietárního rozhraní pomocí Onvif. V případě Onvif podporujících zařízení vypadá tato část následovně.



Jednotlivé profily dle specifikace Onvif obsahují veškerá nastavení rozdělená do několika skupin (konfiguračních entit), ze kterých je výsledný profil sestaven. V částech nastavení videa jsou zobrazeny vlastnosti profilů vybraných v základním nastavení.

Konfigurace zdroje videa: Zdrojem videa může obvykle být celý obraz, tak jak ho snímá kamera, zařízení však může definovat více zdrojů videa, pokud podporuje virtuální kamery nebo pokud má více analogových vstupů na jedné IP adrese.

Konfigurace komprese videa: Komprese videa sdružuje veškerá nastavení ohledně komprese videa jako je formát videa a jeho specifické parametry, kvalita komprese, rozlišení, snímková frekvence apod.

Konfigurace zdroje zvuku: Zdrojem zvuku může být externí či vestavěný mikrofon zařízení.

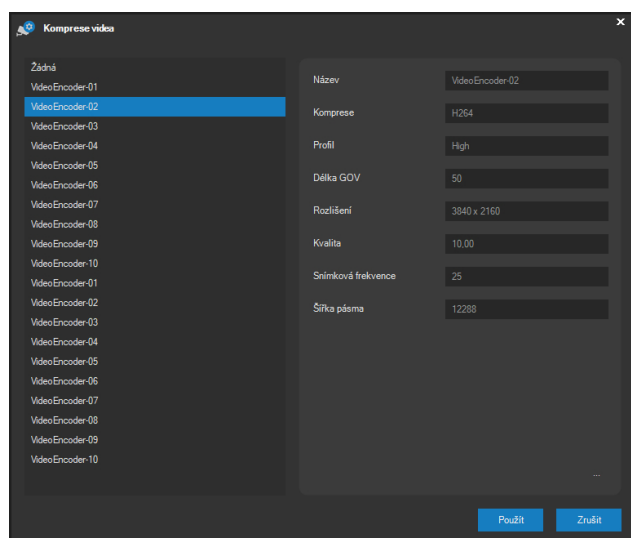
Konfigurace komprese zvuku: Komprese zvuku sdružuje veškerá nastavení ohledně komprese zvuku jako je audio formát a jeho specifické parametry, vzorkovací frekvence či datový tok.

Konfigurace PTZ: Tato konfigurace je vztažena ke způsobu PTZ ovládání kamer. Může se jednat o mechanické ovládání kamery. PTZ konfigurace však bude k dispozici i na (megapixelových) kamerách, které podporují digitální zoom a digitální ovládání přímo v obraze.

Konfigurace video analýzy: Pomocí této konfigurace lze profil doplnit o video analytickou složku, která aktivuje pravidla pro analýzu videa přímo v kameře a určuje, jaká metadata mohou být zasílána.

Konfigurace metadat: Pomocí této konfigurace lze profil doplnit o metadatovou složku, která aktivuje zasílání metadat popisu scény včetně např. typů objektů, jejich umístění a velikosti, hodnoty spolehlivosti rozpoznání atd.

Pomocí tlačítka se třemi tečkami umístěného za názvy konfigurací lze pro každou konfigurační entitu zobrazit seznam všech dostupných konfigurací. Následující obrázek ukazuje seznam konfigurací komprese videa. Postup u dalších konfiguračních entit je analogický.



V tomto dialogu, který obsahuje seznam dostupných konfigurací, lze Vámi požadovanou konfiguraci označit a pomocí tlačítka **POUŽÍT** provést přiřazení konfigurace danému profilu. Pokud profil v rámci dané konfigurační entity (např. komprese videa) již nějakou konfiguraci obsahuje, bude provedeno její nahrazení. Odebrání konfigurace od profilu je možné výběrem položky „Žádná“.

Jednotlivé konfigurace lze v rámci profilu seskupovat libovolně a v libovolném pořadí, neboť specifikace Onvif nekladou žádná omezení až na výjimku uvedenou dále. Onvif doporučuje profilům přiřazovat konfigurace komprese videa až po přiřazení konfigurace zdroje videa (analogicky platí pro

audio konfigurace) a dále doporučuje odebírat konfigurace zdroje videa až po odebrání konfigurace komprese videa (analogicky platí pro audio konfigurace). Tato doporučení jsou implementována v logice klienta ATEAS a aplikace automaticky hlídá dodržování těchto doporučení.

POZOR

Pokud nebude profilu přiřazena žádná konfigurace PTZ, nebude možné kameru při použití tohoto profilu ovládat, ani pokud bude ovládání povoleno v základním nastavení kamery.

Při označení konfigurace se v části dialogu Detaily konfigurace zobrazí veškeré detaily dostupné pro danou konfiguraci. Pomocí tlačítka se třemi tečkami v pravém dolním rohu části Detaily konfigurace lze provést úpravu parametrů této konfigurace.

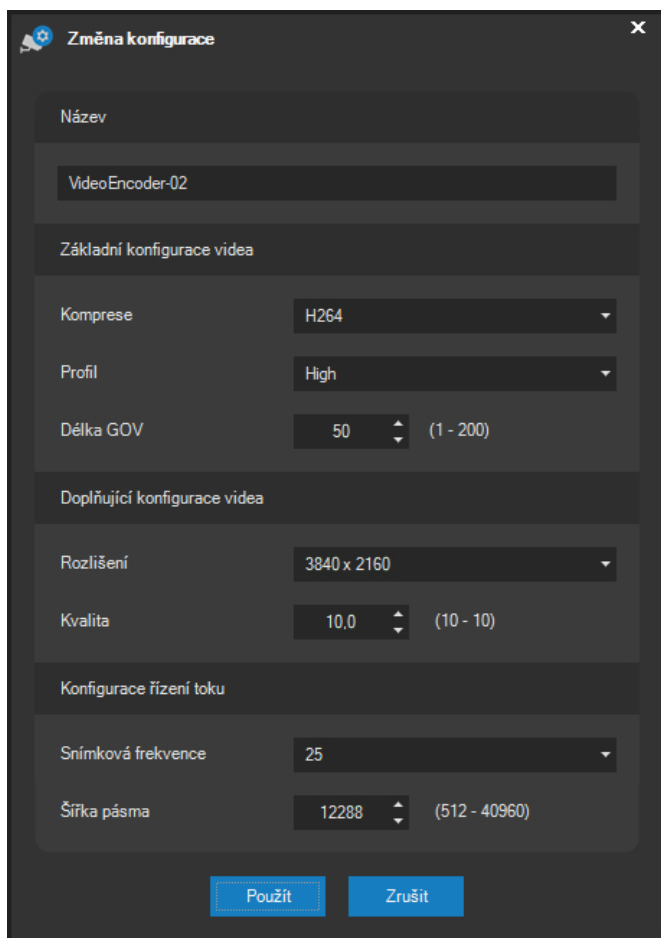
POZNÁMKA

Zatímco je možné vytvářet a mazat profily v kamerách, počet konfigurací je dán výrobcem a nelze jej měnit. Konfiguracím však lze měnit nastavení a parametry.

POZNÁMKA

U některých konfiguračních entit nemusí být tlačítko pro změnu nastavení konfigurace dostupné.

Po stisknutí tohoto tlačítka je zobrazen dialog s možností provedení úpravy dané konfigurace. Následující obrázek zobrazuje dialog s úpravou konfigurace komprese videa.



Na tomto dialogu lze provést změnu názvu konfigurace, volbu formátu videa, případně také volbu profilu a délky GOV, která udává počet snímků od kompletního snímku (klíčový snímek) až po následující kompletní snímek. Dále je možné upravit rozlišení videa, jeho kvalitu a provést nastavení datového toku pomocí snímkové frekvence nebo šířky pásma.

POZNÁMKA

Dialog se může pro jednotlivé kamery drobně lišit například v závislosti na tom, jakou verzi některých služeb Onvif zařízení podporuje.

POZNÁMKA

Pro každý parametr je pomocí Onvif přímo z kamery získán obor hodnot, jakých může daný parametr nabývat. To znamená, že v tomto dialogu Vám bude zobrazen seznam všech video formátů či rozlišení, které kamera podporuje. Pro číselně vyjádřené hodnoty jako např. kvalita komprese bude vždy získán a automaticky vynucen přípustný rozsah hodnot pro dané zařízení.

Nastavení na kartě Video pro rozhraní kamer RTSP

Pokud je zdroj videa (případně i zvuku) přidán přímo pomocí RTSP adresy, není možné v sekci Obecné parametry videa (vstup serveru) provádět žádná nastavení. Některá nastavení videa mohou být např. součástí přímo RTSP adresy.

Další volby

V části Další volby je možné aktivovat některé další možnosti týkající se videa.

Volba Ignorovat informaci o poměru stran je implicitně aktivní a umožňuje ignorovat informaci o změně poměru stran, která může být ve videu volitelně obsažena. Tuto technologii mohou používat některé kamery s jiným než čtvercovým formátem bodů na obrazovém čipu pro dodatečnou korekci poměru stran.

Volba Nepoužívat GPU akceleraci na serveru umožňuje vyjmout dekódování dané kamery z GPU akcelerace na serveru, i pokud je zapnuta.

TIP

Tímto způsobem lze rozdělit zátěž dekódování mezi CPU a GPU na serveru.

Pomocí položky Aktivovat rozšířenou vyrovnávací paměť pro plynulé video je možné aktivovat dodatečnou vyrovnávací paměť (cache) pro plynulé video. Tuto volbu je vhodné aktivovat pouze tehdy, pokud je plynulost negativně ovlivněna přenosem na síti. Negativním důsledkem vyhlazení videa do plynulé podoby je totiž např. zhoršení kvality PTZ ovládání kamery z důvodu vyššího zpoždění videa. Pokud je tato volba aktivována, hodnota se nastavuje v intervalu od 50 do 500 milisekund.

Provedené změny v okně nastavení kamery je nutné potvrdit tlačítkem **POUŽÍT**. Aplikace potvrdí uložení a uplatnění provedených změn zprávou. Poté je možné zavřít okno tlačítkem **ZAVŘÍT**.

POZNÁMKA

Tlačítko **POUŽÍT** provede uložení změn provedených na všech kartách okna nastavení kamery (pokud je jejich počet alespoň dvě). Je tedy možné provádět změny na všech kartách a poté provést aktualizaci nastavení tímto tlačítkem.

11.2.6. Hromadné nastavení a odebírání kamer

Základní nastavení kamer lze provádět pro libovolný počet kamer najednou. Stejně tak je možné provést odstranění libovolného počtu kamer jednou akcí. V každém případě je však nutné provést výběr více kamer v jejich seznamu. Vícenásobný výběr lze provést takto:

- pohybem myši při stisknutém levém tlačítku,
- opakovaným výběrem za současného stisku klávesy CTRL,
- kombinací obou způsobů,
- kombinací kláves CTRL-A lze vybrat všechny kamery v seznamu.

POZNÁMKA

Při provedení vícenásobného výběru nebudou přístupná tlačítka, která zpřístupňují nastavení specifická pro jednotlivé kamery a nelze nebo nemá smysl provádět hromadné nastavení (např. detekce pohybu).

Při vstupu do sekce základního nastavení bude při vícenásobném výběru obsah okna upraven tak, že budou vyplněna pouze ta nastavení, která jsou platná pro všechny kamery ve výběru. Zároveň budou na vybrané kamery uplatněna pouze explicitně provedená nastavení. To znamená, že je možné např. změnit záznamový profil pro 10 vybraných kamer najednou bez toho, aby byly změněny další parametry kamer, které mohou zůstat odlišné.

POZNÁMKA

Při hromadném nastavování kamer není možné zahrnout do výběru kamery připojené různými způsoby – rozhraní výrobce, Onvif či pouze protokol RTSP.

Pro snazší hromadný výběr je možné provádět filtrování seznamu kamer pomocí rozbalovacího seznamu nad seznamem kamer.

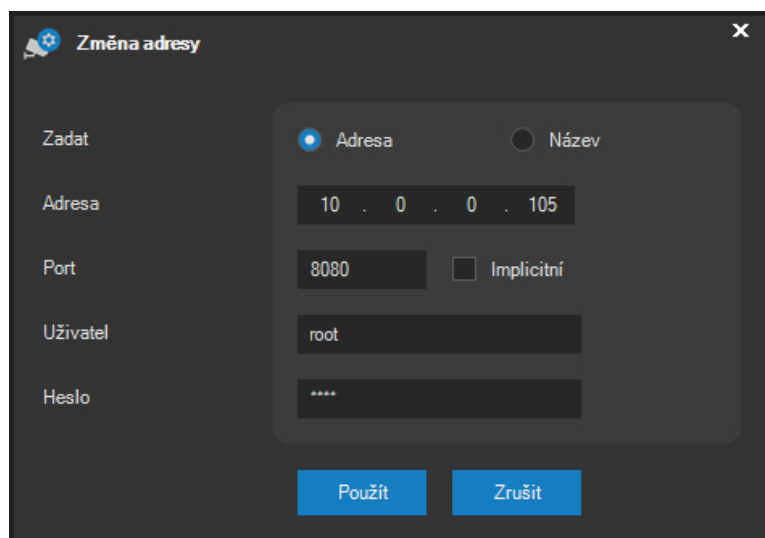
POZNÁMKA

Vzhledem k tomu, že zařízení připojená k serveru pomocí Onvif rozhraní jsou konfigurována pomocí profilů, které jsou uloženy přímo v koncových zařízeních, nelze provádět hromadnou úpravu profilů a jejich konfigurací.

Při vícenásobném výběru je možné tlačítkem **ODSTRANIT** provést odebrání všech vybraných kamer ze systému.

11.2.7. Změna adresy a přihlášení

Pomocí tlačítka **ADRESA** je možné provést dodatečnou změnu IP adresy a http portu kamery. Současně lze v tomto dialogu také změnit přihlašovací údaje ke kameře (uživatelské jméno a heslo).

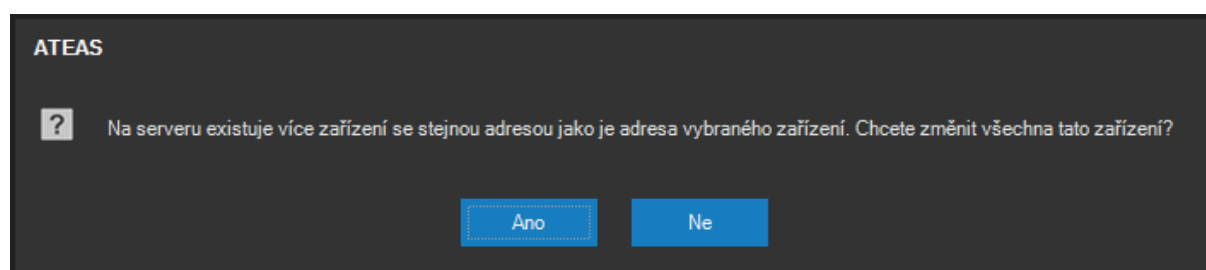


Princip změny adresy a portu je stejný jako při přidávání kamer. Je možné zadat IP adresu nebo název kamery a http port.

POZNÁMKA

Změny IP adres a http portů kamer mohou snížit či zvýšit počet licencovaných kamer přiřazených kamerovému serveru, pokud měníte adresu vícenásobně přidávané kamery anebo změníte adresu tak, že jedna kamera bude přidána vícenásobně.

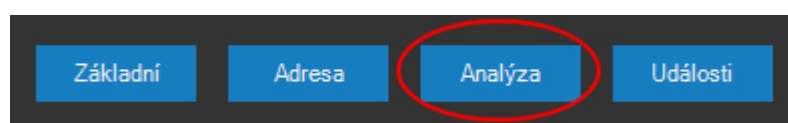
Z toho důvodu je administrátor na tuto situaci upozorněn a může zvolit, zdali bude adresa a ostatní údaje automaticky změněny také u všech ostatních duplicitně přidávaných zařízení (zařízení se stejnou adresou či názvem).



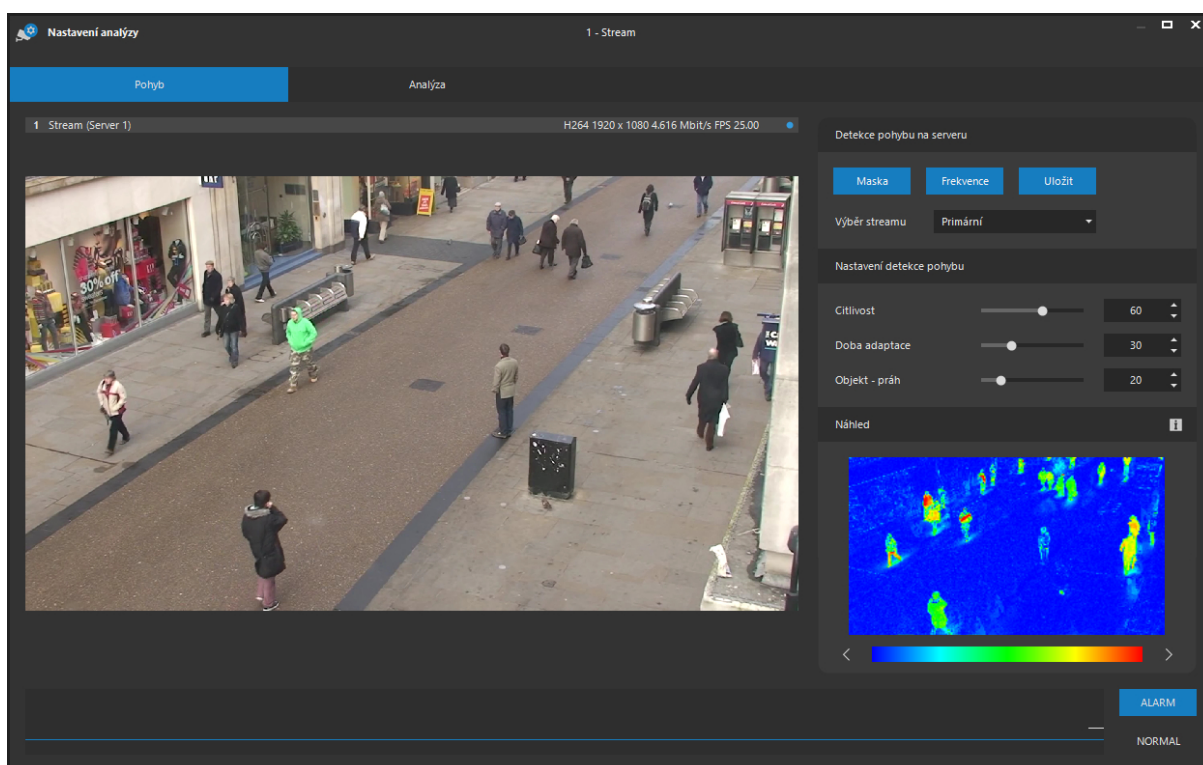
V případě výběru více kamer nelze tuto funkci použít pro změnu adresy či portu, ale je možné hromadně měnit přihlašovací údaje ke kamerám.

11.2.8. Detekce pohybu na serveru

Detekci pohybu lze ovládat po stisku tlačítka **ANALÝZA** na kartě Pohyb.

**TIP**

Nastavení lze měnit též hromadně pro více vybraných kamer současně.

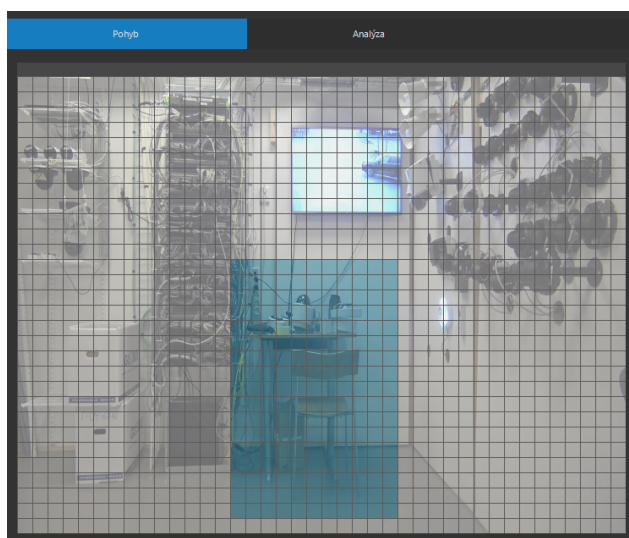


V okně lze sledovat aktuální scénu před kamerou a náhled vyhodnocování pohybu ve scéně v reálném čase. Pohyb a pohybující se objekty jsou v náhledu barevně odlišeny podle intenzity změny ve scéně dané rozdílem v barevnosti a světlosti pohybujícího se objektu. Barevnou stupnici, která je použita pro náhled pohybu ve scéně, lze přepínat pomocí tlačítek s bílými šipkami, jak ukazuje následující obrázek.



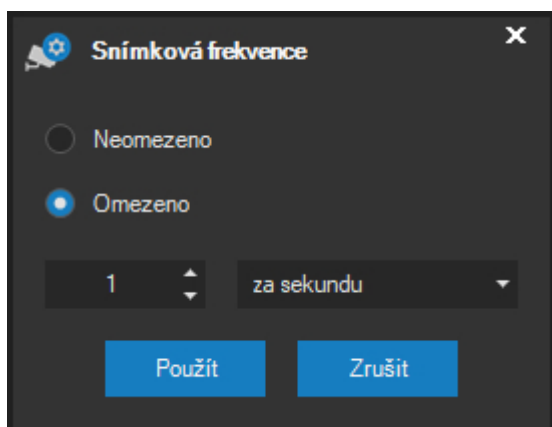
Základní nastavení

V části Detekce pohybu na serveru lze provést základní nastavení masky a snímkové frekvence pro detekci pohybu. Pomocí tlačítka **MASKA** lze aktivovat režim masky, při kterém je možné přesně určit, ve kterých oblastech scény má server provádět detekci pohybu. Masku lze definovat zcela libovolně zahrnutím či vyjmutím jednotlivých bodů masky z monitorovaného prostoru. Vytvoření masky je zcela intuitivní, pomocí techniky kreslení lze levým tlačítkem myši přidávat k masce nové části obrazu a pomocí pravého tlačítka provádět výmaz. Pro jednorázové zahrnutí celého obrazu do masky, smazání celé masky či její inverzi lze také použít tlačítka **VŠE**, **SMAZAT** a **INVERTOVAT**, která jsou dostupná po dobu definice masky.



Po opětovném stisknutí tlačítka **MASKA**, které funguje jako přepínač, bude v náhledu ihned k dispozici aktualizovaná podoba detekce pohybu.

Tlačítko **FREKVENCE** otevírá dialog pro nastavení snímkové frekvence pro detekci pohybu prováděné výpočtem na serveru. Snímkovou frekvenci lze nastavit od 10 snímků za minutu (jeden snímek za 6 vteřin) až po neomezenou snímkovou frekvenci.



Snímková frekvence udává, kolik snímků za vteřinu bude analyzováno. Pro udržení identity objektů je výchozí hodnota nastavena na 5. Snímková frekvence dekomprese videa je řízena automaticky. U formátů jiných než mjpeg tak dochází při hodnotě vyšší než 2 (za předpokladu obvyklé délky GOV) k dekompresi celého video streamu z důvodu závislosti mezi snímky.

POZOR

Nastavení vysokých snímkových frekvencí na mnoha kamerách současně a to zejména při použití megapixelového rozlišení může vést k enormní spotřebě výkonu a přetížení procesoru počítače. Nastavení by tedy mělo být vždy v souladu s možnostmi Vašeho hardware.

V rozbalovacím seznamu Výběr streamu je možné zvolit, zdali má být pro detekci použit primární či sekundární stream videa.

TIP

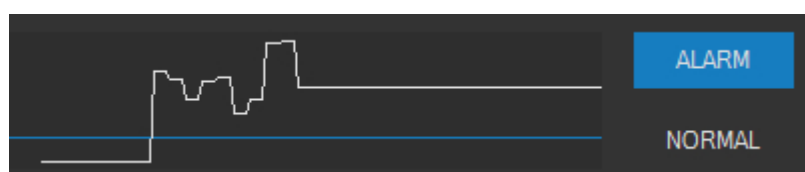
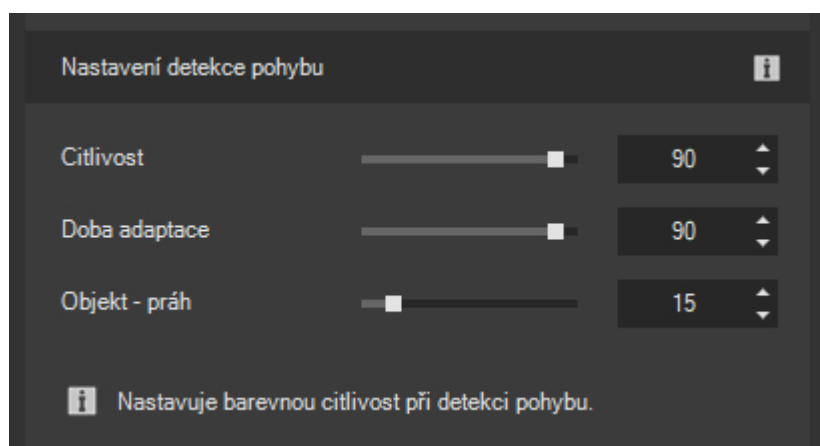
Použitím sekundárního streamu lze významně snížit nároky na výkon i při použití vyšších snímkových frekvencí.

Podrobné nastavení

Aby mohla být detekce pohybu účinně použita jako jeden z událostních vstupů, je nutné provést její vyladění pomocí dostupných parametrů. Mezi tyto parametry patří:

- citlivost – nastavuje barevnou či světelnou citlivost při detekci pohybu,
- doba adaptace – určuje dobu do splynutí pohybujících se objektů s pozadím,
- velikost objektu (práh) – nastavuje velikost objektu, který způsobí detekci pohybu.

Tyto parametry lze měnit pomocí posuvníků opatřených příslušným popisem.



Výše zobrazený ovládací prvek indikuje přepínáním mezi ALARM a NORMAL, zdali aktuálně detekovaná úroveň pohybu povede ke vzniku události. Je důležité si uvědomit, že kamerový server používá inteligentní způsob generování událostí. To znamená že pokud bude ovládacím prvkem indikován stav ALARM, poté NORMAL a v krátké době opět ALARM, systém ponechá otevřenou stále stejnou událost a nebude do systému generovat novou událost či poplach. K nové události dojde vždy až poté, co bude detekovaná úroveň pohybu určitou dobu pod prahovou hodnotou, která vyvolává událost. Tyto časové hodnoty lze nastavit v části Události.

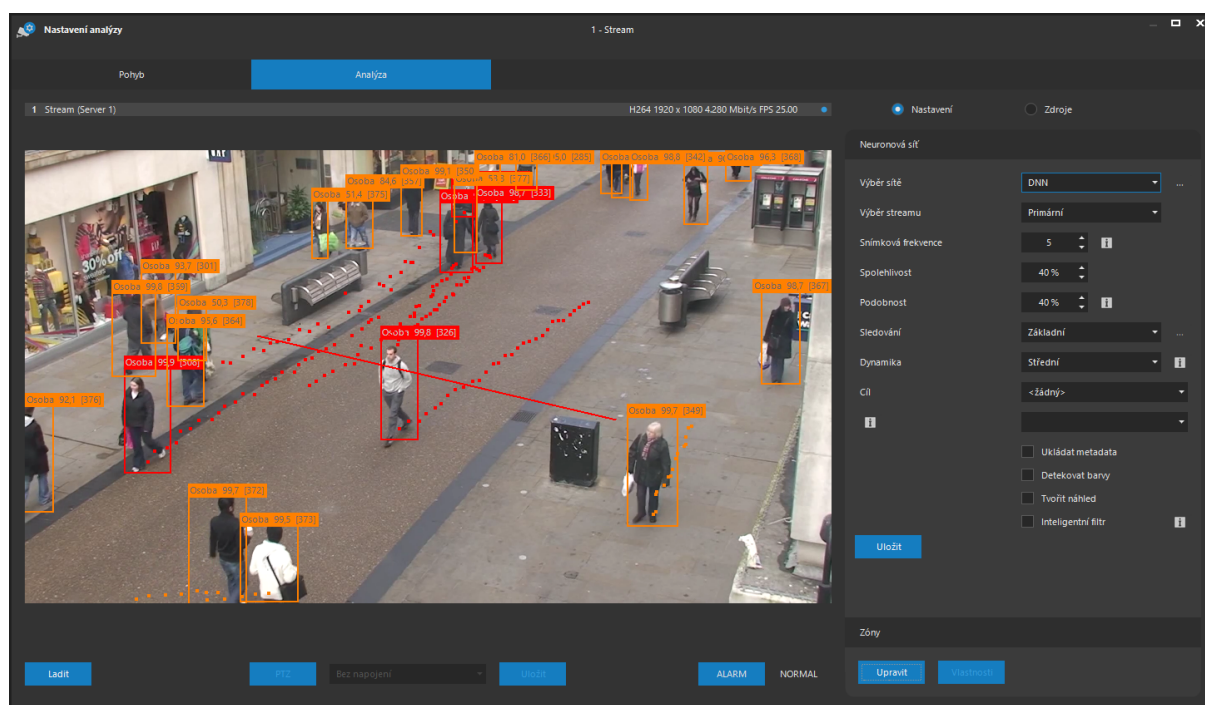
Pokud provedete změny nastavení detekce pohybu, je nutné provést jejich uložení pomocí tlačítka **ULOŽIT**. Teprve poté bude server aplikovat nová nastavení. Potřeba provést uložení je po provedení změn nastavení indikována varovným symbolem vykřičníku. Pokud přesto zapomenete uložit provedené změny nastavení, aplikace bude reagovat varovnou zprávou.

11.2.9. Nastavení zdrojů video analýzy

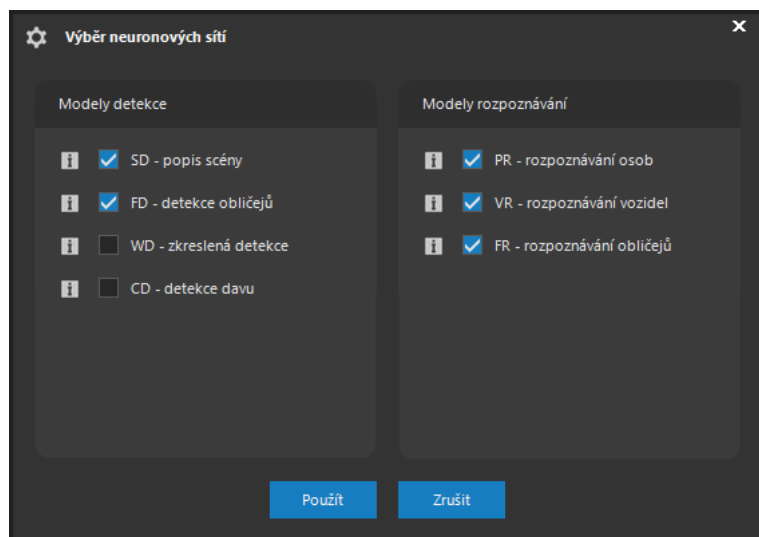
Analytické zdroje lze ovládat po stisku tlačítka **ANALÝZA** na kartě Analýza.

TIP

Nastavení lze měnit též hromadně pro více vybraných kamer současně.



V seznamu Výběr sítě je možné zvolit název odpovídající vytvořenému názvu v části administrace serverů. Název se vztahuje k zařízení (GPU) s jednou či více spuštěnými neuronovými sítěmi. Pokud neurčíme jinak, bude video z dané kamery analyzováno všemi typy sítí spuštěných na daném zařízení. To je však možné omezit po zobrazení dialogu pro výběr typů sítí.



Pokud zde však označíme typ sítě, který není na daném GPU spuštěn, nebudou výsledky analýzy pochopitelně k dispozici.

POZNÁMKA

Některé sítě na první úrovni detekce jako např. model SD a WD nelze kombinovat.

V rozbalovacím seznamu Výběr streamu je možné zvolit, zdali má být pro detekci použit primární či sekundární stream videa.

TIP

Použitím sekundárního streamu lze významně snížit nároky na výkon i při použití vyšších snímkových frekvencí.

Snímková frekvence udává, kolik snímků za vteřinu bude analyzováno. Pro udržení identity objektů je výchozí hodnota nastavena na 5. Snímková frekvence dekomprese videa je řízena automaticky. U formátů jiných než mjpeg tak dochází při hodnotě vyšší než 2 (za předpokladu obvyklé délky GOV) k dekompresi celého video streamu z důvodu závislosti mezi snímky.

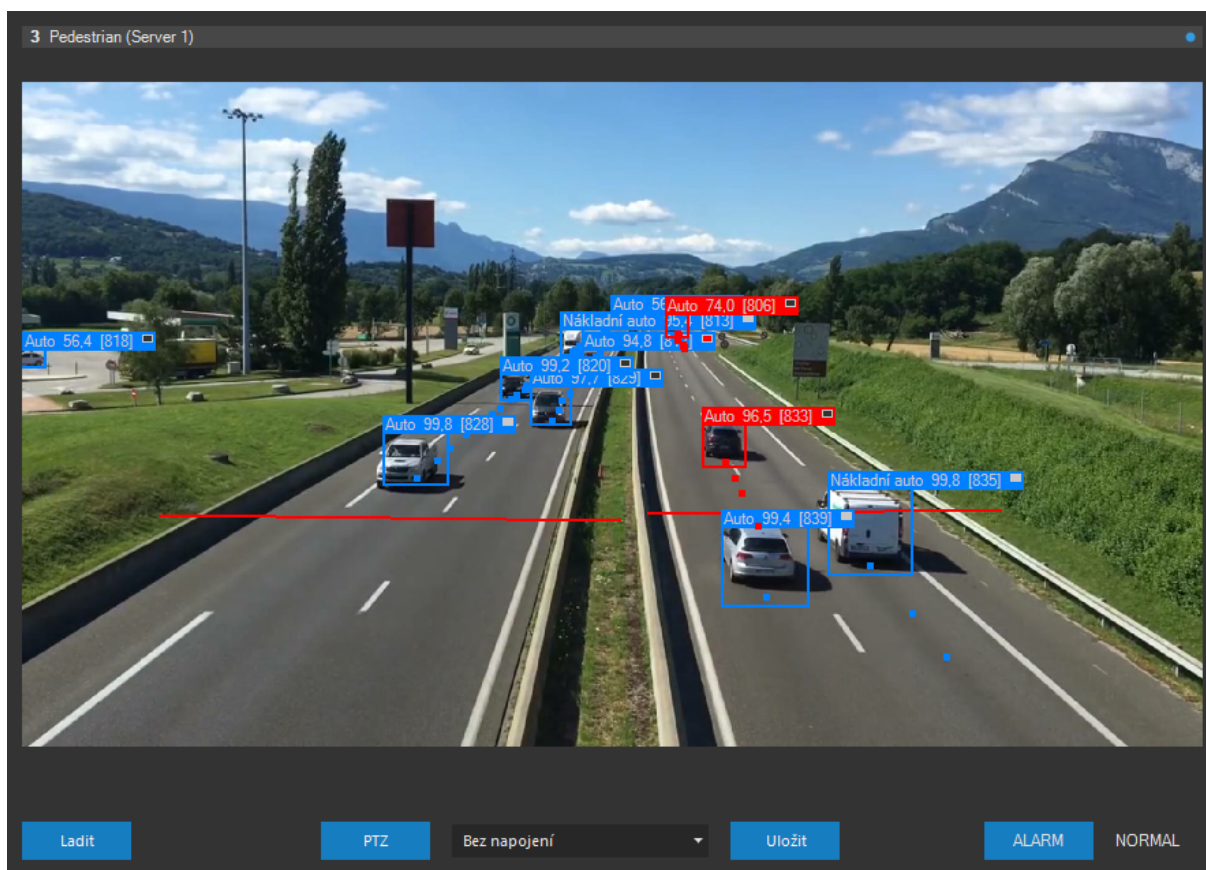
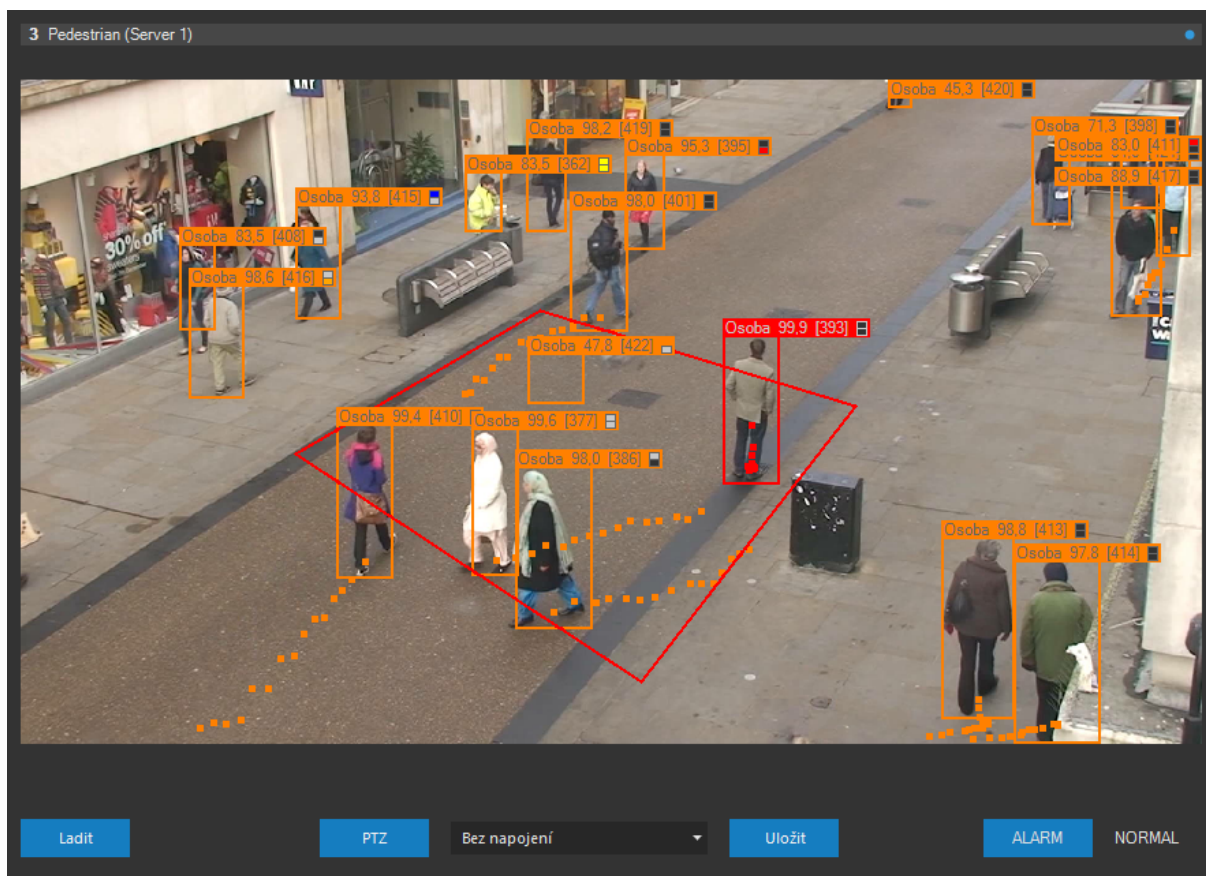
POZNÁMKA

Hodnota nula znamená neomezenou snímkovou frekvenci.

Spolehlivost udává základní prahovou hodnotu v procentech. Udává, nakolik musí neuronová síť být přesvědčena o tom, že rozpoznala určitý typ objektu, aby tento byl vykreslen do scény.

Podobnost je stejně jako spolehlivost metrika v rozsahu 0 až 100, nicméně vyžaduje odlišnou interpretaci než spolehlivost. Jedná se o hodnotu tzv. kosinové podobnosti, kdy již při dosažení hodnoty kolem 0,5 vykazují porovnávané objekty silné znaky podobnosti. V praxi budou tedy použité hodnoty významně nižší. Podobnost se používá např. u sítě Rozpoznávání obličejů.

Sledování objektů umožňuje zachování identity objektu a možnost určení jeho směru či doby setrvání ve scéně. Je tak možné používat událostní zdroje jako je podezřele dlouhé setrvání osoby ve scéně, chůze špatným směrem, protisměrná jízda automobilu anebo počítání objektů při překročení čáry.



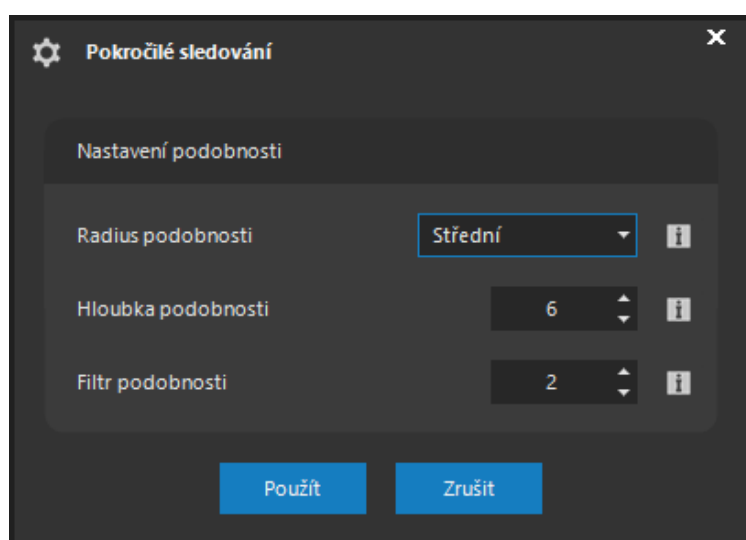
Jsou k dispozici následující typy sledování:

- Základní: Umožňuje sledování objektů až po středně zaplněné scény zájmovými objekty, používá metriky sledování a predikce pohybu objektů.
- Pokročilé: Umožňuje sledování objektů až po velmi zaplněné scény zájmovými objekty, používá kromě základních pohybových metrik též AI podobnost.

POZNÁMKA

Pokročilé sledování vyžaduje použití neuronových sítí pro rozpoznání sledovaných objektů.

Pokročilé sledování je v případě potřeby možné upravit pomocí několika parametrů v dialogu, který je možné otevřít tlačítkem vedle výběru režimu sledování.



Rádus podobnosti udává, jak velký prostorový nesoulad je algoritmus schopen překonat v případě ztráty objektu z dohledu. Přitom se nejedná jen o vzdálenosti, ale také o velikost objektu.

Hloubka a filtr podobnosti určují vliv minulých rozpoznání na sledování objektu. Pokud jsou hloubka a filtr nastaveny jako na předchozím obrázku, budou použity 3 historické vizuální reprezentace každého objektu (6 posledních s vynecháním každé druhé) pro vyhodnocení identity objektu.

Nastavení dynamiky určuje, jak velké změny v rychlosti a velikosti objektů lze ve scéně očekávat, a pomáhá algoritmu sledování optimalizovat výsledky sledování. Dynamiku lze nastavit v pěti stupních

od nízké až po vysokou s ohledem na charakter scény. Dynamika je také v jistém smyslu nepřímo úměrná snímkové frekvenci detekce.

POZNÁMKA

Sníženou detekční snímkovou frekvenci lze tedy kompenzovat použitím vyšší dynamiky scény, nicméně to vždy platí pouze do určité míry a může to snižovat spolehlivost sledování.

Stabilita identity objektů tvořená sledováním je klíčová pro kvalitní výsledky analýzy založené na identitě objektů, jako je počítání či setrvání ve scéně apod. Pro náhled a vyhodnocení sledování je možné použít tlačítko **LADIT**, které identitu objektů určenou jejich číslem zvýrazní barevně.

Nastavení cíle umožňuje přiřadit výsledky neuronové analýzy jinému zařízení v systému. Tato konfigurace je vhodná, pokud máme neuronové sítě delegované na samostatné počítače (např. optimalizované stanice s GPU) a chceme výsledky analýzy ukládat na záznamových serverech. Při nastavení cíle se pak metadata neuronové sítě automaticky přiřadí cílovému zařízení, jako kdyby byla vytvářena přímo na počítači s cílovým zařízením.

POZNÁMKA

Cílové zařízení může být připojeno ke stejnému, ale i k jinému serveru v systému.

POZNÁMKA

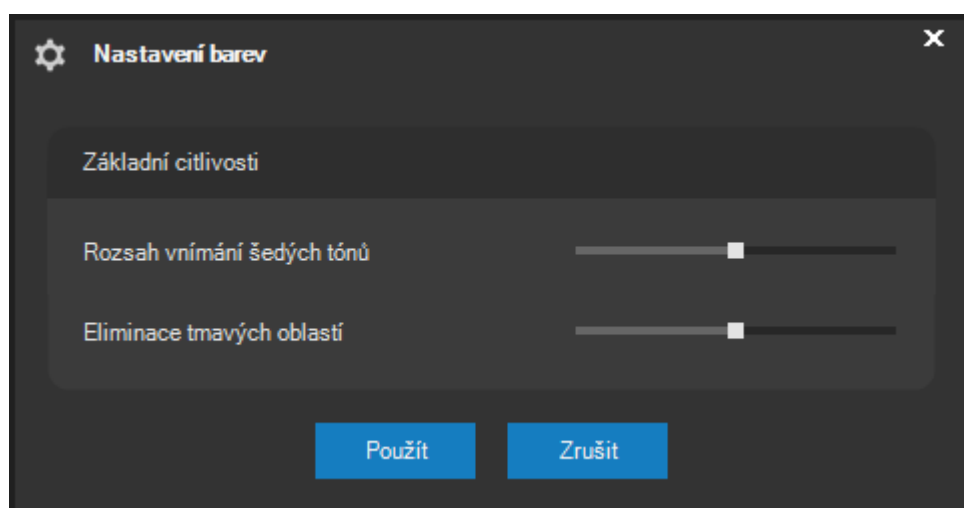
Pokud je nastaven cíl, je analýza pomocí neuronové sítě prováděna vždy, a to nezávisle na tom, zdali jsou ať už staticky anebo dynamicky plánované analytické zdroje událostí aktuálně aktivní nebo nikoliv.

Volba Ukládat umožňuje trvale uložit výstupní metadata neuronové sítě a poté je také přehrávat a vyhodnocovat spolu s videem kamery. Ukládání analytických výstupů neuronové sítě je dále také nezbytné pro použití navazujících funkcí jako je forenzní vyhledávání.

POZOR

Ukládání těchto metadat probíhá do interních databází serveru v jeho instalační složce a může být datově velmi náročné. Data jsou čištěna dle nastavení v dialogu ukládání metadat v administraci záznamu. Ukládání těchto metadat je tak nutné přizpůsobit návrh systému - výkon a velikost instalačních disků.

Volba Detekovat barvy aktivuje graficky akcelerovanou detekci přibližného barevného schématu objektů.



Dle charakteru scény lze u detekce barev upravit dva základní parametry.

Rozsah vnímání šedých tónů určuje možnou odchylku barvy od tónu šedé. Zjednodušeně řečeno tedy nastavujeme barevnou citlivost, tj. zdali bude např. šedomodrý odstín spíše považován za šedý anebo modrý.

Eliminace tmavých oblastí určuje stupeň zvýhodnění určujících barevných odstínů před tmavými částmi objektu. U osob lze tedy takto od sebe např. rozlišit převážně tmavé obleky pouze s menší částí barevného zvýraznění (např. ochranné obleky).

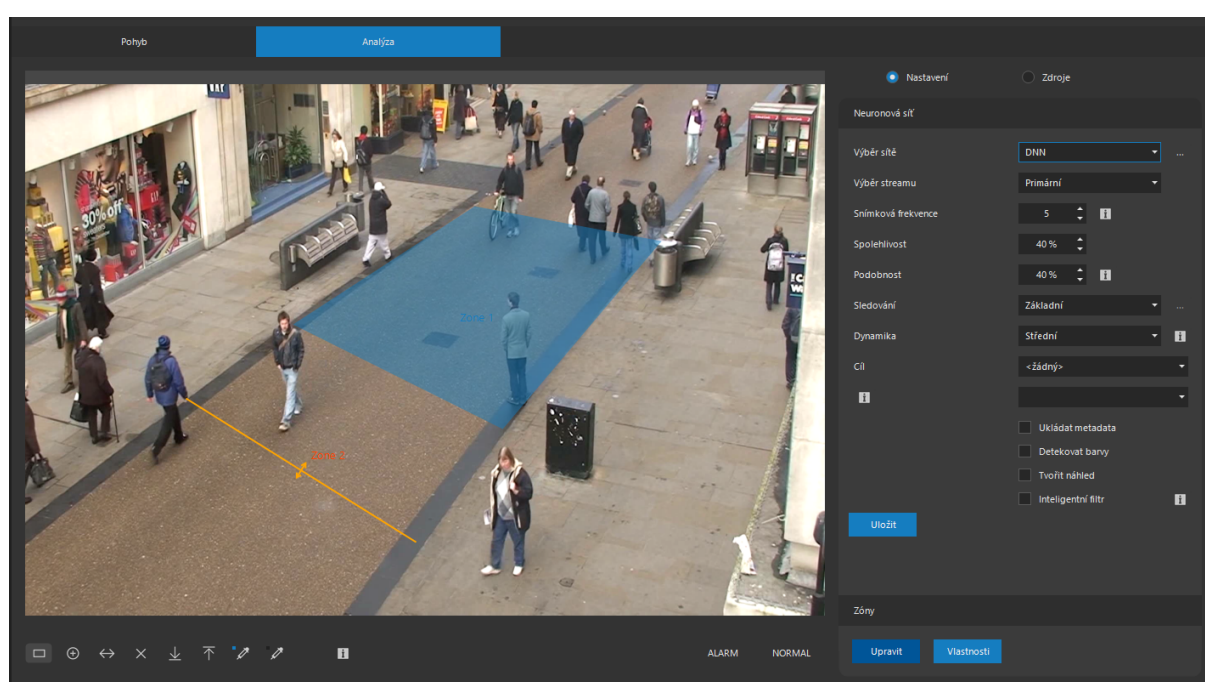
Barvy objektů jsou po aktivaci indikovány přímo ve scéně u detekovaných objektů. Zatímco některé objekty jsou označeny jednou barvou (např. vozidlo), jiné objekty (např. osoba) mohou být označeny dvěma barvami pro horní a spodní polovinu objektu.

Volba Tvořit náhled pro danou kameru aktivuje spolu s ostatními metadaty neuronové sítě také tvorbu náhledových obrazových dat. Tato funkce není podporována všemi typy sítí a používá se např. pro typ

Rozpoznávání obličejů, kde je možné získat náhledy obličejů v kanonickém (základním) tvaru a ty později použít při přidávání do databáze obličejů.

Volba Inteligentní filtr umožňuje ze scény odstranit všechny typy objektů, které nejsou součástí vytvořených zdrojů událostí. Tím se může scéna zpřehlednit. Pokud nejsou žádné zdroje definovány, jsou vždy zobrazeny všechny typy objektů.

V části Zóny lze definovat oblasti, ve kterých, jakmile do nich pronikne objekt určitého typu, může dojít ke vzniku události v systému. Oblasti je možné definovat jako obecné n-úhelníky.



Zónu lze nakreslit po aktivaci zobrazení zón tlačítkem **UPRAVIT**. Definici zóny zahájíme kliknutím myši kamkoliv do obrazu a pokračujeme kliknutím v každém bodě n-úhelníku. Ukončení tvorby zóny provedeme dvojitým kliknutím a zadáním názvu zóny.

POZNÁMKA

Při ukončení definice zóny je n-úhelník automaticky uzavřen, není tedy nutné ručně spojit zónu do uzavřeného tvaru.

Zrušení tvorby zóny lze kdykoliv provést kliknutím pravým tlačítkem myši anebo zrušením dialogu zadání názvu zóny. Vybranou zónu lze odstranit klávesou Delete nebo tlačítkem Smazat. Všechny

provedené změny jako je přidání či odstranění zóny či jejich editace a změna vlastností jsou ihned automaticky ukládány.

POZNÁMKA

Pokud při zahájení definice zóny podržíme klávesu CTRL, bude vytvořena tzv. negativní zóna, objekty v ní budou vyloučeny ze zpracování.

Pokud provedeme ukončení zóny již při druhém bodu, vznikne útvar určený pouze dvěma body, tedy čára. V případě čar dochází k aktivaci v případě překročení této čáry objektem vybraných typů, a to buď v obou směrech či v jednom z možných směrů. Směr lze určit postupným stisknutím tlačítka Směr. Je možné tvořit také lomené čáry, tj. čáry tvořené více než dvěma body. Aby v takovém případě nedošlo po zadání posledního bodu k vytvoření vyplněné zóny, je třeba použít zrušit aktivaci volby Uzavírat zóny vlevo dole pod videem.

Pokud chcete vytvořit zónu (i negativní) s počátkem v jiné zóně, je nutné při zahájení tvorby zóny podržet klávesu SHIFT, jinak by došlo k výběru a posunu aktivní zóny.

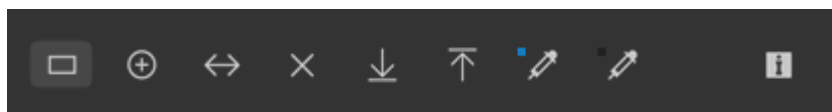
Editace již vytvořené zóny nebo čáry

Již vytvořenou zónu lze po jejím výběru libovolně přesouvat po viditelné oblasti videa. Zároveň jsou také označeny všechny její body. Přesunutím vybraného bodu zóny lze dodatečně měnit tvar zóny či čáry. Vybraný bod lze smazat klávesou Delete anebo tlačítkem Smazat.

POZNÁMKA

U uzavřené zóny nelze snížit počet bodů na méně než tři, u otevřené zóny (čáry) na méně než dva.

Pokud je naopak nutné do zóny bod přidat, je možné tak učinit po výběru bodu zóny pomocí tlačítka Nový bod pod videem.



Pokud barevnost scény neumožňuje dobře vidět nakreslené zóny, je možné změnit jejich barvu pomocí tlačítek s barevným indikátorem pod videem. Samostatně lze měnit barvu běžných zón a čar a negativních zón a čar. Pravým tlačítkem lze vrátit barvu do výchozí podoby.

POZNÁMKA

Šířku pera pro kresbu zón je možné ovlivnit spolu s kresbou dalších analytických výstupů v lokálním nastavení klienta v části Zobrazení videa.

Omezení velikosti detekovaných objektů

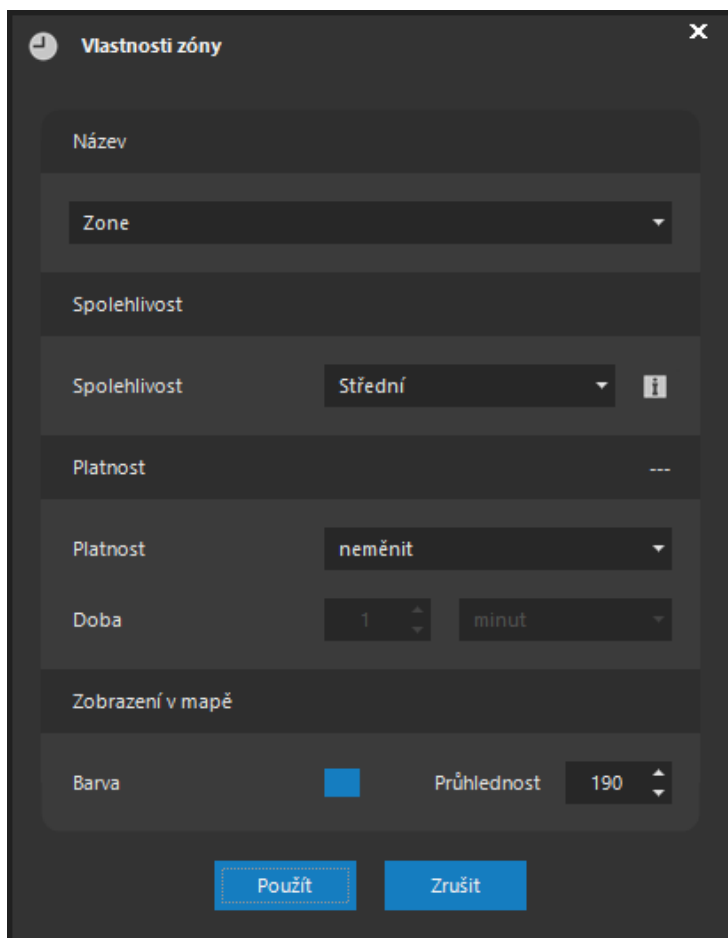
Pomocí tlačítek pro omezení velikosti objektu lze pro každou zónu včetně dvou či vícebodových čar aktivovat minimální a současně též maximální velikosti objektu. Nastavení velikosti se provede úpravou velikosti obdélníku určující rozměr objektu – jeho výšku a šířku. Při aktivaci minimální či maximální velikosti (anebo obou) se za vyhovující objekt považuje ten, který splňuje vždy jak omezení pro výšku, tak pro šířku. Např. při nastavené maximální velikosti nesmí velikost objektu překročit ani výšku, ani šířku.

POZNÁMKA

Při aktivaci filtru velikostí objektů jsou objekty spadající mimo rámec minimální a maximální velikosti nadále zobrazeny ve scéně, jsou však vyloučeny z událostního řízení – nemohou vyvolat událost.

Vlastnosti zóny

Název a další vlastnosti zóny lze kdykoliv změnit po jejím výběru pomocí tlačítka **VLASTNOSTI**. Systém automaticky ohlídí případné duplicity v názvech.



Pro vybranou zónu je možné upravit její spolehlivost, výchozí hodnota je střední spolehlivost. Tento parametr umožňuje doladit vznik poplachového stavu pro vybranou zónu. Vedle samotné spolehlivosti detekce objektu zadané v procentech (skóre objektu) udává tento parametr spolehlivost identifikace objektu v čase (tj. že se jedná o stále stejný objekt). Tímto parametrem je ovlivněn pouze přechod přes liniové zóny, u plošných zón lze podobného efektu zvýšení spolehlivosti dosáhnout nastavením parametru doby setrvání ve scéně.

V tomto dialogu je dále možné omezit platnost zóny pouze na určitou dobu, a to buď zadáním předdefinované anebo vlastní platnosti. Po uplynutí takto nastavené doby je zóna automaticky deaktivována.

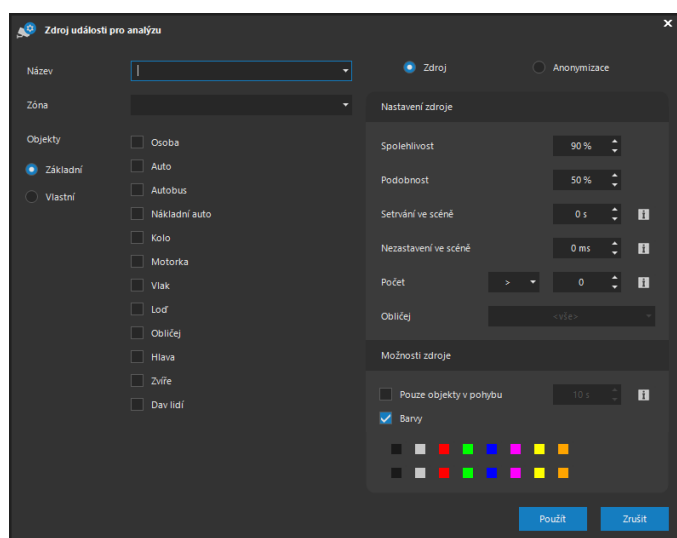
TIP

Omezenou platnost lze s výhodou použít i pro negativní zóny.

V části **Zobrazení v mapě** je možné určit barvu a průhlednost zóny, která je lokalizována a zobrazena v mapě.

Na kartě **Zdroje** v části Zdroje událostí lze pro každou kameru definovat zdroje událostí, se kterými bude dále zacházeno jako s jinými událostními zdroji systému (plánování, událostní scénář).

Pokud je kameře přiřazena neuronová síť, můžeme pomocí tlačítka **NOVÝ** anebo **UPRAVIT** vyvolat dialog pro tvorbu událostního zdroje. Tlačítkem **SMAZAT** je možné vybraný událostní zdroj odstranit.



Při tvorbě nového nebo úpravě zdroje události je třeba zadat jeho název, určit zónu, ve které bude neuronová síť reagovat na vybrané typy objektů, a vybrat jeden či více typů objektů v seznamu. Objekty jsou rozdělené do dvou skupin, je možné provádět výběr současně z obou dvou. V základní skupině jsou uvedeny objekty, které jsou podporovány volně dostupnými neuronovými sítěmi ATEAS, ve vlastní skupině jsou zobrazeny typy objektů, které si vytvoříte sami. Více viz kapitola o vlastních typech objektů.

POZNÁMKA

Objekt typu zvíře podporuje pouze několik běžných druhů zvířat jako pes, kočka, kráva, ovce či kůň a potřebuje pro úspěšnou detekci dostatečné rozlišení, detekce není vhodná pro objekty v pozadí.

TIP

U názvů zdroje aplikace nabízí již existující názvy. Použití stejných názvů umožní zdroje automaticky sdružovat při vyhledávání metadat a tvorbě grafů.

Nastavením spolehlivosti a podobnosti pak určíme prahové hodnoty, nakolik musí být síť přesvědčená, že rozpoznala objekt určitého typu.

Podobnost je jiná metrika než spolehlivost a je vyžadována pro některé typy neuronových sítí jako např. rozpoznávání obličejů. Její popis je uveden výše v části nastavení analýzy.

POZNÁMKA

Spolehlivost či podobnost při vytváření událostního zdroje mohou být nastaveny na vyšší hodnoty než při detekci objektů pro danou kameru. To umožňuje, aby byly vykreslovány objekty s nižší spolehlivostí bez toho, aby systém reagoval událostí.

Jestli má dané nastavení potenciál vyvolat v systému událost, je zjevné po uložení zón a zdrojů událostí přímo v okně analýzy na základě stavů ALARM a NORMAL. Zóna, ve které došlo ke vzniku události, je automaticky zvýrazněna.

U událostí typu překročení čáry může pokročilé sledování zajistit lepší výsledky zejména v zaplněných scénách, protože na rozdíl od základního sledování nevyžaduje dosažení poplachové spolehlivosti přímo při přechodu čáry, ale klidně i později.

Pokud navýšíme hodnotu Setrvání ve scéně z výchozí hodnoty nula, bude událost vytvořena až tehdy, pokud objekt setrvá v dané zóně daný počet vteřin. Je tedy možné generovat událost např. při podezřele dlouhém pobytu osoby ve scéně, příliš pomalé jízdě auta na dálnici, zastavení vozidla v tunelu apod.

POZNÁMKA

Parametr setrvání bude účinný pouze v případě aktivního sledování a u zón určených plochou.

Nastavení Nezastavení ve scéně pomáhá poplachově reagovat na situace, kdy nedojde k zastavení objektu na definovanou dobu. Pro využití této funkce je nutné vytvořit alespoň dvě zóny, z nichž jedna

musí být uzavřená (detekční) a druhá může být i otevřená (poplachová). V poplachové zóně pak dojde k události vždy, když daný objekt nezastaví v detekční zóně alespoň na určenou dobu.

Pro přesné fungování této funkce je pochopitelně nutné, aby detekční snímková frekvence byla kompatibilní s požadovanou dobou zastavení. Např. snímková frekvence 5 nebude schopna reagovat na zastavení kratší než 200 ms.

TIP

Tato funkce může být využita např. jako automatizovaný systém kontroly zastavení vozidla u dopravní značky Stop.

V nastavení Počet můžeme určit, při jakém počtu vybraných objektů vznikne událost. Tímto způsobem (a např. i v kombinaci s parametrem doby setrvání ve scéně) můžeme automaticky reagovat na postávající hlouček více osob, dopravní zácpu apod. Hodnota může být nastavena jako přesná hodnota, anebo hodnota větší nebo menší než zadaný počet. Při nastavení počtu na nula bude událost vyvolána, pokud nebude v zóně detekován žádný objekt (alternativně lze řešit operátorem negace ve složených událostech).

Pokud je označeno více typů objektů, vztahuje se počet na všechny typy. Pokud bychom chtěli reagovat na konkrétní počet více různých typů objektů (s rozlišením podle objektů), lze na základě jedné zóny vytvořit více zdrojů událostí a zkombinovat je pomocí složené události.

Pokud je do události zahrnut objekt typu obličej a probíhá zároveň jejich rozpoznávání, můžeme v části Obličej událost omezit jen na určitou skupinu osob z databáze obličejů. Omezení na pouze jednu osobu lze provést jednoduše tak, že v konkrétní skupině bude pouze jedna zájmová osoba.

Volba Pouze objekty v pohybu umožní reagovat událostí pouze na objekty, které jsou v pohybu. Časová hodnota udává dobu, po kterou musí být objekt v klidu, aby nebyl považován za objekt v pohybu.

TIP

Funkci lze například využít pro snížení počtu planých poplachů i bez tvorby negativních poplachových zón.

Volbou Barvy lze zobrazit přehled barev, které mohou být součástí vyhodnocení události. Pokud jsou nějaké barvy vybrány, bude událostní řízení vztaženo jen na objekty, které jsou zbarveny jednou z vybraných barev. Pro objekty typu osoba mohou být vybrány barvy v obou řadách, které se vztahují na horní a spodní část osoby.

Po vytvoření jednoho či více zdrojů událostí, můžeme tyto v systému dále nastavit či používat v rámci serverových zdrojů událostí.

POZNÁMKA

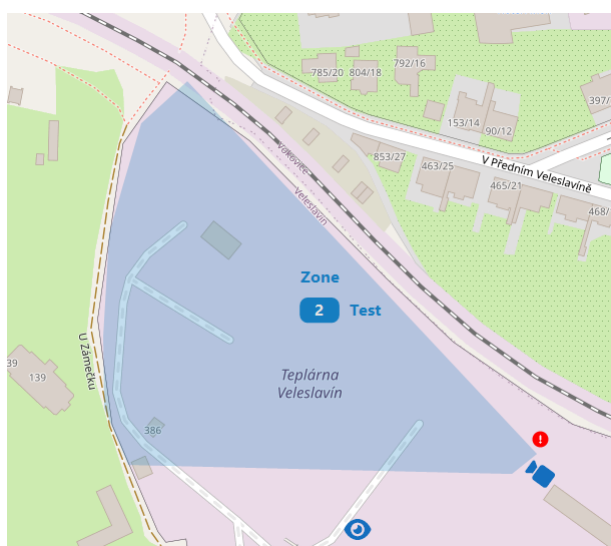
Všechny tyto hodnoty lze také definovat v části inteligentního vyhledávání nad neurálními metadaty, kde mají shodný význam.

POZNÁMKA

V seznamu analytických událostních zdrojů se zobrazují automatické číselné identifikátory, které jsou použity při publikaci událostí přes integrační kanál ATEAS API.

11.2.10. Lokalizace zón v mapě

Velmi podobným způsobem, jakým jsou v mapě lokalizovány kamery, externí prvky či uživatelská tlačítka, mohou být lokalizovány také zóny. Po aktivaci zóny a stisknutí lokalizačního tlačítka v mapě bude v tomto případě nutné postupným klikáním zakončený dvojklikem označit polygon, nikoliv pouze jeden bod.

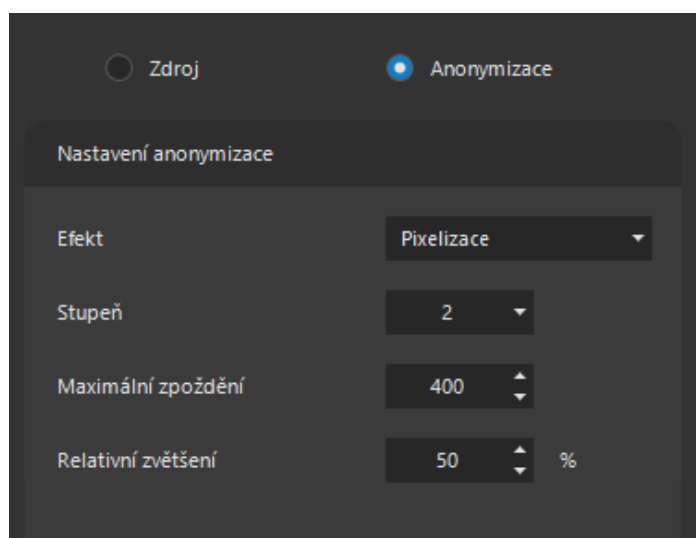


Pokud jsou v mapě lokalizovány zóny, kromě zlepšení přehledu bude možné také automaticky zobrazovat video při najetí na zónu, případně také směřovat kameru na navázaný preset. Dále budou také automaticky zobrazeny automatické zónové čítače, které jsou popsány v samostatné subkapitole.

Zóny jsou také integrovány ve vyhledávání v mapovém okně.

11.2.11. Anonymizace videa

Provozovatel kamerového systému musí nakládat s vizuálními osobními údaji dle požadavků platné legislativy týkající se ochrany osobních údajů. Pomocí voleb v části Anonymizace lze takové požadavky jednoduše naplnit.



Anonymizovány budou všechny typy objektů aktuálně vybrané v nastavení zdroje události. Anonymizace se týká jak živého videa, tak záznamu. Pro prohlížení videa bez anonymizace je nutné mít přiděleno speciální oprávnění pro deanonymizaci.

V seznamu Efekt lze vybrat vizuální provedení anonymizace, tím může být např. kompletní začernění objektů nebo pixelizace. Pro pixelizaci lze dále vybrat i stupeň, čím vyšší stupeň, tím silnější bude efekt anonymizace.

POZNÁMKA

V rámci nastavení konkrétní síly efektu je u bližších a vzdálenějších objektů aplikován shodný stupeň anonymizace, velikost čtverců u pixelizace se tedy automaticky mění s velikostí objektu.

Údaj Maximální zpoždění je zadáván v milisekundách a určuje časovou platnost detekovaných objektů pro účely anonymizace. Jakmile by pro danou zónu nebyly k dispozici údaje o detekovaných objektech v rámci povoleného časového intervalu, zóna by byla anonymizována celá, čímž je zabráněno možnému neautorizovanému zobrazení citlivých údajů v obraze.

Maximální zpoždění zároveň udává i technologické zpoždění anonymizovaného videa, tak aby nedocházelo k částečným zobrazením objektů a neúplné anonymizaci v důsledku zpoždění výpočtů neuronové sítě.

Hodnota Relativní zvětšení udává, o kolik procent bude zvětšena oblast anonymizace oproti skutečné velikosti objektu.

TIP

Nastavení objektů pro anonymizaci může být v každé vytvořené zóně odlišné.

11.2.12. Statické masky tvořené na serveru

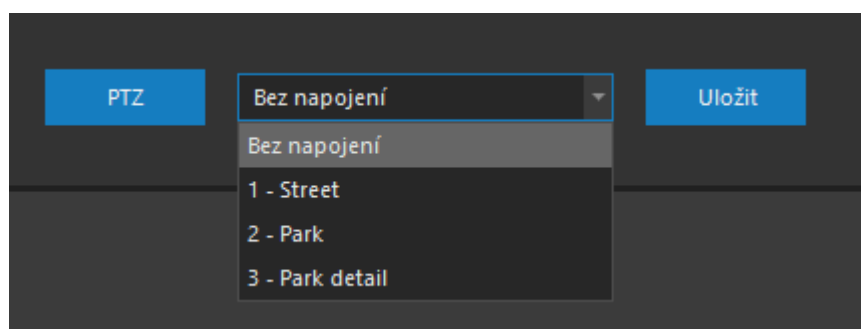
Pokud při tvorbě analytického událostního zdroje určíme zónu, nikoliv však typy objektů, získáme automaticky funkci statické masky. Zóna bude v takovém případě anonymizována vždy celá nastaveným efektem anonymizace.

POZNÁMKA

V porovnání s maskou vytvořenou v kamerách má tento přístup zásadní výhody, neboť možnost odmaskování je vázána pouze na uživatelské oprávnění a nikoliv na nutnost ukládat druhý video stream.

11.2.13. Vazba zdrojů analýzy na prepozice

U otočných kamer je kresba zón a navazující analýza s událostmi složitější o to, že kamera může být volně otáčena. Proto existuje u otočných kamer možnost svázat zóny (vyplněné zóny i čáry) s danou prepozicí (presetem) kamery. Vazba zóny na konkrétní prepozici se provede výběrem prepozice pod náhledem videa.



Po výběru prepozice je kamera automaticky nasměrována a jsou zobrazeny zóny přiřazené k této prepozici, které je možné upravovat anebo tvořit nové.

Aktivní události založené na zónách přiřazených prepozicím kamery budou moci vznikat, pouze nachází-li se kamera na dané prepozici, kam může být přepnuta uživatelem, automaticky túrou anebo při události. Pokud je kamera přesměrována jinam, událost vzniknout nemůže.

Tato funkce se projeví i v inteligentním vyhledávání, kde budou vždy vyhledány jen relevantní výsledky vzhledem k vybranému presetu.

POZOR

Při vícenásobném přidání otočné kamery k serveru a svázání pomocí hodnoty posunu pro detail je pro kamery s nastavenou hodnotou posunu automaticky aktivováno podřízené PTZ ovládání, aby mohl být dodržen princip priorit ovládání. Proto je nutné analýzu s vazbou na preset nastavit vždy na cílové kameře.

Pokud je nutné upravit preset, je možné tak učinit přímo z okna analýzy. Tlačítko **PTZ** aktivuje plnohodnotné ovládání kamery a tlačítko **ULOŽIT** umožní přepis stávající pozice.

TIP

Tento postup urychlí práci, pokud je potřeba jemně posunout preset vzhledem k již nakresleným zónám.

11.2.14. Podrobné nastavení

Nastavení detailních parametrů jednotlivých kamer se provádí přímo v rozhraní, které pro nastavení nabízí jednotlivé kamery (nejčastěji webové rozhraní dostupné protokolem http).

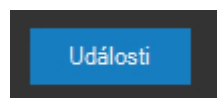
Pomocí tlačítka **NASTAVIT** lze automaticky otevřít výchozí webový prohlížeč, který je přesměrován na web kamery. Základním rozdílem oproti přímému přístupu na web kamery je skutečnost, že přístup na web zprostředkuje přímo kamerový server na své adrese a určeném portu 8506. Pokud má tedy webový prohlížeč otevřenu tuto adresu a v seznamu kamer v administrační sekci dojde k výběru jiné kamery, po obnovení stránky v prohlížeči budete ihned automaticky přesměrováni na další kameru.

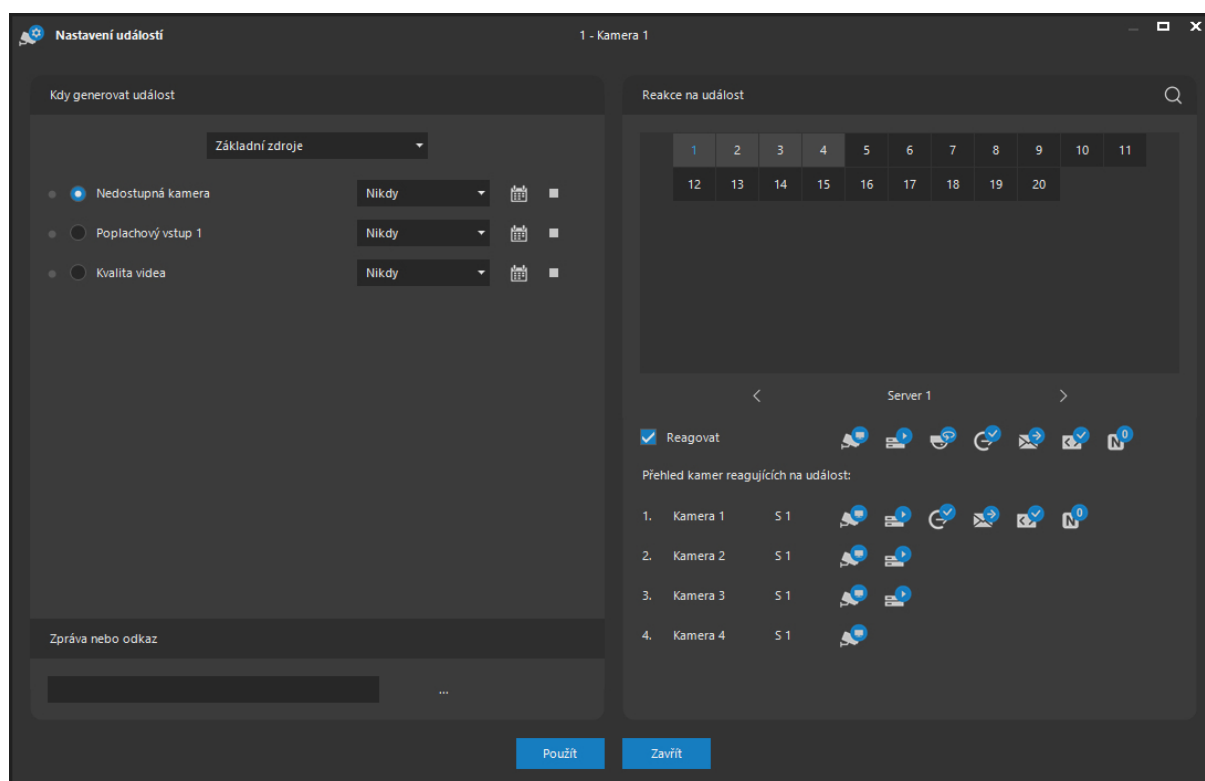
POZNÁMKA

Pomocí této funkce lze tedy kdykoliv přistoupit na web kamer v lokální síti i vzdáleně, a to bez toho, aniž by byly přesměrovány jejich porty např. pomocí NAT. Jediný port, který musí být dostupný, je port 8506 kamerového serveru.

11.2.15. Události a jejich management

Do části nastavení událostí (mapování a nastavení zdrojů události a vytváření událostního scénáře) lze vstoupit po stisku tlačítka **UDÁLOSTI**. V tomto okně lze provádět veškeré funkce událostního managementu. Základním principem je vytvoření událostního scénáře pro daný zdroj události (událostní vstup). Událostní scénář pro vybraný událostní vstup může libovolně obsahovat akce na jiných kamerách i na jiných serverech.





Zdroje událostí

V části Kdy generovat událost je k dispozici seznam všech zdrojů událostí vybrané (právě nastavované) kamery. Jednotlivé zdroje jsou rozděleny do logických skupin podle povahy (základní zdroje, serverové zdroje, vlastní zdroje, poznávací značky vozidel, analýza). Vlevo od každého zdroje události je zobrazen barevný indikátor, zdali je konkrétní událost vyvolaná příslušným zdrojem aktuálně aktivní či nikoliv.

Mezi běžně používané Základní zdroje patří:

- **Nedostupná kamera:** Pro kamery připojené ke kamerovému serveru je nepřetržitě prováděno testování jejich přítomnosti v síti, pokud je detekován výpadek, může dojít ke vzniku události (zde nehovoříme o ztrátě videosignálu u zařízení s analogovým video vstupem, viz níže).
- **Aktivace poplachového vstupu:** V závislosti na nastavení může být událost vyvolána změnou stavu příslušného poplachového vstupu kamery.
- **Kontrola kvality videa** v podobě hlídání snímkové frekvence.

Mezi běžně používané Serverové zdroje patří:

- Detekce pohybu: Na základě analýzy obrazu kamery přímo na serveru jsou neustále vyhodnocovány údaje o detekovaném pohybu dle nastavení masky, citlivosti, velikosti objektu atd.

Mezi běžně používané Vlastní zdroje patří:

- Detekce zvuku: U kamer podporujících tuto funkci je možné vyvolat událost při detekci zvuku (překročení prahu hlasitosti nebo naopak dosažení prahu ztišení).
- Detekce sabotáže: U kamer podporujících tuto funkci je možné vyvolat událost při detekci sabotáže kamery (náhlé otočení, zakrytí výhledu, ztráta světla, postříkání sprejem).

POZNÁMKA

Více o vlastních událostech se dozvíte v kapitole Vlastní události kamer.

Mezi běžně používané zdroje událostí ze skupiny Poznávací značky patří:

- Neregistrovaná RZ: Událost bude vyvolána tehdy, pokud detekovaná RZ není registrovaná v žádném seznamu.
- Povolená RZ: Událost bude vyvolána tehdy, pokud je detekovaná RZ registrovaná v seznamu povolených RZ.
- Zakázaná RZ: Událost bude vyvolána tehdy, pokud je detekovaná RZ registrovaná v seznamu zakázaných RZ.
- Uživatelské RZ: Událost bude vyvolána tehdy, pokud je detekovaná RZ registrovaná v některém z uživatelských seznamů RZ.

POZNÁMKA

Více o detekci RZ vozidel se dozvíte v kapitole Správa doplňků – modul detekce RZ.

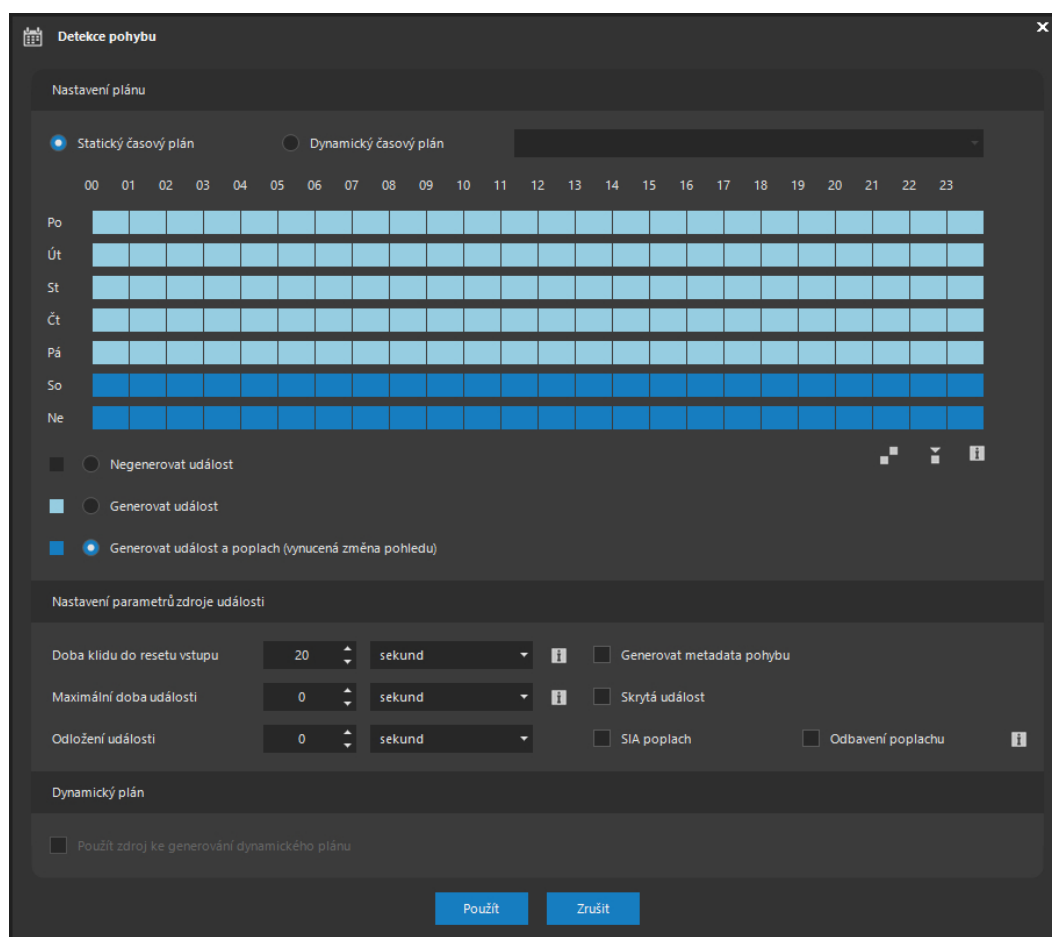
V seznamu Zdroje události je u kamer připojených pomocí rozhraní Onvif k dispozici také volba Onvif, pomocí které je možné vytvářet události ze zdrojů poskytovaných pomocí Onvif rozhraní. Využití těchto zdrojů událostí je popsáno v další subkapitole.

Na konci řádku s každým událostním zdrojem je zobrazena aktuálně přiřazená barva. Barvu je možné změnit kliknutím na barevný symbol a vybrat jakoukoliv uživatelsky definovanou barvu. Tato barva je pak použita u událostí zobrazených na časové ose při přehrávání záznamu.

TIP

K původní výchozí barvě se lze rychle vrátit kliknutím pravým tlačítkem myši.

V rozbalovacím seznamu vedle každého zdroje události je možné zvolit, kdy může daný zdroj události generovat událost či poplach. První možností je Nikdy (zdroj události nebude monitorován), druhou možností je Dle plánu. Po výběru této druhé možnosti nebo po stisku tlačítka kalendáře se zobrazí okno, kde je možné graficky vyznačit dobu, kdy bude daný zdroj události monitorován.



V části Nastavení plánu je možné pro událostní vstup vytvořit statický časový plán nebo využít dynamicky generovaného plánu v systému. Dynamickému plánování je věnována samostatná subkapitola. Pokud je zvolen dynamický plán, je prvek pro design statického plánu nedostupný, neboť

skutečnost, je-li událostní vstup aktivní (např. zdali probíhá detekce pohybu) je určována dynamicky v závislosti na jiném událostním vstupu.

Při použití statického plánování je k dispozici ovládací prvek pro grafické nastavení časového plánu monitorování daného zdroje události (událostního vstupu). Jednotlivé řádky reprezentují dny v týdnu, ve vertikálním směru je k dispozici rozdělení dne do 24 hodin, minimální rozlišení je 15 minut. Jednotlivé čtvrt hodinové úseky lze označit pohybem myši při stisknutí levého či pravého tlačítka myši. Při stisknutí levého tlačítka myši bude použito vždy nastavení přepínače pod ovládacím prvkem. Při použití pravého tlačítka bude vždy docházet k vymazání obsahu tj. překreslení do výchozí podoby (odpovídá levému tlačítku při označeném přepínači Negenerovat událost).

TIP

Pro rychlé označení celého dne nebo týdne lze použít dvojité resp. trojitě kliknutí.

Pro rychlé přenesení statického plánu do jiného zdroje události slouží možnost jeho kopírování a vložení pomocí tlačítek vpravo pod plánem.

TIP

Pro rychlé určení pracovní doby ve více dnech najednou použijte klávesu ALT.

Rozdíl mezi přepínači Generovat událost a Generovat událost a poplach spočívá ve významnosti generované události. Událostní scénář je v obou případech vždy stejný. Vzhledem k tomu, že běžné události nevynutí u klientů automatické přepnutí do událostního pohledu a mohou být navíc klienty též odfiltrovány úplně, lze docílit i velmi účinných scénářů. Průchod osoby chodbou za dne vždy vyvolá spuštění záznamu, ovšem pouze v noci se obsluze automaticky přepne chodba na monitor.

Pro každý událostní zdroj je možné aktivovat volbu Skrytá událost (stejně nastavení je k dispozici i pro plánované události v systému). Pokud je volba aktivována, uživatelé se o události nedozví, neboť bude v čase výskytu skryta před klienty systému. Událostní scénář, všechny reakce na událost a uložení do metadat systému proběhne beze změny. Skrytá událost však není uložena mezi události vyvolávající záznam, není tedy obsažena v seznamu událostí v okně Záznam a nezatěžuje svým zobrazením časovou osu při přehrávání záznamu.

POZNÁMKA

Skryté události je možné využít např. u komplexních událostí, kdy nechceme dílčí události propagovat směrem ke klientům systému. Použití skryté události je vhodnější než alternativní řešení jako je omezení práva uživatelů přijímat události ze všech či konkrétních kamer anebo vypnutí příjmu běžných událostí v lokálním nastavení.

V části Nastavení parametrů zdroje události je možné nastavit dodatečné parametry událostního vstupu.

Pro zdroje událostí typu poplachových vstupů na zařízeních (netýká se např. pohybové detekce) lze určit, jestli událost vznikne při aktivaci nebo deaktivaci vstupu. To je důležité např. u některých pohybových čidel, které elektricky fungují tak, že při absenci pohybu jsou v sepnutém stavu a při detekci pohybu v nesepnutém.

Parametr Doba klidu do resetu vstupu udává minimální dobu, po kterou musí být událostní vstup v klidu, aby jeho další aktivace vedla ke vzniku nové události. Pokud mezi dvěma narušeními neuplyne alespoň tato nastavená doba, systém obě narušení spojí v jednu událost.

Parametr maximální doba události dovoluje omezit maximální dobu trvání jedné události. Tímto způsobem lze tak např. ochránit záznamovou oblast před vyčerpáním, pokud je v reakci na událost prováděn záznam vysokou snímkovou frekvencí, nebo vynutit návrat otočné kamery z poplachové tůry po určité maximální době.

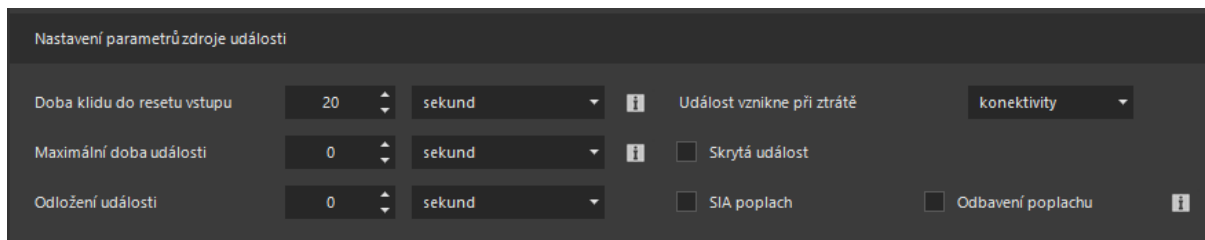
POZNÁMKA

Pokud je maximální doba trvání události nastavena na hodnotu nula, znamená to, že pro událost nebude stanovena žádná maximální doba trvání.

Zmíněnou dobu klidu do resetu vstupu lze pro každý vstup nastavit samostatně.

Pro všechny událostní zdroje lze dále aktivovat odložení události. Je-li nastavena doba odložení události na hodnotu vyšší než nula, bude kamerový server při aktivaci událostního zdroje čekat po nastavenou dobu a teprve poté vygeneruje událost. Pokud v této době dojde k opětovné deaktivaci zdroje, událost nevznikne. Tuto funkci je možné využít v mnoha praktických situacích, např. pokud bychom chtěli monitorovat ponechané otevřené dveře, ale zároveň vyloučit běžné průchody dveřmi, při kterých jsou dveře po několika vteřinách zavřeny.

Pro událostní zdroj Nedostupná kamera je k dispozici rozšiřující nastavení, ve kterém je možné určit, jakým způsobem bude nedostupnost kamery vyhodnocena. Ve výchozím nastavení je nedostupnost kamery vyhodnocena jako její nedostupnost na dané adrese a portu pomocí pravidelných TCPIP zpráv (volba konektivita).



Tento způsob vyhodnocování Vás automaticky upozorní na různé druhy výpadků jako je výpadek kamery na síti, její odpojení, výpadek napájení apod. V praxi se však mohou vyskytnout případy, kdy dojde k výpadku kamery (resp. videa) bez ztráty IP konektivity (např. problém firmware kamery). V takovém případě sice mohou být klienti systému upozorněni výstražným textem přímo v okně zobrazení kamery (pokud je právě sledována), ale nebylo by možné generovat v systému událost. Pokud ovšem nastavíme vyhodnocování nedostupnosti na základě ztráty videa, bude systém schopen vyvolat automaticky událost i v těchto případech.

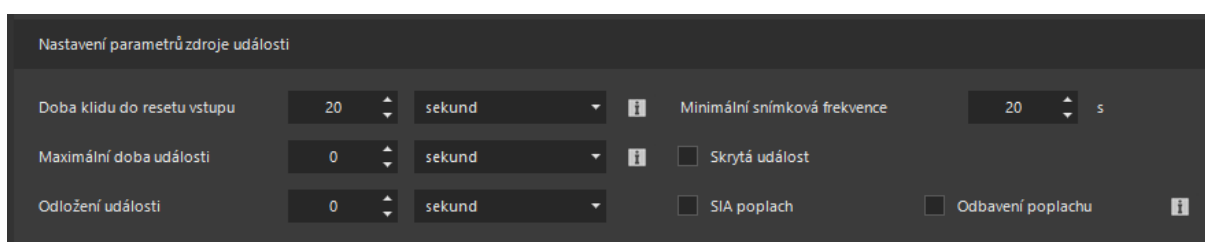
POZNÁMKA

Vyhodnocování nedostupnosti kamery na základě ztráty videa sice pokrývá větší množinu různých výpadků, na druhou stranu ovšem může generovat plané poplachu pokud dojde ke krátkodobému přetížení sítě (a rozpadu videa) apod.

POZOR

Vyhodnocování nedostupnosti kamery na základě ztráty videa také není možné použít, pokud není pro kameru nastaveno udržování permanentního spojení (připojení kamery probíhá, pouze pokud je to nutné – video on demand).

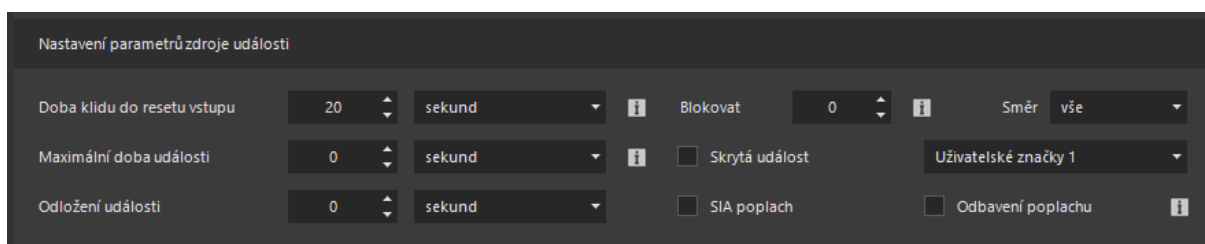
Pro událostní zdroj Kvalita videa lze v rozšířených nastaveních určit mezní hodnotu snímkové frekvence. Pokud aktuální snímková frekvence klesne pod tuto hodnotu, dojde ke vzniku události.



POZNÁMKA

Stejně jako v případě jiných událostních zdrojů lze i hlídání kvality videa kombinovat s nástrojem odložených událostí. Pokud chceme např. tolerovat dočasný pokles kvality videa na dobu 5 vteřin, lze aktivovat odložení události na danou dobu.

Pro událostní zdroje detekce a rozpoznávání RZ vozidel umožňuje rozšířené nastavení určit též počet vteřin, po který bude detekovaná RZ blokována na ostatních kamerách kamerového serveru.



Blokování je vhodné použít např. u obousměrných vjezdů s jedním pruhem se dvěma kamerami – pro příjezd a odjezd vozidel. V takovém případě budeme chtít, aby druhá kamera danou RZ po určitou dobu ignorovala.

Pomocí volby Směr je možné událost navázat jen na zjištěný směr vozidla.

POZNÁMKA

Aby určení směru bylo spolehlivé, je nutné správně nastavit snímkovou frekvenci a prahový počet rozpoznání na hodnotu pokrývající celý rozsah hloubky ostrosti kamery, kde rozměr RZ spadá do nastavených hranic minimální a maximální šířky.

Speciálně pro událostní zdroje uživatelských RZ lze také vybrat jiný než výchozí seznam RZ. Je tak možné, aby různé kamery (např. připojené k různým serverům) svázaly tento událostní zdroj s různými seznamy RZ.

Pro událostní zdroj detekce pohybu na serveru lze aktivovat volbu ukládání metadat pro pozdější vyhledávání změn v obraze pomocí funkce inteligentního vyhledávání v záznamu.

Ukládání těchto metadat probíhá obdobně jako ukládání metadat neuronových sítí a vztahuje se na ně stejná maximální doba archivace. Pokud je tato volba aktivována, bude možné v okně hledání ve videu vyhledávat také obecné objekty, nikoliv jen objekty neuronových sítí.

Vlastní události s kódem UIC lze pomocí volby Směr navázat jen na zjištěný směr vagónu.

POZNÁMKA

Na rozdíl od RZ, kde lze detekovat přiblížení či oddálení, UIC umožňuje detekovat směr vlevo nebo vpravo.

Volba SIA poplach zahrne zaslání poplachu do integračního kanálu SIA, pokud byl otevřen.

Zaškrtnutím volby Odbavení poplachu je možné pro daný zdroj události aktivovat rozšířený mód řešení poplachů. Více viz samostatná subkapitola Režim řešení poplachů.

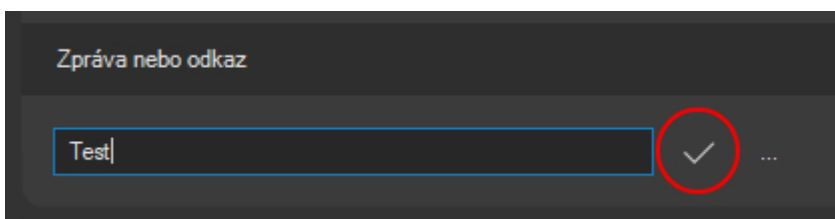
POZNÁMKA

Odeslání do SIA kanálu či odbavení se týká pouze poplachů, tj. situace, kdy je ve statickém časovém plánu použita tmavší barva.

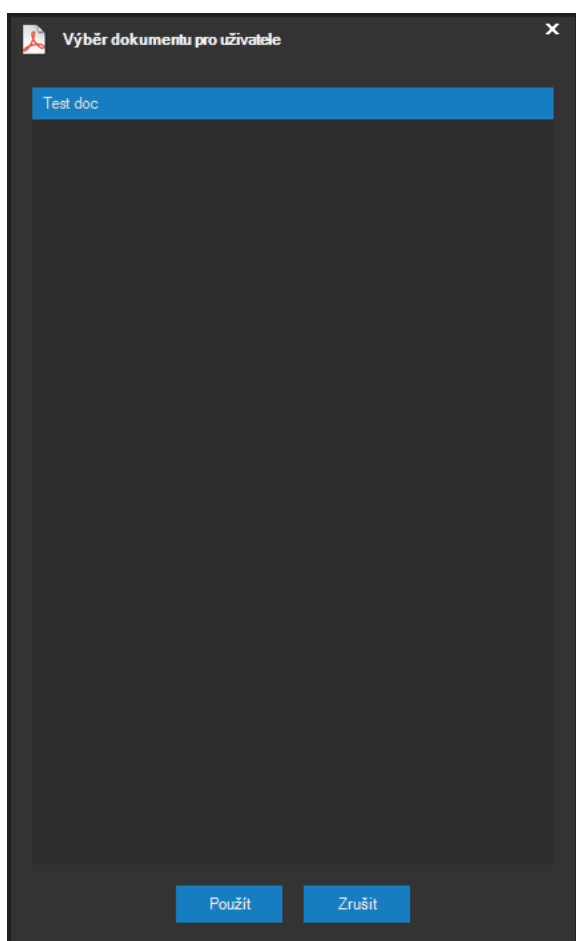
V části Dynamický plán lze pro některé událostní vstupy zvolit, že jejich stav bude použit ke generování dynamického plánu, který může řídit spínání jiných událostních vstupů systému. Více viz samostatná subkapitola.

Tlačítkem **POUŽÍT** je předběžně uložen nastavený časový plán, jeho přenos na server je součástí ukládání nastavení kamery po stisku tlačítka **POUŽÍT** v hlavním okně nastavení událostí.

Ve spodní části okna je možné pro vybraný událostní vstup (s označeným přepínačem) definovat také textovou zprávu, která se při vzniku události z tohoto událostního vstupu zobrazí uživateli na monitoru spolu s dalšími údaji o události. Zpráva se předběžně uloží tlačítkem vedle textového pole.



Pokud není pro daný událostí zdroj dostačující zadání jednoduché textové zprávy, je dále možné k události připojit dokument, který byl před tím nahrán do systému. Vložení dokumentu se provede pomocí tlačítka se symbolem tří teček.



Po vložení dokumentu bude v textovém poli Zpráva zobrazena speciální syntaxe indikující přiřazení dokumentu. Syntaxe sestává z prefixu doc: následovaného názvem dokumentu uzavřeným do hranatých závorek.

POZNÁMKA

Syntaxi je pochopitelně možné zapsat přímo i ručně, jednodušším způsobem je však výběr dokumentu přímo ze seznamu.

Poslední možností je použití hypertextového odkazu, který bude možné při příjmu události aktivovat a přejít na daný odkaz ve webovém prohlížeči. Za odkaz bude automaticky považován text, který bude začínat protokolem http nebo https.

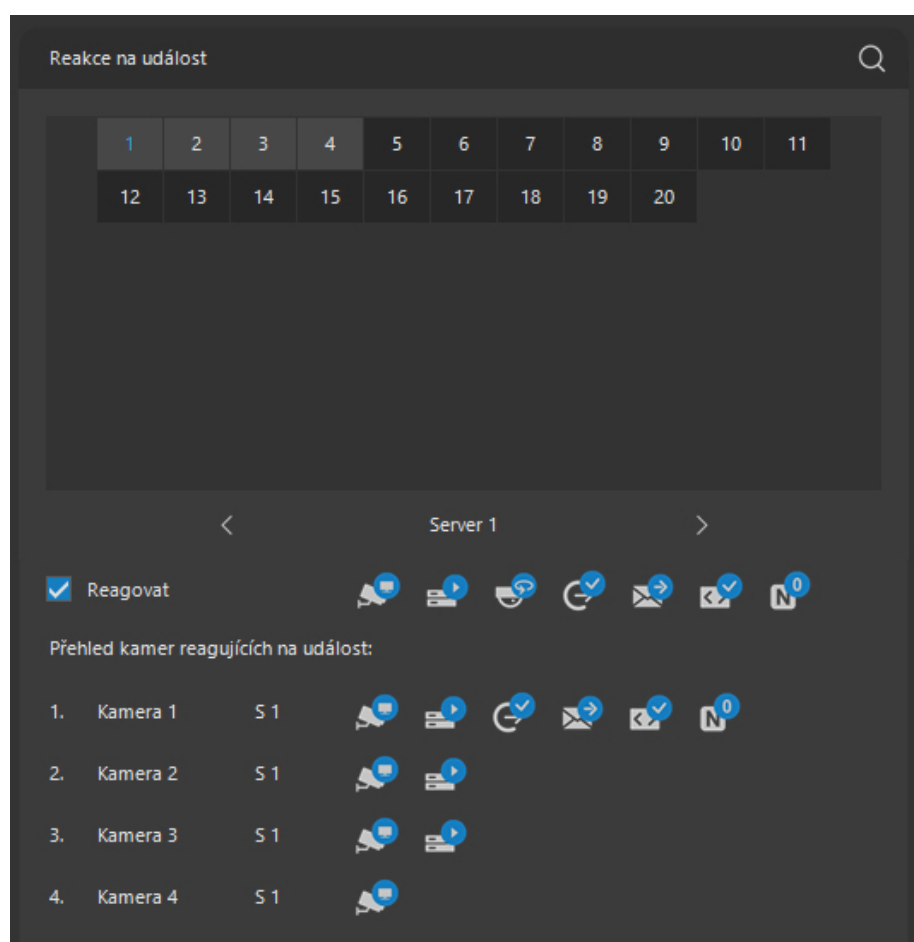
Událostní scénář

Událostní scénář se nastavuje v části Reakce na událost. Událostní scénář se vždy nastavuje pro daný událostní vstup, který musí být označen (označený přepínač).

Součástí událostního scénáře mohou být libovolné kamery z libovolných serverů. Přiřazení kamery do událostního scénáře se provede výběrem serveru (v pravém spodním rohu ovládacího prvku pro zobrazení čísel kamer), výběrem kamery a zaškrtnutím políčka Reagovat na událost. Její vyřazení z událostního scénáře se provede zrušením tohoto zaškrtnutí. Kamery zařazené v událostním scénáři jsou pro vybraný server barevně zvýrazněny. Pod přehledem kamer vybraného serveru se průběžně aktualizuje seznam všech kamer událostního scénáře (ze všech serverů) včetně ikon symbolizujících použité akce.

Stisknutím symbolu pro vyhledávání lze zobrazit textové pole, pomocí kterého lze vyhledat konkrétní kamery podle názvu.

Pro zobrazení kamer na jiném serveru je možné použít šipky u názvu serveru nebo kliknout na název a provést výběr ze seznamu.



Pro vybranou kameru na ovládacím prvku pro výběr kamer (indikováno modrým textem vybrané kamery), která je součástí událostního scénáře, je možné definovat akce, které daná kamera při události provede a které budou součástí scénáře. Automaticky je označena kamera, která je zdrojem události.

V případě většího počtu kamer v systému je možné zobrazit seznam všech dostupných serverů, z nichž je možné učinit přímý výběr bez nutnosti listování. Lze také vybrat server, který aktuálně není online, neboť nastavení událostního scénáře se zapojením jednotlivých kamerových serverů nevyžaduje, aby tyto servery byly online.

POZOR

Jednotlivé kamery mohou samozřejmě být součástí více událostních scénářů. Při současném výskytu více událostí budou na dané kameře spuštěny akce obou scénářů. Pokud je nastaven událostní záznam, bude ukončen až po ukončení všech událostí, které ho vyvolaly.



Při postupném přidávání kamer do událostního scénáře jsou tyto vždy doplňovány na konec seznamu. Celkový limit kamer, které mohou současně reagovat na jeden událostní zdroj, je 64.



Toto tlačítko funguje jako přepínač. Jeho stav lze myší přepínat mezi stavy stisknuto a nestisknuto. Při stisku tohoto tlačítka bude vybraná kamera zařazena do událostního pohledu, tj. bude patřit mezi kamery, které se uživateli automaticky objeví na monitoru při vzniku poplachu na vybraném událostním vstupu.

POZNÁMKA

Pokud součástí událostního scénáře není žádná kamera nebo žádná z kamer nebyla zařazena do událostního pohledu, bude událostní pohled sestávat implicitně pouze z kamery, která událost vyvolala. Ta se také uživateli zobrazí při vzniku poplachu nebo pokud si danou událost vybere ve svém seznamu v dohledovém okně.

POZNÁMKA

Výsledný událostní pohled bude složený ze všech kamer, které mají v událostním scénáři aktivovanu tuto volbu. Událostní pohled je vždy zvolen z předdefinovaných pohledů typu čtverec nebo širokoúhlých pohledů a to tak, aby zobrazil daný počet kamer s co možná nejmenším počtem (ideálně nulovým) prázdných kamerových oken.

POZNÁMKA

Pozice kamer v událostním pohledu jsou implicitně určeny pořadím kamer v událostním scénáři, přičemž se v pohledu postupuje po řádcích zleva doprava.



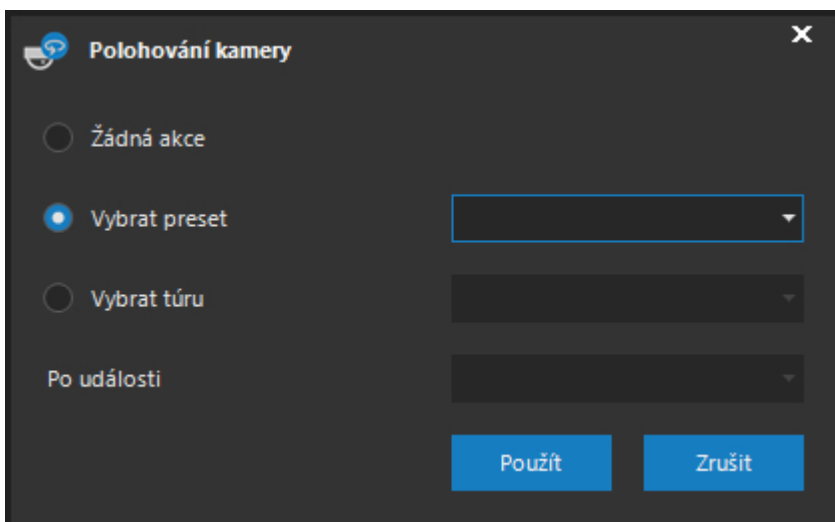
Toto tlačítko funguje jako přepínač a lze pomocí něho určit, zdali bude vybraná kamera při vzniku události nahrávat. Pravým tlačítkem lze aktivovat speciální funkci – viz níže.

POZNÁMKA

Aby mohla daná kamera při vzniku události nahrávat, je nutné, aby měla přiřazené záznamové pravidlo (profil), který nahrávání v daném čase umožňuje (buď je v daném čase aktivováno nahrávání pouze při výskytu poplachu nebo je umožněno zvýšení snímkové frekvence během události). V opačném případě nemusí být událost zaznamenána, nebo nemusí dojít k úpravě parametrů nahrávání.



Toto tlačítko je dostupné pouze pro otočné kamery a umožňuje při události provést automatické natočení kamery do vybraného prepozičního bodu. Alternativně je možné určit poplachovou túru, do které bude kamera přepnuta na dobu trvání události. Třetí možností je vypnutí všech polohovacích akcí vybrané kamery pro daný událostní scénář. Aby bylo možné vybírat presety či túry, musí být nejprve vytvořeny oprávněným uživatelem.



Při zvolení třetí možnosti (tj. kamera bude během události přepnuta do poplachové túry) je možné volitelně zadat preset, na který kamera přejde po skončení události. To lze využít zejména v případě, kdy je kamera nasměrována na konkrétní výchozí pozici, při události je přepnuta do poplachové túry a poté je třeba zajistit její návrat do výchozí pozice.

POZNÁMKA

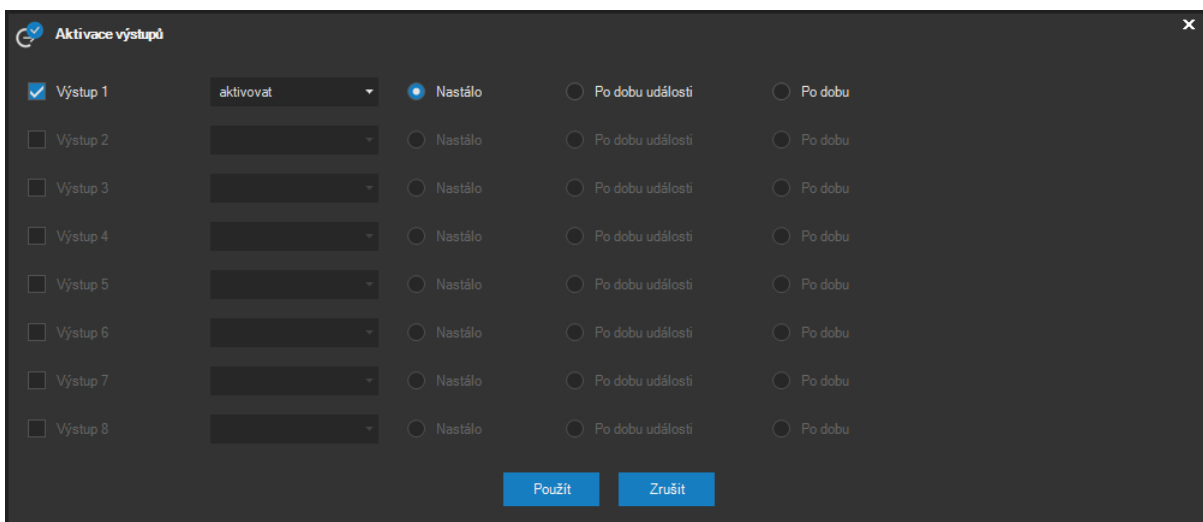
Pokud je kamera přepnuta do nějaké túry ještě před událostí, bude po dobu události aplikována poplachová túra (vybraná v předchozím okně) a po ukončení události bude obnovena původní túra, nastavení koncového presetu tudíž není nutné.

POZNÁMKA

I při použití poplachové túry platí, že je možné ji přerušit ručním zásahem do ovládání kamery. Událostní túra je však přerušena pouze na dobu v řádu několika sekund bez ohledu na nastavení hodnoty automatického obnovení túry.



Tímto tlačítkem lze u kamer či video serverů vybavených výstupy provést automatickou aktivaci nebo deaktivaci výstupů na určitou dobu, nastálo nebo na dobu trvání události. Pomocí dialogu je možné tuto dobu nastavit, nebo aktivaci výstupů při události vypnout.

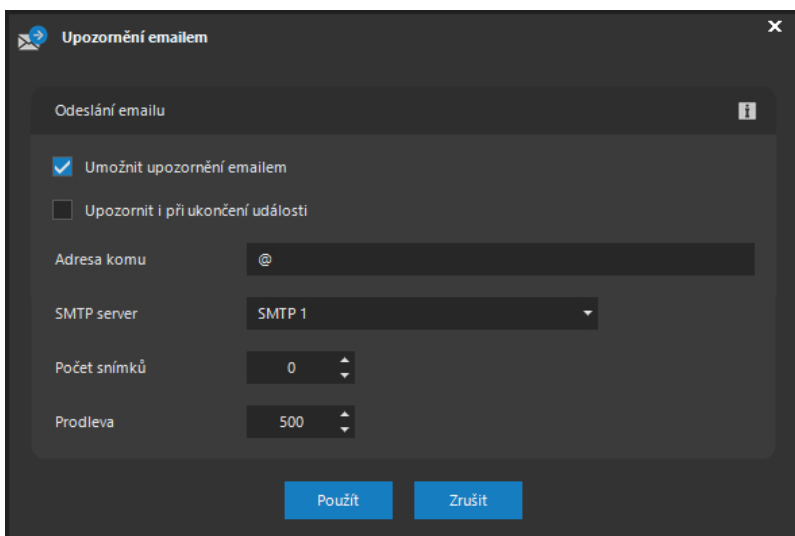


POZOR

U víceportových video serverů je na zařízení standardně k dispozici jedna sada vstupů a výstupů. Aby nedocházelo k protichůdným nastavením, které se týkají jak vstupů, tak výstupů pro různé kamery na tomtéž video serveru, jsou nastavení vstupů a výstupů k dispozici vždy pro kameru, která je na prvním portu víceportového video serveru.



Tímto tlačítkem je možné zapnout notifikaci při události pomocí e-mailu. Administrátoři tak mohou např. dostávat e-maily při výpadcích kamer v systému, při narušení je možné zasílat e-maily s přílohou obrázků z kamer apod. Po stisku tohoto tlačítka se zobrazí okno s nastavením e-mailové komunikace.



V části odesílání e-mailu lze zaškrtnutím políčka Umožnit upozornění e-mailem aktivovat nebo deaktivovat odesílání e-mailu při události pro vybraný zdroj události. Při aktivaci volby Upozornit při ukončení události bude e-mailová notifikace odeslána také při ukončení události.

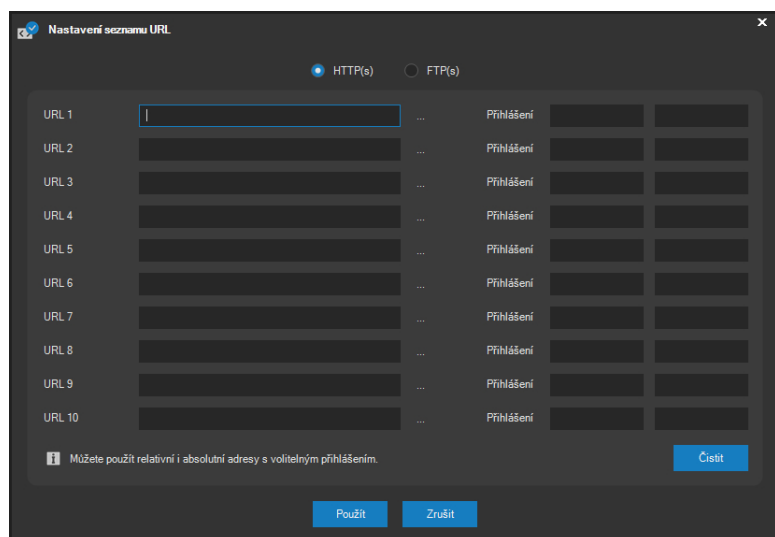
V poli Adresa komu se uvádí e-mailová adresa, kam bude e-mail automaticky odeslán. Dále je možné určit počet snímků a prodlevu jejich sejmutí, které budou zařazeny do přílohy e-mailu. Pokud nebude možné snímky z kamery získat (např. e-mail při výpadku kamery), bude vždy alespoň odesláno tělo e-mailu. Dále musí být vybrán také nějaký SMTP server.

POZNÁMKA

Do pole Adresa komu je možné vložit též více e-mailových adres oddělených středníkem nebo čárkou. Při události pak budou e-maily odeslány na všechny zadané adresy.



Pomocí tohoto tlačítka je možné aktivovat nejrůznější funkce kamer a jiných externích zařízení přímo pomocí http příkazů.



Do jednotlivých textových polí označených URL1 až URL10 je možné zapsat příkazy dostupné přes http nebo https protokol kamery. Volitelně je možné pro každý příkaz zadat také přihlašovací údaje, které budou použity pro přihlášení.

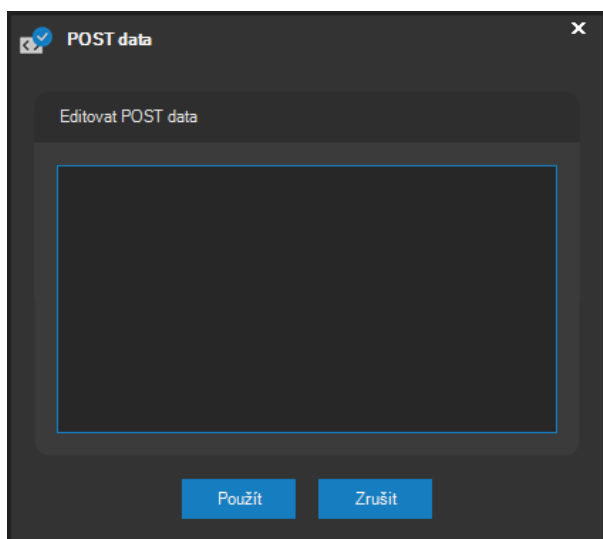
POZNÁMKA

Je možné používat jak absolutní, tak relativní adresy http příkazů. Pokud je použita relativní adresa, příkaz bude spuštěn v kontextu kamery, jejíž reakci na událost právě nastavujeme.

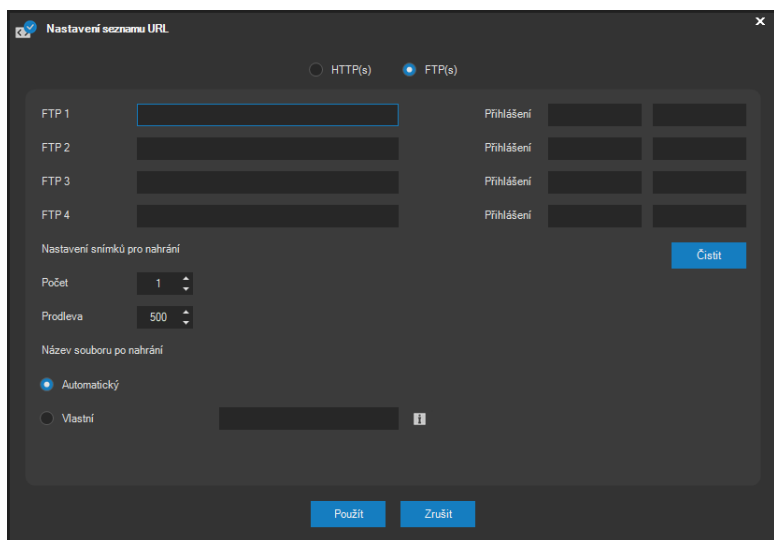
POZNÁMKA

Pokud nejsou pro relativní adresu zadány žádné přihlašovací údaje, budou použity přihlašovací údaje ke kameře použité v systému. Pokud přihlašovací údaje pro relativní adresu zadáte, budou mít přednost před přihlašovacími údaji v systému.

Přestože zapsaná URL mohou obsahovat příkazy včetně např. parametrů pro CGI skripty, některá zařízení mohou vyžadovat zaslání dat jinou než HTTP GET metodou. Pomocí tlačítka za textovým polem lze otevřít dodatečný dialog pro zadání dat pro HTTP POST.



Pokud se přepneme na nastavení FTP, může být součástí událostního scénáře také nahrání snímků na libovolný FTP server.



Do seznamu adres je možné zadat až 4 různé FTP adresy a přihlašovací údaje. Pod seznamem adres je nutné vybrat počet snímků a prodlevu mezi nimi, které budou nahrány na FTP servery při výskytu události.

POZNÁMKA

Pokud bude adresa začínat `ftps://`, bude automaticky použita zabezpečená verze protokolu FTP.

POZNÁMKA

Názvy snímků, které budou nahrány do cílové složky, která může být součástí FTP adresy, budou implicitně sestávat z identifikace serveru, časového razítka, čísla kamery a indexu, jejich názvy tak budou jednoznačné. Úvodní část sestávající z identifikace serveru a časového razítka tvoří tzv. identifikaci snímku, která je publikována v XML notifikaci o události a umožňuje jednoznačně svázat XML notifikaci a exportované snímky.

POZOR

ATEAS používá novější, dnes rozšířenější, pasivní verzi FTP protokolu. Aktivní FTP není podporováno.

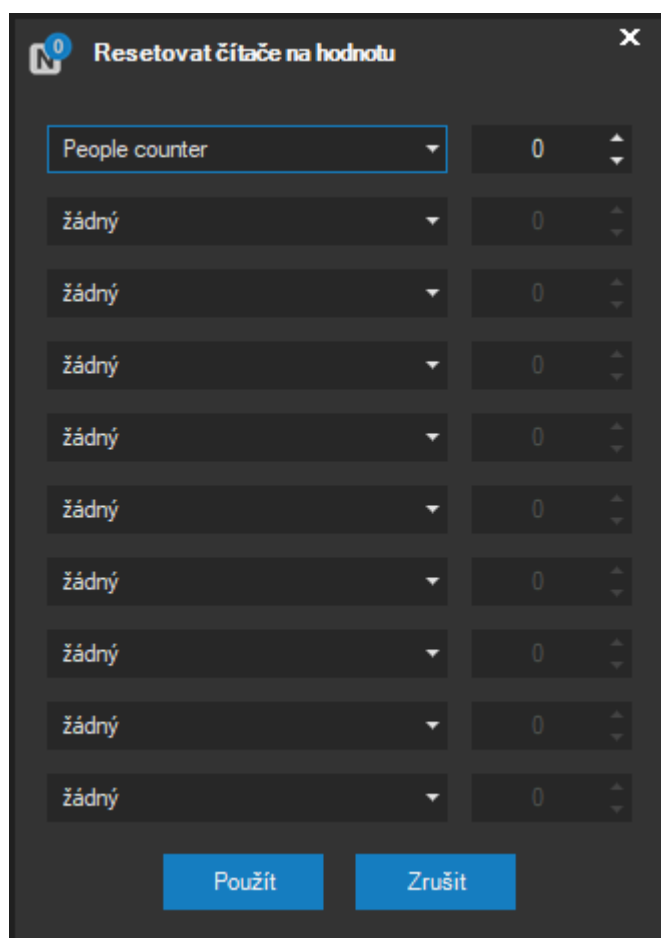
V části Název souboru po nahrání je možné určit režim pojmenování souboru po nahrání na vzdálený FTP server. Pokud nechceme akceptovat implicitní název souboru, je možné určit konkrétní jméno souboru, který bude stále dokola přepisován.

POZNÁMKA

Stále stejné jméno souboru je zejména vhodné pro jednoduché webové aplikace, které např. pomocí JavaScriptu obnovují obrázek na webové stránce. Soubor je vždy nahráván na server pod dočasným názvem a poté přejmenován, aby nehrozilo, že webová aplikace načte neúplně uložený snímek.



Toto tlačítko otevírá možnost v reakci na událost provést reset čítačů kamery na nulu nebo jinou hodnotu. Po stisknutí se zobrazí dialog s možností nastavit hodnotu čítače.



Resetovat čítače na hodnotu	
People counter	0
žádný	0
žádný	0
žádný	0
žádný	0
žádný	0
žádný	0
žádný	0
žádný	0
žádný	0

Použít Zrušit

Po vytvoření událostního scénáře pro všechny požadované událostní vstupy vybrané kamery je nutné stisknout tlačítko **POUŽÍT**, veškeré změny budou aplikovány na příslušných serverech okamžitě. Uložení scénáře a aktualizace nastavení je potvrzena zprávou.

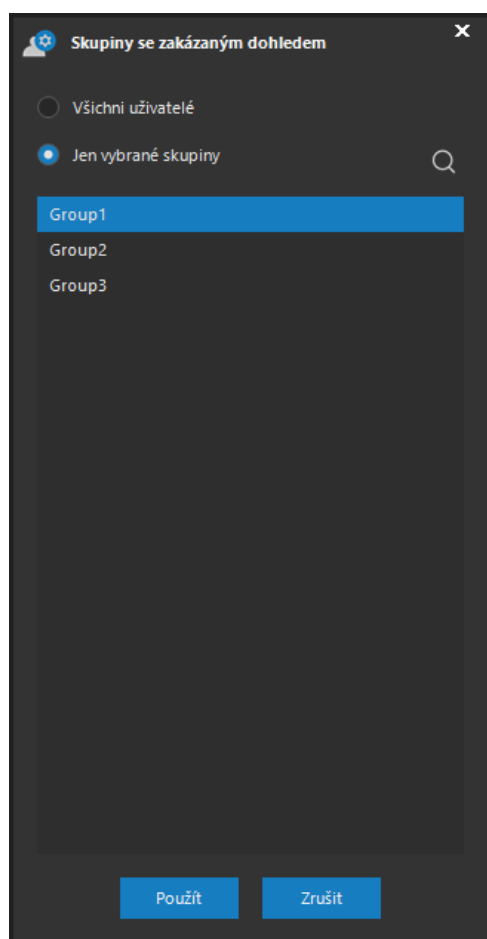
Speciální volby

V rámci tvorby událostního scénáře je také možné aktivovat některé speciální volby. Ty se aktivují pomocí pravého tlačítka myši u příslušného tlačítka.

První speciální volbou je možnost zakázat šíření živého videa a zvuku z vybraných kamer během události. Tato možnost je dostupná pomocí pravého tlačítka myši použitého u tlačítka pro zařazení do událostního pohledu. Symbol tlačítka se změní na speciální podobu, jak ukazuje následující kombinace obrázků. V případě, že dojde k zákazu distribuce živého videa a zvuku jako důsledek události, uživatel je informován nejen událostí, ale explicitně také informací v oknech kamer, kde je umístěn text informující o aktuálním zákazu dohledu dané kamery.



Zákaz dohledu může být buď platný pro všechny uživatele systému anebo jen pro vybrané skupiny, které je možné označit v následujícím dialogu.



Další speciální volbou je zákaz nahrávání během události (využitelný ve speciálních případech). Tuto možnost do událostního scénáře zahrnete kliknutím pravým tlačítkem myši na tlačítko událostního nahrávání. Tlačítko se v takovém případě změní na speciální symbol zákazu nahrávání.



POZOR

Při použití těchto speciálních voleb je třeba dbát na odpovídající nastavení maximální doby trvání události, aby nedošlo k jejímu předčasnému ukončení.

11.2.16. Dynamické zdroje a zdroje událostí Onvif

Kamery připojené pomocí nativního rozhraní anebo Onvif mohou disponovat vlastními zdroji událostí, které je možné v ATEAS Security využít. Výběrem položky Dynamické zdroje nebo Onvif zdroje ze seznamu Zdroje události je možné zobrazit seznam zdrojů.

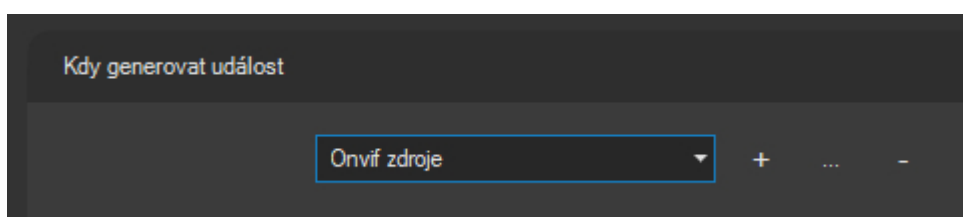
POZNÁMKA

Na rozdíl od jiných zdrojů událostí musí být dynamické nebo Onvif zdroje událostí nejprve vytvořeny, seznam tudíž může být zpočátku prázdný.

Základní výhodnou využití dynamických nebo Onvif událostních zdrojů je to, že mohou být využity zcela libovolné zdroje událostí včetně analytických aplikací či jiných specifických zdrojů událostí, o kterých nemusí mít aplikace dopředu žádné informace.

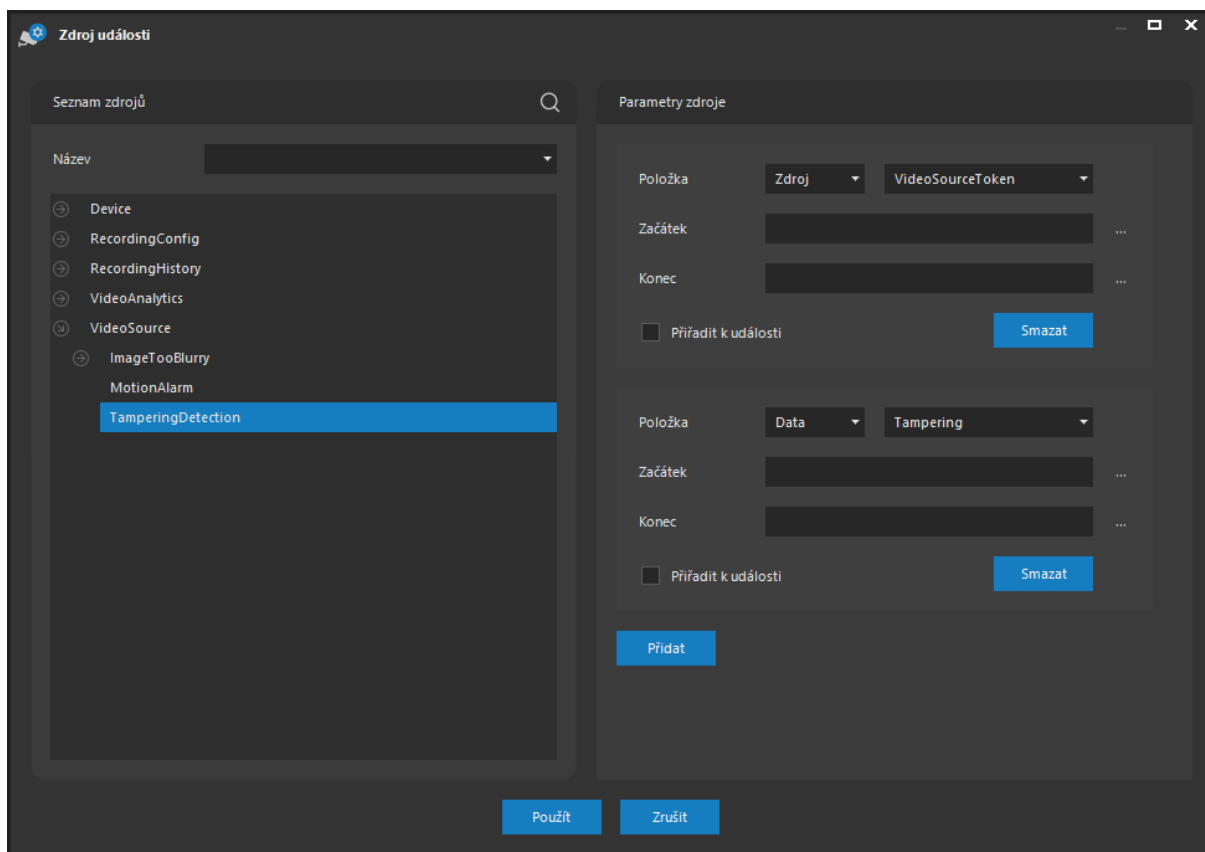
POZNÁMKA

Přestože se implementačně mohou dynamické a Onvif událostní zdroje lišit např. v použitých síťových protokolech, jejich logika a využití je shodné, proto je možné podat jednotný popis pro jejich využití v systému.



Vedle rozbalovacího seznamu s vybranou položkou Onvif zdroje jsou zobrazena tři tlačítka. Tlačítko se symbolem plus slouží k vytvoření nového zdroje události, tlačítko se symbolem teček k úpravě existujícího zdroje událostí a tlačítko se symbolem minus slouží k jeho odstranění.

Při tvorbě zdroje události je přímo z kamery automaticky získán seznam všech možných zdrojů.



Pro nový zdroj události je nutné zadat jeho název a provést výběr zdroje z nabídnutého seznamu. Parametry zdroje události se zobrazují v pravé části dialogu po výběru položky z nabídnutého seznamu. V rámci každého zdroje události může kamera nabídnout dodatečné hodnoty k události. Pomocí nastavení podmínek můžeme docílit vzniku události jen při jejich splnění.

TIP

U názvů zdroje aplikace nabízí již existující názvy. Použití stejných názvů umožní zdroje automaticky sdružovat při vyhledávání metadat a tvorbě grafů.

V části Parametry zdroje je možné blíže specifikovat datové položky, které budou přiřazeny k události, a také podmínky, které musí být splněny pro zahájení a ukončení události. Položky mohou být dvou různých typů (zdroj a data).

POZNÁMKA

Některé zdroje událostí mohou mít pouze jeden nebo dokonce žádný dodatečný parametr.

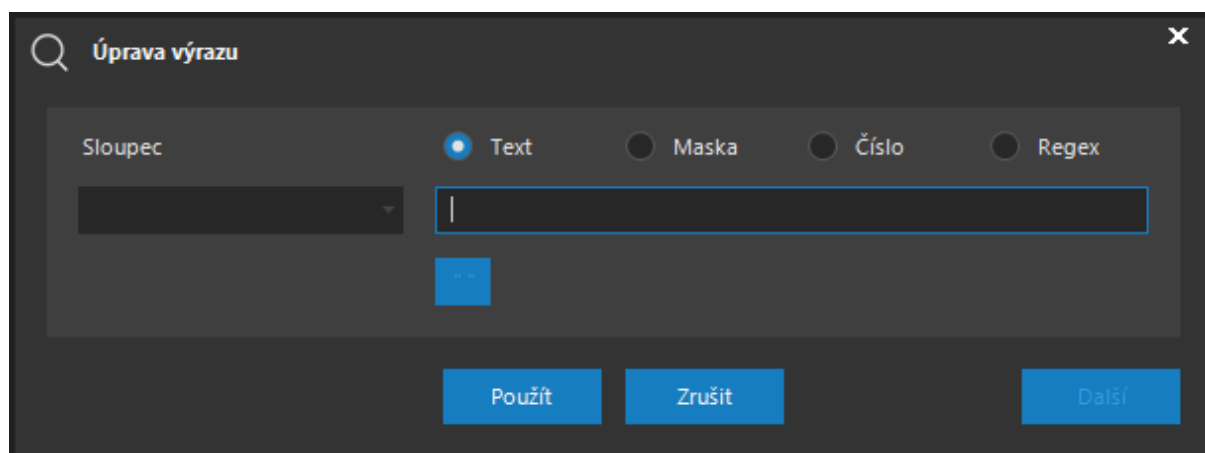
Pomocí zaškrťovacích polí Přřadit k události se můžeme rozhodnout, zdali budou tyto dodatečné parametry přiřazeny k události. Pokud jsou parametry přiřazeny, budou při události zobrazovány uživateli a bude možné podle nich také provádět vyhledávání v metadatech. Přiřazené parametry budou automaticky formátovány tak, aby bylo možné ideálně vyhledávat. Název parametru bude následován dvojtečkou a jeho hodnotou.

TIP

Toto automatické formátování metadat je ideální pro pokročilé vyhledávání v metadatech.

Jelikož existuje velké množství Onvif kompatibilních kamer, není dopředu jasné, jaké hodnoty budou mít dodatečné parametry zdrojů událostí. Proto je při vytváření zdrojů události u Onvif kamer dobré dodržovat postup, při kterém nejprve přiřadíme všechny potřebné položky k události, omezíme maximální dobu události a na vznikajících událostech sledujeme, jaké hodnoty kamera posílá. To nám umožní vhodně nastavit případné podmínky pro začátek a konec události.

Nastavení podmínek pro zahájení a konec události u jednotlivých položek můžeme provést přímo zadáním textu anebo pomocníkem po stisku tlačítka se třemi tečkami za textovým polem.



Stejný dialog je použit i při vyhledávání v metadatech, kde jsou popsány jeho funkce a možnost tvorby textové podmínky, podmínky na základě vyhodnocení masky, či numerického a regulárního výrazu. Oproti tvorbě podmínky pro vyhledávání metadat jsou zde však některé rozdíly.

- Nelze zapisovat hodnotu pro Sloupec, neboť ten je určen názvem datové položky.
- Nelze použít tlačítko **DALŠÍ**, neboť vždy tvoříme podmínku pro vybranou položku.

- Textový výraz je v případě dynamických zdrojů událostí vyhodnocen jako jeho přesná shoda, a chybí tudíž i možnost použít tlačítko se symboly uvozovek.

POZOR

Textový výraz bez použití masky v případě dynamických zdrojů událostí vyžaduje přesnou shodu s datovou položkou s výjimkou rozdílu ve velkých a malých písmenech.

Pokud jsou nastaveny podmínky pro více datových položek, musí být pro vznik či ukončení události splněny všechny. Pokud nejsou zadány žádné podmínky, berou se za splněné tehdy, pokud se datová položka objeví v dynamickém zdroji události s libovolným obsahem, a to vždy pro zahájení události.

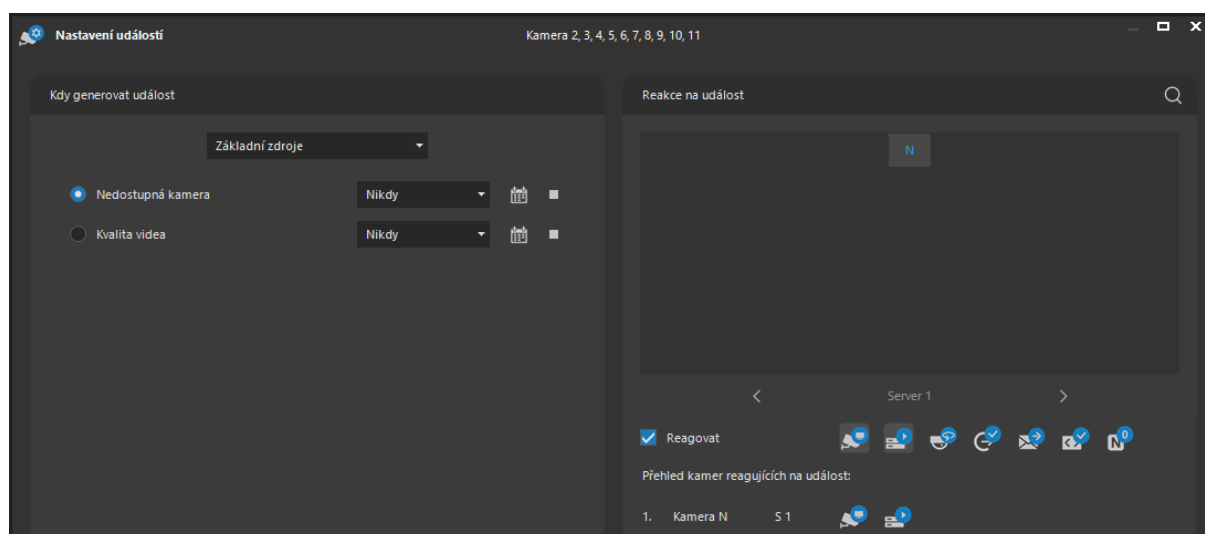
POZNÁMKA

V rámci jedné položky lze zadat podmínku také buď jen pro začátek či konec události. V takovém případě je podmínka vyhodnocena a pokud je výsledek vyhodnocení negativní, bere se za splněnou nevyplněná část podmínky (začátek či konec).

11.2.17. Hromadné nastavení událostí

Události lze konfigurovat i pro více vybraných kamer současně, tedy např. i pro všechny kamery daného kamerového serveru. Princip hromadného nastavení spočívá v tom, že je možné najednou nastavit zdroje událostí společně všem kamerám ve výběru a také reakci na událost. Obecně mohou být součástí reakce na událost (událostního scénáře) akce na jedné či více kamerách na jednom či více kamerových serverech.

Jelikož jsou kamery určeny číslem, je třeba při hromadném nastavení vytvořit možnost nastavit reakci na událost na všech vybraných kamerách shodně. To se provede tak, že v nastavení reakce na událost použijeme relativní (zástupné) číslo kamery N, které reprezentuje všechny kamery ve výběru.



POZNÁMKA

Pomocí hromadného nastavení událostí lze tedy vždy nastavit pouze takový událostní scénář, který sestává z reakcí na kameře, která událost vyvolala. Pokud má být událostní scénář rozšířen o akce na jiných kamerách či serverech, je třeba provést nastavení individuálně.

POZNÁMKA

Pro dynamické, komplexní či Onvif událostní zdroje při hromadném nastavení platí, že jejich konkrétní název může být zobrazen jen tehdy, pokud je pro všechny kamery shodný. Jinak bude zobrazen název obecný.

11.2.18. Dynamické plánování událostí

Běžně je možné vytvořit statické časové scénáře, ve kterých lze naplánovat, kdy má být např. sepnuta detekce pohybu či monitoring poplachového vstupu. Toto časové plánování lze navíc učinit ve dvou prioritních stupních - běžná událost a poplach. V obou případech je provedena kompletní reakce na událost, v případě poplachu dojde navíc k přepnutí na monitor operátora.

V případě dynamického plánu se vyhodnocování událostí jako poplach (detekce pohybu, poplachové vstupy, PIR čidla kamer, zakázané RZ vozidel) spíná dynamicky v závislosti na jiném událostním vstupu. Tímto vstupem může být

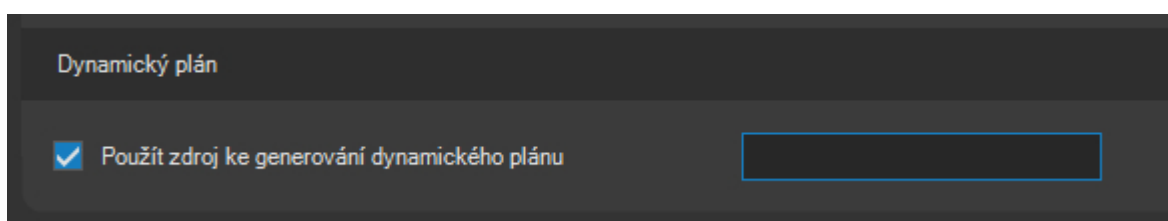
- nativní vstup - poplachový vstup kamery,

- externí vstup - vstup externího zařízení nebo zpráva z PCO pultu (aktivace pomocí SNMP protokolu nebo ATEAS API).

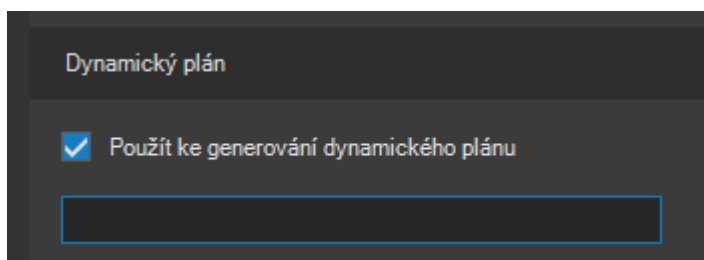
Vytvoření dynamického plánu

Do systému lze tudíž dynamický plán přidat dvěma způsoby.

Dynamický plán generovaný na základě nativního vstupu kamery lze vytvořit zaškrtnutím ovládacího prvku Použít zdroj ke generování dynamického plánu v části Dynamický plán v okně Nastavení zdroje události pro vybraný vstup kamery. Po uložení událostního nastavení kamery bude dynamický plán automaticky vytvořen, aktualizován a připraven pro použití.



Dynamický plán generovaný na základě externího vstupu či zprávy PCO lze vytvořit zaškrtnutím ovládacího prvku Použít ke generování dynamického plánu v okně Prvek objektu při jeho vytváření či úpravě v administrační části Propojení.



Použití dynamického plánu v systému

Použití dynamického plánu pro libovolný událostní vstup je jednoduché. V okně Nastavení zdroje událostního vstupu lze v horní části okna volit mezi statickým a dynamickým časovým plánem. V rozbalovacím seznamu dynamických plánů budou abecedně seřazeny veškeré vytvořené dynamické časové plány.

Nastavení plánu

☐ Statický časový plán ☒ Dynamický časový plán

Pro dokreslení funkcionality dynamických plánů uvádíme pár poznámek.

POZNÁMKA

Je tedy velmi jednoduché sepnout možnost generování poplachu na základě detekce pohybu kamery (tj. zapnout detekci pohybu) např. v závislosti na stavu vstupu téže nebo jiné kamery. Taktéž lze jednoduše zastřežit objekty pomocí externích vstupů či zpráv PCO.

POZNÁMKA

Dynamický plán je generován a rozpoznáván v celém systému. Vybraný vstup kamery nebo externí vstup, který je použit pro generování dynamického plánu, tak může být použit na libovolném počtu jiných kamer připojených ke zcela jiným kamerovým serverům.

POZNÁMKA

Vstup kamery, který je použit pro generování dynamického plánu, může samozřejmě dále sloužit ke generování běžných událostí či poplachů, a to jak na základě statického plánu, tak i dynamického plánu! Daný vstup ovšem logicky nebude generovat události, pokud je závislý na dynamickém plánu, který sám generuje.

11.2.19. Složené zdroje událostí

Pokud budeme chtít v systému reagovat až na situaci, kdy bude aktivní více než jeden událostní zdroj, budeme potřebovat vytvořit složený (komplexní) zdroj události. Složené zdroje událostí se mohou skládat z několika základních (elementárních) událostních zdrojů, které mohou být spojeny nejen logickou podmínkou A, ale také logickou podmínkou NEBO, případně XNEBO (exkluzivní NEBO, při kterém musí platit právě jedna z podmínek). Složený zdroj události nám tedy pomůže vyřešit např. požadavek na vytvoření události až tehdy, kdy bude generován pohyb na více kamerách současně nebo kdy bude detekce pohybu spojena též s aktivací pohybového čidla PIR nebo kdy bude aktivní

externí prvek 1 nebo externí prvek 2 a současně bude kamera 1 detekovat pohyb nebo bude aktivní vybraná analytická událost.

Vedle těchto binárních logických operátorů také můžeme využít unární operátor negace (tlačítko **NEG**). V praxi ho lze využít tehdy, budeme-li chtít vyvolat událost, pokud událostní zdroj nebude aktivní (např. zastavení výrobní linky a ukončení detekovaného pohybu).

Komplexní zdroje událostí v systému automaticky slouží též jako čítače. Systém pro každou komplexní událost udržuje počet aktivací jejich elementárních zdrojů, přičemž zdroje bez logické negace jsou sečítány, zdroje s logickou negací jsou odečítány. Výsledkem pak může být hodnota, kterou lze sledovat v reálném čase v dohledovém okně. Více o čítačích naleznete v kapitole Práce s čítači ve funkcích dohledového okna.

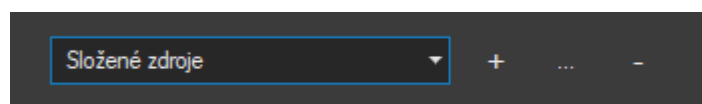
Podle priorit vyhodnocování jsou jednotlivé operátory seřazeny následovně (od nejvyšší priority po nejnižší):

- NEG (unární operátor negace)
- A (binární operátor A)
- NEBO (binární operátor NEBO)
- XNEBO (binární operátor exkluzivní NEBO)

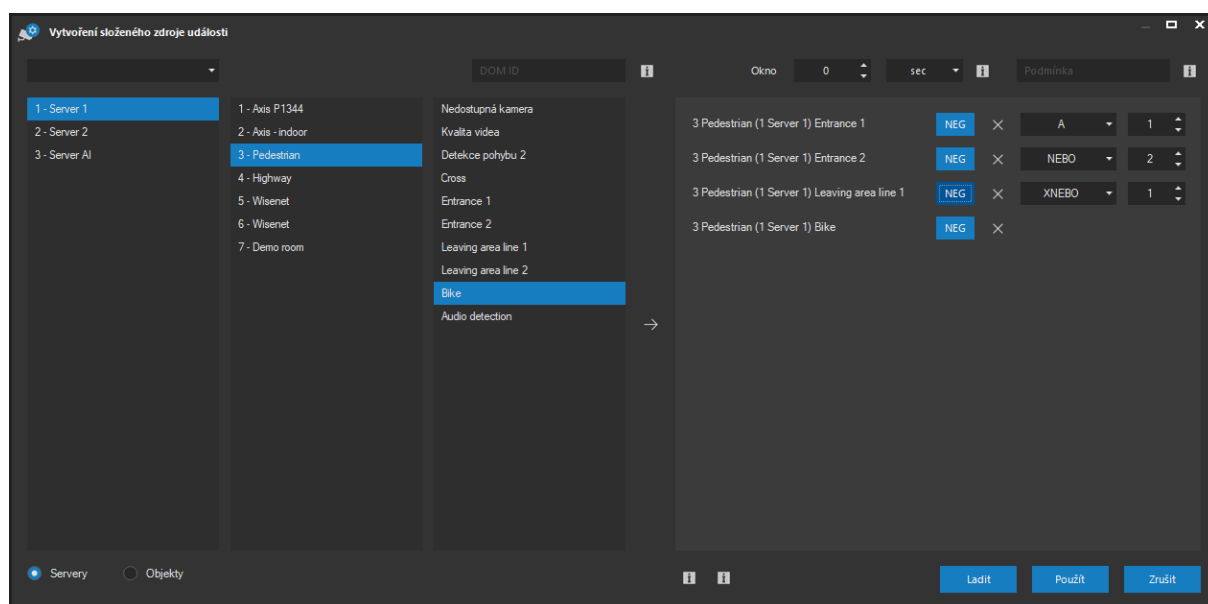
POZNÁMKA

Složené zdroje událostí jsou tedy ideálním nástrojem k řešení náročnějších bezpečnostních požadavků na systém a současně také nástrojem pro významné snížení planých poplachů a přetížení operátorů systému.

Vytvoření komplexního zdroje události určité kamery provedeme tak, že v seznamu Zdroje události vybereme volbu Složené zdroje.



Tlačítka vedle seznamu slouží pro vytvoření nového, editaci stávajícího a odstranění vybraného složeného zdroje události. Klinutím na tlačítko se symbolem plus otevřeme dialog, ve kterém můžeme vytvořit složený zdroj události.



V levé části okna můžeme vybírat ze všech událostních zdrojů, které máme v systému k dispozici, a to včetně např. základních zdrojů jako detekce pohybu či aktivace vstupů, analytických zdrojů, detekce RZ vozidel, vlastních událostních zdrojů nebo Onvif zdrojů. Pomocí přepínačů pod seznamem můžeme volit mezi zdroji z kamerového systému a zdroji externími. Vybraný zdroj lze do komplexní události zařadit pomocí tlačítka se šipkou. Již zařazené zdroje je možné jednoduše přesouvat přetažením a umístit je tak na jiné pozice.

POZNÁMKA

Při tvorbě složeného zdroje nejsme omezeni kamerou ani serverem. Složený událostní zdroj tedy může záviset na zdrojích z jedné či více kamer připojených k jednomu či více kamerovým serverům a dokonce též na externích událostech.

Vytvořenému složenému zdroji události je třeba přiřadit nějaký název, pod kterým se bude v systému pro danou kameru objevovat.

TIP

U názvů zdroje aplikace nabízí již existující názvy. Použití stejných názvů umožní zdroje automaticky sdružovat při vyhledávání metadat a tvorbě grafů.

Vedle názvu je umístěno textové pole DOM ID, pomocí kterého je možné vložit hodnotu čítače do webové stránky zobrazené přímo v klientu ATEAS anebo na video stěně. K tomu, aby ATEAS zobrazil na daném místě stránky hodnotu čítače, postačí ve zdrojovém html dokumentu vytvořit libovolný prvek s ID odpovídajícím nastavené hodnotě, např. `<div id="xxx"></div>`.

Hodnoty čítačů mohou být integrovány i do webových stránek, které nejsou zobrazeny v klientech ATEAS (standardní klient nebo klient video stěny). Zde pochopitelně nestačí označit místo pro vložení hodnoty pomocí html značky, ale je potřeba použít komplexnější integrační logiku. ATEAS administrační server obsahuje ve složce httproot podsložku api, ve které jsou uvedeny příklady integrace s potřebnými komentáři pro tvůrce či správce webů.

Kromě komplexních čítačů existují v systému i automaticky vytvořené zónové čítače odpovídající všem analytickým událostním zdrojům navázaným na uzavřené zóny. Integrace těchto čítačů do webových stránek probíhá tudíž také pomocí automatické identifikace prvků ve stránce. Formát jejich ID sestává z rezervované části a (v tomto pořadí) čísla serveru, kamery a zdroje (číslo zdroje je zobrazeno v nastavení analýzy), např.:

auto-zone-1-10-201

Jednotlivé událostní zdroje, které jsou součástí složeného zdroje, mohou být ze seznamu v pravé části okna kdykoliv odstraněny pomocí tlačítka se symbolem křížku. Pro každý zdroj lze aktivovat operátor negace a provést spojení s následujícím událostním zdrojem pomocí operátoru, který vybereme z rozbalovacího seznamu. Při vyhodnocování složeného zdroje jsou aplikovány výchozí priority operátorů popsané výše. Pokud je třeba pořadí vyhodnocování změnit, je možné změnit prioritu jednotlivých logických spojení ve sloupci Priorita.

POZNÁMKA

Navyšování priorit ve sloupci Priorita je tedy uživatelským způsobem vytváření logického výrazu opatřeného závorkami pro změnu pořadí vyhodnocování.

Složený zdroj události vyvolá událost tehdy, když bude splněna podmínka jejího vzniku dle nastavených logických spojení elementárních událostních zdrojů. Složená událost bude ukončena, jakmile tato podmínka již naplněna nebude.

POZOR

Aby mohl složený zdroj události vytvořit událost, musí být v systému vytvořeny a vyhodnocovány všechny události, na nichž složený zdroj závisí.

POZNÁMKA

Je třeba mít na paměti, že složený zdroj události má vlastní nastavení doby do resetu vstupu a vlastní plánování. To znamená, že pokud podmínky pro vznik složené události přestanou být naplněny, komplexní událost bude ukončena až po době do resetu vstupu. Pokud v této době budou podmínky opět naplněny, původní složená událost bude pokračovat.

Je-li složená událost primárně využívána jako čítač, je její faktické zahájení či zakončení na základě logických souvislostí mezi elementárními zdroji událostí často nevýznamné, a je proto vhodné komplexní událost nastavit jako skrytou. V praxi je však mnohem častější požadavek vyvolat takovou událost tehdy, pokud je splněna nějaká numerická podmínka. Tuto podmínku lze zadat do textového pole ve spodní části okna, podporováno je přímé zadání čísla, operátory $>$ a $<$ a zadání intervalu jako např. (50,100).

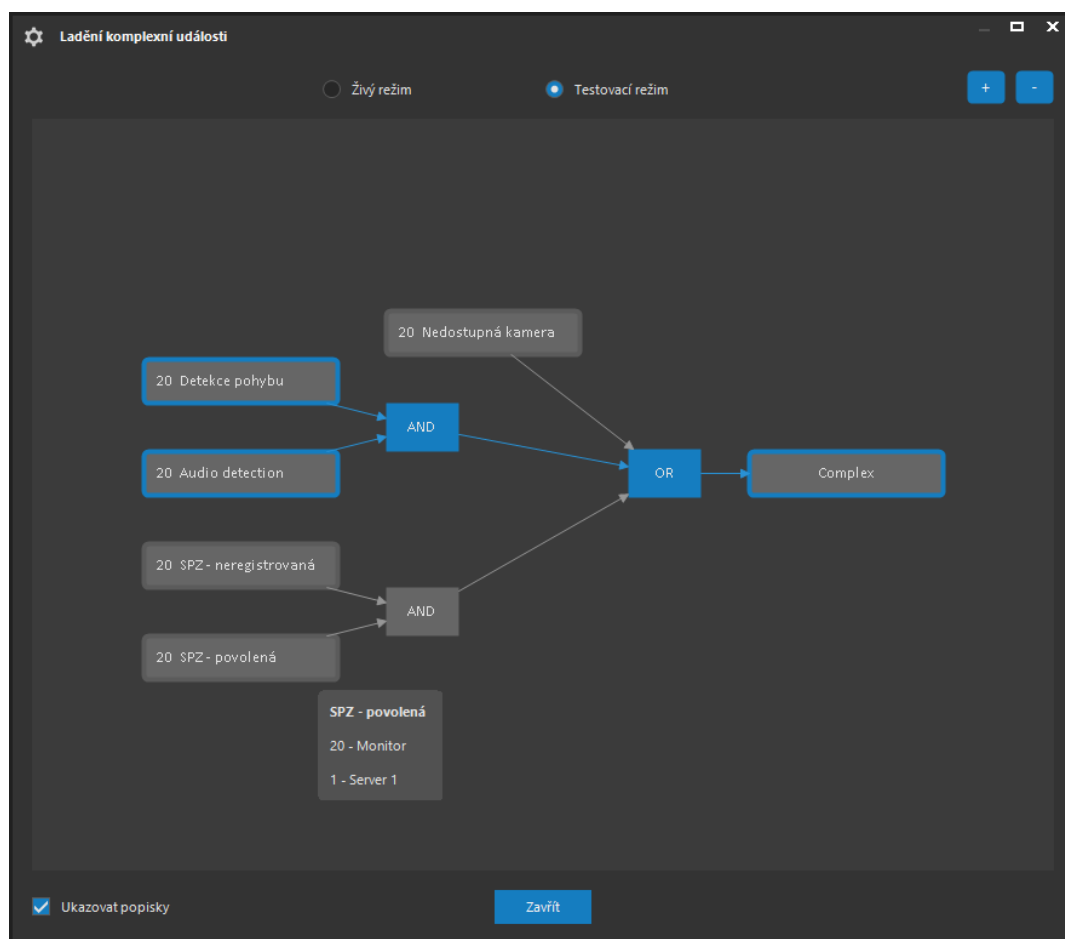
Je-li nastavena pozitivní hodnota pro Okno, změni se komplexní událost – čítač na dynamický čítač. To znamená, že zvýšení či snížení hodnoty čítače v důsledku aktivaci základního zdroje události bude po uplynutí časového okna následováno opačnou operací (snížením či zvýšením) hodnoty čítače. Takto lze např. zobrazit či reagovat na počet průchodů osob za poslední hodinu apod.

POZNÁMKA

U dynamických čítačů platí, že ruční či událostní reset jejich hodnoty resetuje i všechny opačné operace čekající na uplynutí časového okna. Zároveň také nejsou hodnoty uloženy a obnoveny po restartu služby kamerového serveru.

Ladění komplexních událostí

Komplexní událost mohou sestávat z mnoha základních zdrojů a mohou používat různé operátory a priority vyhodnocování. Z tohoto důvodu nemusí být jednoduše představitelné, kdy má událost nastat, a pokud nenastane, jaký k tomu byl důvod. Nástroj ladění komplexních událostí dostupný přes tlačítko **LADIT** proto umožňuje vizuální kontrolu.



Náhled události může fungovat v živém či testovacím režimu. Zatímco v živém režimu odpovídá stav základních událostí stavu v systému, v testovacím režimu lze jednotlivé zdroje aktivovat či deaktivovat ručně. V obou případech je vidět, jak je výsledek vyhodnocení propagován skrz vizuální strukturu komplexní události. Ve vizualizaci je dobře vidět fungování jednotlivých operátorů a priorit.

Vizualizaci lze přiblížit či oddálit pomocí tlačítek pro ovládání zoomu nebo pomocí kolečka myši. Jednotlivé části lze také přesouvat na jiné pozice.

Deaktivací volby Aktivovat popisky lze zabránit zobrazování rozšiřujících informací o zdroji události při setrvání kurzoru myši nad ním.

Data komplexních událostí

Do dat komplexních událostí jsou automaticky zařazena data všech základních událostí, ze kterých je komplexní událost složena.

POZNÁMKA

Tuto vlastnost lze využít při vyhledávání v metadatech, kde lze komplexní události vyhledat na základě dodatečných dat.

11.2.20. Umístění kamery do mapy

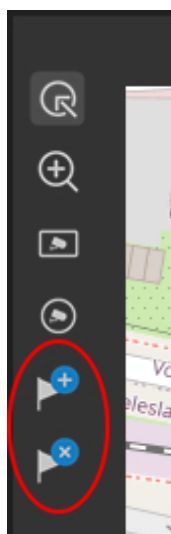
Administrátor s přístupem k danému kamerovému serveru má možnost určit a poté kdykoliv změnit souřadnice kamery (její umístění v mapě). Ovládání mapového okna je popsáno v samostatné kapitole, na tomto místě si pouze ukážeme, jakým způsobem lze určit pozici kamery v mapě.

Pokud není při práci v administrační sekci systému zobrazena mapa, lze ji otevřít z nabídky Nástroje. Při otevřeném mapovém okně bude při výběru kamery ze seznamu provedena automatická synchronizace mapy (centrování a volitelný zoom) a to i při vypnuté či pouze událostní mapové synchronizaci. Tím je usnadněn postup při přesunu kamer na nové souřadnice.

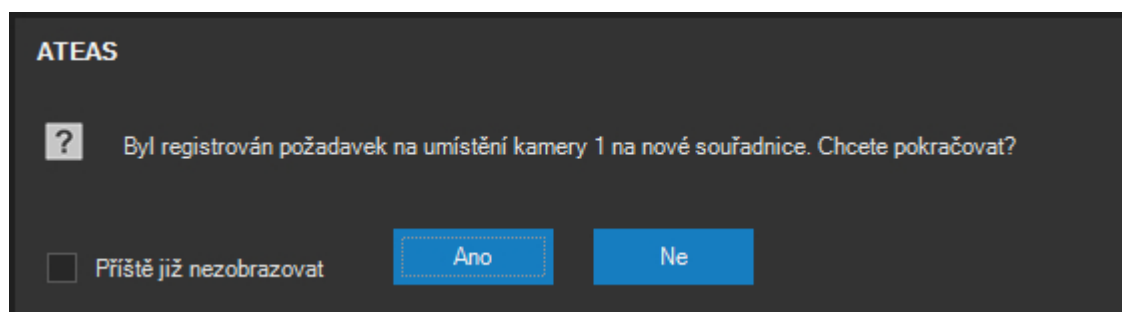
POZNÁMKA

Pro lepší názornost bude symbol kamery v mapě po jejím výběru vždy na pár vteřin zvýrazněn.

Administrátor systému má pro lokalizaci kamer k dispozici následující funkce.



Po výběru kamery ze seznamu kamer, kterou chcete lokalizovat v mapě (nebo její lokalizaci změnit) aktivujte v mapě funkci pro umístění prvku a klikněte na místo nového umístění kamery. Poté je bude potřeba potvrdit následující zprávu tlačítkem **ANO**.

**TIP**

Již lokalizované kamery lze rychleji přemístit či odstranit z mapy pomocí kontextové nabídky symbolu kamery v mapě.

Po potvrzení dojde k přesunu kamery na nové mapové souřadnice a k automatické aktualizaci zobrazení u všech uživatelů, kteří mají zobrazenou mapovou scénu. Umístění či přesun na nové souřadnice jsou potvrzeny zprávou. Stejným způsobem lze kameru z mapy odstranit, pouze se použije tlačítko s popisem Odstranit prvek.

Do mapy mohou být lokalizovány i mobilní kamery na Vašich telefonech či jiných zařízeních s operačním systémem iOS nebo Android, tj. kamery přidané do systému pod uživatelským jménem. Pokud je z takovéto mobilní kamery zahájen přenos videa (a zvuku), pak může být toto zařízení automaticky lokalizováno v mapě pomocí GPS. Mapové okno zobrazuje vždy aktuální pozici všech zařízení, která má operátor zobrazena v některém z dohledových oken.

POZNÁMKA

Předpokladem pro využití této funkce je GPS přijímač, kterým musí být mobilní zařízení vybaveno.

POZNÁMKA

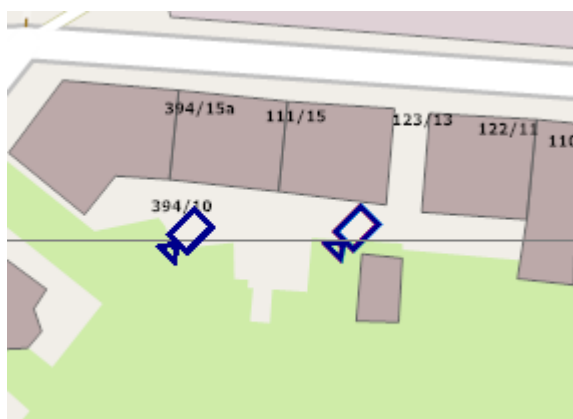
Pokud nemá mobilní kamera určenou výchozí pozici v mapě, nebude zasílané video opatřené GPS metadaty a zařízení nebude možné lokalizovat. Pokud tedy není mobilní kamera lokalizována anebo nejsou mapové podklady vůbec k dispozici, zařízení nebude zbytečně spotřebovávat energii na určování své GPS pozice.

POZNÁMKA

Trasu jednotlivých zařízení je možné zobrazovat též ze záznamu při přehrávání videa. Při více spuštěných dohledových oknech mapu využívá vždy poslední aktivní okno, aby bylo možné určit, jestli budou zobrazovány aktuální nebo zaznamenané GPS souřadnice.

Režim přichytávání

Jak napovídá popisek u tlačítka Umístit prvek, je možné při současném použití klávesy CTRL umísťovat kamery v režimu přichytávání. V tomto režimu se cílová pozice kamery (horizontální a vertikální) nastaví na stejnou hodnotu jakou má kamera, která je v horizontálním či vertikálním směru (nebo obou) nejbližší (tj. přichytí se). Přichycení ukazuje následující obrázek.



Pomocí přichytávání lze kamery velmi jednoduše umístit přesně vedle sebe i na delší vzdálenost mezi kamerami, a vylepšit tak vizuální dojem mapové scény. Mezi aktuálně umísťovanou kamerou a kamerou, ke které jsme aktuálně přichyceni, je vždy zobrazena tenká vodící linka. Pokud je přichycení provedeno v horizontálním i vertikálním směru současně (většinou ke dvěma rozdílným kamerám), jsou zobrazeny vodící linky dvě.

POZNÁMKA

Nástroj přichycení je aktivován vždy až při určitém přiblížení k cílové kameře.

11.2.21. Export a import kamer

Pomocí tlačítek **EXPORT** a **IMPORT** je možné uložit konfiguraci vybraných kamer a později ji načíst na stejném či jiném serveru, případně též i v jiném systému stejné verze. Tato funkce je dostupná pomocí dvojice tlačítek, jak ukazuje obrázek.



Tímto způsobem lze rychle a jednoduše přenést kamery na jiný server, pokud provádíme jejich přerozdělení v rámci edice UNLIMITED. Při importu do stejného serveru lze velmi rychle vytvořit konfiguraci s vícenásobně přidanými kamerami pro mobilní dohled anebo záznam v jiné kvalitě či formátu. Přenosem do zcela nového systému lze připravit konfiguraci kamer v laboratorních podmínkách a poté ji na cílovém systému pouze importovat.

POZNÁMKA

Základní rozdíl oproti zálohování a obnovení kompletní konfigurace serveru v souborech XML spočívá v tom, že nástrojem exportu lze exportovat a importovat pouze vybrané kamery, což je velmi cenné ve výše zmíněných případech.

Kamery nelze exportovat a importovat mezi systémy různých verzí, aplikace také proto nabízí název souboru obsahující datum exportu a verzi systému.

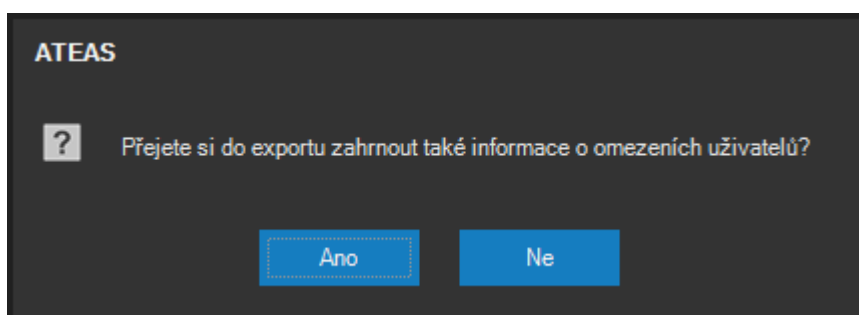
Při importu kamer je zobrazen stejný dialog jako při automatickém přidávání kamer do systému, kde je možné vybrat počáteční číslo kamery pro import (pokud je číslo obsazeno, použije se nejbližší vyšší) a určit, zdali budou přidávány duplicitní kamery.

Součástí exportu jsou veškerá nastavení vázaná na kamery včetně kompletního nastavení událostních zdrojů, zón pro analýzu pomocí neuronové sítě, symbolických názvů, prepozičních bodů, tůr atd.

POZNÁMKA

Součástí exportu je též událostní scénář, nicméně pouze ta část, která se týká samotné exportované kamery. U scénáře, který zahrnuje i jiné kamery na stejném či jiném kamerovém serveru, takové části scénáře nelze převést, neboť systém nemůže určit logiku pro pozdější import.

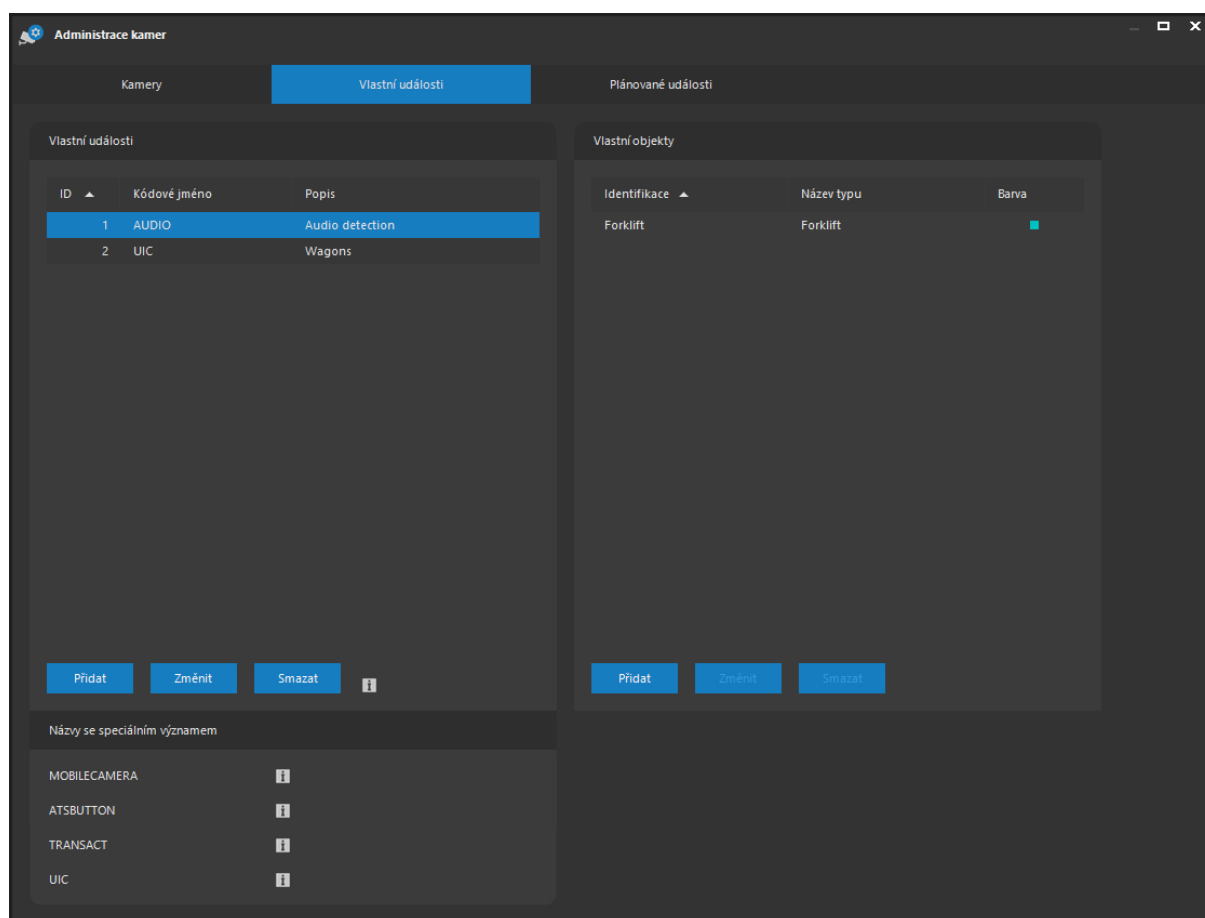
Součástí exportu mohou být i data o omezeních uživatelů a skupin pro exportované kamery. Taková data mají smysl, budou-li kamery importovány v rámci jednoho kamerového systému (byť na jiném serveru). Proto je možné jejich zahrnutí do exportu odmítnout.



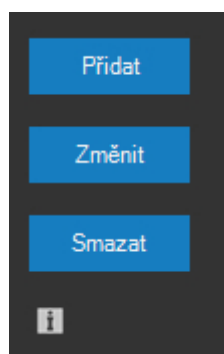
11.3. Vlastní události a typy objektů

11.3.1. Vlastní události

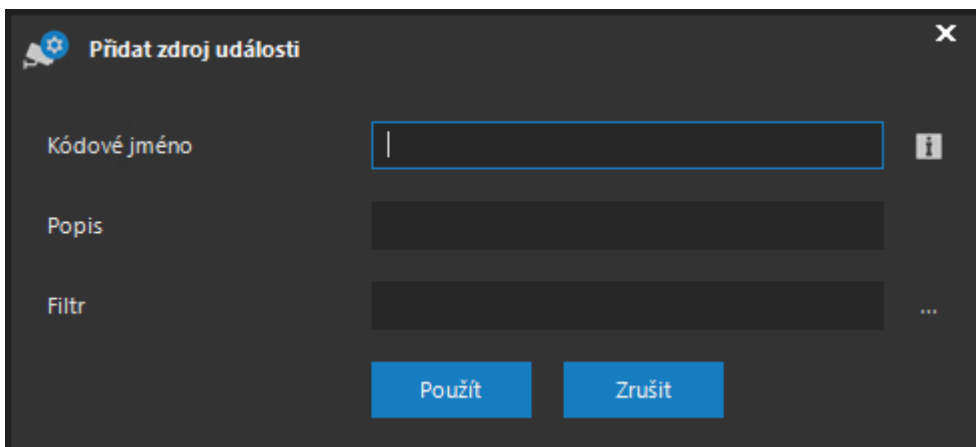
Vedle zdrojů událostí implicitně dostupných pro jednotlivé kamery v systému, lze do systému přidat další dodatečně uživatelsky definované zdroje událostí. Ty lze přidávat a mazat na kartě Vlastní události v části Administrace kamer a lze pomocí nich do systému propojit libovolné události vztažené ke kamerám.



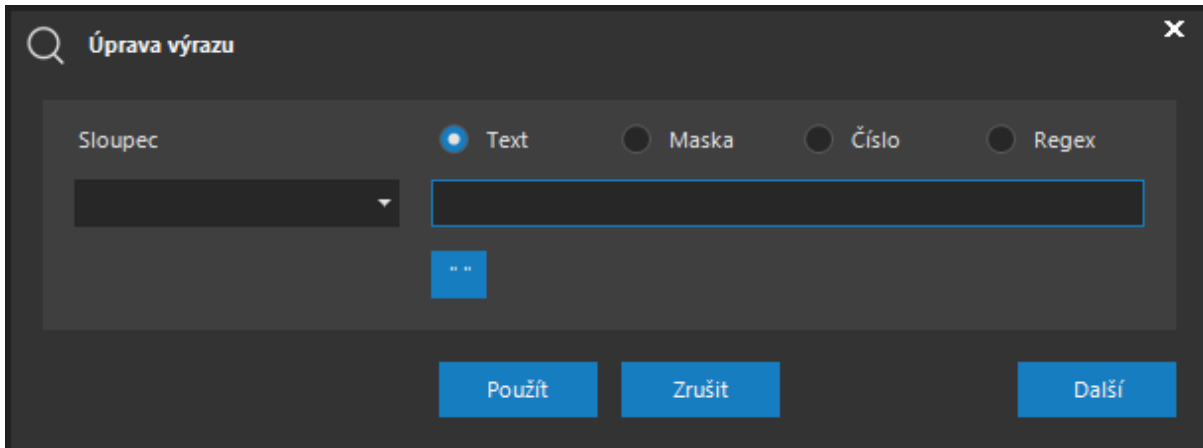
Uživatelsky definované události kamer jsou v systému přijímány pomocí ATEAS API, aplikačního rozhraní pro příjem externích událostí. Tato část ATEAS API, její princip a příklady použití jsou popsány v samostatném dokumentu dostupném na domovské stránce ATEAS Security (na adrese Vašeho administračního serveru ATEAS Security).



Pomocí tlačítek **PŘIDAT**, **ZMĚNIT** a **SMAZAT** lze v systému registrovat a posléze i upravovat (respektive zrušit) uživatelsky definované vlastní události kamer. Tyto operace jsou centrální a týkají se všech kamerových serverů v systému. Po stisku tlačítka **PŘIDAT** se zobrazí jednoduchý dialog, ve kterém je třeba vyplnit údaje o novém zdroji události.



Kódové jméno je symbolický jedinečný název pro zdroj události, který je také součástí externí notifikace o tomto typu události v ATEAS API. Popisem se rozumí uživatelský popis tohoto zdroje události, který se bude používat při vzniku této události a také na panelu událostí u jednotlivých kamer. Nepovinně je také možné vyplnit pole Filtr. Zde je možné určit podmínku, která musí být splněna, aby událost nastala. Nastavení podmínky můžeme provést přímo zadáním textu anebo pomocníkem po stisku tlačítka se třemi tečkami za textovým polem.



Stejný dialog je použit i při vyhledávání v metadatech, kde jsou popsány jeho funkce a možnost tvorby textové podmínky, podmínky na základě vyhodnocení masky, či numerického a regulárního výrazu. Stejně tak je zde možné použít i sloupcovou syntaxi.

POZNÁMKA

Předchozí funkcionalitu filtru lze využít například při napojení na transakční data pokladního systému, když chceme vyvolat událost při nákupu určitého druhu zboží či stornování položky apod.

Stiskem tlačítka **POUŽÍT** je nový zdroj události registrován na administračním serveru.

11.3.2. Systémové názvy vlastních událostí

Některé názvy vlastních zdrojů událostí jsou v systému předdefinované a automaticky napojené na události určitého typu. Seznam těchto názvů je přímo uveden ve spodní části okna. V současné verzi se jedná o tyto systémové názvy vlastních zdrojů události:

MOBILECAMERA – Vlastní událost s tímto názvem je generována pro kamery telefonů a dalších mobilních zařízení přidaných do systému pod jménem přihlášeného uživatele. Událost vzniká při zahájení vysílání videa z mobilního zařízení a umožňuje tak v reakci na tuto akci spustit událostní scénář (zobrazení události na monitoru, notifikace operátorů, záznam, další akce). Více také viz kapitola o přidávání kamer do systému.

ATSBUTTON<n> – Vlastní událost s tímto názvem (kde <n> je číslo v rozsahu 1 až nejvyšší číslo uživatelského tlačítka v systému) je generována pro stisk uživatelského tlačítka s daným číslem. Událost vzniká při stisku tlačítka. Pokud je tlačítko konfigurované jako přepínač, dojde při uvolnění tlačítka k ukončení události.

TRANSACT – Vlastní událost s tímto názvem je generována pro každý řádek transakce. Je tedy velmi vhodné nastavit pro tuto vlastní událost nějaký filtr, aby událost vznikla jen v určitých konkrétních situacích – např. při stornování položky v pokladním systému atd.

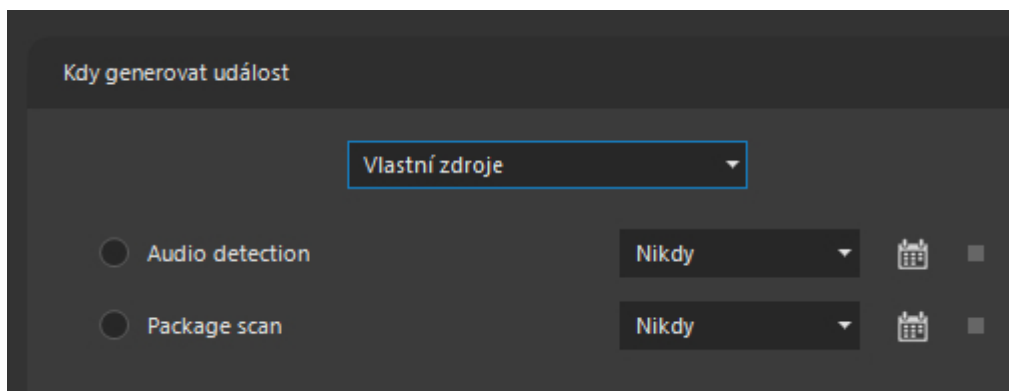
UIC – Vlastní události s tímto názvem se týkají detekce UIC čísel vagónů.

POZNÁMKA

Pokud nejsou tyto vlastní zdroje událostí s předdefinovanými názvy vytvořeny, žádné události těchto typů nebudou vznikat.

11.3.3. Řízení událostí

Uživatelsky definované vlastní zdroje událostí mají naprosto stejné uplatnění jako již existující zdroje událostí v systému. Jediný rozdíl spočívá v tom, že vlastní události jsou zahájeny (případně ukončovány) pomocí ATEAS API. Na panelu událostí jsou vlastní zdroje událostí k dispozici v samostatné skupině Vlastní zdroje.



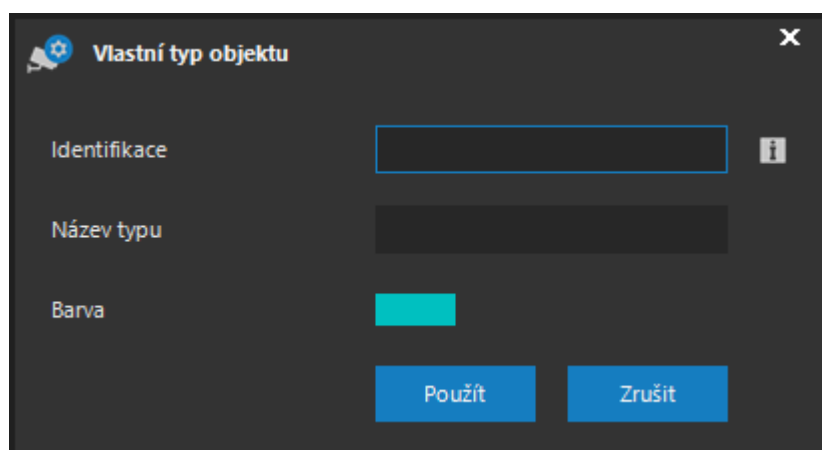
Určení časového plánu (kdy může událost či poplach vzniknout) a vytvoření událostního scénáře, který může zahrnovat více kamer a obsahovat nejrůznější akce, je zcela shodné s postupy u předdefinovaných zdrojů události.

11.3.4. Vlastní typy objektů

V části Vlastní objekty lze pomocí tlačítka **PŘIDAT** vytvořit nové typy objektů, které nejsou podporovány běžně dostupnými neuronovými sítěmi ATEAS.

POZNÁMKA

Nové typy objektů může být nutné přidat např. u zákaznických neuronových sítí nebo u analýz, které probíhají přímo v kamerách.



Do pole Identifikace je nutné zadat jednoznačný identifikátor daného typu objektu v místě jeho vzniku (v neuronové síti či v kameře), v poli Název typu je možné použít název, pod kterým bude objekt zobrazen uživatelům.

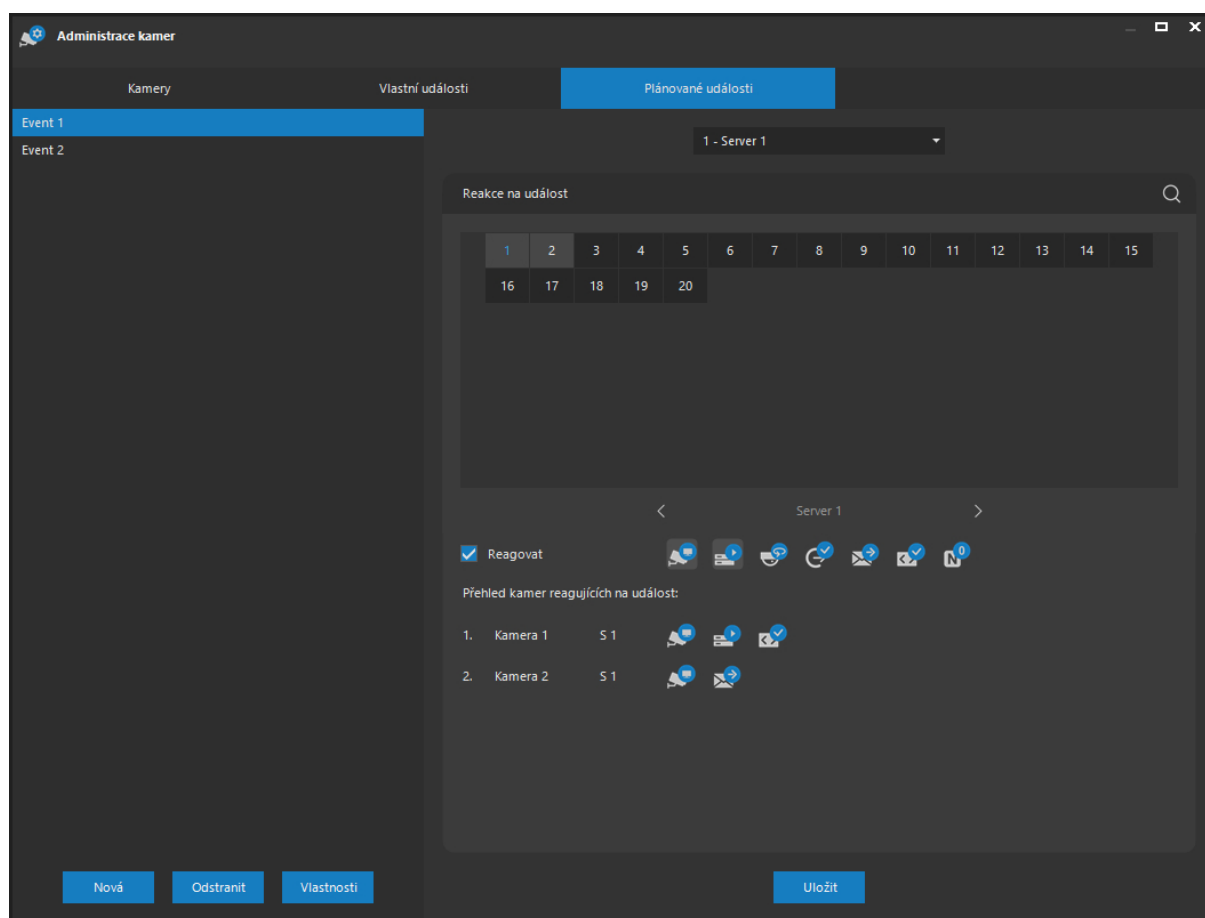
Kliknutím na barevnou oblast lze dále zvolit libovolnou barvu pro tento typ objektu. Barva bude použita při vykreslování metadat vč. vykreslování na mobilních klientech či v SDK. Po jejich vytvoření se s vlastními typy objektů pracuje velmi podobně jako se systémovými typy objektů, a to při tvorbě událostních zdrojů nebo ve forenzním vyhledávání.

Již vytvořený vlastní typ objektu lze změnit případně odstranit pomocí tlačítek **ZMĚNIT** a **SMAZAT**.

11.4. Plánované události

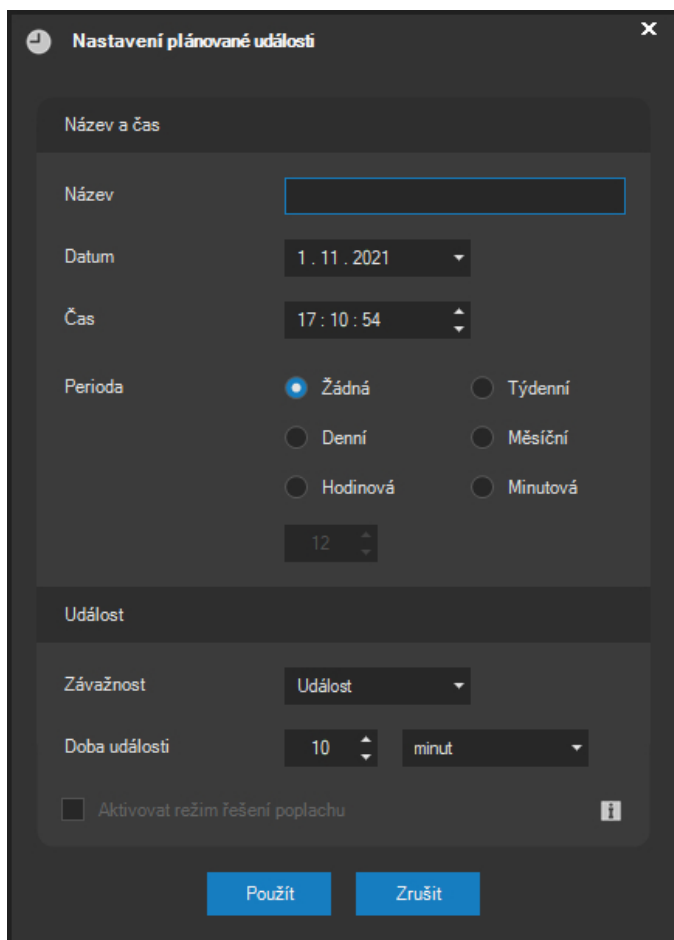
11.4.1. Základní nastavení

Platforma ATEAS Security umožňuje také naplánování událostí na pevné časové okamžiky. Pokud například potřebujeme, aby se určité otočné kamery v konkrétní čas jednorázově nebo opakovaně nasměrovaly do přednastavené pozice nebo aby po určitý čas monitorovaly určité body v túře, můžeme tyto události v systému naplánovat. Kromě zmíněných případů plánovaného pohybu na preset anebo dočasné přepnutí do túry lze samozřejmě naplánovat i jiné reakce kamer jako je přepnutí kamer na monitor obsluhy, aktivace výstupů, zahájení záznamu nebo odeslání e-mailu. Plánované události lze tvořit v části administrace kamer.



Okno pro správu plánovaných událostí je rozděleno na dvě části. V levé části je k dispozici ovládací prvek pro výběr kamerového serveru, po jehož výběru se pod ním zobrazí aktuální seznam plánovaných událostí. Pomocí tlačítek pod tímto seznam lze vytvořit novou plánovanou událost, provést její výmaz nebo ji upravit. Pravá část okna obsahuje událostní scénář pro vybranou plánovanou událost.

Při vytvoření nové plánované události pomocí tlačítka s nápisem Přidat událost se zobrazí uživatelský dialog, kde je nutné vyplnit základní parametry pro vytvářenou plánovanou událost.



V tomto dialogu je nutné uvést název pro novou událost a také určit přesné datum a čas, kdy má k události dojít.

Vytvářená událost může mít přiřazenu časovou periodu anebo může být vytvořena bez periody. Toto nastavení se provádí pomocí volby některého z přepínačů ve skupině Perioda. Pokud je zvoleno nastavení žádná perioda, událost vznikne pouze jednou v nastavený čas. Při volbě jiného přepínače může událost vznikat periodicky každý den, týden, měsíc nebo po uplynutí určitého počtu hodin nebo minut.

V části Událost je možné přiřadit plánované události určitý stupeň závažnosti (běžná událost nebo poplach) a určit dobu jejího trvání.

V rozbalovacím seznamu Závažnost se nachází položka Skrytá, která znamená, že při události sice bude proveden nastavený událostní scénář v plném rozsahu, ale událost se nebude objevovat uživatelům v živém náhledu. Alternativně by bylo možné uživatele zbavit práv k příjmu událostí anebo v lokálním nastavení změnit chování aplikace při jejich příjmu, nicméně nastavení události na skrytou je jednodušší možností.

POZNÁMKA

To může být výhodné např. pokud časové události použijeme k pravidelnému nahrávání snímků na FTP server, kdy není nutné, aby taková událost vytvářela samostatný řádek v okně událostí.

Zaškrtnutím volby Aktivovat režim řešení poplachu je možné pro daný zdroj události aktivovat rozšířený mód řešení poplachů. Více viz samostatná subkapitola Režim řešení poplachů.

POZNÁMKA

Plánované události jsou v systému běžně dohledatelné stejně jako jiné typy událostí v záznamu jednotlivých kamer.

POZNÁMKA

Pokud má plánovaná událost nastavenou delší dobu trvání než je její perioda, nová událost v daném čase vznikne pouze za předpokladu, že předchozí událost již byla ukončena. Kamerový server brání vícenásobnému vzniku jedné plánované události. Různé plánované události se samozřejmě mohou časově překrývat.

POZOR

Odstraněním plánované události ji však nelze přerušit nebo předčasně ukončit, pokud již byla na kamerovém serveru zahájena.

Tlačítko s nápisem Vlastnosti zobrazuje stejný uživatelský dialog jako v případě tvorby nové plánované události. Nastavené parametry události jsou automaticky předem vyplněny a je možné je pomocí tohoto dialogu upravit.

11.4.2. Řízení událostí

Vytváření událostních scénářů pro plánované události je zcela shodné jako v případě vytváření scénářů pro události kamer nebo pro externí události. Ovládací prvek pro vytváření událostního scénáře vždy zobrazuje událostní scénář aktuálně vybrané plánované události. Součástí událostního

scénáře mohou být veškeré dostupné akce jako je zobrazení kamer na monitoru obsluhy, událostí řízený záznam, aktivace výstupů kamer, odesílání e-mailu, ovládání otočných kamer, aktivace výstupů externích zařízení atd. Součástí událostního scénáře pro jednu plánovanou událost může být samozřejmě také více než jedna kamera.

POZNÁMKA

Na rozdíl od událostních scénářů pro události kamer či externí události nemohou být součástí událostního scénáře pro plánované události jiné kamery, než které jsou aktuálně přiřazené ke kamerovému serveru, na kterém je plánovaná událost vytvořena. Pokud chcete vytvořit reakci na jiném kamerovém serveru, je zapotřebí vytvořit plánovanou událost přímo na tomto serveru. Tlačítka pro přepínání serverů nejsou tedy v tomto kontextu dostupná.

Vytvořený událostní scénář musí být vždy uložen pomocí tlačítka **ULOŽIT**.

POZNÁMKA

V systému není k dispozici žádné speciální oprávnění, které by povolovalo nebo zakazovalo příjem plánovaných událostí klienty systému (na rozdíl od externích událostí). Pokud je pro událost vytvořen neprázdný událostní scénář, klient událost ovšem přijme pouze tehdy, pokud má přístup alespoň k jedné z kamer, které jsou jeho součástí. Tímto způsobem lze plánované události inteligentně distribuovat v systému s větším počtem serverů, kamer a klientů.

11.5. Režim řešení poplachů

11.5.1. Princip a aktivace režimu

Pro všechny zdroje událostí v systému ATEAS (události kamer včetně vlastních událostí kamer, plánované události či externí události) může být aktivován rozšířený režim řešení poplachů.

V příslušném dialogu postačí při úpravě nastavení zdroje události zaškrtnout volbu Aktivovat režim řešení poplachů. Pokud v systému vznikne poplach, který má aktivovaný režim řešení, změní se chování systému ve srovnání s běžnými událostmi a poplarchy následujícím způsobem:

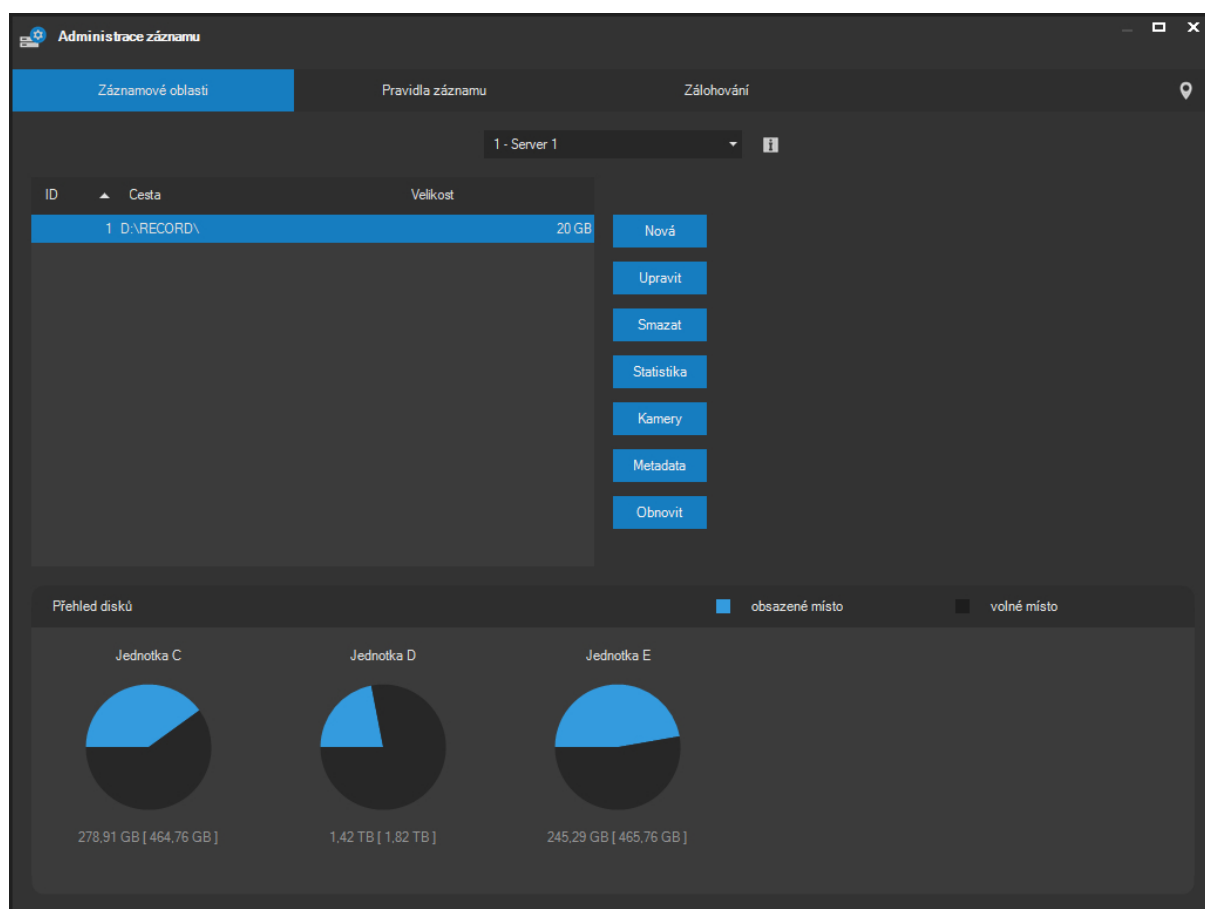
- Poplarchy s aktivovaným režimem řešení mají tmavší červenou výstražnou ikonu ve srovnání s běžnými poplarchy (události mají šedivou výstražnou ikonu).

- Poplarchy s aktivovaným režimem řešení budou v dohledovém okně, které přijímá poplarchy, zobrazeny do té doby, než některý oprávněný uživatel poplach aktivně vyřeší. Řešení poplachů z pohledu operátora systému je popsáno v kapitole Dohled.
- Dokud nejsou tyto poplarchy vyřešeny, nepodléhají lokálnímu nastavení maximální hranice zobrazených událostí a poplachů v seznamu v dohledovém okně.
- Tyto poplarchy jsou automaticky ukládány do deníku poplachů, který je k dispozici v okně Záznam. Funkce deníku poplachů je popsána v kapitole Práce se záznamem - Deník poplachů.
- Tyto poplarchy nemohou v systému zaniknout ani v případě, že není připojen žádný klient s oprávněním daný poplach přijmout či vyřešit. Pro tyto poplarchy je tedy aktivováno pozdější doručování, např. ihned po přihlášení klienta, který má oprávnění je vyřešit.
- Nevyřešené poplarchy nemohou v systému zaniknout, ani pokud dojde k výpadku či restartu serverů.
- K vyřešení poplachu musí mít uživatel přiděleno nejen oprávnění k příjmu poplachů z daného zdroje (kamera, externí systém), ale také oprávnění k jeho vyřešení.

11.6. Správa záznamu

11.6.1. Záznamové oblasti

Vymezení záznamové oblasti na kamerových serverech je prvním krokem při nastavování záznamu. Kamerový server bude moci pro svou záznamovou databázi používat pouze vymezené diskové oblasti omezené velikostí. Pro zahájení správy záznamu je nutné zvolit z administrační nabídky Záznam a na kartě **Záznamové oblasti** vybrat z rozbalovacího seznamu Kamerové servery příslušný server. Server musí být aktuálně připojený, jinak bude aplikace reagovat varovnou zprávou a nebude možné provádět žádná nastavení.



Na této kartě jsou zobrazeny všechny záznamové oblasti, které již byly vytvořeny. V části přehled disků je k dispozici přehled pevných disků kamerového serveru s náhledem volného místa (podrobné údaje jsou vypsané pod grafem disku). Tlačítkem **OBNOVIT** lze údaje o discích aktualizovat.

Vytváření záznamových oblastí

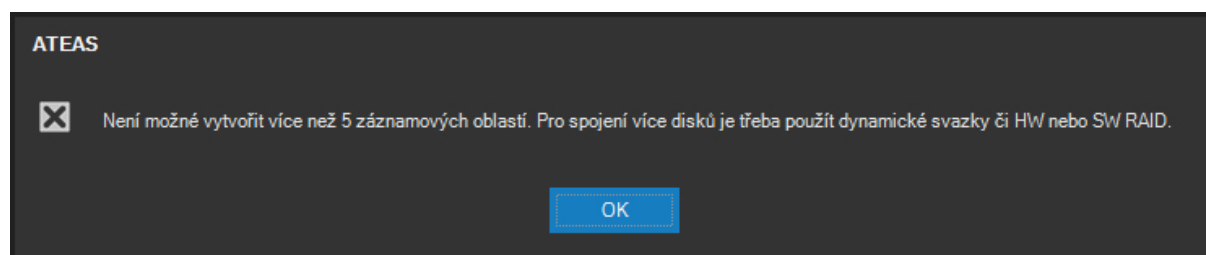
Novou záznamovou oblast lze vytvořit pomocí tlačítka **NOVÁ**. Počínaje verzí ATEAS Security 3.9.4 je možné vytvořit až 5 nezávislých záznamových oblastí. Mezi důvody pro tvorbu více než jedné záznamové oblasti může patřit například:

- potřeba využít více nezávislých diskových oblastí, které nelze nebo to není vhodné provést jejich spojení v jeden logický celek,
- potřeba definovat různé doby uchovávání záznamu pro různé skupiny kamer pomocí různého nastavení omezovače pro každou záznamovou oblast.

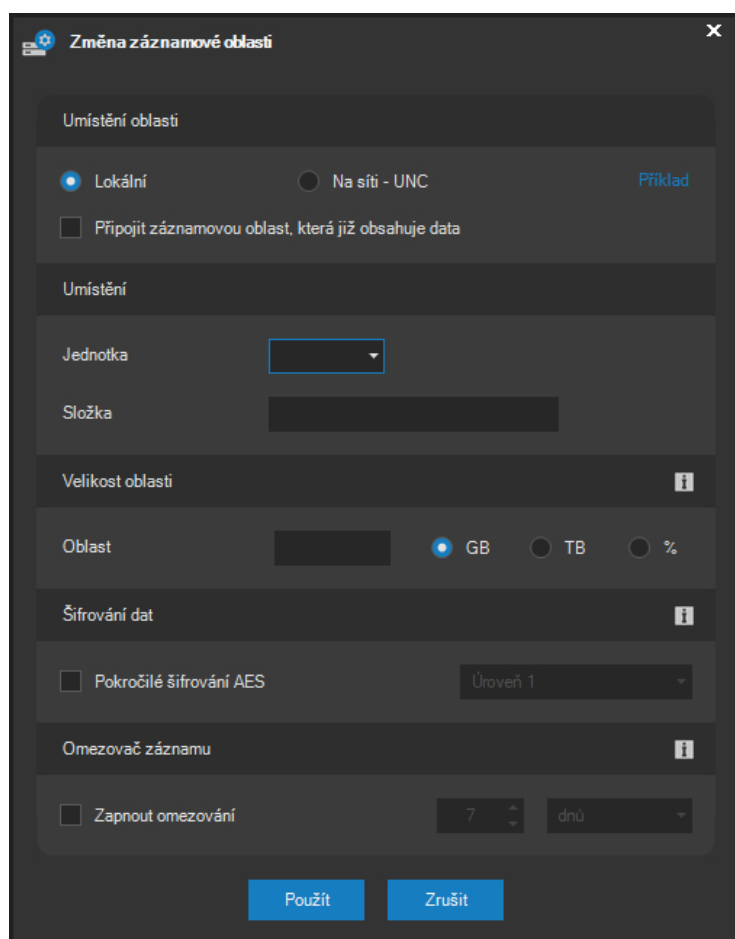
POZOR

Možnost vytváření více záznamových oblastí by neměla, přestože to je možné, sloužit jako primární nástroj pro navýšení celkové velikosti záznamového prostoru. Je nutné mít na paměti, že mezi jednotlivými záznamovými oblastmi neplatí žádná pravidla redundance (pro zálohování celých serverů viz kapitola o clusterech). Pokud je jediným cílem vytvoření více záznamových oblastí zvýšení celkové kapacity záznamového prostoru, je dobré vždy zvážit použití výkonných nástrojů pro spojení oblastí či celých disků do jednoho logického celku, který může zajistit také určitou redundanci např. při výpadku disku. Jedná se zejména o technologii RAID řešenou na bázi softwarové nebo hardwarové (hardwarové řešení je významně výkonnější).

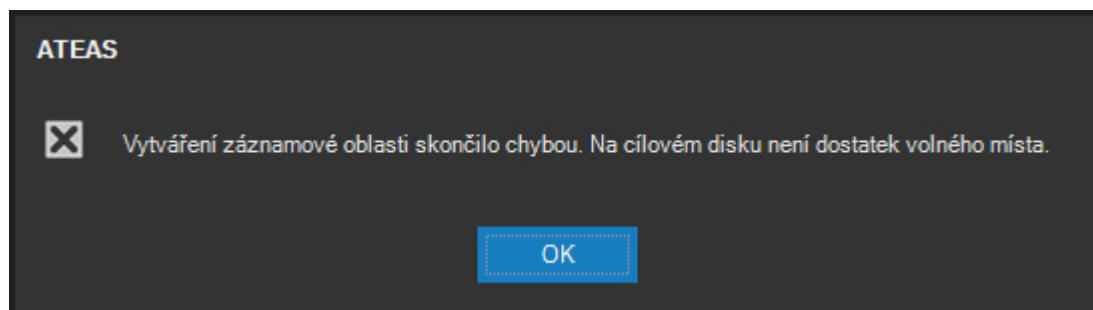
Pokud se pokusíte vytvořit více než pět záznamových oblastí na jednom kamerovém serveru, aplikace bude reagovat varovnou zprávou a vytvoření další oblasti nepovolí.



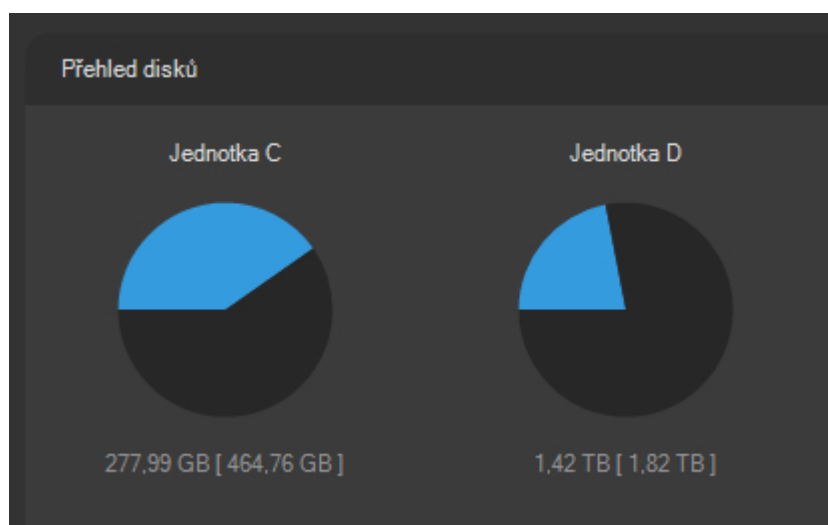
Po stisku tlačítka **NOVÁ** se zobrazí dialog, ve kterém je nutné zadat základní parametry pro vytvářenou záznamovou oblast.



Pokud je záznamová oblast uložena lokálně, je nutné určit jednotku z rozbalovacího seznamu, dále napsat název složky, která bude na vybraném disku serveru vytvořena a provést nastavení maximální velikosti vytvářené části databáze. Maximální hranici lze určit v jednotkách GB, TB nebo v procentech velikosti disku. Minimální velikostí oblasti databáze je 1 GB, maximální velikostí je velikost daného disku. Při nedodržení maximální hranice aplikace reaguje příslušnou zprávou.



Dále se také nepodaří vytvořit záznamovou oblast větší než je aktuální volné místo na cílovém disku.



Volitelně lze také ihned při vytváření oblasti aktivovat funkci omezovače, která je popsána dále v textu.

Záznamová oblast může být také vytvořena kdekoliv na síti. V takovém případě je nutné označit přepínač Na síti – UNC a namísto výběru pevného disku je nutné zapsat cestu UNC začínající znaky \\ a poté opět složku, která bude v daném umístění vytvořena serverem.

POZOR

Služba kamerového serveru ATEAS Server je po instalaci spuštěna pod účtem Local System. Tento účet však nemá přístup k síťovým prostředkům. Pokud tedy budete chtít vytvořit záznamovou oblast na síti se zadáním cesty UNC, musíte v aplikaci Service Control Manager změnit účet, pod kterým bude služba spuštěna. Je třeba použít takový administrátorský účet, který má přístup na dané umístění v síti.

POZNÁMKA

Je zajištěno, že záznamový server vždy automaticky ponechá určitou rezervu volného místa na daném disku volnou i pokud ještě nedosáhl maximální přidělené hranice pro záznamovou oblast. To platí, i když je např. velikost záznamové oblasti nastavena na 100 procent využití disku. Tím se předchází úplnému vyčerpání volného místa disku.

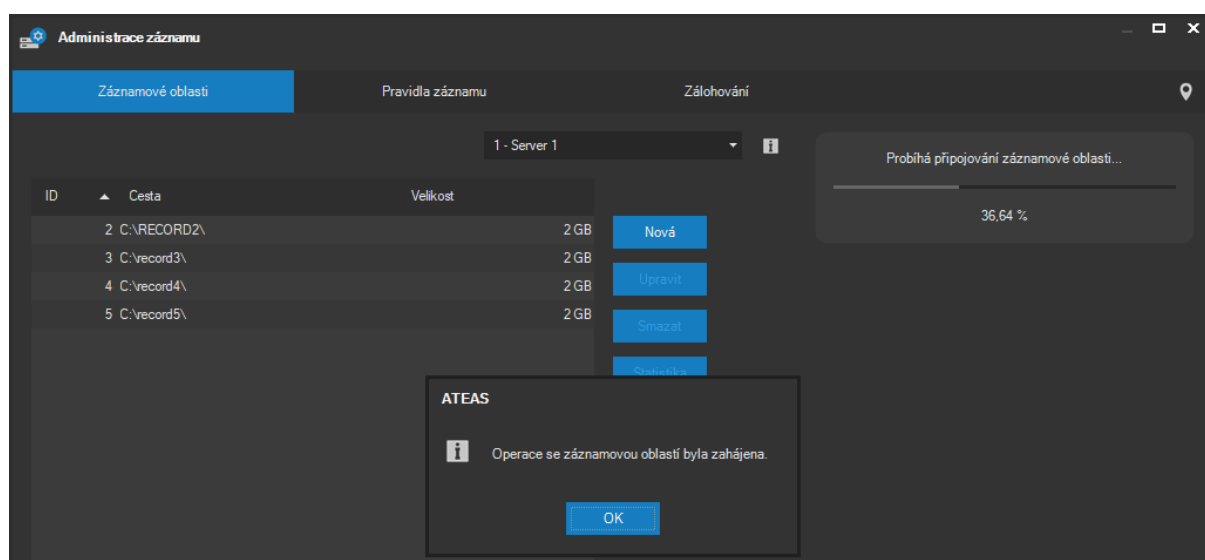
POZNÁMKA

Maximální velikost záznamové oblasti není v ATEAS Security nikterak omezena a je dána pouze velikostí cílového disku či diskového pole. Koncepce a výkon záznamové oblasti zajišťuje použitelnost a nulové čekací vyhledávací doby i při velikostech do 100 TB.

Po úspěšném vytvoření záznamové oblasti na severu aplikace reaguje zprávou. Vytváření záznamové oblasti však může skončit též chybou, např. pokud není možné na příslušný disk zapisovat nebo nebylo možné vytvořit složku s daným názvem (složka již existuje nebo název není přípustný).

Připojení existující záznamové oblasti

Nejčastěji vytváříme prázdnou záznamovou oblast, do které bude kamerový server dle nastavených pravidel záznamu provádět záznam z kamer. Je však také možné ke kamerovému serveru připojit též záznamovou oblast, která již obsahuje data. Tuto funkci budeme potřebovat např. tehdy, pokud dojde k havárii disku, na kterém je nainstalován kamerový server, a po jeho nové čisté instalaci budeme chtít připojit původní (již existující) záznamovou oblast. Připojení provedeme tak, že při vytváření oblasti aktivujeme volbu Připojit záznamovou oblast, která již obsahuje data. Průběh připojování je poté zobrazen přímo v okně administrace.



POZNÁMKA

Operace se záznamovou oblastí je spuštěna na pozadí, klienti a kamerový server mohou pokračovat ve své běžné činnosti.

Po dokončení připojování bude nová záznamová oblast naplněna daty a bude možné s daty ihned normálně pracovat pomocí nástrojů přehrávání, exportů apod.

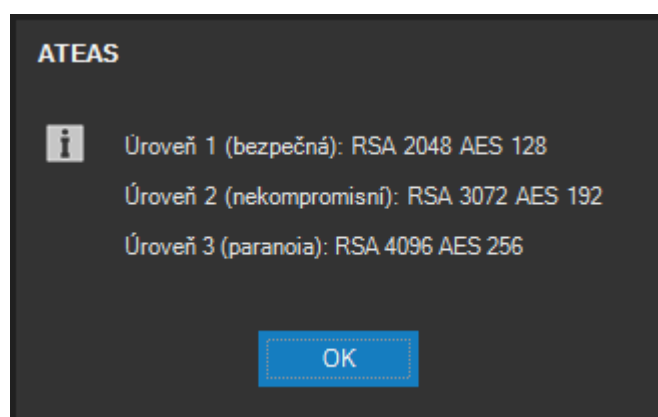
POZNÁMKA

Pokud připojujeme záznamovou oblast s již vytvořenými daty, není samozřejmě prováděna kontrola volného místa na cílovém disku.

Šifrování záznamové oblasti

Pomocí volby Aktivovat pokročilé šifrování AES lze již při vytváření nebo později při změně oblasti aktivovat šifrování dat v záznamové oblasti pokročilou šifrou AES (Advanced Encryption Standard).

Úroveň šifrování je možné nastavit v rozmezí 1 až 3. Přestože i první úroveň nabízí ochranu neprolomitelnou současnými prostředky, je možné zvolit i vyšší úroveň zabezpečení spočívající zejména v délce použitých kryptografických klíčů.



Při aktivaci pokročilého AES šifrování dat pro záznamovou oblast je možné předejít např. těmto útokům:

- Přímý přístup k datům záznamové oblasti: Pokud jsou šifrovaná data z nezabezpečeného datového úložiště načtena jiným softwarem (přímým přístupem na disk záznamové oblasti), její obsah nemůže být převeden do čitelné podoby.
- Zcizení serveru včetně instalovaného software ATEAS Security. V distribuovaném systému je možné zamezit přístupu k datům serveru, i pokud se celý server ocitne v rukou útočníka. Pokud je takový server již mimo původní instalaci ATEAS Security, kamerový server nemůže žádným způsobem získat klíč pro dešifrování dat záznamové oblasti.

POZNÁMKA

Možnost šifrování záznamových oblastí je dostupná až od edice ATEAS Security PROFESSIONAL.

Úprava záznamové oblasti

Vytvořenou záznamovou oblast lze dodatečně upravovat pomocí tlačítka **UPRAVIT**. Při úpravě vybrané záznamové oblasti je aktivován stejný dialog jako při vytváření záznamové oblasti s tím rozdílem, že není možné měnit umístění záznamové oblasti (lokální či síťové) a nelze ani měnit název složky. Je však možné změnit velikost záznamové oblasti, nastavení omezovače, nastavení šifrování atd.

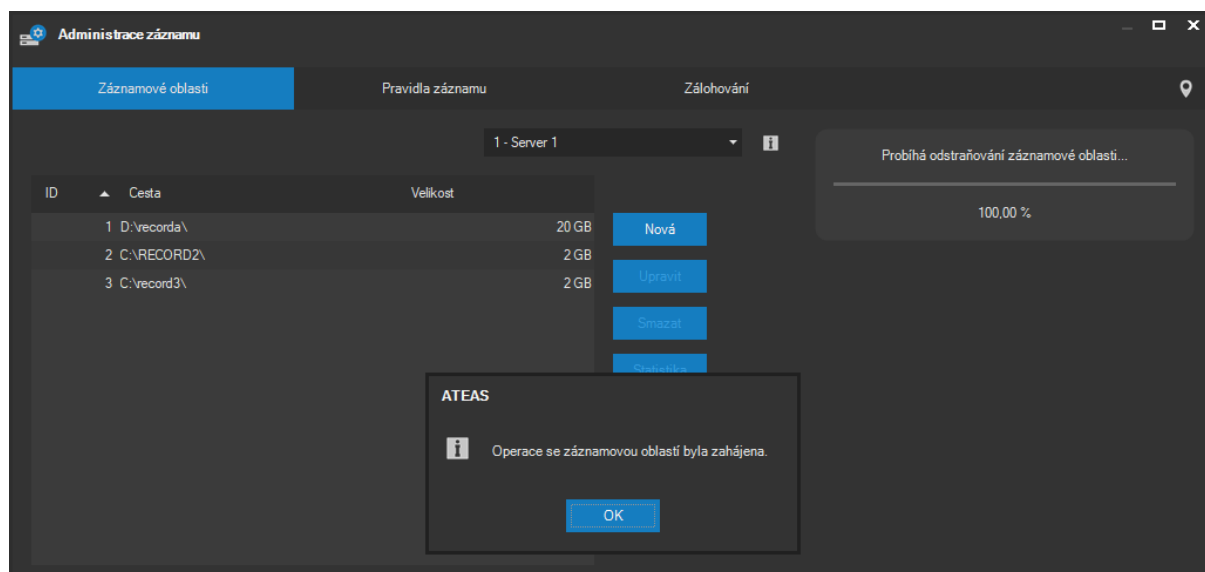
POZOR

Z důvodu konzistence záznamové databáze nedochází ke změně velikosti záznamové oblasti okamžitě, nýbrž nejpozději během dvou následujících zápisových cyklů, kdy je velikost záznamové oblasti inteligentně upravena (tj. při snižování velikosti jsou smazána nejstarší data).

Vzhledem k tomu, že kamerový server používá pokročilé metody manipulace s daty a volným prostorem na disku včetně například automatické alokace nefragmentovaného prostoru, mohou velmi časté a významné změny velikosti záznamové oblasti způsobit její zvýšenou fragmentaci. Po velmi mnoha změnách velikosti (mnoha desítkách až stovkách) je tak dobré z hlediska výkonu záznamové databáze provést defragmentaci disku. Pouhý cyklický přepis databáze stupeň její fragmentace nezvyšuje.

Odstranění záznamové oblasti

Pomocí tlačítka **SMAZAT** lze provést odstranění záznamové oblasti. Toto odstranění způsobí ztrátu všech dat v záznamové oblasti a fyzické odstranění všech souborů z disku. Pro definitivní odstranění záznamové oblasti je nutné potvrdit dvojí upozornění. Odstraňování záznamové oblasti může být v závislosti na její velikosti časově poměrně náročná operace (v délce trvání i v řádu minut), a proto je tato operace doprovázena informací zobrazující průběh odstraňování včetně hodnoty průběhu vyjádřené v procentech.

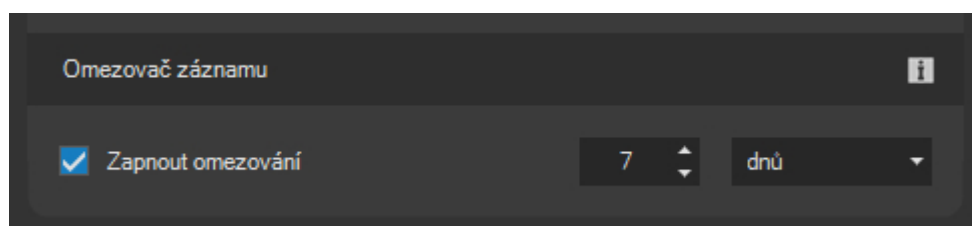


POZNÁMKA

Operace se záznamovou oblastí je spuštěna na pozadí, klienti a kamerový server mohou pokračovat ve své běžné činnosti.

Nastavení omezovače

Při vytváření nebo úpravě záznamové oblasti lze aktivovat unikátní funkci omezovače. Tato funkce dokáže automaticky omezovat stáří dat v záznamové oblasti, tak aby nebyla překročena nastavená maximální hranice, čímž je možné automaticky naplnit zákonné požadavky na kamerový záznam ve vztahu k ochraně osobních údajů. Pro každou záznamovou oblast lze definovat jiné nastavení omezovače, a je tudíž možné uchovávat různé skupiny kamer různou dobu v záznamu.



Zaškrtnutí políčko Zapnout omezování slouží k aktivaci resp. deaktivaci funkce omezovače pro video a audio data. Je zde možné nastavit počet dnů (či hodin), po které mají být data v záznamu udržována. Jednotky hodin lze použít v případě, že potřebujete stáří dat v záznamové oblasti omezit na dobu kratší než jeden den nebo v případě potřeby přesnější definice.

POZNÁMKA

Změna nastavení omezovače se začne uplatňovat ihned po vytvoření nebo změně parametrů záznamové oblasti pomocí tlačítka **POUŽÍT**.

POZNÁMKA

Při omezení stáří dat v záznamové oblasti nedochází k žádnému snížení celkové velikosti záznamové oblasti. Pro uvolnění části záznamové oblasti v podobě volné diskové kapacity zpět operačnímu systému je zapotřebí změnit její velikost pomocí tlačítka **UPRAVIT**.

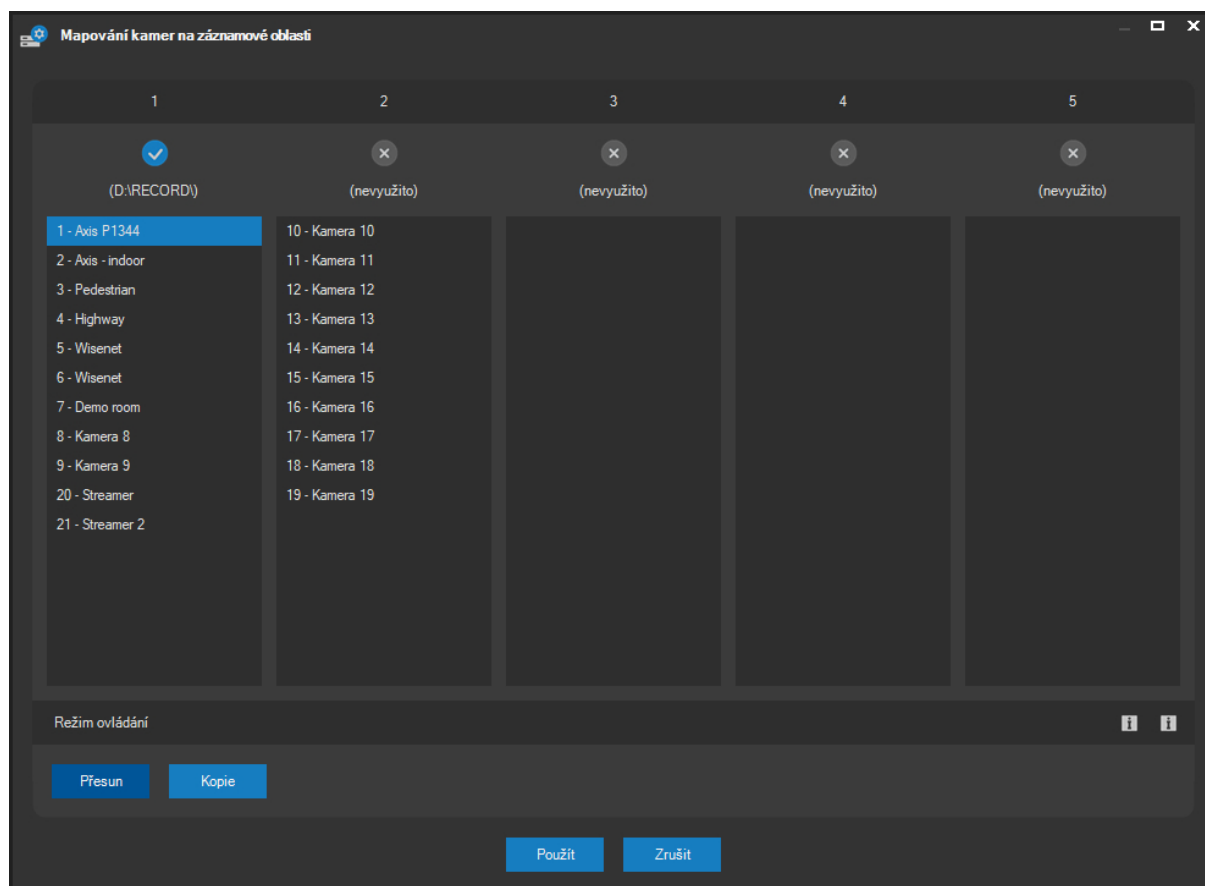
Přiřazení kamer k záznamovým oblastem

Pokud je na kamerovém serveru vytvořeno více záznamových oblastí, je možné určit, které kamery budou využívat tu či onu záznamovou oblast. Je tak možné pro některé kamery vymezit rozsáhlou záznamovou oblast, zatímco pro jinou skupinu kamer pouze oblast menší, nemáme-li tak vysoké nároky na dobu uchování dat v záznamu. Pro záznamové oblasti lze také definovat různá nastavení omezovače.

POZNÁMKA

Při přidání nové kamery do systému bude kamera automaticky přiřazena záznamové oblasti s číslem jedna.

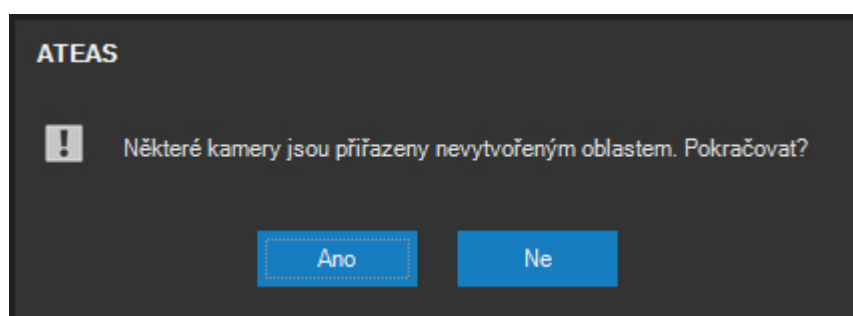
Pro přiřazení jednotlivých kamer k různým záznamovým oblastem je třeba použít tlačítko **KAMERY**. Poté se otevře okno Mapování kamer na záznamové oblasti.



Na obrázku je vidět maximální počet pěti záznamových oblastí, je možné také ihned rozpoznat, kolik oblastí bylo již vytvořeno a kolik jich kamerový server používá. Seznamy pod označením záznamových oblastí obsahují čísla a názvy kamer, které jsou dané záznamové oblasti aktuálně přiřazeny. Kamery lze velmi jednoduše přesouvat mezi jednotlivými seznamy pouhým přetažením pomocí myši. Je možné takto přesunout i větší počet kamer najednou, pokud se v seznamu provede vícenásobná výběr (např. pomocí klávesy CTRL nebo tažením myši přes více položek). Pro zahájení přesunu či kopie vybraných položek do jiného seznamu je nutné opětovné stisknutí tlačítka myši na jedné z již vybraných položek.

POZNÁMKA

Kamery lze přesouvat také k záznamovým oblastem, které ještě nebyly vytvořeny. Po uložení tohoto nastavení takové kamery samozřejmě nemohou provádět záznam. Záznam však začne automaticky poté, co byla záznamová oblast vytvořena. Pokud aplikace zjistí tento stav, budete upozorněni příslušnou zprávou.



Ve výchozím nastavení tohoto dialogu ke při přetažení pomocí myši proveden přesun kamer do jiného seznamu pod cílovou záznamovou oblastí. Pokud však namísto tlačítka **PŘESUN** aktivujeme tlačítko **KOPIE**, dojde ke zkopírování položek. To znamená, že dané kamery budou současně zaznamenávat do více oblastí. Tuto funkci lze využít např. pro zajištění delší doby uchování videa a zvuku kamer v nižší kvalitě v jiné oblasti.

POZNÁMKA

Kamery mohou pro záznam do různých oblastí používat různá záznamová pravidla. Toto nastavení se provádí v okně Základní nastavení kamery u aktivace pravidel záznamu.

POZNÁMKA

Pokud chcete kameru ze seznamu odstranit, můžete ji přesunout do jiného seznamu. Pokud kamera v cílovém seznamu již existuje, bude provedeno pouze její odstranění z původního seznamu.

Při přesunu či kopírování položek seznamu je možné nezávisle na stisknutém tlačítku ve spodní části okna vynutit změnu operace pomocí klávesy CTRL (vynutí kopírování) nebo SHIFT (vynutí přesun).

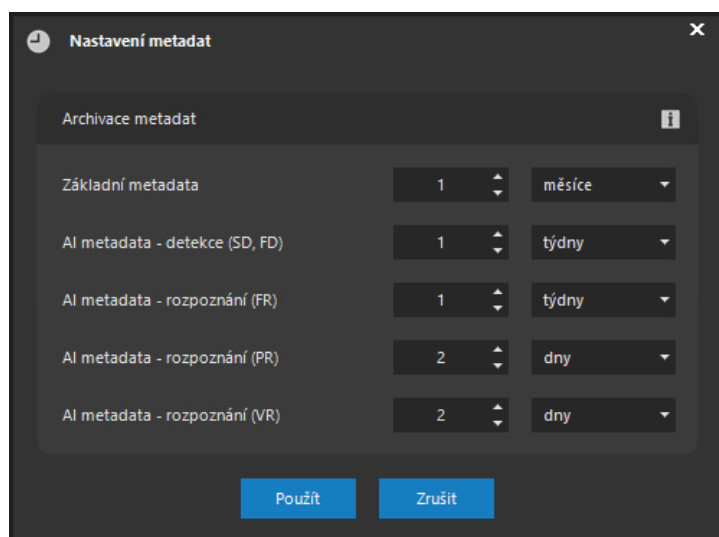
Archivace metadat

Pro každý kamerový server je možné nastavit dobu uchovávání metadat. Mezi základní metadata patří např. informace o detekci pohybu či aktivaci poplachových vstupů. Metadata neuronových sítí pak umožňují funkci pokročilého forenzního vyhledávání ve videu (pohyb v zónách, překročení čáry apod.) a také vyhledávání obličejů či osob podle vybraného vzoru.

POZOR

Zejména metadata generovaná neuronovou sítí mohou být datově náročnější, nastavené době je tedy nutné přizpůsobit návrh systému.

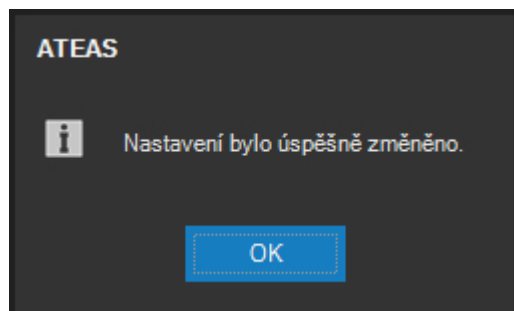
Dobu archivace metadat lze změnit pomocí tlačítka **METADATA**. Toto nastavení lze provést kdykoliv a zcela nezávisle na vytváření záznamových oblastí.



Archivace metadat		
Základní metadata	1	měsíce
AI metadata - detekce (SD, FD)	1	týdny
AI metadata - rozpoznání (FR)	1	týdny
AI metadata - rozpoznání (PR)	2	dny
AI metadata - rozpoznání (VR)	2	dny

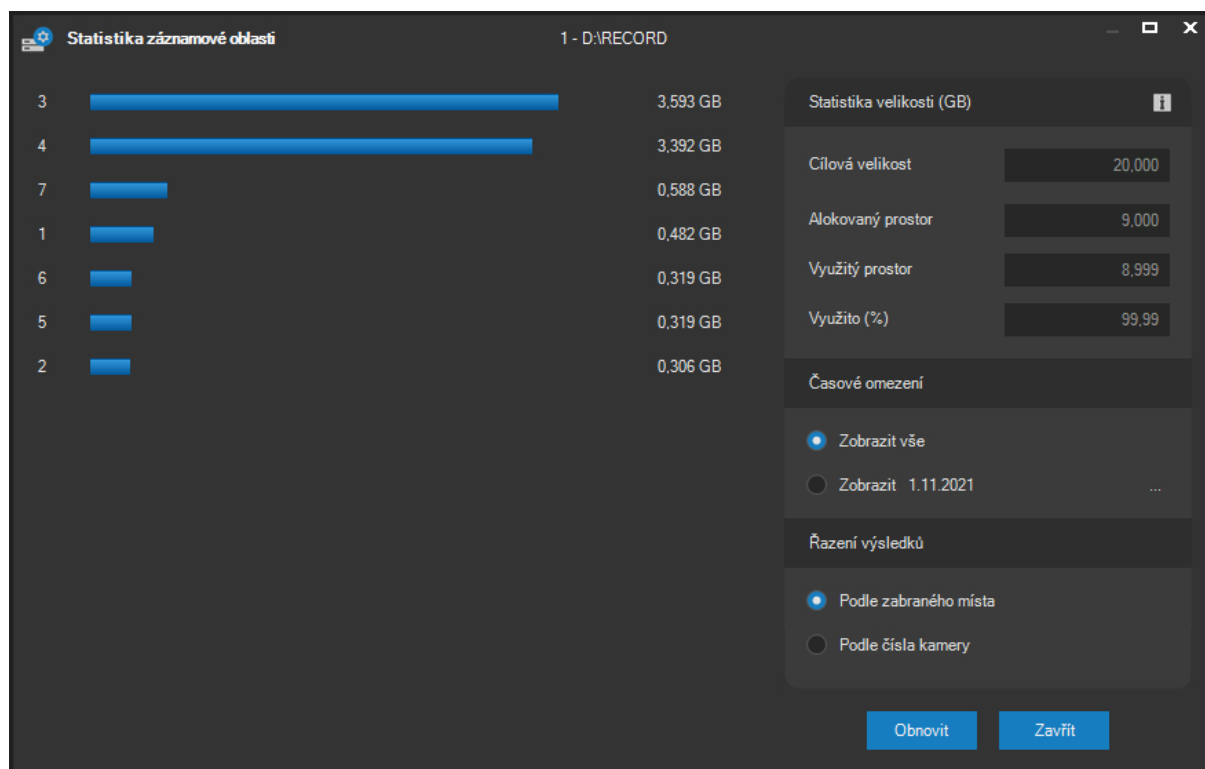
Použít Zrušit

Po úspěšné změně nastavení se zobrazí potvrzující zpráva.



Statistika záznamových oblastí

Pomocí tlačítka **STATISTIKA** lze pro vybranou záznamovou oblast kamerového serveru zobrazit statistiku využití alokovaného prostoru. Tyto informace mohou být zásadní při rozhodování o změně nastavení záznamových pravidel (profilů).



Okno obsahuje sloupcový graf vyjadřující, kolik prostoru v záznamové databázi nárokuje jednotlivé kamery. Jedná se o relativní graf, kde maximální hodnota (100 procent) je nastavena na hodnotu kamery s maximálním obsazeným místem. Vedle jednotlivých řad je obsazeno místo vypsáno také v absolutní hodnotě v jednotkách GB s přesností na 3 desetinná místa.

Okno zobrazuje také celkové údaje o záznamové oblasti:

Cílová velikost: Velikost záznamové oblasti nastavená administrátorem.

Alokovaný prostor: Aktuální skutečný alokovaný prostor.

Využitý prostor: Aktuálně využitý prostor pro video, audio a metadata.

Veškeré údaje jsou zobrazeny v jednotkách GB s přesností na 3 desetinná místa nebo relativně v procentech.

POZNÁMKA

Alokovaný prostor může být dočasně vyšší či nižší než cílová velikost, dokud není databáze zaplněna prvním zápisovým cyklem nebo při změně cílové velikosti administrátorem. V takovém případě dochází k adaptaci velikosti postupně během jednoho až dvou zápisových cyklů.

POZNÁMKA

Skutečně využitý prostor může být nižší než alokovaný prostor, pokud databáze vytváří rezervu v oblasti v důsledku působení automatického omezovače stárání dat v databázi. Jako nevyužitý prostor se také jeví záznam vytvořený verzemi ATEAS Security před verzí 4.0.0, než dojde k jeho přepisu.

Statistiku v podobě relativního grafu lze zobrazit buď pro celou záznamovou oblast nebo také pro vybraný den, což může poskytnout další cenné informace při vyhodnocování změn nastavení videa z kamer, záznamových pravidel, četnosti událostí apod.

Graf je automaticky řazen od kamery s největšími nároky na prostor v databázi po kameru s nejnižším nárokem. Pomocí přepínačů ve skupině Řazení výsledků lze však graf seřadit také podle čísla kamery.

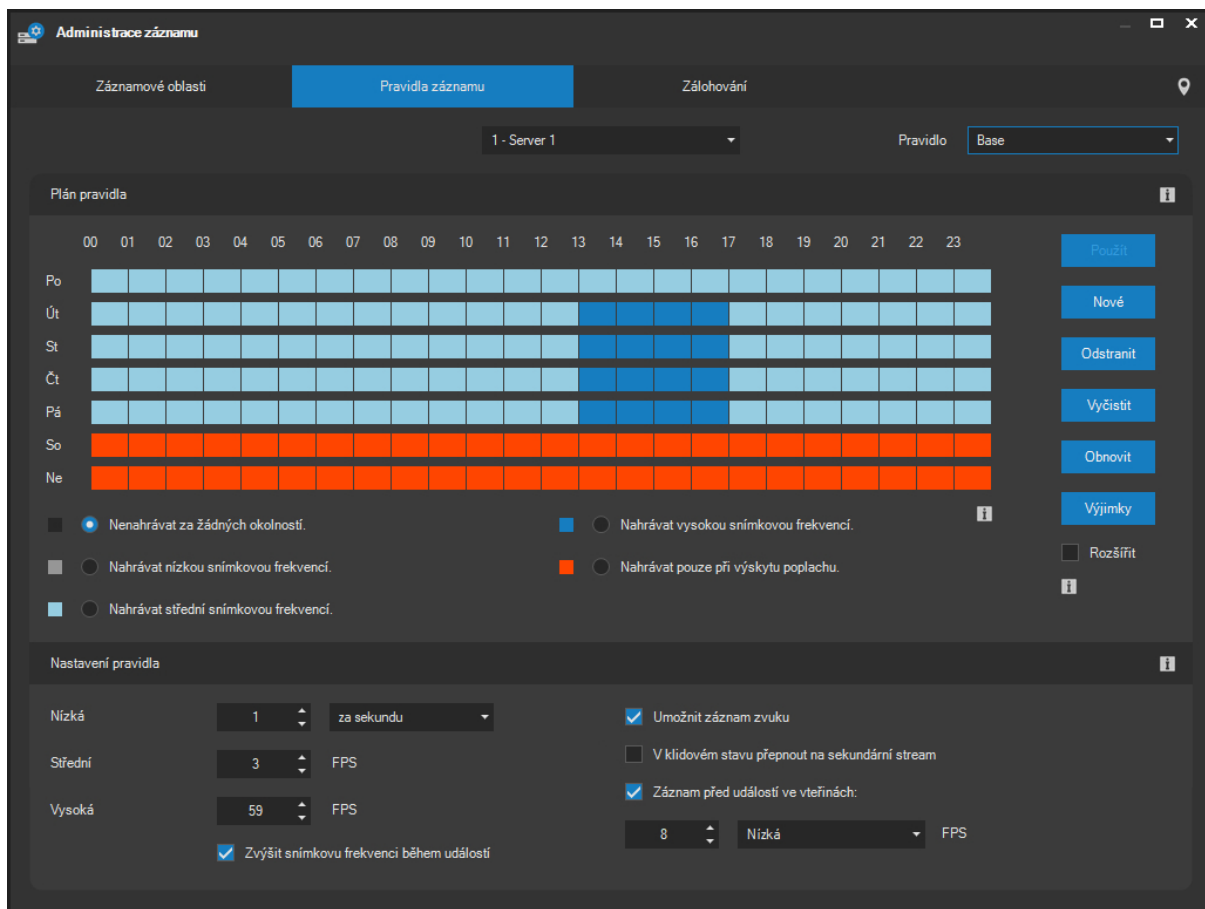
11.6.2. Záznamové profily

Záznamový profil je soubor pravidel pro provádění záznamu z kamery. Tento profil je vytvořen vždy na příslušném kamerovém serveru a může být použit pro jednu či více kamer daného serveru. Pro přístup k záznamovým profilům je nutné zobrazit kartu **Pravidla záznamu** v části administrace záznamu.

POZNÁMKA

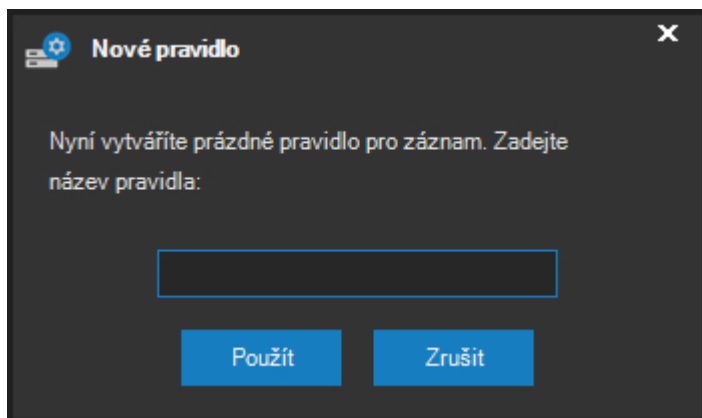
Vytvořené profily je možné jednotlivým kamerám přiřazovat v části administrace kamer, základní nastavení kamery.

Pro práci s profily na daném serveru je nutné tento server vybrat z rozbalovacího seznamu Kamerové servery. Poté se v rozbalovacím seznamu označeném Vyberte pravidlo objeví veškeré záznamové profily nahrané na vybraném serveru. Výběrem pravidla z tohoto seznamu je možné ho zobrazit.



Vytváření a odstraňování záznamových profilů

Nový záznamový profil (pravidlo) lze na vybraném serveru vytvořit po stisku tlačítka **NOVÉ**. V dalším kroku je nutné zadat název pravidla, které nesmí být duplicitní.



Po stisku tlačítka **POUŽÍT** dojde na serveru k vytvoření prázdného záznamového pravidla, jeho vytvoření je potvrzeno zprávou. Nově vytvořené pravidlo je také automaticky vybráno pro další úpravu.

Vybrané pravidlo lze odstranit po stisku tlačítka **ODSTRANIT** a potvrzení zprávy tlačítkem **ANO**.

Úprava pravidel záznamu (profilů)

Vybrané pravidlo lze upravit pomocí ovládacího prvku pro úpravu záznamového pravidla. Jednotlivé řádky reprezentují dny v týdnu, ve vertikálním směru je k dispozici rozdělení dne do 24 hodin, minimální rozlišení je 15 minut. Jednotlivé čtvrt hodinové úseky lze označit pohybem myši při stisknutí levém či pravém tlačítku myši. Při stisknutí levém tlačítku myši bude použito vždy nastavení přepínače pod ovládacím prvkem. Při použití pravého tlačítka bude vždy docházet k vymazání obsahu tj. překreslení do výchozí podoby (odpovídá levému tlačítku při označeném přepínači Nenahrávat za žádných okolností). Při použití levého tlačítka myši je tak k dispozici pro zákres do ovládacího prvku několik možností:



TIP

Pro rychlé označení celého dne nebo týdne lze použít dvojité resp. trojitě kliknutí.

TIP

Pro rychlé určení pracovní doby ve více dnech najednou použijte klávesu ALT.

Snímkové frekvence s označeními nízká snímková frekvence, střední snímková frekvence a vysoká snímková frekvence mohou být upraveny pomocí příslušných ovládacích prvků. Nízkou snímkovou frekvencí lze nastavit také počtem snímků za minutu (vedle standardní možnosti FPS – počet snímků za vteřinu).

Nastavení pravidla

Nízká	1	za sekundu
Střední	3	FPS
Vysoká	59	FPS

☒ Zvýšit snímkovou frekvenci během událostí

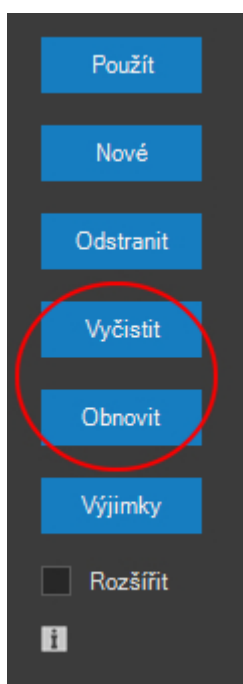
POZOR

U video formátů jiných než MJPEG nemusí být tyto snímkové frekvence zcela přesně dodrženy, neboť zcela přesné řízení je vyloučeno kompresními závislostmi mezi snímky. Platí, že nízká a střední frekvence je počítána pouze z kompletních snímků. Vysoká snímková frekvence vždy znamená záznam všech snímků.

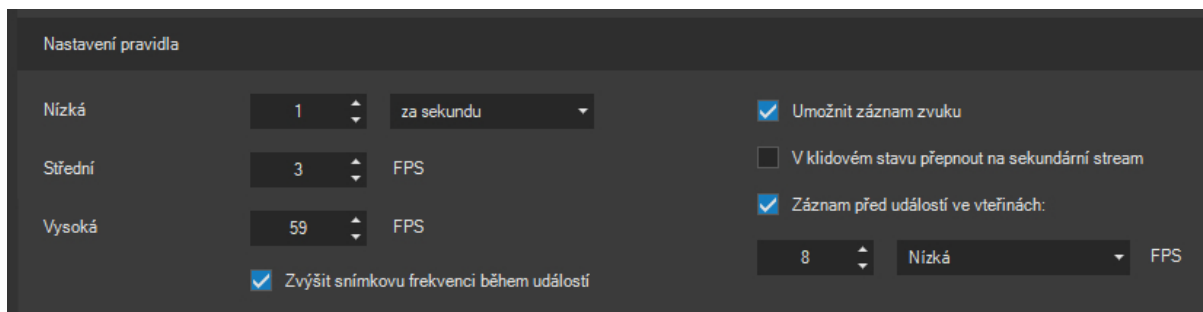
Pro speciální kamery s vysokou snímkovou frekvencí poskytující formát MJPEG lze hodnotu zvýšit až na 500, kdy se aktivuje stejný efekt jako pro ostatní video formáty, tj. zápis všech snímků z video streamu.

Při úpravě záznamového pravidla jsou k dispozici dvě pomocná tlačítka s následujícími funkcemi:

Tlačítko **VYČISTIT** provede vyčištění pravidla do podoby, ve které je aplikováno nastavení nenahrávat za žádných okolností v celém časovém plánu. Tlačítko **OBNOVIT** uvede pravidlo do stavu, ve kterém je uloženo na serveru (tj. při posledním uložení změn).



V rámci úpravy záznamového profilu je možné učinit ještě některá dodatečná nastavení v podobě zaškrťovacích políček.



Pokud je zaškrtnuto políčko označené Zvýšit snímkovou frekvenci během událostí a v daném čase je aplikována nízká nebo střední snímková frekvence, bude během poplachu záznamová snímková frekvence zvýšena na vysokou.

Pokud je zaškrtnuto políčko Umožnit záznam zvuku, bude spolu s videem zaznamenáván též zvuk.

POZOR

Zvuk bude zaznamenáván pouze tehdy, jeli pro dané zařízení aktivován v nastavení příslušné kamery a pokud je zároveň zaznamenáváno také video alespoň nízkou snímkovou frekvencí.

Pomocí záznamového pravidla lze nastavit snížení snímkové frekvence záznamu, pokud neprobíhá událost. Pokud bychom chtěli ušetřit kapacitu záznamu nejen pomocí snížení snímkové frekvence, ale také pomocí snížení rozlišení videa anebo změnou video formátu, můžeme aktivovat volbu V klidovém stavu přepnout na sekundární stream.

POZNÁMKA

Aby mohlo k přepnutí dojít, musí být sekundární stream povolen v nastavení kamer.

Při zaškrtnutí políčka Záznam před událostí ve vteřinách bude možné při vzniku události do záznamu vložit ještě určitou dobu před vznikem události (pre-alarm buffer). Časový parametr udává počet vteřin záznamu, který bude uložen z doby před výskytem události. Dále je také možné určit snímkovou frekvenci, která bude použita pro tvorbu předpoplachového bufferu.

TIP

Předpoplachový buffer dokáže zpětně nahradit daný úsek záznamu i v situaci, kdy probíhá stálý záznam s nižší snímkovou frekvencí nebo v jiném rozlišení.

POZOR

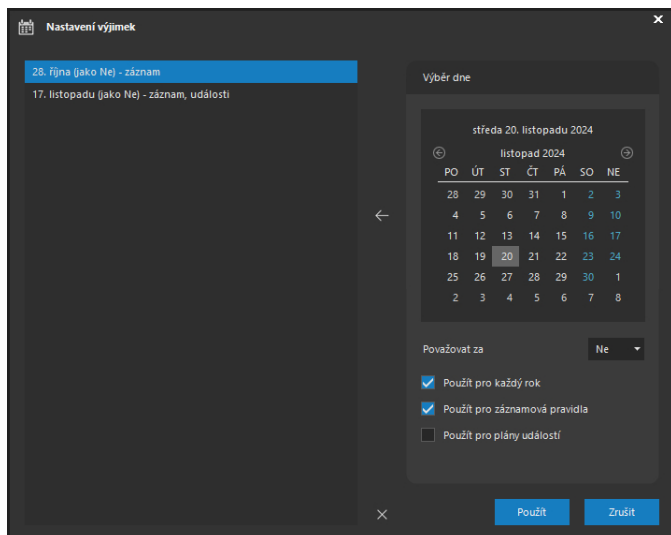
Pokud bude na určitou kameru aplikován záznamový profil aktivovaným předpoplachovým záznamem, nebude účinná volba Udržovat permanentní spojení ke kameře v nastavení kamery, neboť toto spojení bude nutné udržovat permanentně.

Tlačítkem **POUŽÍT** lze provedené změny záznamového pravidla uložit. Aplikace uložení potvrdí zprávou. Změny v nahrávacím profilu se u všech kamer, který mají tento profil přiřazen, projeví okamžitě.

Pokud bude při vytváření nového nebo změně stávajícího pravidla aktivována volba Rozšířit, budou provedené změny v záznamovém pravidlu provedeny na všech kamerových serverech, ke kterým má administrátor přístup.

Pomocí tlačítka **VÝJIMKY** lze na daném kamerovém serveru vytvořit databázi speciálních dnů, které budou chápány jinak, než jak jim určují záznamová pravidla. Výjimky lze použít například na státní svátky, pro které lze nastavit, aby byly z hlediska záznamu chápány vždy jako neděle namísto

všedních dnů. Nastavení výjimek je platné pro všechna záznamová pravidla, nikoliv pouze pro jedno vybrané.



V dialogu, který se zobrazí po stisku tlačítka **VÝJIMKY**, se nachází prvek kalendáře. Pomocí tohoto prvku lze vybrat libovolný kalendářní den v libovolném roce, který chceme označit jako výjimečný, tudíž ho vyjmout z nastavení záznamových profilů. Pro vybraný den, který na kalendáři označíme, můžeme zvolit, za jaký den bude z hlediska záznamu považován. Svátky tedy mohou být považovány např. za neděli, víkendové dny s plánovanou pracovní aktivitou v objektu zase za pondělí. U každého dne se můžeme dále rozhodnout, zdali bude tato výjimka platná pouze v konkrétním vybraném roce anebo se bude opakovat každoročně.

Po výběru dne a doplňujících nastaveních lze výjimku přidat do seznamu pomocí tlačítka s bílou šipkou, které se nachází mezi prvkem kalendáře a seznamem výjimek. Odstranění výjimky lze provést pomocí tlačítka se symbolem křížku. Výjimky, pro které není nastaveno periodické opakování každý rok, jsou v seznamu uvedeny bez určení roku, výjimky bez periody jsou opatřeny také údajem o roce.

Aby byla výjimka použita pro záznamová pravidla, musí být při přidání dne aktivní volba Použít pro záznamová pravidla. Aktivací volby Použít pro plány událostí lze výjimku použít též pro statické (nikoliv dynamické) plány událostí.

Pro uložení změn v nastavení výjimek je nutné stisknout tlačítko **POUŽÍT**.

POZNÁMKA

Aplikace nepovolí do seznamu vložit duplicitní výjimku (stejně datum a stejná perioda). Je však možné vložit do seznamu tentýž výjimečný den s roční periodou a bez roční periody. V takovém případě je den bez roční periody chápán jako výjimka z výjimky a bude z hlediska záznamu upřednostněn před použitím dne s nastavenou roční periodou.

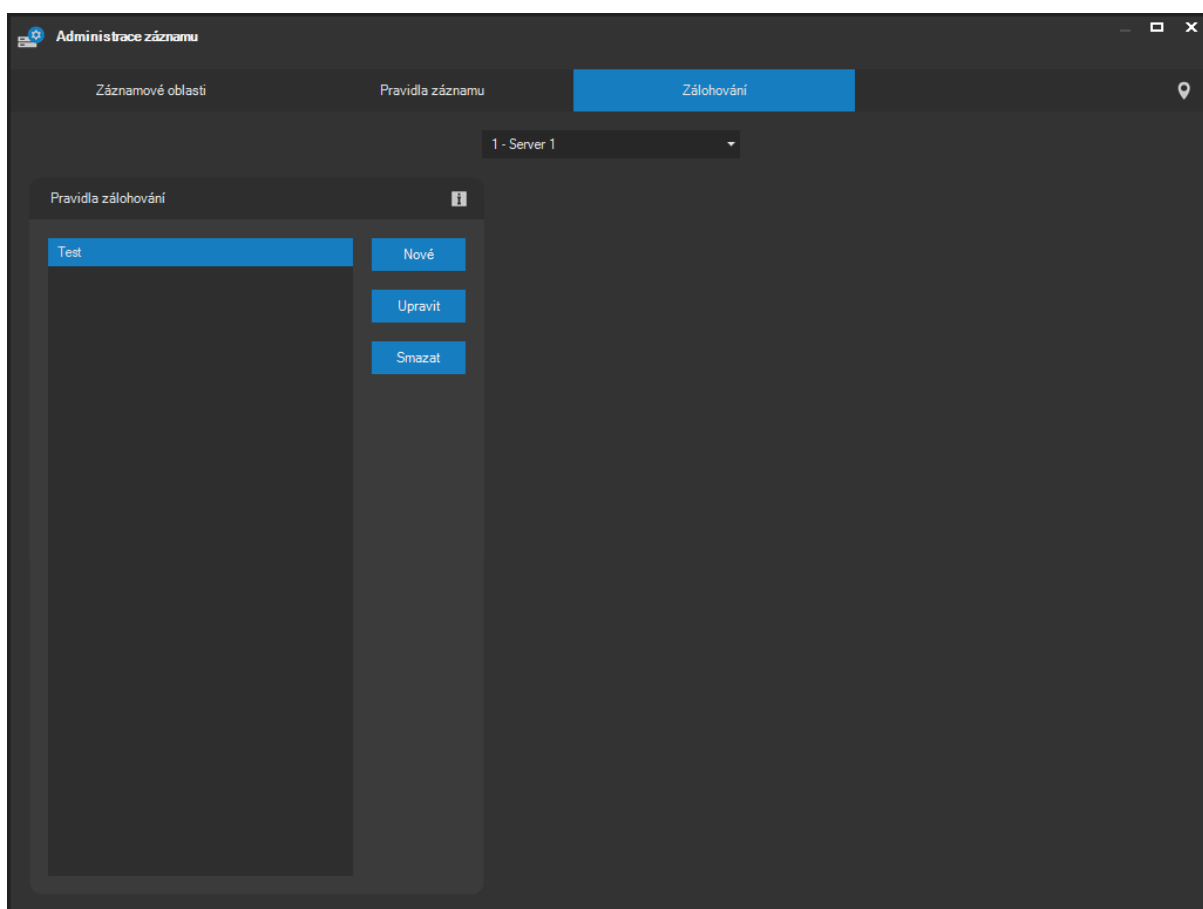
11.6.3. Zálohování

Záznamové oblasti a možnost jejich velmi velké velikosti omezené v podstatě jen použitým hardware umožňují uchovávat data po dlouhou dobu, která je samozřejmě ovlivněna dalším nastavením, zejména nastavením záznamového pravidla pro příslušné kamery. Pokud však vznikne požadavek na tvorbu trvalých záloh uložených mimo záznamové oblasti a pokud mají tyto zálohy být pořizovány pravidelně, a není tudíž ideální je tvořit pomocí klientského nástroje Manažeru stahování, je možné využít přímo nástroj serveru Zálohování.

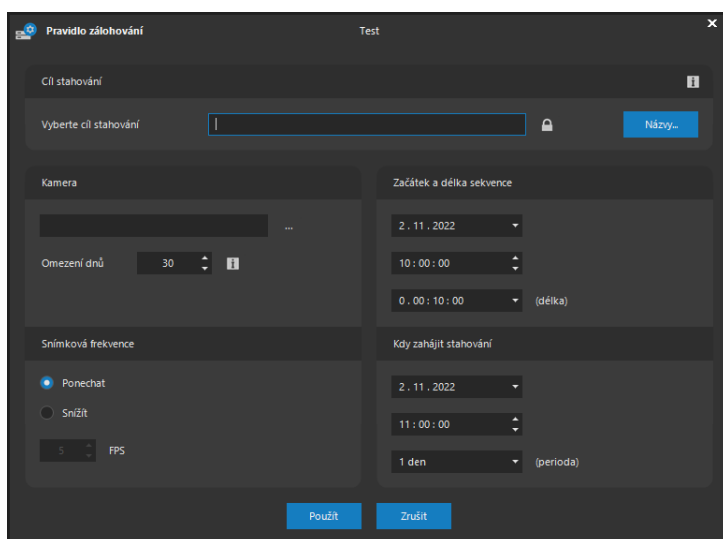
POZNÁMKA

Možnost využití nástroje zálohování je k dispozici až od edice ATEAS Security PROFESSIONAL.

Nástroj Zálohování umožňuje definovat pravidla zálohování, která bude server automaticky a pravidelně uplatňovat a pořizovat tak zálohu dat záznamové oblasti na jiná úložiště. Zálohovaná data jsou ve formátu ATS a umožňují tak maximální zabezpečení pomocí pokročilého AES šifrování. Zálohovaná data jsou v označeném cílovém umístění automaticky přehledně organizována podle serveru, kamer a data. Jednotlivé soubory jsou poté vhodně pojmenovány podle času záznamu. Struktura a konvence názvů souborů je shodná jako v případě stahování dat pomocí klientského nástroje Manažer stahování.



Při vytváření pravidla zálohování pomocí tlačítka **NOVÉ** je po zadání názvu nutné zadat některé základní parametry, jak ukazuje následující obrázek.



V první řadě je nutné doplnit cíl stahování, což je lokální nebo síťové umístění pro zálohovaná data. Umístění tedy lze zadat jako lokální cestu ve tvaru např. e:\backup nebo jako UNC cestu ve tvaru např. \\ext1\backup.

POZNÁMKA

Přestože toto umístění zadáváte z prostředí ATEAS klienta, musí se jednat o cestu, která je platná pro daný kamerový server, na kterém toto pravidlo zálohování vytváříte. To je logické, neboť to bude právě kamerový server, který bude zálohy vytvářet.

POZNÁMKA

Při použití UNC cesty platí zcela shodná zásada jako v případě tvorby záznamové oblasti určené UNC cestou. Služba kamerového serveru nemůže být v takovém případě spuštěna pod účtem Local System, ale musí využít přihlášení administrátora, který má přístup k danému umístění.

Pomocí tlačítka vedle textového pole pro zadání cílového umístění je možné aktivovat pokročilé AES šifrování pro zálohované ATS soubory.

V části Nastavení zálohování - Kamera je možné provést výběr kamer, které budou součástí tohoto pravidla. Dále je nastavit omezení na počet dnů. Toto omezení určuje, že při vytváření nových záloh budou automaticky mazána data starší než udaný počet dnů, aby mohlo být získáno volné místo pro nové zálohy.

POZOR

Pokud nejsou žádné soubory starší než uvedený počet dnů a není k dispozici dostatek volného místa, nebude možné vytvářet nové zálohy.

POZNÁMKA

Pokud je hodnota Omezení dnů nastavena na nula, nebude prováděn výmaz žádných souborů. To je vhodné v případě, kdy jsou zálohy ukládány trvale a dochází např. k výměně zálohovacích médií (připojení jiného externího disku apod.).

V části Začátek a délka sekvence a Kdy zahájit stahování určíme, z jaké doby mají být data zálohována a též kdy se má zálohování spustit. Je tak možné např. naplánovat zálohování na noční hodiny, kdy je očekáváno nižší vytížení sítě apod. Hodnota perioda určuje režim pravidelnosti zálohování. Při nastavení na 1 den tedy bude ve výchozí zadaný čas pro zahájení stahování provedena příslušná záloha z doby, které se též posune o 1 den směrem dopředu.

V části Snímková frekvence můžeme určit, zdali bude při zálohování ponechána nebo snížena snímková frekvence dat v záznamové oblasti. Při snížení snímkové frekvence tedy můžeme zálohovat daný úsek záznamové oblasti s nižším nárokem na volné místo.

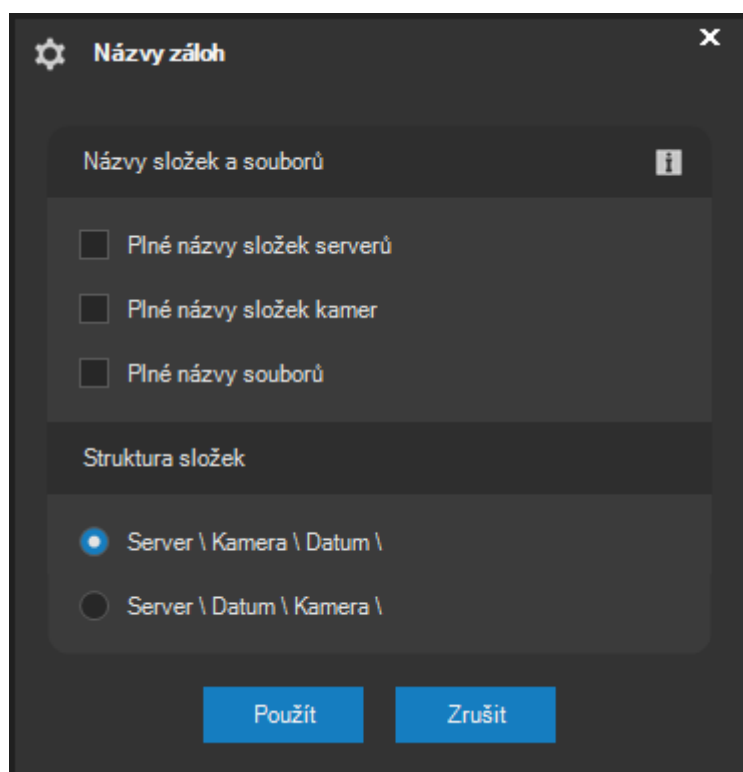
POZNÁMKA

Při použití jiného video formátu než MJPEG je možné snímkovou frekvenci buď ponechat nebo snížit nejméně na frekvenci kompletních snímků (nebo nižší), protože vynechání pouze některých závislých snímků (P snímků) by způsobilo nečitelnost videa.

Pomocí tlačítek **UPRAVIT** a **SMAZAT** je možné vytvořená pravidla zálohování kdykoliv změnit nebo odstranit. Změny nebo odstranění pravidla nemá vliv na dokončení zálohování, pokud v dané chvíli právě probíhá.

Výsledná struktura složek a souborů

Zálohovaná data jsou umístěna do složek podle serverů. Poté mohou být dále rozdělena podle jednotlivých kamer, v rámci kamer pak podle data. Druhou možností je rozdělení nejprve podle data a až pak podle kamer. Způsob rozdělení do složek a také případnou aktivaci dlouhých názvů pro složky a soubory (tj. včetně názvů serverů a kamer) je možné provést v dialogu po stisku tlačítka **NÁZVY**.



11.7. Správa pohledů

11.7.1. Sdílení pohledů

Administrátor systému může sdílet vybrané pohledy či celé skupiny jednoduše tak, že je přetáhne do části Sdílené pohledy v hlavním menu aplikace. Přepnutí menu do stavu editace, tvorba nových a odstranění skupin či přesun a kopírování pohledů v rámci sdílených pohledů probíhají zcela shodně jako při editaci struktury lokálních pohledů, kde jsou tyto postupy popsány.

Změny ve sdílených pohledech se u uživatelů projevují okamžitě. Jejich odstranění se provádí tlačítkem přímo v dohledovém okně stejně jako v případě lokálních pohledů.

POZNÁMKA

Uživatelům jsou automaticky skryty pohledy či celé jejich skupiny, pokud nemají oprávnění k žádné z kamer v nich obsažené. Není tedy potřeba speciálně nastavovat přístup uživatelů k pohledům, jejich nabídka jim je generována zcela automaticky.

11.7.2. Systémové sdílené skupiny pohledů

Některé názvy sdílených skupin pohledů na první úrovni stromové struktury mohou mít systémový význam a mohou tak plnit další rozšíření či speciální funkce. V systému jsou podporovány tyto rezervované názvy pro sdílené skupiny pohledů:

- **Mobile:** Pokud vytvoříte sdílenou skupinu pohledů s tímto názvem, budou klienti na mobilních platformách tyto pohledy nabízet pro zobrazení. Tímto způsobem je možné inteligentně oddělit pohledy pro mobilní dohled od pohledů pro standardní dohled. V současné době jsou podporovány pouze pohledy sestávající ze 4, 9 anebo 16 kamer. Jiné pohledy není možné v této skupině sdílet.

11.7.3. Video stěna

POZNÁMKA

Možnost použití video stěny je dostupná až od edice ATEAS Security PROFESSIONAL.

V ATEASu je možné vzdáleně ovládat monitory připojené k jiným klientským stanicím. Pomocí této možnosti je velmi snadné video stěnu konfigurovat a používat. Princip spočívá v nasazení a instalaci klientských aplikací na stanice, ke kterým je připojeno až osm monitorů, které jsou součástí video stěny nebo je budeme chtít v systému vzdáleně ovládat.

POZNÁMKA

Ovládané monitory samozřejmě nemusí být nutně sestaveny ve video stěnu. Video stěna může být také virtuální s možností ovládat vzdálené monitory na různých pracovištích.

Vytvoření a nasazení video stěny (fyzické či virtuální) probíhá tedy pomocí tohoto postupu. Nejprve vytvoříme speciální uživatelské účty, které budou podřízeny video stěně (viz správa uživatelů). Následně tyto uživatele přihlásíme na jednotlivých podřízených stanicích a určíme počet monitorů. Poté nakonfigurujeme video stěnu (viz další text) a z hlavní nabídky aplikace spustíme okno ovládání video stěny. Ovládání video stěny je popsáno v samostatné subkapitole v kapitole Dohled.

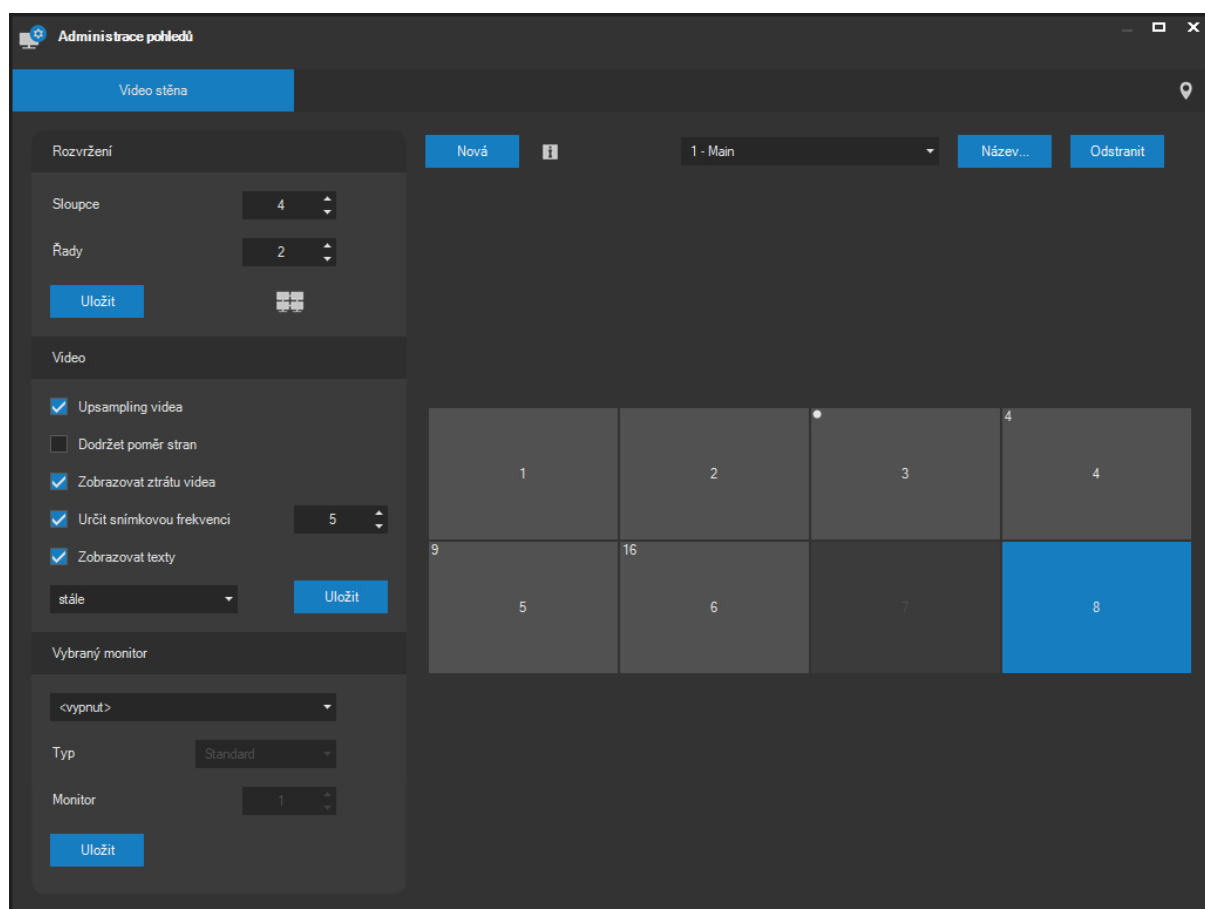
POZOR

Aby byla zajištěna správná interpretace rozložení monitorů připojených k podřízeným video stanicím ve všech možných konfiguracích závislého a nezávislého režimu (span, multiview), je zapotřebí podřízenou video stanici nastavit tak, aby její rozložení monitorů bylo vždy N:1. Při použití například 4 monitorů musí tedy být rozvržení monitorů na stanici 4:1 a nikoliv například 2:2. To samozřejmě není určující pro konečné uspořádání monitorů ve video stěně, které může být libovolné, zde jde pouze o to, aby ATEAS klient mohl na dané stanici vždy korektně detekovat všechny monitory.

Jako podřízené stanice či monitory mohou sloužit jednak libovolné počítače s nainstalovaným plným klientem ATEAS, jednak také televize a displeje vybavené operačním systémem Android, kde se spustí klient ATEAS pro Android. Pro uživatele video stěny není v ovládání externích monitorů žádný rozdíl.

Speciální podřízené účty mají u standardního plného ATEAS klienta některá specifika, která je nutné si uvědomit.

- Po přihlášení jsou do několika vteřin otevřena dohledová okna na příslušném počtu monitorů (obdobně funguje u standardních klientů systému pracovní prostor s nastaveným automatickým startem).
- Hlavní nabídka aplikace je omezená pouze na volbu Konec a Nastavení. Volbu Nastavení lze použít pro vypnutí automatického startování aplikace se startem operačního systému a zamezení automatického přihlášení podřízeného účtu. Jedině tak lze poté přihlásit standardního uživatele na dané stanici.
- Po přihlášení podřízeného účtu jsou automaticky upravena lokální nastavení aplikace ATEAS Observer v části automatického startování. Po přihlášení je automaticky zapnuto startování aplikace se startem operačního systému a dále je aktivováno automatické přihlašování uživatelského účtu. Tím je zajištěn bezobslužný chod stanic a obnovení po restartech systému.
- Podřízený účet video stěny je samozřejmě schopen se při výpadku spojení s administračním serverem systému znovu k serveru připojit a automaticky se znovu přihlásit pod svým účtem. To opět přispívá k automatické obnově fungování video stěny při nejružnějších výpadcích v systému (server, síť).
- Klient video stěny automaticky ukrývá ukazatel myši, pokud není používána.



V systému je dopředu vytvořena jedna video stěna s číslem jedna. Pomocí tlačítek **NOVÁ** a **ODSTRANIT** je však možné přidávat do systému další video stěny nebo je případně odstranit. Již vytvořenou video stěnu lze kdykoliv přejmenovat tlačítkem **NÁZEV**.

POZNÁMKA

Nelze odstranit video stěnu s číslem jedna.

Při konfiguraci video stěny je nejprve rozumné určit její rozvržení. V levé horní části okna jsou k dispozici ovládací prvky pro nastavení počtu sloupců a řádků. Tlačítkem **ULOŽIT** lze nastavení přenést na server, změny se projeví okamžitě na Vaši obrazovce. U všech přihlášených klientů se také automaticky aktualizuje hlavní nabídka aplikace, ve které se buď zobrazí nebo naopak skryje položka Video stěna. Její použití je pak ještě vázáno na oprávnění, které musí mít uživatel nastaveno, aby mohl video stěnu používat.

Maximální počet monitorů ve video stěně (podřízených monitorů) je 192 ve virtuálním rozložení 16 ku 12 monitorům při celkovém počtu 1000 video stěn. Z jednoho standardního klientského pracoviště tak lze ovládat 16 dohledových oken vlastní této stanici a maximálně 192 tisíc podřízených monitorů.

POZNÁMKA

Opět připomínáme, že ačkoliv Vámi nastavené rozvržení video stěny může přesně odpovídat fyzickému rozmístění monitorů, není to podmínkou. V praxi může třeba video stěna s rozvržením 4 x 2 odpovídat dvěma odděleným podřízeným pracovištím se čtyřmi monitory. Stejně tak může být nutné některé monitory při konfiguraci neobsazovat, pokud Vaše video stěna sestává z monitorů různé velikosti.

V levé části okna se dále nachází část Video s možnostmi nastavení videa. Pomocí těchto ovládacích prvků je možné nastavit následující vlastnosti video stěny:

- Upsampling videa – udává, zdali bude automaticky zvětšeno rozlišení videa, pokud je rozlišení obrazovky vyšší než rozlišení videa, implicitně je volba zapnuta.
- Dodržet poměr stran – udává, zdali bude při změně (zvýšení i snížení) rozlišení videa dodržen originální poměr stran, implicitně je volba zapnuta. Pokud je dodržován poměr stran, mohou se na monitorech video stěny objevit buď vertikální nebo horizontální tmavé pruhy kompenzující rozdíl mezi poměry stran videa a monitoru.
- Zobrazovat ztrátu videa - udává, zdali bude ztráta videa indikována viditelným nápisem Není video. Funkce je pro video stěnu implicitně zapnuta.
- Určit snímkovou frekvenci – udává, jaká snímková frekvence bude použita pro zobrazení na video stěně. Implicitně není snímková frekvence omezována.
- Zobrazovat texty – udává, kolik vteřin budou ve videu zobrazeny texty. Textem bude označení kamery (číslo a název kamery, číslo a název serveru) a případně také doplňující text identifikující zdroj události, pokud byla kamera na monitor přepnuta v důsledku události. Z rozbalovacího seznamu lze vybrat počet vteřin pro zobrazování textů (včetně možnosti stálého zobrazení), zrušením zaškrtnutí lze zobrazování textů zakázat. Implicitně je hodnota nastavena na pět vteřin.

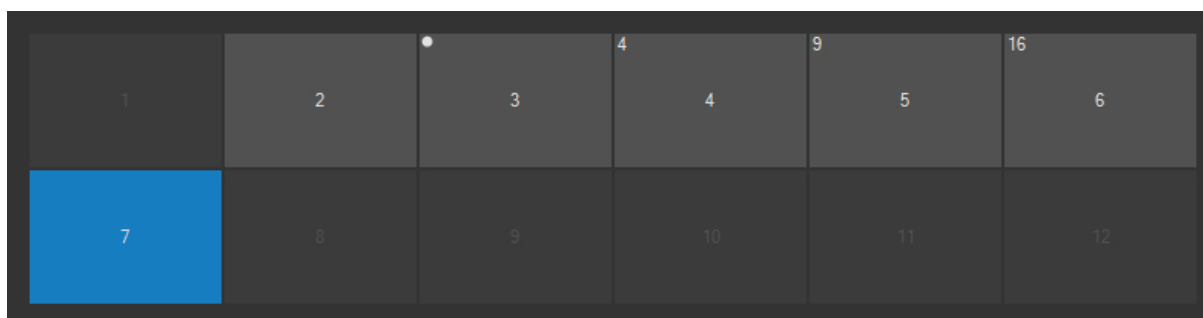
Klíčovou částí konfigurace monitorů video stěny je část Vybraný monitor v levé spodní části okna. Zde je nutné každému monitoru, který budeme chtít v rámci video stěny používat, přiřadit podřízený uživatelský účet a pořadové číslo monitoru z hlediska podřízené klientské stanice (nikoliv pořadové číslo monitoru na video stěně). V rozbalovacím seznamu lze navíc pro daný monitor určit jeho typ, k dispozici jsou následující typy monitorů:

- Standard – běžný monitor, na který může být přepnuta vždy jedna kamera,
- Poplach – jako Standard, navíc bude monitor součástí skupiny monitorů, které automaticky zobrazují poplachové události systému,
- Quad – monitor bude rozdělen do 4 dílčích monitorů, bude tedy možné na něm zobrazovat až 4 kamery.
- Triple - monitor bude rozdělen do 9 dílčích monitorů, bude tedy možné na něm zobrazovat až 9 kamer.
- Šestnáct - monitor bude rozdělen do 16 dílčích monitorů, bude tedy možné na něm zobrazovat až 16 kamer.

POZNÁMKA

Při příjmu události na video stěně se systém pokusí zobrazit všechny kamery, které jsou v událostním scénáři dané události zařazeny s příznakem Zařadit do pohledu. Při příjmu události jsou monitory obsazovány vždy od nejnižšího čísla monitoru ve skupině událostních monitorů s tím, že je proveden automatický posun kamer. Kamery z nově obsazených monitorů při události jsou přepnuty na monitory s vyššími čísly. Poslední kamery ze skupiny událostních monitorů zmizí.

Monitor na video stěně může být buď neaktivní nebo aktivní (přiřazen podřízené stanici) a může být používán oprávněnými uživateli. Aktivní monitory mohou být navíc zařazeny do skupiny událostních monitorů, nebo mohou být typu Quad. Skupina událostních monitorů může být používána stejně jako ostatní aktivní monitory, navíc jsou na nich zobrazovány poplachové události. Všechny stavy jsou indikovány přímo v zobrazení symbolů monitorů ve video stěně. Abyste mohli provádět nastavení jednotlivých monitorů, je nutné vždy nějaký monitor vybrat (výběr je indikován modrým pozadím). Následující obrázek obsahuje monitory těchto typů (zleva): neaktivní monitor, běžný monitor, událostní monitor, Quad monitor, Triple monitor a monitor typu Šestnáct.



POZNÁMKA

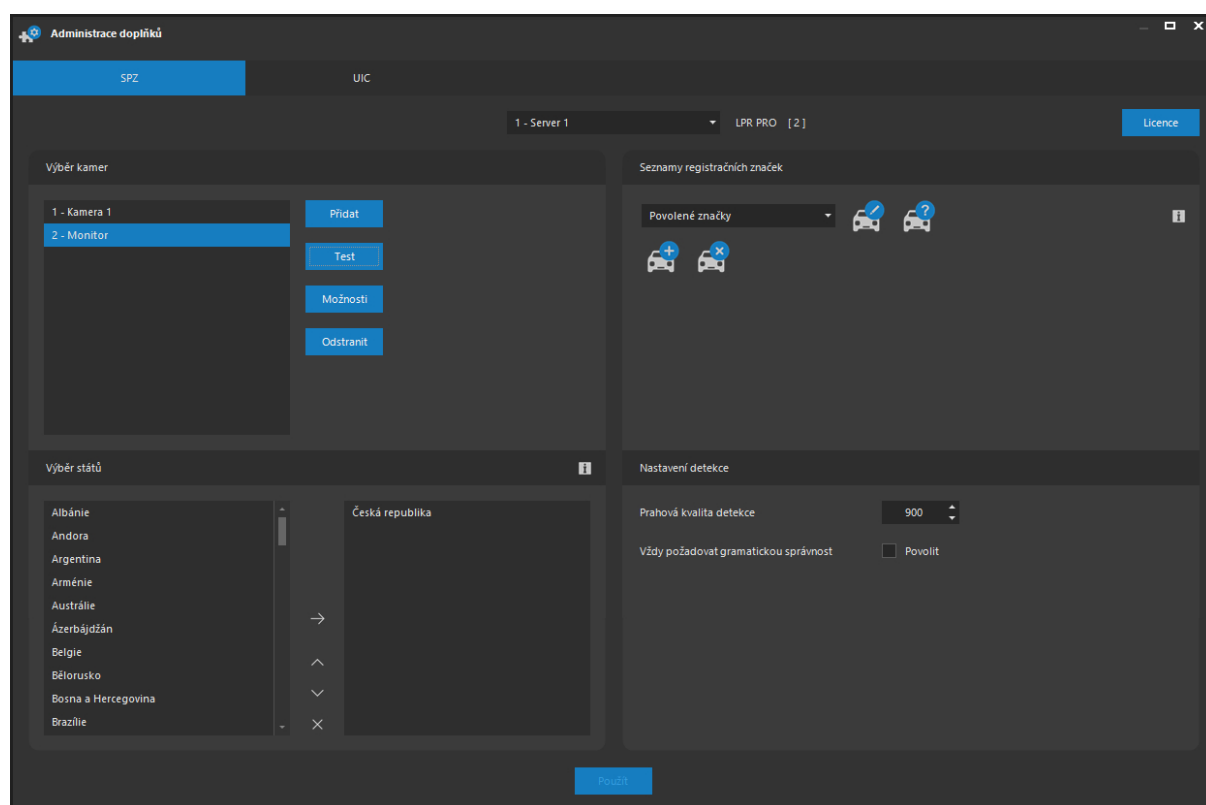
Nastavení video stěny v části Video automaticky mění chování celé video stěny, tedy všech podřízených video dohledových stanic bez nutnosti jakékoliv manipulace s nimi či jejich konfigurace.

Video stěna je vybavena mechanismem automatické obnovy po restartu či výměně libovolného klienta video stěny a také automatickou obnovou po restartu všech serverových komponent systému.

11.8. Správa modulu detekce RZ

11.8.1. Výběr kamer pro detekci

Správa modulu detekce RZ se provádí v části administrace doplňků na kartě SPZ. Po výběru této karty je nutné v rozbalovacím seznamu vybrat kamerový server, na který byl nainstalován modul pro detekci RZ. Pokud vybraný kamerový server tento modul neobsahuje, není aktivovaný ve zkušební verzi nebo na počítači chybí hardwarový klíč, objeví se výstražná zpráva a nebude možné provádět žádná nastavení.



Pomocí tlačítka **PŘIDAT** je možné zobrazit seznam všech dostupných kamer na kamerovém serveru, provést výběr některé z nich a stiskem tlačítka **POUŽÍT** zařadit kameru do seznamu kamer, u kterých bude možné provádět detekci a rozpoznávání RZ. Jeden kamerový server může provádět detekci až pro 64 kamer současně. Odebrání kamery ze seznamu se provede pomocí tlačítka **ODSTRANIT**.

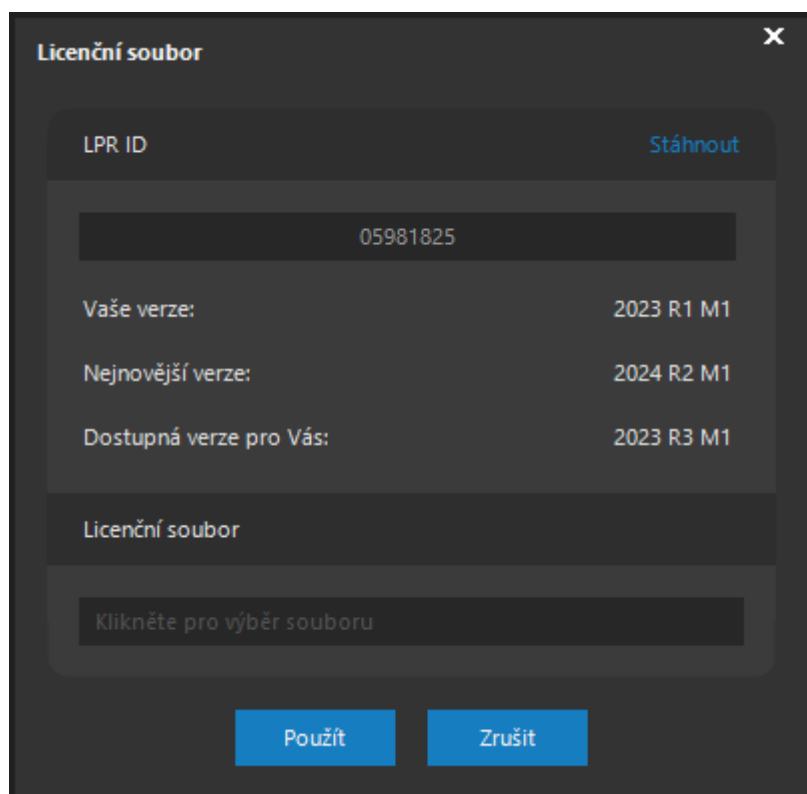
POZNÁMKA

Aktuální licence počtu kamer pro detekci a rozpoznávání RZ se zobrazuje vedle aktuálně vybraného kamerového serveru.

POZOR

Pro CPU neuronové sítě nelze doporučit použití video formátu AV1 kvůli softwarové konverzi barevných modelů vedoucí ke ztrátě výkonu.

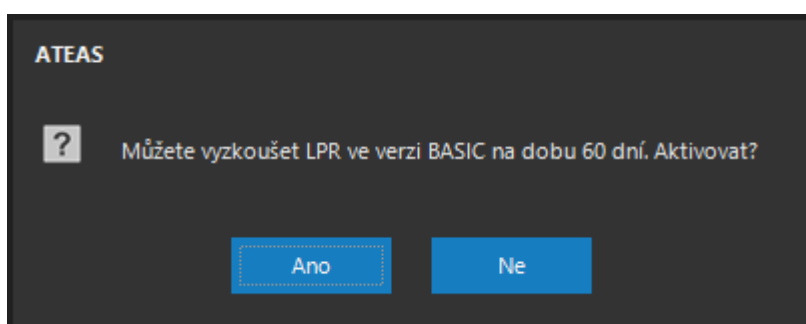
Při rozšíření licence modulu pro rozpoznávání RZ (přechod na vyšší edici anebo rozšíření počtu kamer) je možné tlačítkem **LICENCE** zobrazit dialog pro nahrání nové licence pro vybraný kamerový server.



V horním textovém poli je zobrazeno ID Vašeho hardwarového klíče, které budete potřebovat při rozšíření licence. V části Licenční soubor je možné jednoduchým či dvojitým kliknutím vyvolat dialog pro vložení nového licenčního souboru.

Dialog také zobrazuje důležité informace o verzích doplňku včetně nejvyšší možné verze, kterou lze použít pro dané LPR ID bez objednání upgrade.

Pokud není v systému použit hardwarový klíč, je možné pomocí tlačítka **LICENCE** aktivovat modul pro detekci a rozpoznávání RZ vozidel na dobu 60 dní verzi BASIC pro jednu kameru, a vyzkoušet tak jeho vlastnosti.

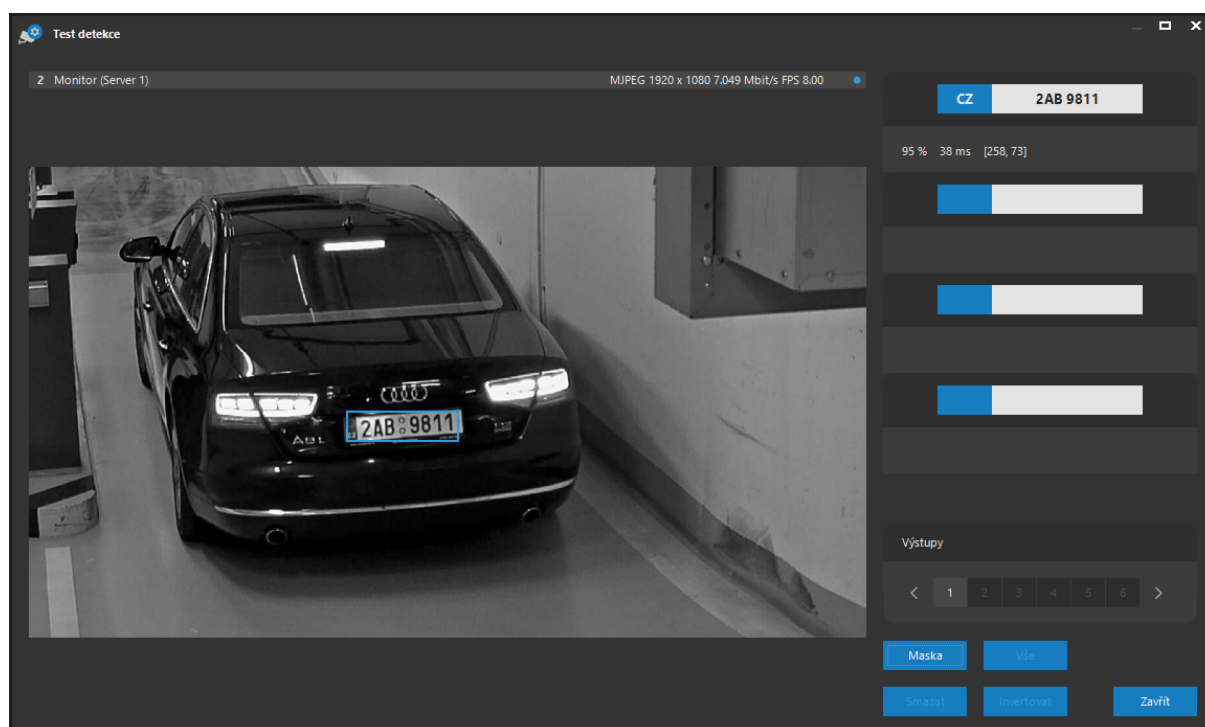


Po aktivaci v režimu zkušební verze bude spolu s licenčními údaji zobrazeno také datum vypršení. Po uplynutí lhůty již na daném kamerovém serveru nebude možné provést opětovnou aktivaci zkušební verze.

POZNÁMKA

Pro aktivaci zkušební verze doplňku je vždy nutné dočasné připojení klienta kamerového systému (nikoliv serveru, kde je doplněk instalován) k internetu.

Tlačítkem **TEST** lze spustit testovací okno detekce.



POZOR

Při spuštění testovacím okně výsledků detekce a rozpoznávání RZ vozidel nejsou její výsledky pro danou kameru předávány serveru k dalšímu zpracování. V průběhu testování a ladění tak nebudou vznikat pro danou kameru události detekce RZ, pokud již byly nastaveny.

Pro jeden video stream dokáže server publikovat až čtyři RZ současně včetně všech jejich dalších atributů jako směr apod. Kromě rozpoznaných RZ jsou dále zobrazeny i tyto údaje:

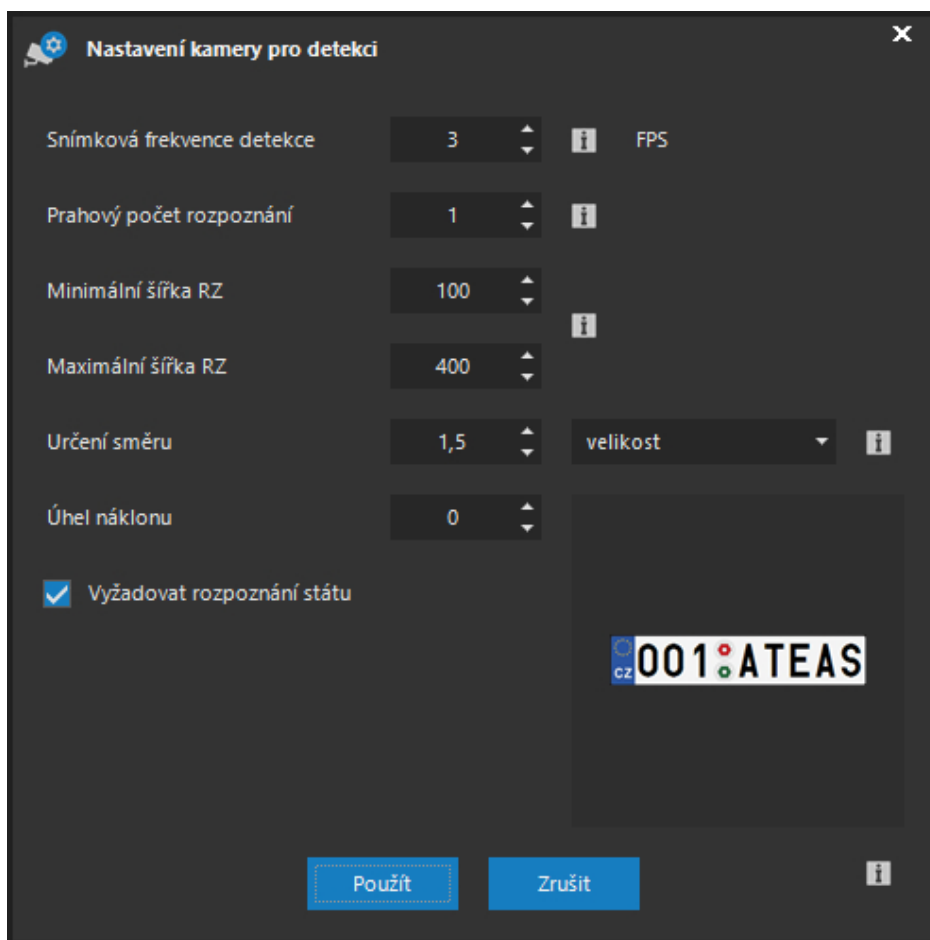
- Kvalita detekce udávající spolehlivost detekované RZ s maximální hodnotou 1. Hodnoty pod 0,9 lze označit za nedostatečně spolehlivé.
- Příslušnost k danému systému RZ (stát či jiná skupina).
- Doba detekce poslední RZ v milisekundách.
- Směr pohybu RZ (indikováno též šipkou vedle RZ), pokud je použit nějaký vyšší prahový počet rozpoznávání, aby mohl být směr určen.
- Přesné hranice obdélníku s detekovanou RZ.

V dialogu je možné také aktivovat výstupy stejným způsobem jako v dohledovém okně.

POZNÁMKA

Tuto funkci může být výhodné použít pro přechod mezi jednotlivými soubory, pokud se jedná o kameru přehrávající složku se soubory.

Pomocí tlačítka **MOŽNOSTI** lze pro vybranou kameru nastavit snímkovou frekvenci, se kterou budou poskytovány snímky pro detekci RZ. Zvýšení FPS vede k rychlejší detekci a rozpoznání poznávací značky (čili je nutné použít i tam, kde vozidlo je v obraze pouze krátkou dobu), znamená ovšem vyšší nároky na výkon serveru (zejména pokud jsou RZ detekovány současně na více kamerách). Snímkovou frekvenci detekce RZ lze nastavit pro každou kameru jinak.



Nastavení kamery pro detekci

Snímková frekvence detekce: 3 FPS

Prahový počet rozpoznání: 1

Minimální šířka RZ: 100

Maximální šířka RZ: 400

Určení směru: 1,5 velikost

Úhel náklonu: 0

☒ Vyžadovat rozpoznání státu

001 ATEAS

Použít Zrušit

POZNÁMKA

Pokud je hodnota snímkové frekvence nastavena na hodnotu nula, bude použita neomezená frekvence.

POZNÁMKA

U formátů jiných než MJPEG bude nutné při snímkové frekvenci detekce vyšší než 2 dekodovat celý video stream. Aktivací využití GPU na serveru lze tento úkol dedikovat na podporovaná GPU.

Parametr prahového počtu rozpoznání RZ udává minimální počet rozpoznání téže RZ před vytvořením události v systému. Tento počet je implicitně nastaven na hodnotu jedna, což znamená, že již po prvním rozpoznání RZ s požadovanou mírou spolehlivosti bude v systému vytvořena událost. Pokud tento parametr zvýšíte např. na hodnotu dva, server vytvoří událost až poté, co úspěšně a nad hranicí požadované spolehlivosti rozpozná RZ ve dvou různých snímcích.

TIP

Parametr prahového počtu rozpoznání je klíčový pro dosažení maximální spolehlivosti čtení a určení směru RZ.

Pomocí nastavení minimální a maximální šířky RZ v obraze je vhodné omezit velikost RZ pro detekci. Tím se lze vyhnout nepotřebným detekcím v pozadí a zrychlit proces detekce. Doporučené hodnoty jsou 30 procent pod a nad očekávanou šířku RZ.

Určení směru lze provést v závislosti na scéně z velikosti RZ anebo z její pozice v obraze.

Při použití velikosti udává hodnota Určení směru minimální nutnou relativní změnu velikosti plochy RZ pro úspěšnou detekci směru (směr ke kameře či od kamery). Aby určení směru fungovalo spolehlivě, musí být správně nastaveny parametry snímkové frekvence, prahového počtu rozpoznání a určení směru, aby docházelo k úspěšným detekcím v celém rozsahu hloubky ostroty kamery.

Při použití pozice udává hodnota Určení směru minimální posun v pixelech, který musí být detekován, aby došlo k určení směru.

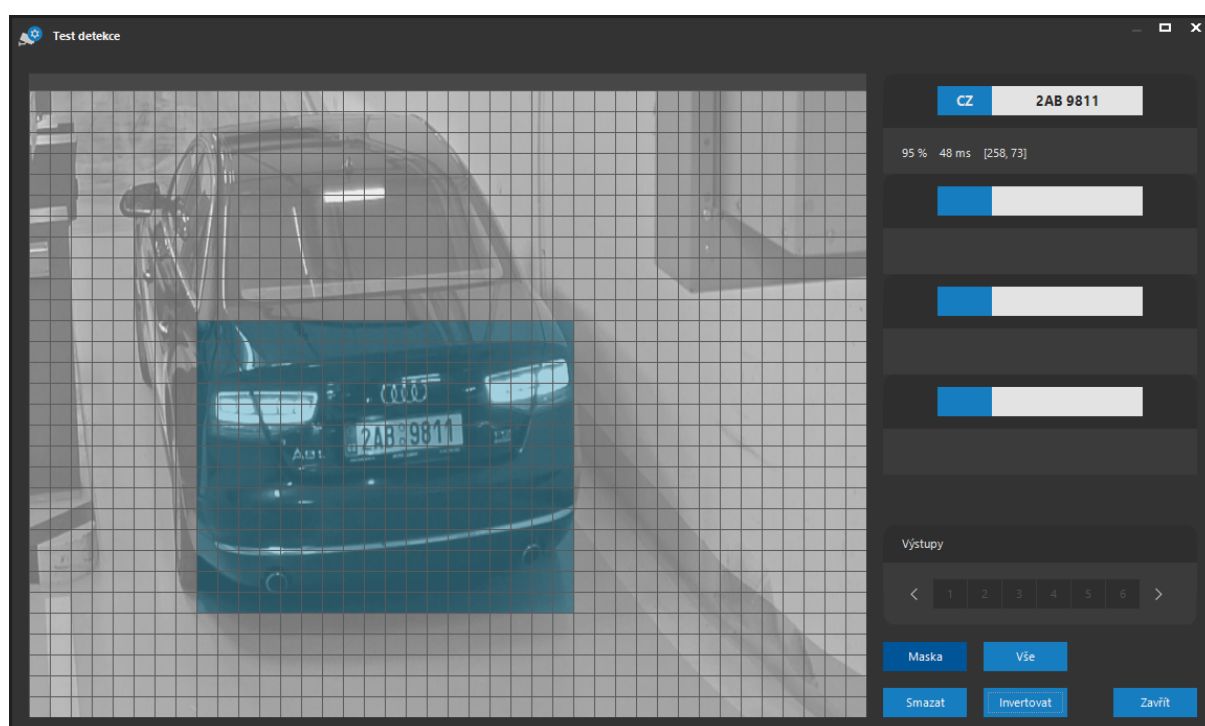
Úhel náklonu by měl odpovídat skutečnému náklonu RZ v obraze tak, aby odchylka činila maximálně 15 stupňů.

Volba Vyžadovat rozpoznání státu určuje, zdali budou publikovány RZ bez zjištěné státní příslušnosti k nějakému z vybraných států.

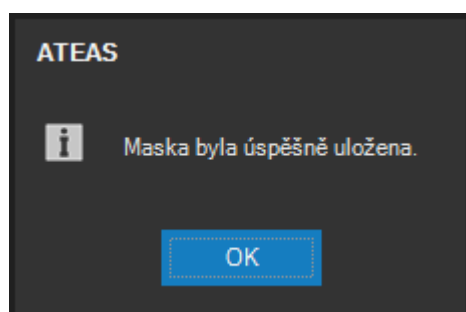
11.8.2. Nastavení masky

V testovacím okně detekce a rozpoznávání RZ vozidel je k dispozici tlačítko **MASKA**, pomocí kterého je možné libovolně vymezit části obrazu, které budou vyjmuty či zahrnuty do detekce přítomnosti RZ v obraze.

Po stisknutí tlačítka dojde k zastavení obrazu a objeví se aktuálně nastavená maska. Pomocí myši lze do masky přidávat části obrazu, které budou do detekce zahrnuty anebo z ní budou vyjmuty. Pro vyjmutí z masky se používá pravé tlačítko myši.



Masku lze v obraze definovat zcela libovolně. Maska může sestávat z libovolného počtu nespojitých oblastí různých tvarů. Masku lze dále upravit pomocí tlačítek **VŠE**, **SMAZAT** a **INVERTOVAT**, které provedou rozšíření masky na celý obraz, její kompletní odstranění nebo inverzi. Uložení masky se provede tak, že uvolníme tlačítko **MASKA**, uložení a okamžité použití masky bude potvrzeno zprávou.



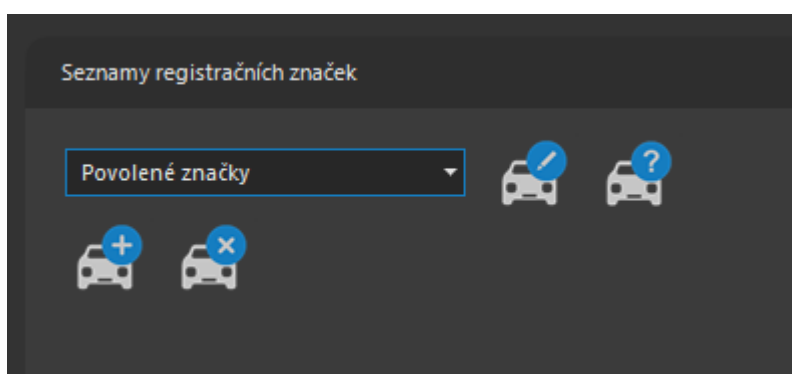
V praxi tak můžeme velmi pružně reagovat na změnu dopravního režimu v místě instalace, na vozidla v částech obrazu, kde nemá být detekce prováděna, či na nové rušící elementy v obraze, které generují chybné detekce anebo ubírají výkon.

POZNÁMKA

Nastavení masky na úrovni detekce může být lepším řešením než nastavení masky na úrovni kamery, neboť vymaskované oblasti zůstávají součástí kamerového záznamu.

11.8.3. Práce se seznamy RZ

Pro rozšíření možností událostního řízení je možné v systému evidovat seznamy RZ. Ty slouží k tomu, aby bylo možné příslušným způsobem reagovat pouze na RZ obsažené v určitém seznamu. Je tedy možné vyhlásit poplach např. pouze pokud je RZ na seznamu zakázaných RZ nebo automaticky zvednout závoru u vjezdu do objektu pouze pro vozidla se značkou registrovanou v seznamu povolených RZ, další reakce je možné přiřadit RZ evidovaným v uživatelských seznamech.

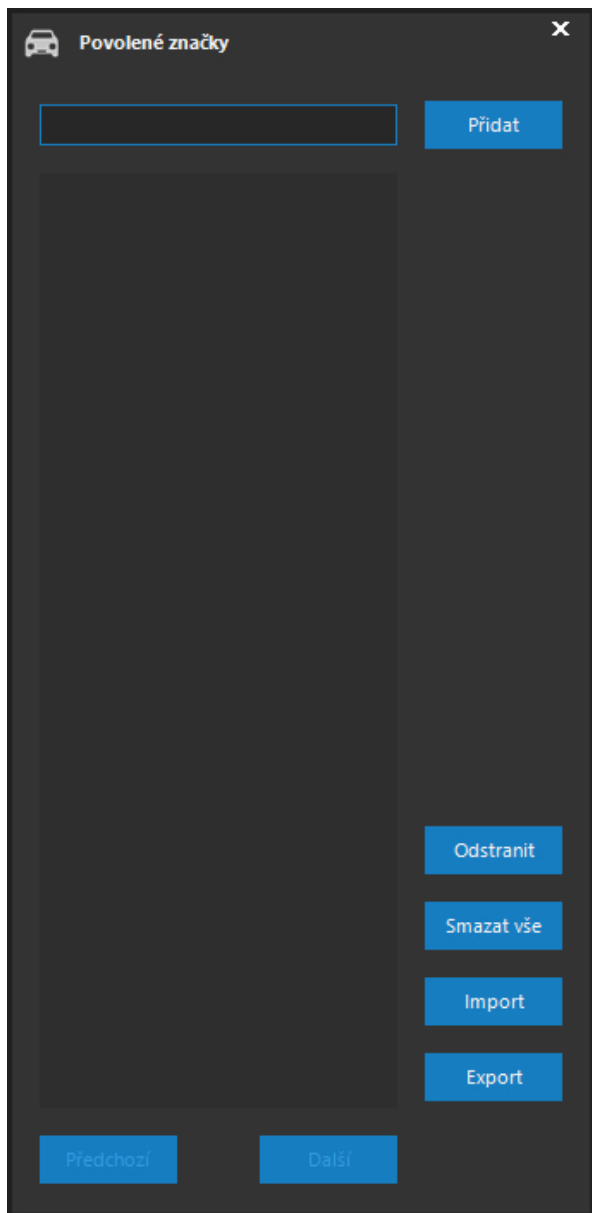


Pomocí tlačítek Přidat seznam a Odebrat seznam lze vytvářet a případně odstranit nové seznamy. Jejich počet není reálně nijak omezen, odstranit nelze předdefinované seznamy RZ jako jsou Povolené značky a další.

TIP

Zdroje událostí pro uživatelské RZ značky umožňují provést výběr libovolného nově přidaného seznamu.

Otevření vybraného seznamu RZ se provede tlačítkem Upravit seznam umístěném vedle vybraného seznamu. V následujícím okně lze pak seznam RZ upravit.

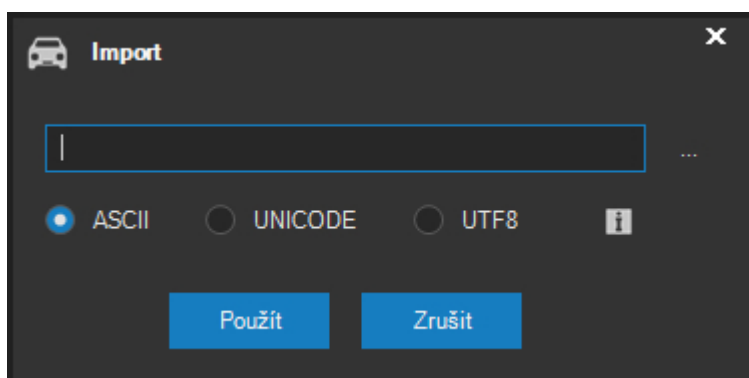


Přidání nové RZ se provede tak, že se запиše do textového pole pod seznamem a stiskne se klávesa ENTER, stejnou funkci má i tlačítko **PŘIDAT**. Po uložení do seznamu se seznam automaticky aktualizuje. Vybranou RZ lze ze seznamu odebrat tlačítkem **ODSTRANIT**, celý seznam je možné smazat pomocí tlačítka **SMAZAT VŠE** (bude vyžadováno potvrzení akce).

POZNÁMKA

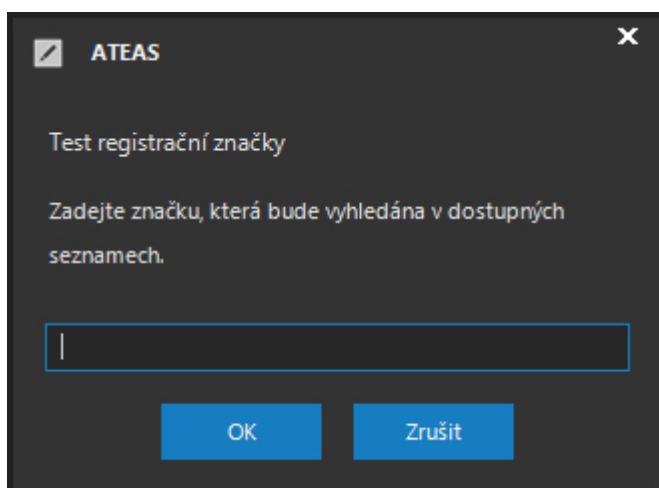
RZ je do seznamu možné zapisovat v dekorativním či normalizovaném tvaru, tj. včetně mezer a pomlček, ale i bez nich.

Pokud je zapotřebí do seznamu přidat více RZ najednou, je možné namísto ručního přidávání použít tlačítko **IMPORT**. V následujícím dialogu je možné vyhledat soubor obsahující seznam RZ a zvolit kódování textu v souboru. Soubor musí být organizován tak, že každý řádek je tvořen právě jednou poznávací značkou. Oddělovač řádku může být jak ve stylu OS Windows (CR + LF) nebo Linux (LF). Pomocí textového výměnného formátu je tak možné převést rozsáhlé seznamy RZ z nejrůznějších databázových systémů.



Pomocí tlačítka **EXPORT** je možné naopak vytvořit textový soubor, který bude obsahovat seznam RZ v právě upravovaném seznamu značek.

Tlačítkem **TEST** lze ověřit konkrétní zadanou RZ, zdali se již nachází v nějakém ze seznamů RZ.



11.8.4. Nastavení rozpoznávání RZ

Nastavení detekce RZ se provádí ve spodní části administračního okna. Pomocí dvou seznamů lze provést konfiguraci systémů RZ, které budou použity při detekci RZ. Tlačítkem šipky mezi oběma seznamy lze vybraný systém RZ přiřadit do seznamu s použitými systémy. V seznamu vybraných systémů RZ (zemí) lze dále měnit pořadí anebo provést odstranění položky ze seznamu.

POZNÁMKA

Národní systémy RZ v sobě mohou obsahovat i další podsystémy (např. různé formy či typy RZ v konkrétním státě).



Pro vytvoření seznamu platí následující pravidla a doporučení:

- Seznam musí obsahovat alespoň jednu položku.
- Přidání určitého systému RZ (určitě země) není nutnou podmínkou pro její správnou detekci a rozpoznání. Je však zárukou vyšší spolehlivosti díky schopnosti ATEAS LPR Engine provádět kontrolu gramatiky.
- Pro dosažení maximálního výkonu je vhodné seřadit seznam od nejčastěji se vyskytujících RZ.
- Vyšší počet položek v seznamu zvyšuje pravděpodobnost, že jsou správně rozpoznány i značky velmi řídky se vyskytující, to vše je ovšem za cenu možného častějšího výskytu chyb u států s podobnými značkami.
- Není doporučeno zařazovat mezi aktivované systémy takové systémy, u nichž nelze předpokládat, že jejich podíl na celkovém počtu dosáhne alespoň půl procenta.

Vedle určení systémů RZ lze nastavovat i další parametry s následujícím významem:

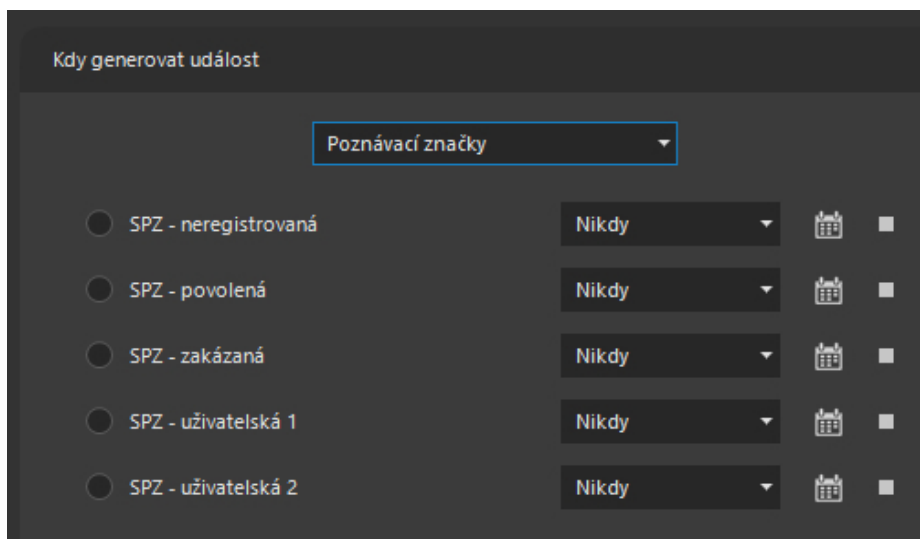
Prahová kvalita detekce: Udává minimální úroveň kvality detekce (spolehlivost), které musí být dosaženo, aby modul detekce RZ poskytl danou značku dále do systému (pro vznik události, poplachu, přímé zaslání klientovi). Nastavení je možné v rozsahu 700 – 999. Čím vyšší je nastavená prahová kvalita detekce a rozpoznání, tím nižší je chybovost. Zároveň s tím se ovšem sníží také

poměr rozpoznaných RZ, neboť některé správně detekované RZ nebudou publikovány z důvodu nepřekročení prahové kvality. Standardní hodnota je 900.

11.8.5. Integrace do systému řízení událostí

Sledování detekovaných RZ vozidel popsané výše spolu s dalšími parametry slouží administrátorům systému k ověření spolehlivosti detekce a rozpoznání RZ v konkrétních podmínkách. Pokud mají však jednotlivé RZ vést ke vzniku událostí či poplachů, je nutné provést nastavení v části administrace událostí.

Jakmile je určitá kamera přidána do seznamu kamer použitých pro detekci RZ, jsou pro ni v části administrace událostí automaticky k dispozici nové událostní zdroje ve skupině Poznávací značky – RZ neregistrovaná, RZ povolená, RZ zakázaná, RZ uživatelská 1, RZ uživatelská 2. Veškerá manipulace s těmito zdroji událostí (časové mapování, tvorba událostních scénářů) je naprosto shodná jako v případě jiných zdrojů (detekce pohybu, poplachové vstupy atd.).



Kdy generovat událost		
	Poznávací značky	
☐ SPZ - neregistrovaná	Nikdy	 ☐
☐ SPZ - povolená	Nikdy	 ☐
☐ SPZ - zakázaná	Nikdy	 ☐
☐ SPZ - uživatelská 1	Nikdy	 ☐
☐ SPZ - uživatelská 2	Nikdy	 ☐

Pomocí tohoto rozdělení je tedy možné definovat rozdílné událostní scénáře pro situace, kdy je detekována povolená RZ, zakázaná RZ nebo například RZ neregistrovaná v žádném seznamu. Je tedy velmi snadné nastavit v systému např. následující chování:

- Pro povolené RZ bude automaticky otevřena závora u vjezdu do areálu (aktivace výstupu).
- Kamera vyvolá poplach, pokud je detekováno zakázané (např. kradené) vozidlo.
- Uživatel může pomocí otočné kamery sledovat vozidla a ověřovat jejich RZ. V řádku událostí (či pomocí odlišné zvukové notifikace pro události a poplachy) je možné online ověřovat např. kradená vozidla.

TIP

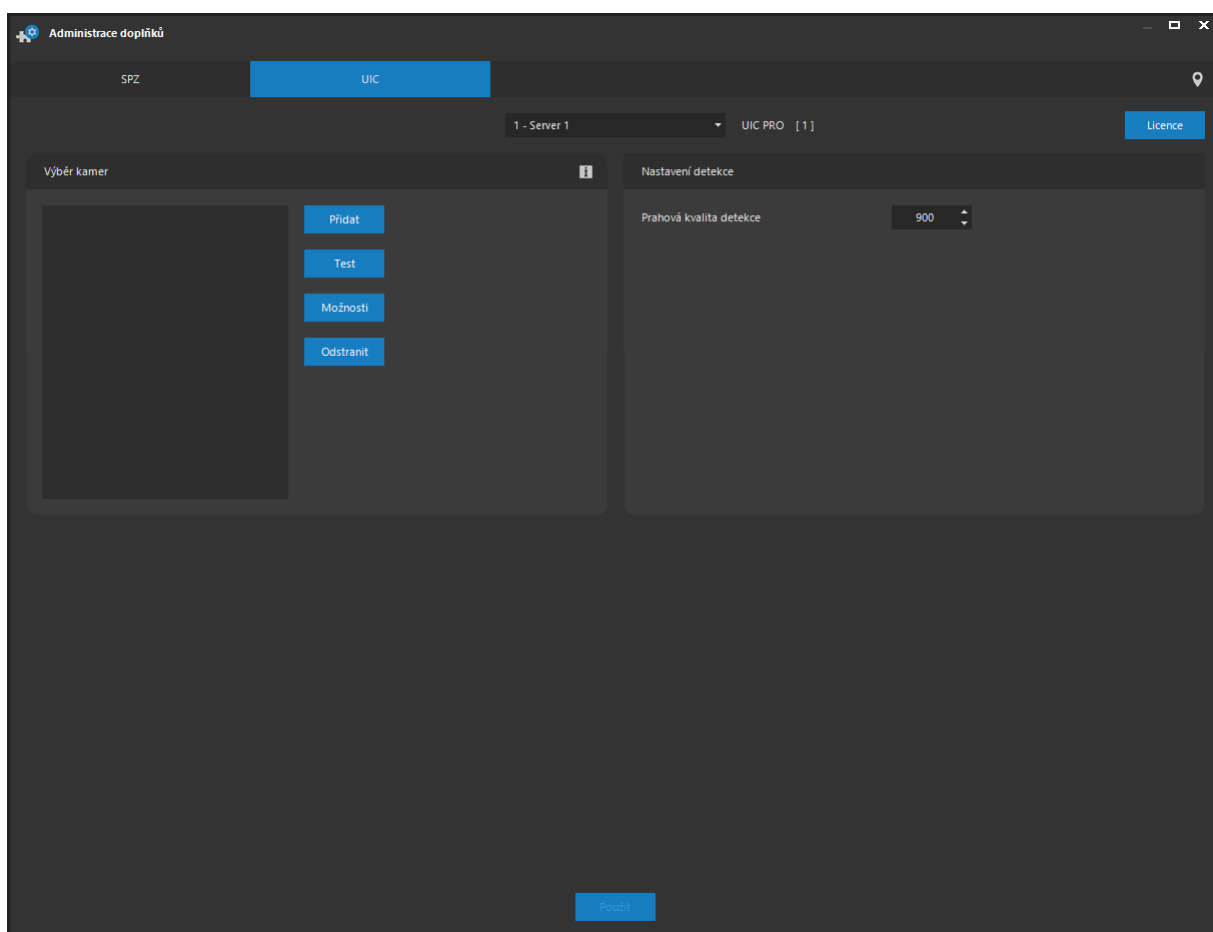
Události je také možné omezit na daný směr RZ, pokud je detekován.

Detekované RZ jsou uloženy v databázi metadat a je možné je cíleně vyhledávat. Při procházení záznamu v části Vyhledávání jsou samozřejmě pro jednotlivé úseky zobrazovány všechny události a poplachy včetně všech událostí a poplachů vzniklých na základě detekce RZ s možností jejich přesného online dohledání v záznamu a možnosti stažení konkrétní sekvence. Pokud však chceme prohledat záznam na určitou konkrétní RZ, není toto časově a událostně orientované vyhledávání ideální. V části záznamu je tak k dispozici karta Meta vyhledávání, kde je možné provádět vyhledávání v záznamu nikoliv podle času, ale podle zadané skupiny metadat, tj. např. podle RZ. Blíže viz kapitola o vyhledávání v záznamu.

11.9. Správa modulu detekce UIC

11.9.1. Výběr kamer pro detekci

Správa modulu detekce UIC se provádí v části administrace doplňků na kartě UIC. Modul detekce UIC musí být nejprve nainstalován a aktivní s příslušným hardwarovým klíčem. Některé principy jsou shodné s modulem detekce RZ.

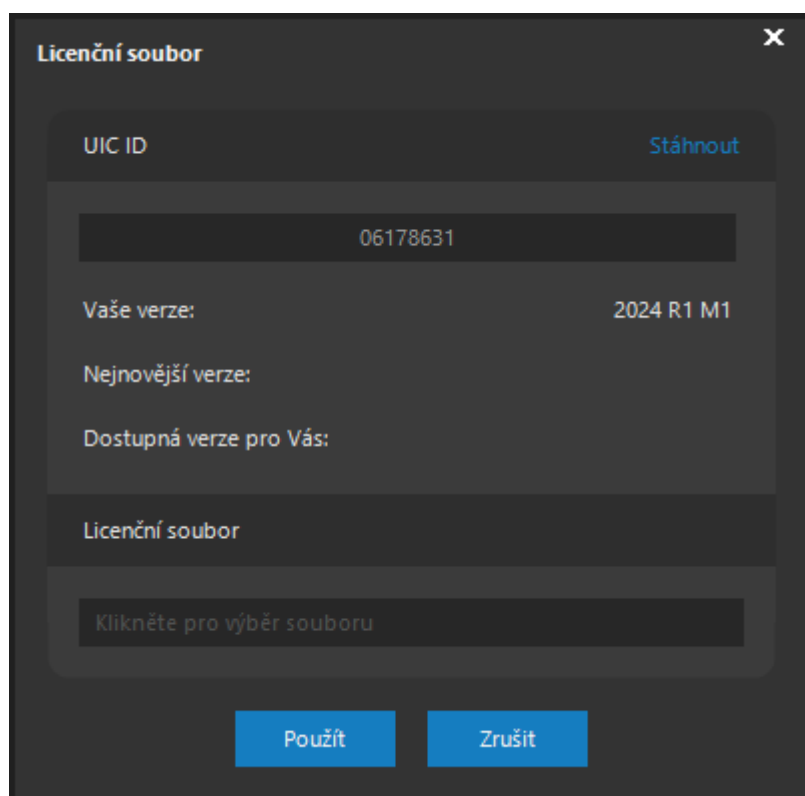


Pomocí tlačítka **PŘIDAT** je možné zobrazit seznam všech dostupných kamer na kamerovém serveru, provést výběr některé z nich a stiskem tlačítka **POUŽÍT** zařadit kameru do seznamu kamer, u kterých bude možné provádět detekci a rozpoznávání RZ. Jeden kamerový server může provádět detekci až pro 64 kamer současně. Odebrání kamery ze seznamu se provede pomocí tlačítka **ODSTRANIT**.

POZNÁMKA

Aktuální licence počtu kamer pro detekci a rozpoznávání UIC se zobrazuje vedle aktuálně vybraného kamerového serveru.

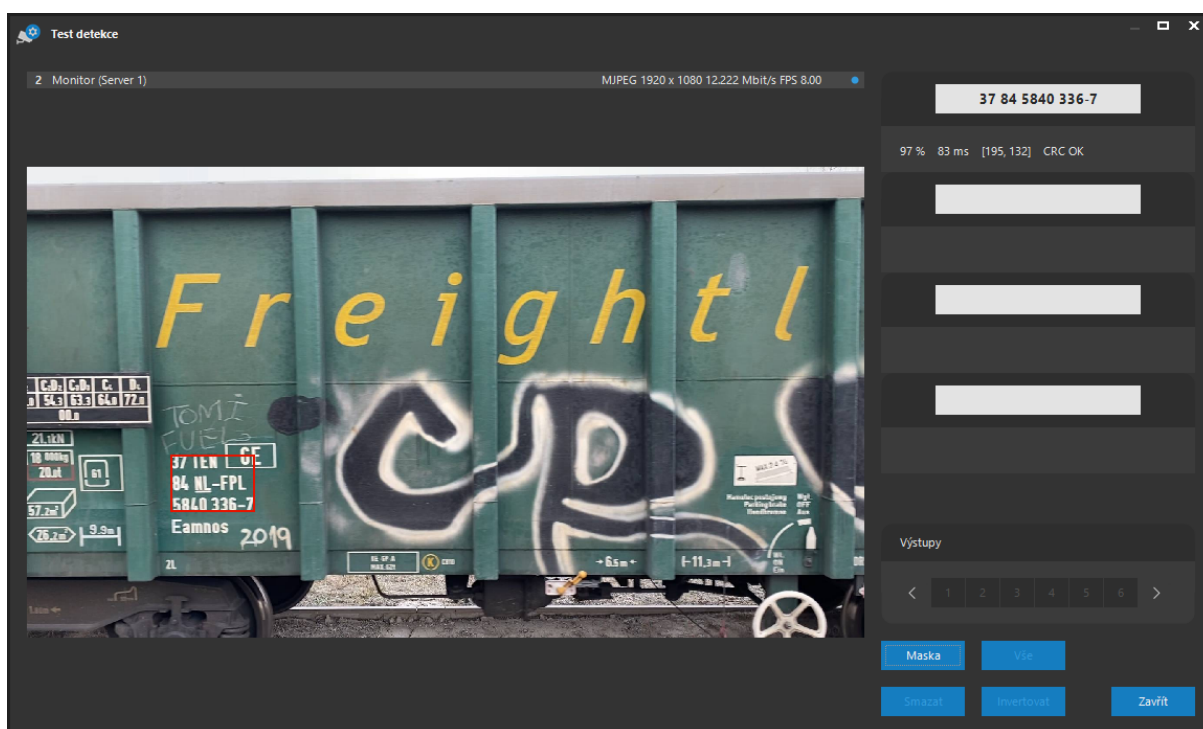
Při rozšíření licence modulu pro rozpoznávání UIC (přechod na vyšší edici anebo rozšíření počtu kamer) je možné tlačítkem **LICENCE** zobrazit dialog pro nahrání nové licence pro vybraný kamerový server.



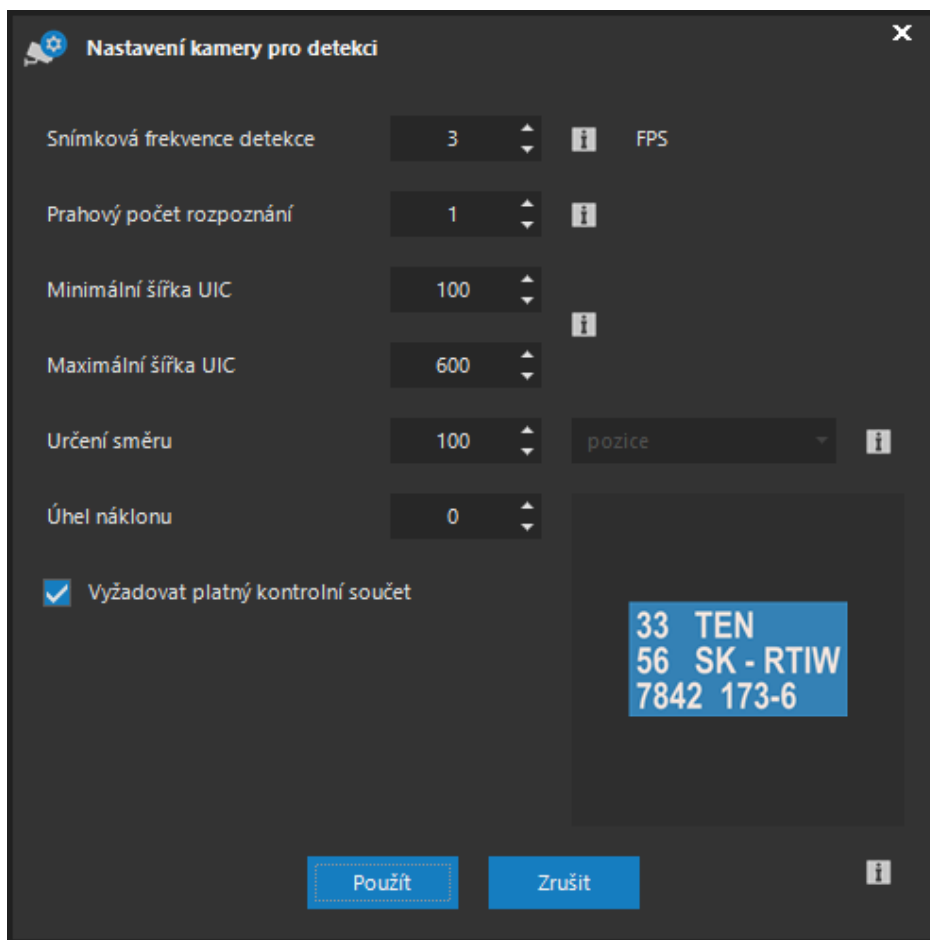
V horním textovém poli je zobrazeno ID Vašeho hardwarového klíče, které budete potřebovat při rozšíření licence. V části Licenční soubor je možné jednoduchým či dvojitém kliknutím vyvolat dialog pro vložení nového licenčního souboru.

Dialog také zobrazuje důležité informace o verzích doplňku včetně nejvyšší možné verze, kterou lze použít pro dané UIC ID bez objednání upgrade.

Tlačítkem **TEST** lze spustit testovací okno detekce.



Zobrazené údaje jsou analogické zobrazení RZ s výjimkou údaje o platnosti kontrolního součtu. To platí i pro nastavení masky tlačítkem **MASKA** a v nastavení detekce pomocí tlačítka **MOŽNOSTI**.



Nastavení kamery pro detekci

Snímková frekvence detekce: 3 FPS

Prahový počet rozpoznání: 1

Minimální šířka UIC: 100

Maximální šířka UIC: 600

Určení směru: 100 pozice

Úhel náklonu: 0

☒ Vyžadovat platný kontrolní součet

33 TEN
56 SK - RTIW
7842 173-6

Použít Zrušit

V případě detekce UIC je použita větší výchozí maximální šířka a určení směru je vztaženo k posunu vpravo či vlevo v pixelech.

Speciálně je pro UIC k dispozici volba Vyžadovat platný kontrolní součet, která určuje, zdali je pro publikaci detekce nutné, aby výsledek splňoval kontrolní součet dle Luhnova algoritmu. Pokud to není vyžadováno, text události a API obsahují v případě neplatného součtu příslušnou informaci.

11.9.2. Integrace do systému řízení událostí

Detekce UIC nemá v systému předdefinované událostní zdroje. Pro událostní využití je tak potřeba vytvořit vlastní událost s kódovým označením UIC a vytvořit příslušné časové plány.

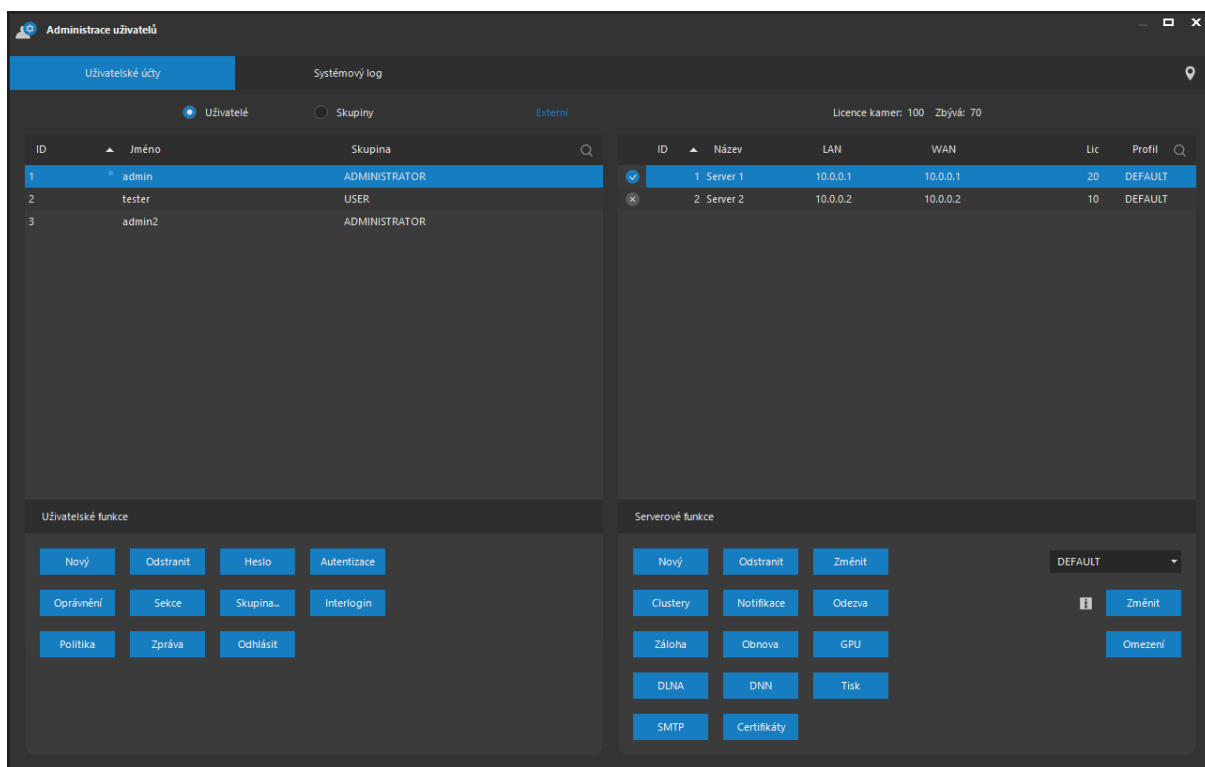
TIP

Události je také možné omezit na daný směr UIC, pokud je detekován.

11.10. Správa uživatelů a serverů

11.10.1. Základní správa serverů

Správa serverů a správa uživatelů se provádí v jedné části, a to v administraci uživatelů. V edici HOME a PROFESSIONAL je možné do systému přidat maximálně jeden kamerový server umístěný nejčastěji na stejném počítači nebo serveru jako administrační server. Edice UNLIMITED umožňuje přidání libovolného počtu kamerových serverů.



The screenshot displays the 'Administrace uživatelů' (User Management) interface. It features two main panels: 'Uživatelské účty' (User Accounts) on the left and 'Serverové funkce' (Server Functions) on the right. The 'Uživatelské účty' panel shows a table of users with columns for ID, Name, and Group. The 'Serverové funkce' panel shows a table of servers with columns for ID, Name, LAN, WAN, License, and Profile. Below these tables are sections for 'Uživatelské funkce' (User Functions) and 'Serverové funkce' (Server Functions), each containing various configuration buttons.

ID	Jméno	Skupina
1	admin	ADMINISTRATOR
2	tester	USER
3	admin2	ADMINISTRATOR

ID	Název	LAN	WAN	Lic	Profil
1	Server 1	10.0.0.1	10.0.0.1	20	DEFAULT
2	Server 2	10.0.0.2	10.0.0.2	10	DEFAULT

Kamerové servery systému jsou součástí seznamu v části Přehled serverů. U každého serveru jsou uvedeny informace o jeho unikátním identifikačním čísle, názvu, IP adrese LAN a WAN, aktuálně přiřazenému maximálnímu počtu kamer a případně též (pokud je současně vybrán uživatel) také profil vybraného uživatele k tomuto serveru. Úvodní symbol na řádce kamerového serveru indikuje, zdali je server aktuálně připojen nebo odpojen. Obnovování stavu serverů v seznamu je automatické.

POZNÁMKA

Klientská aplikace sama automaticky obnovuje spojení ke všem serverům, pokud tato byla ztracena. Při nedostupnosti některého ze serverů tak automaticky dojde k jeho opětovnému připojení, až bude server opět k dispozici. Odpojení od a připojení ke kamerovému serveru se také automaticky zobrazuje uživatelům v dohledovém okně určeném pro příjem událostí.

POZOR

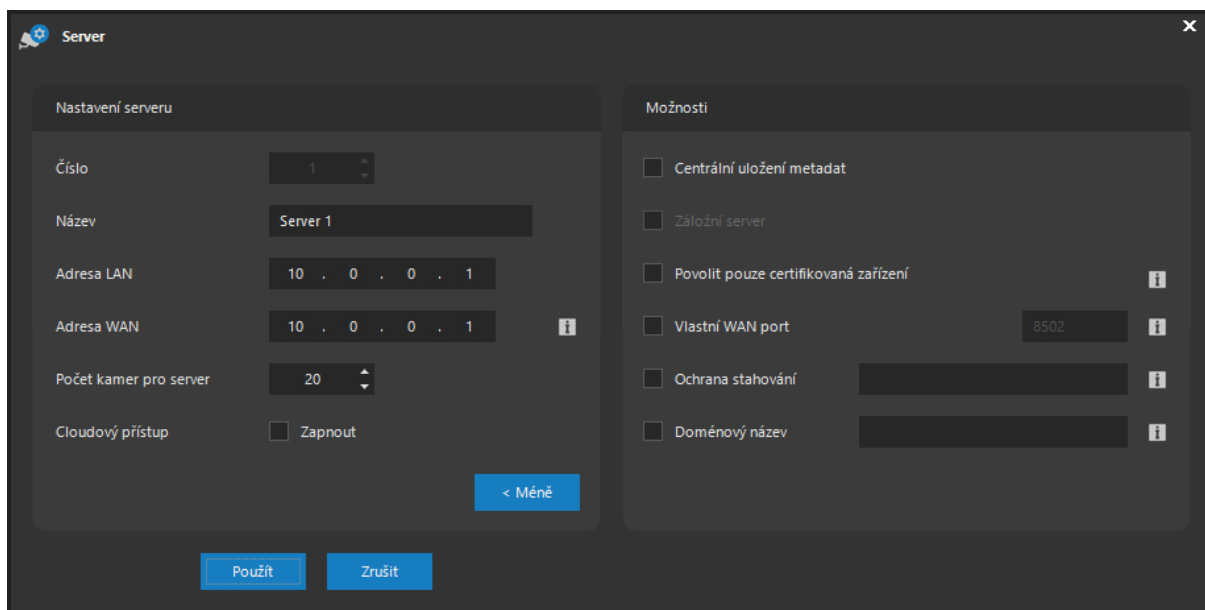
Klientská aplikace však nemůže obnovit spojení k administračnímu serveru (indikováno ve spodní části okna, které obsahuje hlavní nabídku aplikace). Pokud je symbol online spojení změněn na offline, je nutné restartovat aplikaci a znovu se autorizovat.

POZNÁMKA

Nad seznamem serverů je k dispozici souhrnná informace o celkovém počtu licencí kamer a o počtu zbývajících volných licencí, které mohou být použity pro stávající či nové kamerové servery.

Přidávání a odebrání kamerových serverů

Nový server je možné do systému přidat tlačítkem **NOVÝ** v části Serverové funkce. V následujícím dialogu je nutné vyplnit název serveru, jeho IP adresu LAN a WAN (viz níže) a určit maximální počet kamer, které bude server obsluhovat. K serveru nebude možné přidat více než zadaný počet kamer. Tento údaj musí být v souladu s celkovým počtem kamer, který je možné přidat do celého Vašeho systému dle licenčního čísla. Licencovaný počet kamer tedy nesmí být překročen součtem všech počtů kamer přiřazených jednotlivým kamerovým serverům. Při porušení tohoto pravidla bude zobrazena varovná zpráva.



Při otevření tohoto dialogu aplikace navrhne první volné identifikační číslo pro nově přidávaný server. V UNLIMITED edici je možné toto číslo změnit na libovolnou hodnotu, a vhodným způsobem tak seskupovat postupně přidávané servery. Nejvyšší možné identifikační číslo pro server je 999, což je zároveň limit pro celkový počet serverů v systému.

POZNÁMKA

Identifikační číslo serveru je možné měnit pouze v edici UNLIMITED. V ostatních edicích je možné přidat pouze jeden kamerový server s identifikačním číslem 1.

Adresy LAN a WAN je nutné nastavovat s ohledem na konfiguraci sítě a způsoby připojení klientů k systému. Aby se mohl kamerový server úspěšně identifikovat administračnímu serveru, musí se připojit z adres, které jsou zadány v tomto dialogu, v opačném případě není kamerový server identifikován v systému a nemůže zahájit svou činnost.

Adresu LAN je nutné vyplnit vždy, neboť se jedná o primární identifikaci serveru pro připojení uživatelů. Adresa WAN je použita pouze pro uživatele s profilem REMOTE, kteří mohou k danému serveru přistoupit také mimo svou lokální síť.

POZNÁMKA

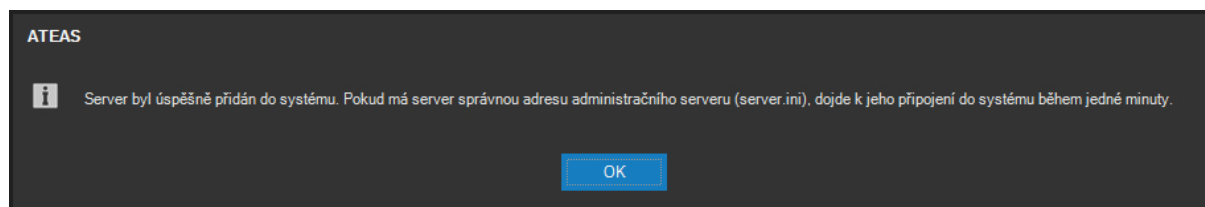
Zadání WAN adresy není v edici HOME a PROFESSIONAL nutné. Pokud uživatel s profilem REMOTE k systému přistupuje vzdáleně, jako WAN adresa kamerového serveru je použita adresa administračního serveru, ke kterému se uživatel přihlašuje. Tím je implicitně podporována konfigurace dynamicky přidělovaných veřejných adres, neboť uživatel se může přihlásit k serveru i zadáním jeho názvu.

Adresu WAN je tak nutné zadat pouze u UNLIMITED edice produktu, a to jen pokud budou uživatelé s profilem REMOTE přistupovat k systému vzdáleně.

POZNÁMKA

Nastavení LAN a WAN adresy nesouvisí s počtem síťových rozhraní (karet) v počítači či serveru. Pro bližší informace viz kapitola o instalaci systému, kde je popsán případ více síťových karet v počítači.

Po úspěšném přidání serveru do systému je opět zobrazena příslušná zpráva.



Pokud je právě přidáný kamerový server již korektně nainstalovaný, dojde po chvíli k automatickému procesu identifikace tohoto kamerového serveru směrem k administračnímu serveru (ATEAS Administrator), což otevře možnost klientského propojení na kamerový server. Automaticky by tak po pár desítkách vteřin mělo být potvrzeno připojení daného kamerového serveru do systému a ke klientovi. Pokud není kamerový server napojen na administrační jádro systému, nebude možné k němu přistupovat, přiřazovat kamery apod.

Odebrat kamerový server je možné tlačítkem **ODSTRANIT**. K odstranění dojde po potvrzení zprávy tlačítkem **ANO**. Úspěšné odebrání serveru bude taktéž potvrzeno zprávou.

Dialog zobrazený při přidávání nového nebo změně existujícího kamerového serveru obsahuje alternující tlačítka **VÍCE** a **MÉNE**, pomocí kterých lze zobrazit případně skryt dodatečné možnosti serverů.

Centrální uložení metadat

Metadata jsou popisná data, která poskytují další informace k uloženým video a audio datům z kamer. Může se jednat např. o informace o detekci pohybu, aktivaci poplachových vstupů, vlastní události kamer doplněné o libovolná dodatečná data nebo o registrační značky vozidel. Tato metadata jsou pořizována jednotlivými kamerovými servery v systému, a proto je při jejich prohledávání vždy nejprve nutné vybrat příslušný kamerový server.

Pokud však chcete mít možnost (např. při větším počtu kamerových serverů) prohledávat metadata centrálně pro všechny servery najednou, můžete pro server aktivovat volbu Centrální uložení metadat. Poté budou metadata tohoto serveru ukládána centrálně na administračním serveru systému.

Záložní servery

Servery je možné vytvořit jako záložní. Záložní servery jsou speciální servery, které mají význam v režimu clusteru. Více informací najdete dále v dokumentaci o clusterech.

POZNÁMKA

Tuto volbu není možné po vytvoření serveru dodatečně měnit.

Záložní servery nejsou dostupné pro přímou správu s několika výjimkami, kterou jsou např. záznamové oblasti, které je třeba záložním serverům nastavit. Ani při nastavení záznamových oblastí však nejsou k dispozici dodatečné volby jako je přiřazování kamer oblastem anebo stáří metadat. Tyto položky jsou již převzaty při zálohování v rámci clusteru. Další výjimkou je základní nastavení detekce a rozpoznávání RZ vozidel (bez přiřazení kamer).

Certifikace zařízení

Aktivací volby Povolit pouze certifikovaná zařízení je možné zapnout verifikaci certifikátů připojených zařízení, pokud jsou přepnuty do režimu https. Aby bylo zařízení vpuštěno do systému, musí se prokázat certifikátem, který je kryptograficky odvozený od certifikátů, které administrátor vložil do systému (jinými slovy, musí být nalezen totožný nebo nadřazený certifikát).

TIP

Lze tedy doporučit import přímo kořenových certifikátů výrobců kamer.

POZOR

Nadřazené či přímo kořenové certifikáty je zároveň nutné importovat i na úrovni operačního systému.

Použití vlastních WAN portů kamerových serverů

Kamerový server funguje na portech, které jsou popsány v příloze dokumentace o konfiguraci sítě. Pokud však nastane situace, že dva či více kamerových serverů má být dostupných přes totožnou WAN adresu, je nutné provést změnu výchozích síťových portů používaných kamerovým serverem. Po aktivaci zaškrtnutí pole Vlastní WAN port, je možné zadat novou hodnotu pro výchozí síťový port.

POZNÁMKA

Tento port nesmí být obsazen jinou aplikací.

POZNÁMKA

Port je vždy použit pouze v kombinaci s WAN adresou serveru, tj. pro uživatele, kteří mají k danému serveru profil REMOTE.

POZNÁMKA

Spolu s výchozím komunikačním portem kamerového serveru jsou posunuty i ostatní porty kamerového serveru o stejnou hodnotu oproti hodnotě výchozí (viz příloha dokumentace o konfiguraci sítě).

Administrační server identifikuje kamerové servery podle jejich IP adres. Pokud však existují dva či více serverů, které se k administračnímu serveru připojují pomocí své WAN adresy (např. se dva kamerové servery v jedné lokální síti velké pobočky připojují přes WAN do centrály k administračnímu serveru), aby je mohl administrační server odlišit a přiřadit jim správnou identifikaci, je nutné v souboru server.ini těchto kamerových serverů vyplnit klíč FORCEDSERVERID, kde se číselná identifikace serveru přímo zapíše.

Ochrana stahování

Uživatelé s přiděleným právem stahování záznamu ze serverů mohou za normálních okolností získat stažený záznam v nezaheslované podobě ve formátu ATS a provést i jeho další export. Pokud chceme uživatelům ponechat možnost stahovat záznam, ale zároveň chceme omezit možnosti nakládání s ním, je možné pro kamerový server definovat automaticky aplikované heslo u volby Ochrana stahování.

Pokud je takové heslo nastaveno, bude stažená data v čitelné podobě moci získat pouze uživatel s přiděleným oprávněním pro export dat mimo systém.

Změna serveru a rozdělení licencovaného počtu kamer

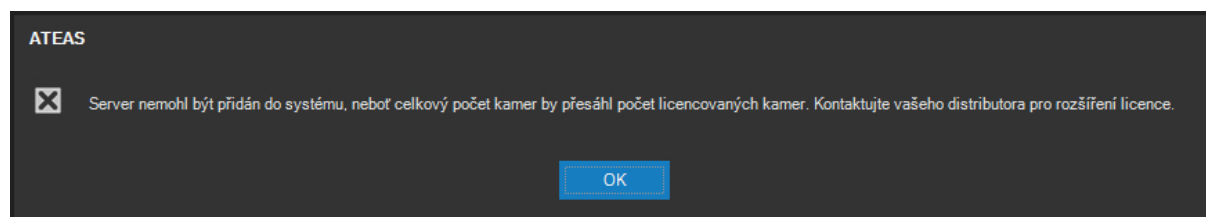
Celkový počet kamer, který může být dle licenčního čísla součástí systému je možné libovolně rozdělovat mezi jednotlivé kamerové servery v systému. U edice HOME a PROFESSIONAL je toto rozdělení nevýznamné, neboť v systému je pouze jeden kamerový server, který bude mít přiřazen maximální počet kamer. U edice UNLIMITED je však možné licencovaný počet rozdělovat mezi jednotlivé servery. Pokud je tedy maximální počet omezen na 40 kamer, mohou být v systému dva servery s 30 a 10 kamerami nebo také 10 serverů po 4 kamerách. Úprava maximální hodnoty připojitelných kamer pro vybraný kamerový server se provádí tlačítkem **ZMĚNIT**. V dialogu, který se objeví, je možné změnit počet kamer. Kromě úpravy počtu kamer pro daný kamerový server je také možné změnit jeho název a obě IP adresy (LAN a WAN).

POZOR

Při snižování počtu kamer by měl být počet připojených kamer k serveru snížen odebráním některých kamer tak, aby jejich počet byl nejvýše rovný nastavované maximální hranici, v opačném případě může za nějakou dobu (nikoliv ihned) dojít k zablokování distribuce videa z kamer.

Pokud není předchozí požadavek naplněn, aplikace bude reagovat varovným podbarvením hodnoty ve sloupci s počtem kamer. Tato situace musí administrátorem následně vyřešena, jinak může dojít k omezení funkcí kamerového serveru.

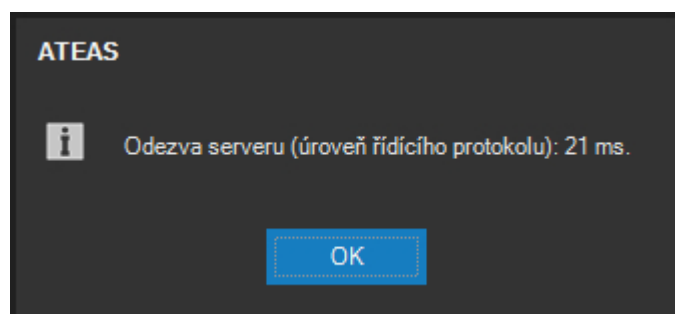
Opět je nutné dbát na dodržení celkového počtu, aplikace vydá varovnou zprávu, pokud by celkový součet kamer na všech serverech měl překročit licencovaný počet.



POZNÁMKA

Při změně kamerového serveru není možné měnit jeho identifikační číslo (sloupec ID).

Pomocí tlačítka **ODEZVA** je možné otestovat odezvu vybraného serveru. Jedná se o odezvu na úrovni řídicího protokolu systému, nelze tedy porovnávat s hodnotami získanými např. pomocí příkazu PING apod. Odezvu aplikace oznámí pomocí informační zprávy.



11.10.2. Cloudový režim připojení kamerového serveru

Platforma ATEAS podporuje speciální cloudový režim připojení kamerových serverů do systému. Pokud je tento režim pro kamerový systém aktivován, může být kamerový server nasazen kdekoliv s přístupem k internetu a bude možné ihned získat plný přístup k serveru včetně videa, zvuku a všech ostatních funkcí.

POZNÁMKA

To platí, i když je server uvnitř lokální sítě, nemá veřejnou adresu, bez přesměrování portů (NAT), se zapnutým firewallem, při dynamických změnách adres apod.

Základní výhodou cloudového režimu připojení je tedy naprostá nezávislost na nastavení sítě, ve které je služba kamerového serveru provozována, předpokládá se pouze dostupnost administračního serveru.

POZNÁMKA

Pro fungování tohoto režimu může být nutné upravit nastavení sítě v prostředí, kde je provozována služba administračního serveru, zejména povolení portu pro cloudový režim. Tyto porty jsou popsány v příloze dokumentace o síťové konfiguraci.

Připojení kamerového serveru v cloudovém režimu se provede jednoduchým postupem:

- V dialogu kamerového serveru aktivujeme položku Cloudový přístup pomocí volby Zapnout.
- Název položky Adresa WAN se automaticky změní na WAN klíč a v příslušném textovém poli bude vytvořen unikátní klíč pro daný kamerový server.
- Vygenerovaný klíč je nutné použít v konfiguračním souboru služby kamerového serveru server.ini (klíč WANKEY), následovat musí restart služby kamerového serveru.

POZNÁMKA

V režimu cloudového připojení kamerového serveru nejsou dostupná anebo účinná některá nastavení kamerového serveru jako je zadání adresy LAN, dostupnost pro offline uživatele nebo zadání vlastního WAN portu.

POZNÁMKA

V režimu cloudového připojení přistupují klienti kamerového systému k datům serveru vždy přes službu administračního serveru, přenosy tedy nemusí respektovat optimální možnou trasu.

11.10.3. Použití doménového názvu pro kamerový server

Při vytváření nového či změně stávajícího serveru je možné přidat serveru doménové jméno. Doménové jméno bude využito např. při přístupu k serverům z webového klienta za účelem zjednodušení nasazení certifikátů v edici UNLIMITED při přístupu přes https. V systému ATEAS platí následující:

- Nezávisle na nastavené WAN adrese kamerového serveru je pro uživatele s profilem REMOTE v edicích s jedním serverem použita pro přístup ke kamerovému serveru adresa zadaná při přihlášení. Tím je automaticky zajištěna podpora pro dynamické DNS názvy Vašeho kamerového systému.
- Při přístupu z webového klienta se klient připojuje jak k administračnímu, tak ke kamerovým serverům. Proto při přístupu přes https musí být instalovány certifikáty na všech serverech systému.
- Z toho vyplývá, že pro jiné než UNLIMITED edice je možné využít shodný certifikát na IP adresu anebo doménový název instalovaný pro obě serverové služby bez nutnosti doménový název kamkoliv zadávat.
- V edici UNLIMITED musí být pro každý server instalován odpovídající certifikát. Pokud je certifikát vystaven na doménový název, pak je nutné tento název zadat v nastavení kamerového serveru.
- Předchozí bod lze obejít aktivací režimu cloud, kdy postačí tentýž certifikát na administračním serveru a kamerových serverech systému, nicméně všechna data v takovém případě budou procházet administračním serverem systému.
- Z uvedeného tedy vyplývá, že zadat doménový název pro kamerový server je nutné pouze pokud uvažujeme edici UNLIMITED, nepoužíváme režim cloud, chceme použít webového klienta přes https a máme certifikáty vystaveny na doménové jméno.

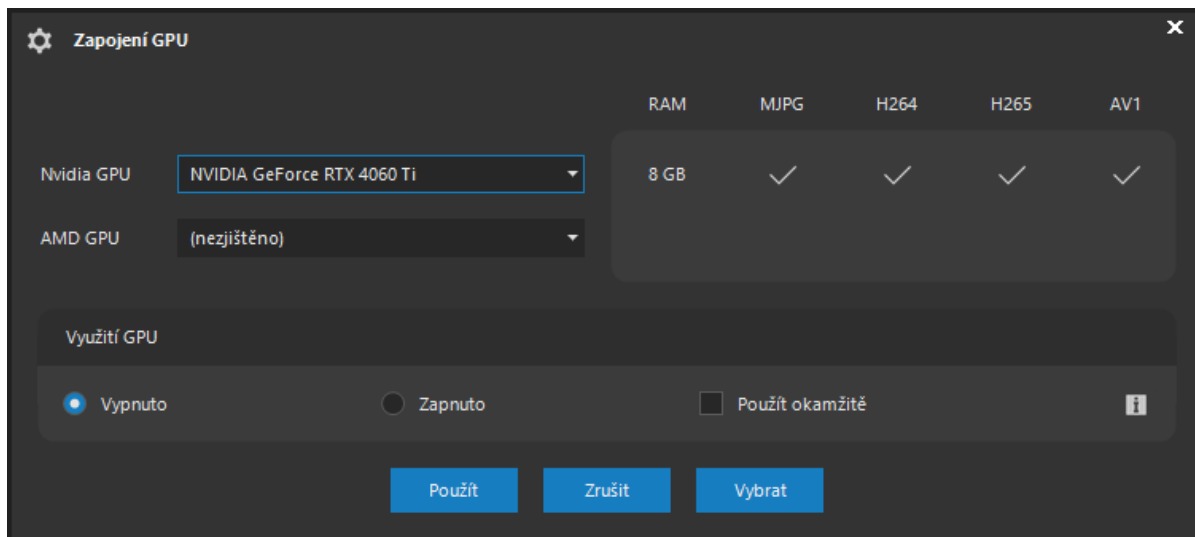
11.10.4. GPU akcelerace ve službě serveru

Stejně jako klientská aplikace může služba ATEAS Server využít GPU akcelerace pro zvýšení výkonu některých operací. Mezi tyto operace patří zejména dekomprese videa ve všech video formátech anebo převody mezi barevnými modely videa. To umožní zvýšení výkonu např. detekce pohybu na serveru, detekce RZ vozidel či video analýzy.

POZNÁMKA

Na rozdíl od klientské aplikace nelze na straně serveru pro akceleraci využít grafické procesory Intel GPU.

Využití GPU akcelerace lze nastavit po stisku tlačítka **GPU** pod seznamem serverů.



Zapojení GPU

	RAM	MJPG	H264	H265	AV1
Nvidia GPU: NVIDIA GeForce RTX 4060 Ti	8 GB	✓	✓	✓	✓
AMD GPU: (nezjištěno)					

Využití GPU

☒ Vypnuto ☐ Zapnuto ☐ Použít okamžitě

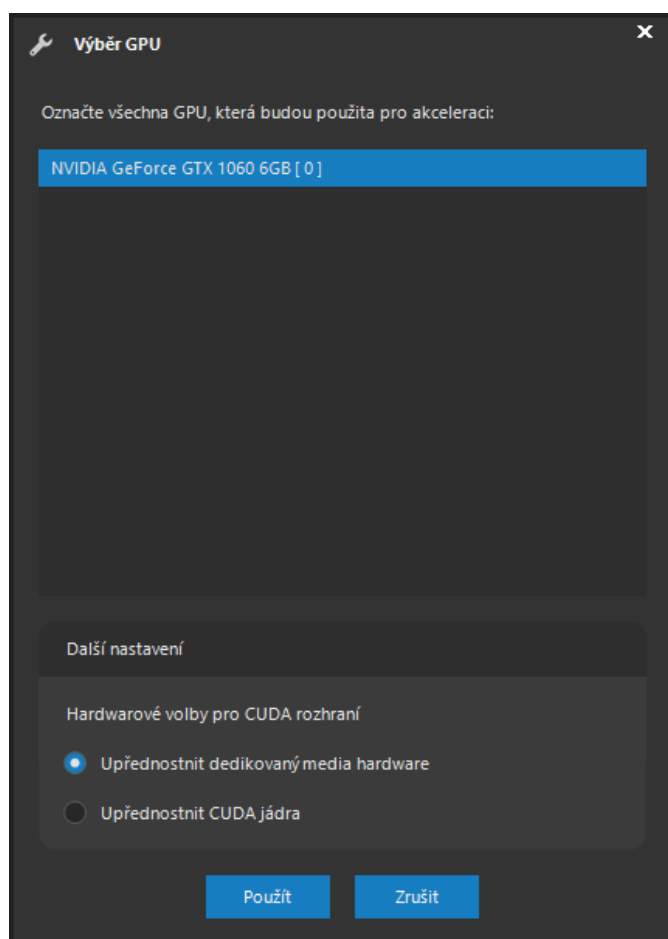
Použít **Zrušit** **Vybrat**

Chceme-li změnu ve využití akcelerace vynutit okamžitě, můžeme aktivovat volbu Použít okamžitě. V takovém případě budou automaticky všechny kamery na serveru odpojeny a znovu připojeny stejně jako při změně jejich nastavení.

Tlačítko **VYBRAT** zobrazí dialog se seznamem všech grafických karet. Ze seznamu je nutné zvolit jednu anebo více grafických karet, které budou použity pro akceleraci videa. Server je tedy schopen využít různé technologie GPU akcelerace a více GPU i v rámci jedné aplikace pro dosažení maximálního výkonu.

POZNÁMKA

Pro rozhraní CUDA je navíc možné i učít některé hardwarové preference, zejména je možné určit, jestli pro akceleraci budou použita CUDA jádra anebo bude využit dedikovaný hardware pro dekompresi videa.



POZNÁMKA

Pokud je na grafické kartě současně spuštěna neuronová síť, GPU akcelerace pro kamery přiřazené této síti bude probíhat nezávisle na Vašem výběru GPU na stejné kartě. To je nutné z důvodu optimalizace pohybu dat přes sběrnice počítače.

11.10.5. Spuštění neuronové sítě na serveru

Kamerový server podporuje spuštění neuronové sítě, pokud je vybaven hardware, který je pro její provoz potřeba. ATEAS používá různé typy především hlubokých konvolučních neuronových sítí vhodných pro analýzu videa. Nastavení lze provést po stisku tlačítka **DNN**.

POZNÁMKA

Možnost spuštění neuronových sítí je dostupná až od edice ATEAS Security PROFESSIONAL.

Nastavení neuronových sítí

	Zařízení	Typ		Rozlišení	Název				
1.	NVIDIA GeForce GTX 1060 6GB [6,0 GB]	SD + FD + FR	...	Střední	DNN	Zapnuto	Vypnuto	Uložit	Test
2.									
3.									
4.									
5.									
6.									
7.									
8.									
9.									
10.									
11.									
12.									
13.									
14.									
15.									
16.									

Zavřít

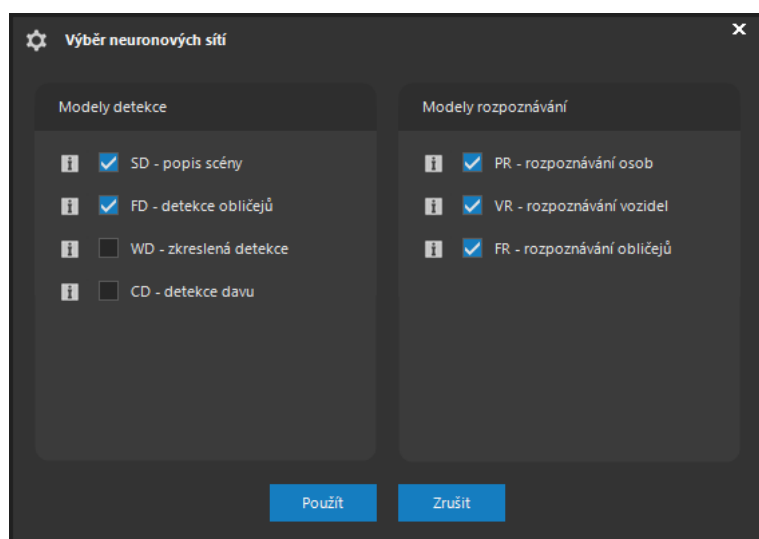
Nastavení neuronové sítě je rozděleno do sloupců s tímto významem:

Zařízení – Udává název zařízení, které bylo zjištěno na serveru a je způsobilé ke spuštění neuronové sítě.

POZNÁMKA

Aktuálně může být neuronová síť spuštěna na libovolném GPU Nvidia s architekturou Pascal a vyšší s minimálně 4 GB grafické paměti. Architektura Volta a vyšší umožňuje významné zvýšení výkonu díky tensor jádrům, které ATEAS umí využít.

Typ – Zde je možné vybrat jeden či více typů neuronové sítě. Výběr je možné provést po zobrazení dialogu výběru typů neuronové sítě.



Mezi podporované modely detekce patří:

- Popis scény. Síť je specializovaná na rozpoznávání osmi typů objektů (osoba, vozidlo, nákladní vozidlo, autobus, kolo, motorka, vlak, loď) s možností určení přítomnosti objektů v zónách, překročení čáry, určení počtu, doby setrvání v zóně apod.
- Detekce obličejů. Síť je specializována na detekci obličejů a umožňuje stejné funkce jako Popis scény.
- Zkreslená detekce: Síť je specializovaná na detekci osob z kamer s 360 stupňovým objektivem (rybí oko).
- Detekce davu: Síť specializovaná na přesný odhad početní velikosti davů. Davem se rozumí takové uskupení lidí, kdy již není možné sítí pro popis scény odlišovat od sebe jednotlivé osoby.

Mezi podporované modely rozpoznávání patří:

- Rozpoznávání osob: Síť je specializována na rozpoznávání konkrétních osob z různých kamer, úhlů pohledu či velikostech.
- Rozpoznávání vozidel: Síť je specializována na rozpoznávání konkrétních vozidel z různých kamer, úhlů pohledu či velikostech.
- Rozpoznávání obličejů. Síť je specializována na rozpoznávání obličejů a přiřazení konkrétním osobám dle databáze obličejů.

Síť Rozpoznávání obličejů je závislá na síti Detekce obličejů, proto nelze rozpoznávání provádět bez současně spuštěné detekce, obráceně však ano. Podobně je síť Rozpoznávání osob či vozidel napojena na výsledky sítě Popis scény a nelze je tedy provozovat samostatně.

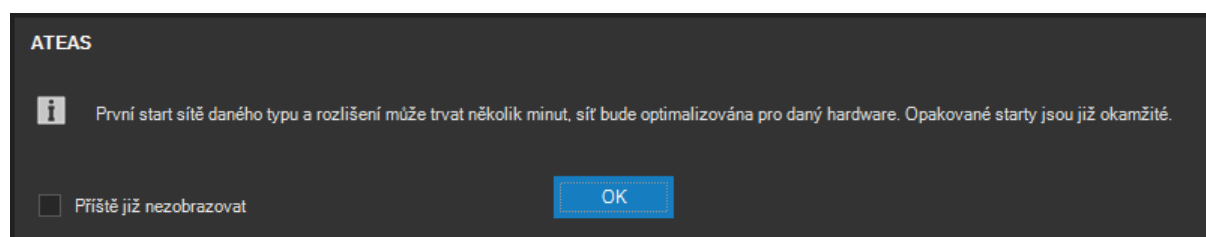
Pro úspěšné rozpoznání obličeje je očekávána velikost obličeje od 100 pixelů na výšku či šířku. Sít se velmi dobře vyrovná s otočením obličeje kolem osy z, otočení kolem osy y a x však redukuje počet zjistitelných markerů a bude snižovat spolehlivost.

Rozlišení – Pro detekci zejména menších objektů je důležitý dostatečný počet pixelů na objekt. Podle konkrétní scény a nároků na analýzu je tak možné zvolit ze tří přednastavených normalizovaných rozlišení pro neuronovou síť.

Název – Udává název sítě, pod kterým ji najdete v nastavení analýzy.

Tlačítka – Pomocí tlačítek **ZAPNUTO** a **VYPNUTO** lze nastavit, zdali bude neuronová síť spuštěna či ukončena. Tlačítkem **ULOŽIT** dojde k uložení všech změn včetně spuštění či ukončení běhu sítě.

Při prvním startu neuronové sítě dané hloubky a rozlišení na každém GPU dojde v první fázi k optimalizaci sítě pro detekci na daném typu GPU dle všech jeho technologických možností, což umožní významně zrychlit vyhodnocování. První start sítě tedy může trvat i několik minut.



Opakované starty sítě v již jednou použité konfiguraci a na GPU, kde již byla síť spuštěna, jsou již okamžité.

Pomocí tlačítka **TEST** lze provést AI test výkonu pro dané GPU.

POZOR

Během testů mohou být omezeny nastavené funkce neuronových sítí.

Před spuštěním testu je možné vybrat typy testů, které budou spuštěny.

 **Test GPU**

Parametry testu 

☒ Systém (několik sekund) ☒ Průchod sítí (asi minuta) ☐ Dekódování na CPU (asi 5 minut) ☐ Dekódování na GPU (asi 10 minut)

Během testu mohou být omezeny funkce serveru.

Výsledky mohou být ovlivněny jinými procesy zatěžujícími CPU nebo GPU.

Dekódovací výkon bude nejpřesněji otestován na serveru bez přidáných kamer.

Dekódovací výkon je testován na plynulém toku videa s 25 FPS.

Zvýšení počtu kamer lze docílit u analýz bez udržení identity objektů či pomocí dodatečných toků videa z kamer.

Použít

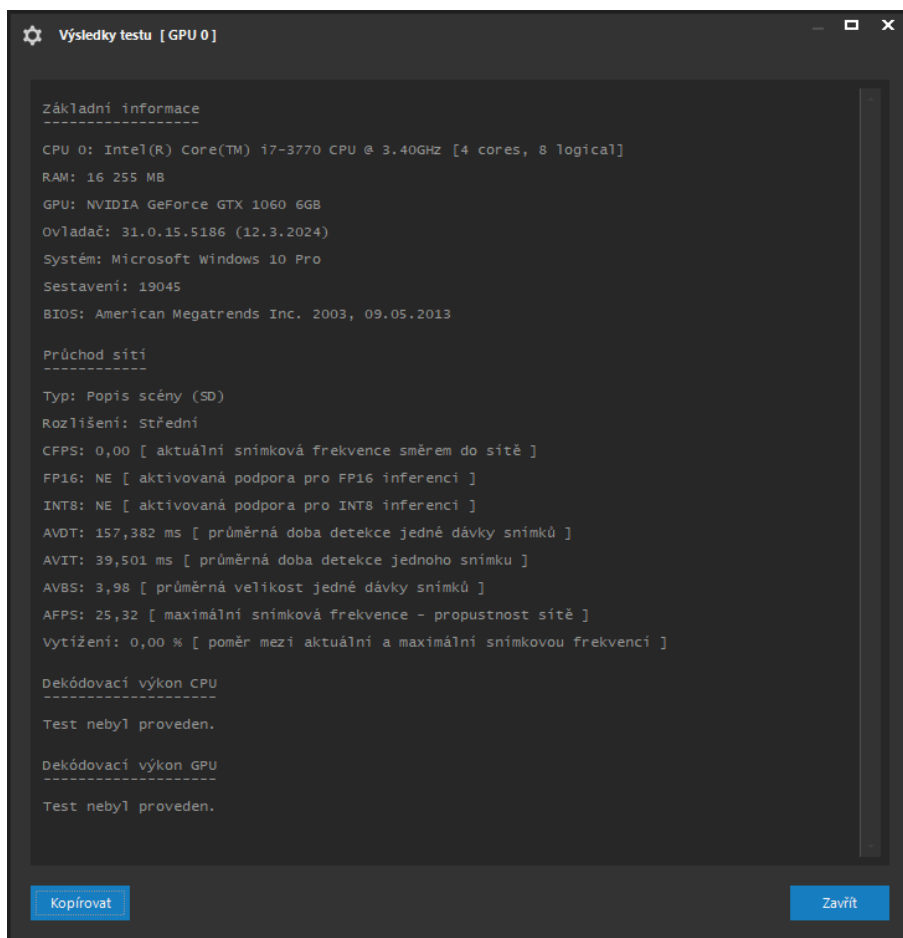
Zrušit

Systémový test vrátí základní informace o operačním systému, hardwarové konfiguraci včetně např. verze ovladačů GPU či verze BIOS.

Test průchodu sítí měří aktuální a maximální možný průchod neuronovou sítí. Pro tento test musí být vybrána vždy jedna nezávislá síť (např. SD či FD) volitelně včetně sítě na ní závislé (PR či FR).

Dekódovací testy CPU či GPU provedou test výkonu dekodování videa pro hlavní video formáty, a zkompletují tak celkovou představu o výkonových nárocích dané konfigurace.

Možný výsledek testu je ukázán zde.



```
Výsledky testu [GPU 0]

Základní informace
-----
CPU 0: Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz [4 cores, 8 logical]
RAM: 16 255 MB
GPU: NVIDIA GeForce GTX 1060 6GB
Ovladač: 31.0.15.5186 (12.3.2024)
Systém: Microsoft Windows 10 Pro
Sestavení: 19045
BIOS: American Megatrends Inc. 2003, 09.05.2013

Průchod sítě
-----
Typ: Popis scény (SD)
Rozlišení: Střední
CFPS: 0,00 [ aktuální snímková frekvence směrem do sítě ]
FP16: NE [ aktivovaná podpora pro FP16 inferenci ]
INT8: NE [ aktivovaná podpora pro INT8 inferenci ]
AVDT: 157,382 ms [ průměrná doba detekce jedné dávky snímků ]
AVIT: 39,501 ms [ průměrná doba detekce jednoho snímku ]
AVBS: 3,98 [ průměrná velikost jedné dávky snímků ]
AFPS: 25,32 [ maximální snímková frekvence - propustnost sítě ]
Vytížení: 0,00 % [ poměr mezi aktuální a maximální snímkovou frekvencí ]

Dekódovací výkon CPU
-----
Test nebyl proveden.

Dekódovací výkon GPU
-----
Test nebyl proveden.

[Kopírovat] [Zavřít]
```

11.10.6. Správa clusterů

Pomocí funkce clusterů je možné v systému zajistit redundanci pro případ výpadku jednoho serveru, který je součástí clusteru.

Součástí clusteru vždy musí být záložní server. Při výpadku jakéhokoliv ze zbylých serverů záložní server plně převeze všechny funkce původního serveru včetně řízení událostí či neuronové sítě. Je možné přidat maximálně jeden záložní server do jednoho clusteru.

POZOR

Aby mohli mít uživatelé přístup ke kamerám i po výpadku kamerového serveru, je nutné, aby měli vytvořen profil na serverech, které jsou součástí clusteru.

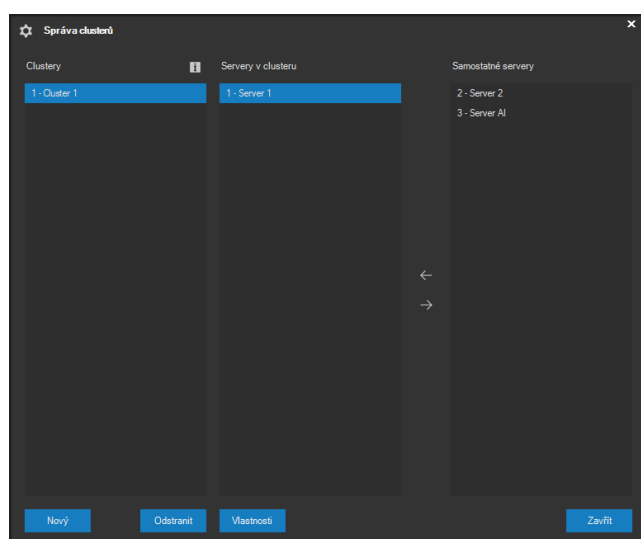
POZNÁMKA

Každý cluster je schopen vyrovnat se s výpadkem nejvýše jednoho serveru v clusteru, dojde-li k selhání druhého serveru, nebudou jeho funkce zálohovány. Jednotlivé servery však mohou selhávat postupně a pokud neselžou ve stejný čas, bude vždy havarovaný server zálohován

Clusters jsou řízené administračním serverem systému. V případě výpadku samotného administračního serveru jsou funkce kamerových serverů zachovány (až na událostní scénáře přesahující jeden server). K dispozici je také funkce offline přihlášení a online dostupnost kamerových serverů při tomto výpadku. Administrační server může být zálohován např. nástroji operačního systému, instalován ve virtuálním prostředí atd.

Vytváření clusterů

Máte-li zakoupenou licenci edice UNLIMITED, můžete po stisku tlačítka **CLUSTERY** vstoupit do části vytváření a nastavení clusterů.



Hlavní část okna tvoří tři seznamy. V levém seznamu jsou k dispozici všechny aktuálně vytvořené clustery. V prostředním seznamu jsou k dispozici kamerové servery náležející k aktuálně vybranému clusteru v levém seznamu. Konečně pravý seznam obsahuje kamerové servery, které aktuálně nejsou součástí žádného clusteru.

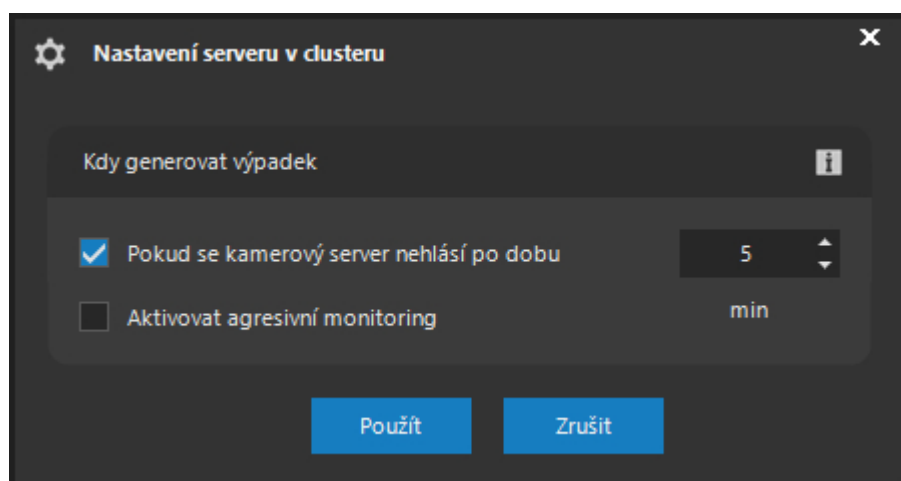
Pomocí tlačítka **NOVÝ** lze po zadání názvu vytvořit nový cluster. Existující cluster lze odstranit pomocí tlačítka **ODSTRANIT**, v tomto případě budou všechny kamerové servery, které jsou součástí clusteru přeřazeny opět mezi samostatné servery bez příslušnosti ke clusteru.

Mezi seznamy Servery v clusteru a Samostatné servery jsou umístěna dvě tlačítka se symboly bílých šipek. Pomocí těchto tlačítek lze vždy daným směrem přesouvat vybrané kamerové servery mezi těmito seznamy. Lze tak přiřazovat clusterům jednotlivé kamerové servery nebo je opět odebrat a následně například opět přiřadit jinému clusteru.

Poslední možností v okně je tlačítko **VLASTNOSTI**, které je dostupné pro vybraný kamerový server, který již je součástí nějakého clusteru.

POZNÁMKA

Tato volba není dostupná pro záložní servery, jejichž výpadek sám o sobě není zálohován.



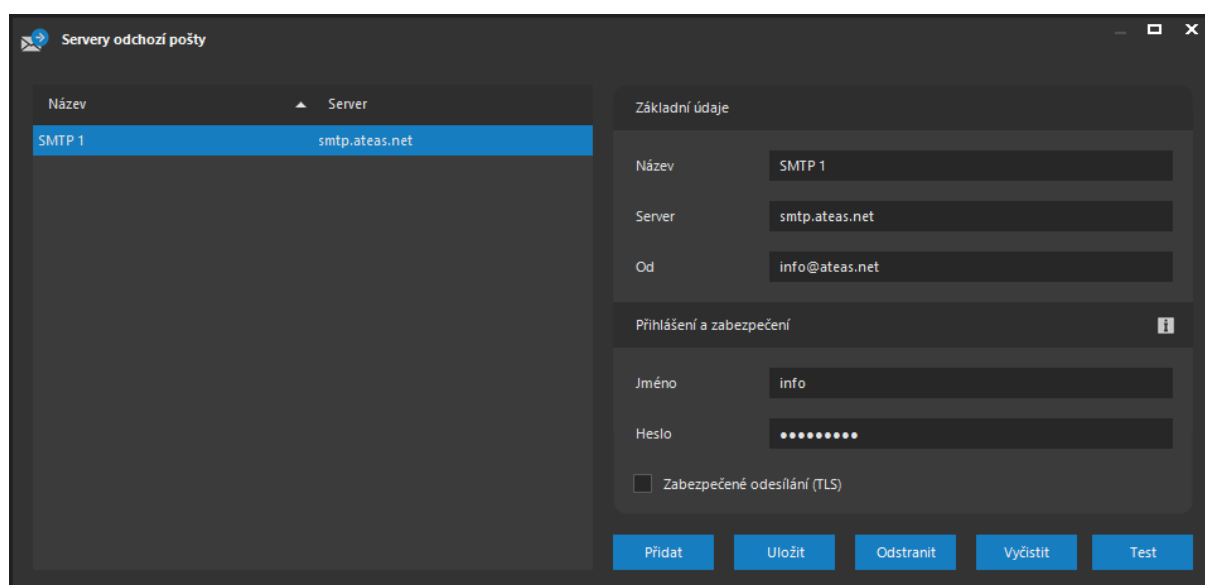
V tomto dialogu je možné nastavit rozhodnou dobu pro vyhlášení výpadku serveru v případě, že se server nehlásí administračnímu serveru systému. Ve výchozím nastavení se interval určuje v minutách, při aktivaci agresivního monitoringu ho však lze v kritických systémech snížit až na 5 vteřin.

POZOR

Při aktivním agresivním monitoringu tak může k zálohování serveru dojít i při velmi krátkých výpadech sítě, proto by měl být aktivován zejména v prostředí stabilně fungujících lokálních sítí.

11.10.7. SMTP účty

Pomocí tlačítka **SMTP** je možné otevřít seznam všech účtů serverů odchozí pošty, které jsou používány v nejrůznějších případech, jako je např. zasílání informací o událostech včetně obrazových příloh, odesílání systémových notifikací nebo automatické zasílání grafů a statistik metadat v systému.



Pomocí tlačítek **PŘIDAT**, **ULOŽIT** a **ODSTRANIT** je možné provádět základní správu e-mailových účtů. Tlačítkem **VYČISTIT** lze rychle vyprázdnit všechna textová pole. Tlačítko **TEST** slouží pro zaslání testovacího e-mailu pro aktuálně vybraný účet.

V sekci Základní údaje je nutné vyplnit název a adresu SMTP serveru a také adresu Od. Část přihlášení a zabezpečení poté obsahuje možnost SMTP autentizace a zabezpečení odesílání pomocí protokolu TLS.

POZNÁMKA

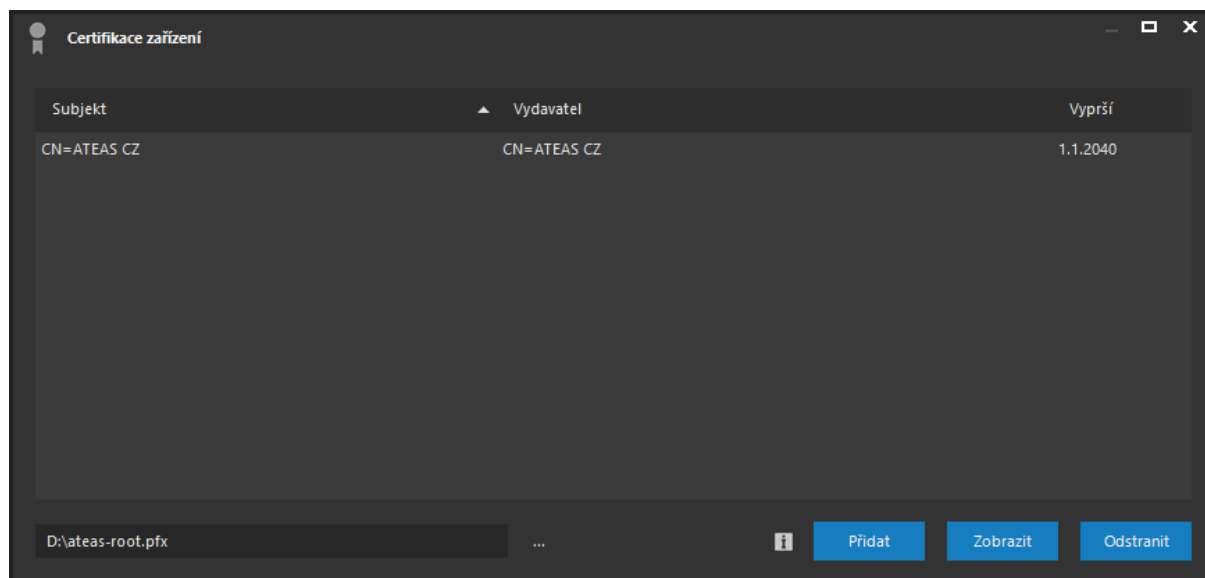
Pro šifrované odesílání je používán protokol SMTP a STARTTLS schéma s implicitním portem 587. Jiná používaná varianta SMTPS s portem 465 vykazuje shodnou úroveň zabezpečení pomocí TLS.

11.10.8. Certifikace zařízení

Administrátor může pomocí tlačítka **CERTIFIKÁTY** do systému přidávat certifikáty, které mohou sloužit k ověření zařízení připojených ke kamerovým serverům systému.

POZNÁMKA

Možnost použití a ověřování certifikátů je dostupná až od edice ATEAS Security PROFESSIONAL.



Pomocí tlačítka **PŘIDAT** lze nahrát certifikát, jehož cestu je nutné zadat v poli Cesta k certifikátu. Podporovány jsou všechny hlavní formáty pro uložení certifikátů včetně formátu cer, crt, pfx nebo p12.

POZNÁMKA

Některé formáty mohou vyžadovat heslo pro otevření souboru, to je možné nastavit v poli Heslo pro otevření.

Tlačítkem **ZOBRAZIT** lze otevřít okno s podrobnostmi o vybraném certifikátu, tlačítkem **ODSTRANIT** je možné provést jeho odebrání. Certifikát pochopitelně nemusí obsahovat soukromý klíč, ale pouze veřejný klíč nutný pro ověření.

Certifikáty mohou být použity na úrovni jednotlivých kamerových serverů i na úrovni jednotlivých kamer a představují ideální řešení pro certifikaci videa a dalšího souvisejícího obsahu. Více také v dialogu změny serveru a nastavení kamer.

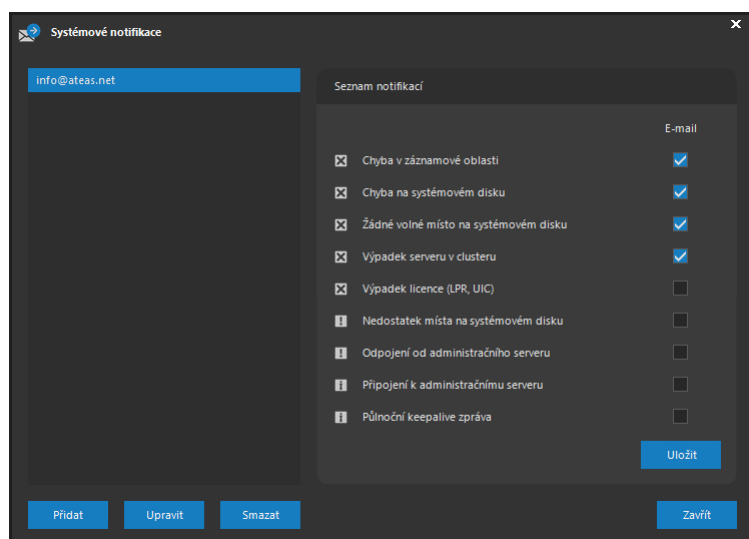
11.10.9. Notifikace

Pro kamerové servery v systému je k dispozici funkce notifikace při vzniku nějaké systémové události. Při vzniku systémové události je poté možné poslat e-mail. Kamerová server ATEAS umí e-maily odesílat v několika jazycích a na libovolný počet e-mailových adres.

POZNÁMKA

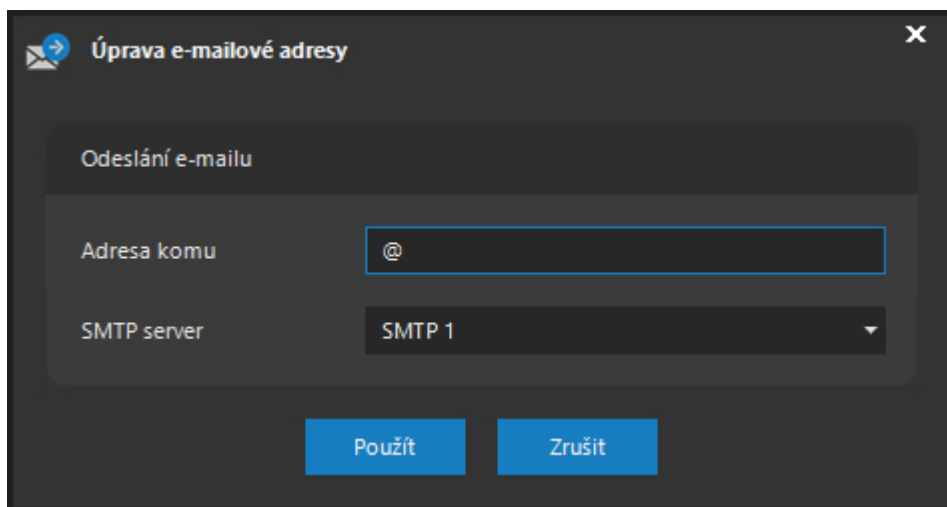
Zde nehovoříme o možnosti odesílat e-maily při události či poplachu v systému (například při aktivaci poplachového vstupu kamery, výpadku kamery či rozpoznání zakázané RZ). Tato reakce může být součástí událostního scénáře při reakci kamer na událost, viz kapitola o managementu událostí a vytváření událostních scénářů.

Okno s nastavením notifikací lze otevřít stiskem tlačítka **NOTIFIKACE**. Při použití tohoto tlačítka je zapotřebí, aby byl vybrán kamerový server ve stavu online.



E-mailové adresy

Seznam v levé části okna obsahuje e-mailové adresy, na které bude odeslán e-mail při výskytu nějaké systémové události. Pomocí tlačítka **PŘIDAT** lze provést vložení nové e-mailové adresy do seznamu dle následujícího obrázku.



Povinně je třeba vyplnit pole Adresa komu a SMTP server.

POZNÁMKA

Aplikace při zadávání nové e-mailové adresy kontroluje její syntaxi dle platných standardů a upozorní na neplatný formát adresy.

Vloženou adresu lze kdykoliv upravit pomocí shodného dialogu jako v případě přidávání nové adresy pomocí tlačítka **UPRAVIT**. Libovolnou adresu lze ze seznamu odstranit tlačítkem **SMAZAT**.

Seznam notifikací

Kamerový server rozesílá e-maily v případě vzniku libovolné systémové události, u které v seznamu zaškrtnete možnost zasílat e-maily. Je tedy možné obdržet notifikace e-mailem např. při výpadku záznamové oblasti (nebo pokud není po startu serveru k dispozici), výpadku serveru v clusteru (zprávu zašlou servery, na které jsou delegovány funkce), chybě na systémovém disku služby ATEAS Server, docházejícím místě na systémovém disku apod. Za systémový disk se považuje jednak umístění při instalaci, jednak i umístění pro ukládání metadat, pokud je toto na jiném disku.

K dispozici jsou také čistě informativní zprávy jako je znovu připojení k administračnímu serveru (po předchozím rozpadu spojení) či půlnocní keep-alive zpráva, která je automaticky odeslána každý den v půlnoci a indikuje, že server je v provozu.

TIP

Upozornění na výpadek LPR licence lze použít i pro upozornění na vypršení časově omezené demo licence.

Na každou adresu mohou být odesílány notifikace jiného druhu. Po přidání e-mailové adresy bude implicitně aktivováno pouze zasílání kritických zpráv na tuto adresu. Změnou zaškrtnutých notifikací a následným stiskem tlačítka **ULOŽIT** je možné pro vybranou adresu aktivovat zasílání pouze vybraných notifikací.

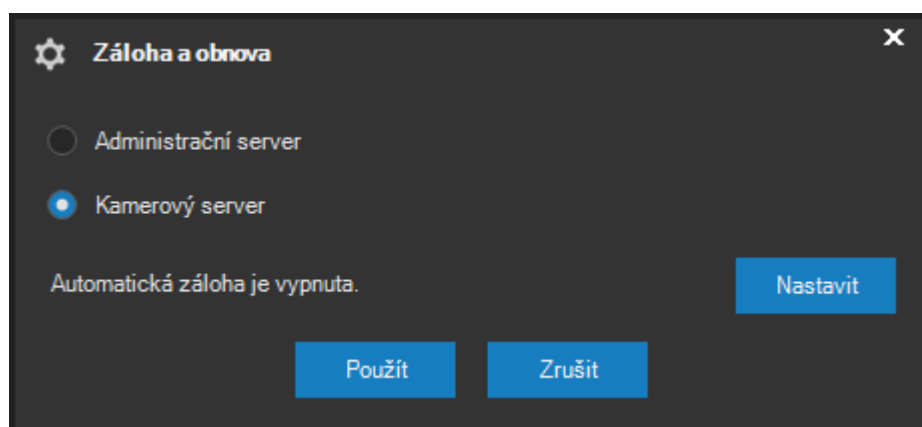
POZNÁMKA

Jelikož notifikace Odpojení od administračního serveru může být způsobena ztrátou konektivity na kamerovém serveru, kamerový server nemusí mít možnost tuto notifikaci řádně odeslat. Proto je tato notifikace paralelně zasílána též administračním serverem systému.

11.10.10. Záloha a obnova konfigurace

Zálohu a obnovu nastavení lze provést pomocí dvojice tlačítek **ZÁLOHA** a **OBNOVA** v části Serverové funkce. Použitím těchto dvou tlačítek lze kdykoliv zálohovat či obnovit kompletní konfiguraci administračního serveru nebo vybraného kamerového serveru. Nastavení je uloženo v souboru XML.

Při zálohování nastavení je nutné vybrat příslušný server, viz následující obrázek. Po výběru umístění výsledného XML souboru bude proveden export kompletního nastavení dané serverové aplikace.



Při obnově nastavení postačí pouze vyhledat příslušný XML soubor, potvrdit výběr a konfigurace daného serveru bude kompletně obnovena. Pokud obnovujeme konfiguraci kamerového serveru, je nutné příslušný kamerový server nejdříve vybrat v seznamu serverů.

POZNÁMKA

Zálohu a obnovení konfigurace může provádět pouze administrátor systému. Zálohu a obnovení konfigurace administračního serveru může provádět pouze master administrátor (administrátor s číslem 1).

POZOR

Při obnově konfigurace musí být vždy použit XML soubor, ve kterém je uloženo nastavení ve verzi odpovídající verzi systému.

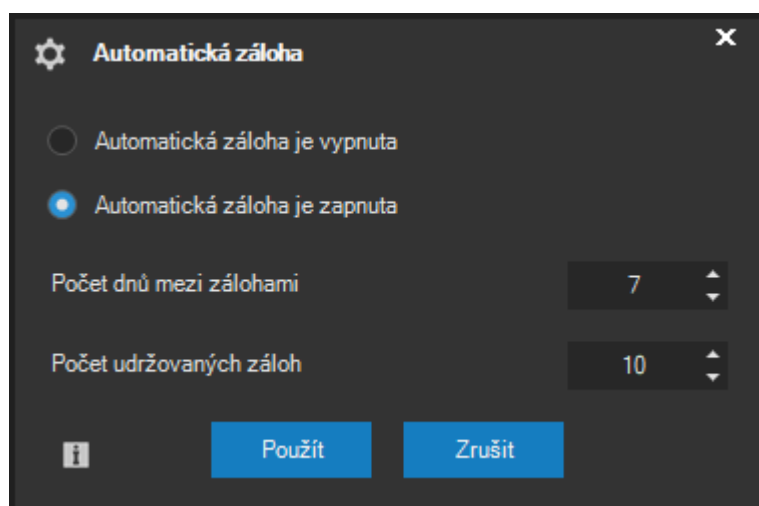
TIP

Tlačítko **OBNOVA** se nachází také v licenčním dialogu, odkud je možné po čisté instalaci systému konfiguraci obnovit rychleji a bez aktivace licence.

Automatické zálohování konfigurace

Konfiguraci pro administrační server a všechny kamerové servery v systému lze také pohodlně zálohovat zcela automaticky. To je vhodné, zejména pokud jsou změny konfigurací prováděny často anebo máme v systému větší počet kamerových serverů, pro který může být provedení ruční zálohy zdlouhavé.

Automatické zálohování je možné aktivovat v dialogu, který se zobrazí po stisknutí tlačítka **NASTAVIT** v dialogu, kde provádíme zálohu ručně.



V tomto dialogu je možné automatické zálohování konfigurace vypnout anebo zapnout. Pokud je automatické zálohování zapnuto, je možné určit počet dnů mezi jednotlivými automatickými zálohami a maximální počet udržovaných záloh (staré zálohy konfigurace jsou automaticky mazány).

POZNÁMKA

Při automatickém zálohování se XML soubory s konfigurací ukládají vždy na administračním serveru systému v podsložce configuration-backup, kde jsou automaticky rozděleny do složek dle serveru a jednotlivé soubory jsou opatřeny údajem o datu, kdy byla záloha provedena.

POZNÁMKA

V rámci daného dne, kdy má být záloha provedena, je tato vždy provedena o půlnoci. Pokud server není v tomto čase online, je automatická záloha provedena po připojení serveru.

Konfiguraci nelze exportovat a importovat mezi systémy různých verzí, aplikace také proto nabízí při ruční záloze název souboru obsahující datum exportu a verzi systému. Identické názvy jsou použity také při automatické záloze.

I bez nastavené automatické zálohy nastavení je záloha provedena vždy před přechodem na vyšší verzi systému v podsložce recover administračního i kamerového serveru.

11.10.11. Podpora DLNA vysílání

Aktivaci vysílání DLNA pro daný kamerový server lze provést pomocí tlačítka **DLNA** pod seznamem serverů. DLNA je označení pro technologii, která umožňuje zařízením typu televizních přijímačů a dalším (např. VLC) automaticky detekovat zdroje vysílání videa v síti spolu s jejich názvy a dalšími parametry a k těmto zdrojům videa se připojit.

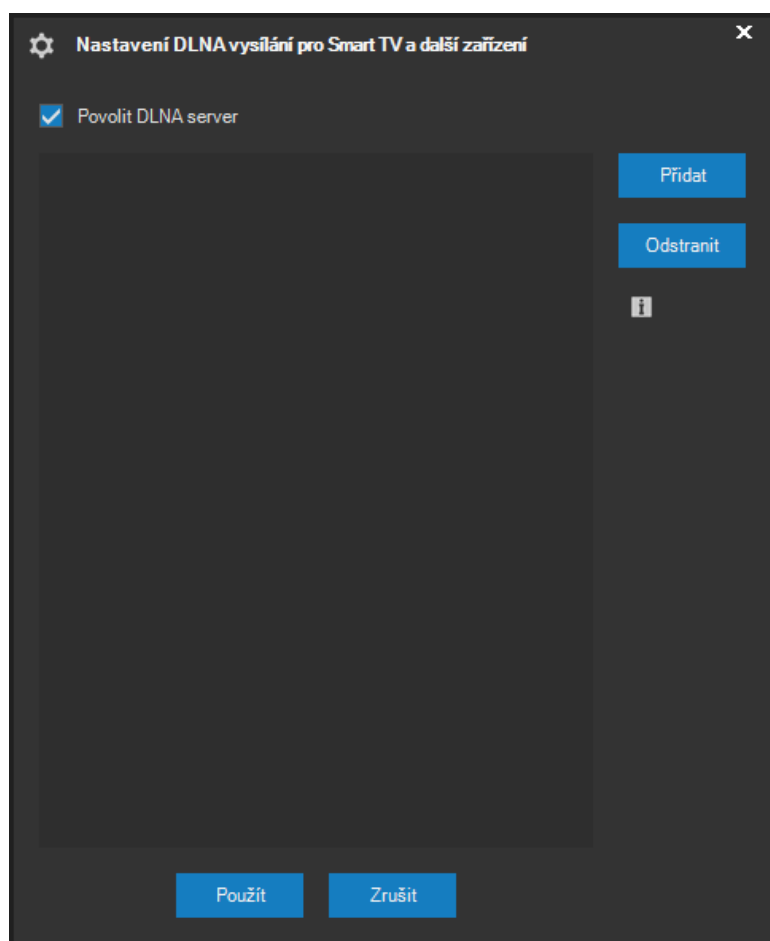
POZNÁMKA

ATEAS Server používá pro DLNA vysílání port 8509 a dále také protokol SSDP pro publikaci kanálů DLNA vysílání.

POZOR

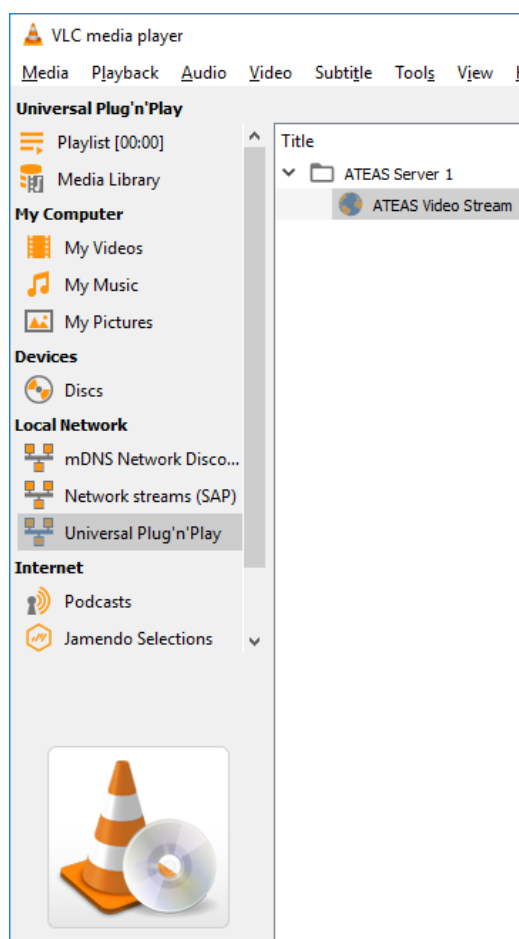
ATEAS pro DLNA vysílání používá nový způsob MP4 kontejneru pro živé vysílání (fragmentovaný MP4 přenos). Zařízení nepodporující tento formát nebudou schopna video přehrát.

Po stisku tlačítka DLNA se zobrazí následující dialog.



Pomocí volby Povolit DLNA server lze aktivovat a případně deaktivovat server DLNA. Aby klienti serveru mohli přijímat video z kamer, musí být vytvořeny nějaké DLNA vysílací kanály. Vysílací kanál lze jednoduše vytvořit kliknutím na tlačítko **PŘIDAT** a zadáním názvu kanálu následovaného číslem kamery v hranatých závorkách, např. kanál s kamerou 1 lze vytvořit pomocí zadání Kamera 1 [1].

Na obrázcích níže je vidět přehrávač VLC přistupující k ATEAS DLNA serveru.



POZOR

Klienti DLNA serveru se nijak neautorizují, měly by tedy být vytvořeny pouze takové vysílací kanály, k nimž je možné a přípustné přistupovat anonymně.

POZNÁMKA

Možnost využití DLNA serveru je k dispozici až od edice ATEAS Security PROFESSIONAL.

11.10.12. Migrace na nové servery

Pokud vznikne potřeba přenosu ATEAS služeb na nový server, je možné použít způsob přenosu konfigurace v XML formátu popsany výše. Po instalaci příslušné služby ATEAS se pak jen provede import konfigurace z předchozího serveru.

POZOR

V případě, kdy má být po migraci na nový server dostupný též kamerový záznam, může být třeba provést dodatečné kroky popsané níže.

Pokud jsou záznamové oblasti dostupné stále na stejné cestě jako na předchozím serveru, je třeba po instalaci nového serveru provést zkopírování obsahu podsložky data kamerového serveru z předchozího na nový server a restartovat službu kamerového serveru.

Pokud mají být záznamové oblasti na jiných cestách, je možné provést odstranění původních záznamových oblastí a vytvoření nových oblastí z již existujících dat. Tento postup je popsán v kapitole o správě záznamových oblastí.

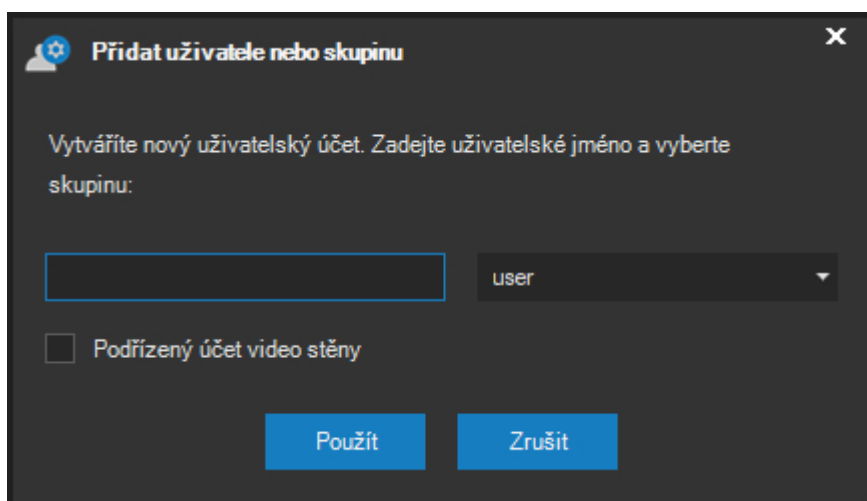
11.10.13. Správa uživatelů

V seznamu v části Přehled uživatelů je uveden seznam všech uživatelů. Pro každého uživatele je uvedeno jeho unikátní identifikační číslo, jméno a skupina. Skupinou může být buď USER (běžní uživatelé) nebo ADMINISTRATOR (administrátoři) nebo jiná administrátorem vytvořená skupina. Více o skupinách najdete také v další subkapitole o správě skupin. Na systému může být vytvořeno libovolné množství uživatelských účtů pro běžné uživatele i administrátory. Uživatelské účty je možné

vzestupně a sestupně třídit podle všech sloupců v seznamu. Seznam též obsahuje indikátor, který barevně odlišuje uživatele, kteří jsou aktuálně přihlášení do systému od offline uživatelů.

Přidání uživatele

V části Uživatelské funkce je třeba stisknout tlačítko **NOVÝ**. V následujícím dialogu je třeba vyplnit uživatelské jméno a určit skupinu.



Před vytvořením účtu je kontrolována duplicita uživatelského jména. Pokud je uživatelské jméno již v systému, aplikace zobrazí příslušnou zprávu. Po úspěšném vytvoření uživatelského účtu aplikace zobrazí zprávu a je aktualizován seznam uživatelů. Zaškrtnutí políčko Podřízený účet video stěny slouží k tvorbě speciálních uživatelských účtů pro podřízené video stanice, které lze ovládat z jiných klientských stanic. Více se dozvíte v kapitole o administraci pohledů v části věnované video stěně.

Operace s uživateli, u kterých to má smysl a vypovídající vizuální hodnotu, lze provádět hromadně s vícenásobným výběrem uživatelů. Lze tedy např. hromadně odstranit uživatele či je přiřadit do jiné skupiny apod. Hromadné operace ale nelze např. provést současně nad administrátory a běžnými uživateli systému.

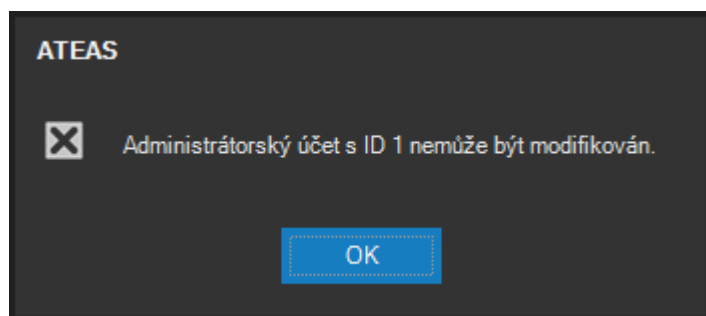
TIP

Uživatele je možné přejmenovat přímo v seznamu kliknutím na jeho jméno.

Odebrání uživatele

Libovolného uživatele (běžného uživatele i administrátora) lze ze systému odebrat. Po stisku tlačítka **ODSTRANIT** v části Uživatelské funkce je nutné potvrdit zprávu a vyčkat potvrzení.

Výjimku tvoří administrátorský účet s číslem 1 a uživatelem admin, který odebrán být nemůže (nemůže být ani nikterak modifikován). Při pokusu o odebrání nebo modifikaci tohoto účtu aplikace zobrazí varovnou zprávu a odebrání nebude provedeno.



POZNÁMKA

Administrátorský účet s číslem uživatele 1 a s uživatelským jménem admin má v systému speciální význam. Chování tohoto účtu se liší v následujících bodech.

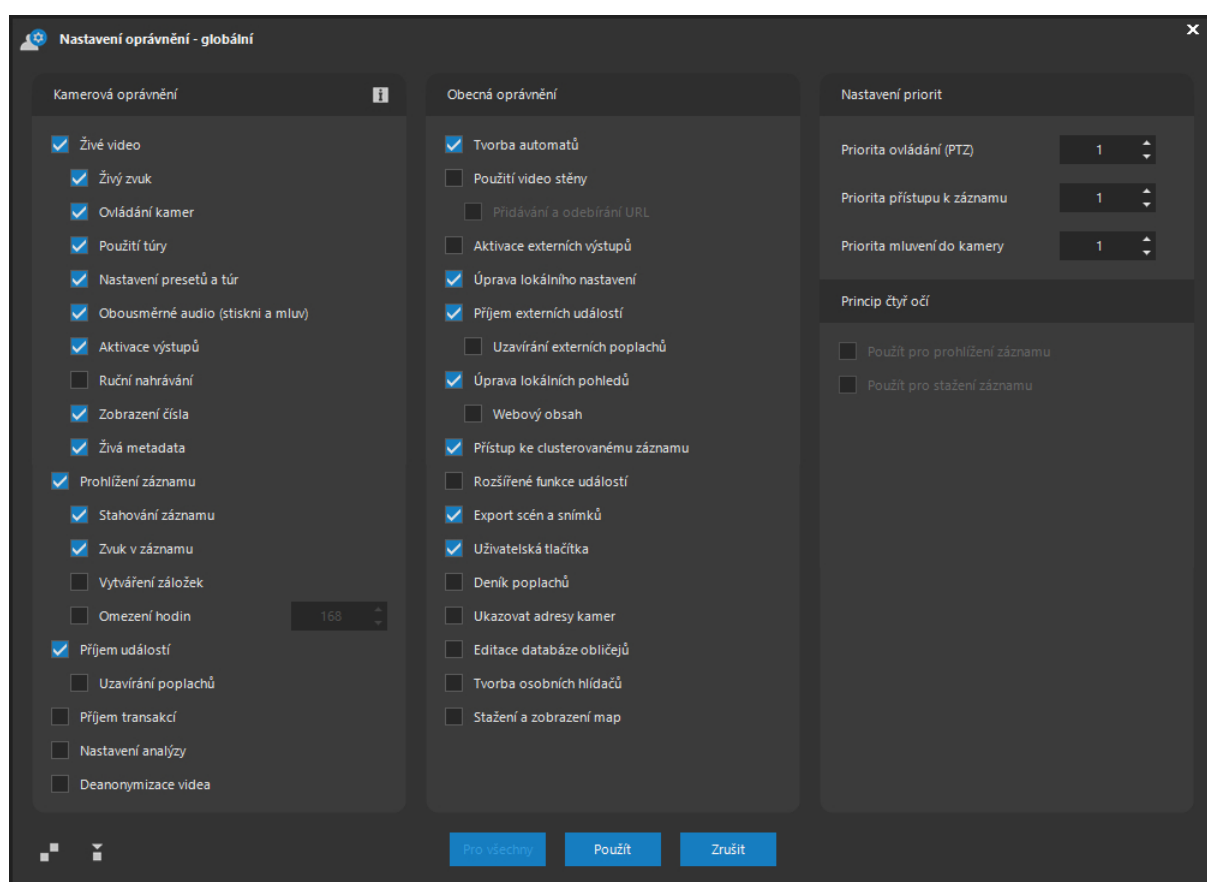
- tento účet nemůže být nikým odstraněn a nemohou být modifikována jeho oprávnění,
- tento účet má vždy vytvořen profil na všech nově přidaných kamerových serverech a nemůže být těchto profilů zbaven, ostatní uživatelé (včetně administrátorů) implicitně nemají na nově vytvořeném kamerovém serveru žádný profil a není pro ně viditelný,
- má jako jediný administrátor možnost spravovat kamerové servery a uživatele, ostatní administrátoři mohou provádět správu na serverech, ke kterým je jim zřízen přístup (s výjimkou danou nástrojem řízení přístupu do administračních sekcí - viz níže),
- má jako jediný možnost provést upgrade licenčního čísla platného pro celý systém,
- má jako jediný oprávnění ovládat ostatní administrátorské účty a nástroj řízení administrátorských účtů pomocí sekcí - viz níže).

Hesla a jejich reset

Heslo nově přidaného uživatele je vždy shodné s jeho uživatelským jménem. Vzhledem k tomu, že systém tuto shodu neakceptuje, bude uživatel při svém přihlášení přinucen heslo změnit. Pokud některý uživatel své heslo zapomene, je možné provést jeho reset pomocí tlačítka **HESLO**. Po potvrzení následující zprávy tlačítkem **ANO** dojde k resetu hesla vybraného uživatele na výchozí hodnotu (shodné s jeho uživatelským jménem).

Oprávnění uživatelů

Pro vybraného uživatele lze dále definovat oprávnění. Tato oprávnění budou pro daného uživatele vztažena globálně (tj. na všechny kamery na všech kamerových serverech, ke kterým daný uživatel přístup) s výjimkou případu, kdy jsou uživateli vytvořena omezení s možností definovat kamerová oprávnění pro každou kameru samostatně. V seznamu oprávnění lze pomocí zaškrtnutí políček modifikovat oprávnění uživatele, změny lze aplikovat tlačítkem **POUŽÍT**. Po uložení změn se objeví potvrzení v podobě zprávy.



Oprávnění jsou rozdělena do dvou skupin. V levé části se nacházejí kamerová oprávnění (oprávnění přímo související s kamerami), v pravé části jsou obecná oprávnění (bez přímé souvislosti s kamerami).

POZOR

Pokud jsou uživateli vytvořena omezení, mají nastavená oprávnění pro každou kameru přednost před obecnými oprávněními v tomto dialogu.

Většina položek v seznamech obecných a kamerových oprávnění nepotřebuje díky výstižnému označení žádný další komentář, níže doplňujeme jen vybrané poznámky.

Oprávnění Zobrazení čísla kamery se vztahuje k zobrazení čísla kamery v přehledu čísel kamer v primárním dohledovém okně a nijak neovlivňuje možnost k této kameře přistoupit v rámci pohledu, přehrávání záznamu apod. Oprávnění lze však využít tehdy, pokud jsou kamery k serveru přidány vícekrát a mají-li nastaveny hodnoty offsetu pro zobrazení detailu a záznamu (viz základní nastavení kamery). V takovém případě můžeme pro duplicitně přidané kamery uživatelům odebrat oprávnění k zobrazení jejich čísla v dohledovém okně z důvodu větší přehlednosti.

Pokud chcete uživateli zpřístupnit možnost ovládání video stěny (pokud je v systému použita), musí mu být v tomto okně uděleno oprávnění. Speciálně je nutné uživateli či skupině povolit tvorbu URL pro zobrazení webového obsahu na video stěnách.

Oprávnění s názvem Rozšířené funkce událostí se váže k možnosti pro některé události přijaté v dohledových oknech či dohledaných v záznamu pomocí pravého tlačítka myši vyvolat kontextovou nabídku s doplňujícími možnostmi pro danou událost. Využívá se například tehdy, pokud chceme, aby mohl běžný uživatel měnit zařazení RZ vozidel do evidovaných seznamů RZ (povolené, zakázané atd.). Dále je tímto oprávněním řízen přístup i ke kontextové nabídce resetu hodnoty čítačů v dohledovém okně.

V sekci Nastavení priorit lze nastavit hodnotu Priorita ovládání (PTZ) - od 1 do 20, čím vyšší číslo, tím vyšší priorita. Tato priorita (při přidání nového uživatele implicitně 1) je důležitá v situaci, kdy se dva uživatelé (nebo více) současně pokoušejí ovládat jednu a tutéž kameru. Při současném přístupu k jedné kameře platí, že přednost má uživatel s vyšší prioritou. Po dobu ovládání kamery uživatelem s vyšší prioritou, ji nemůže ovládat žádný uživatel s nižší prioritou. Pokud však uživatel s vyšší prioritou určí dobu kamery neovládá, může ji začít ovládat uživatel s nižší prioritou (po uplynutí časového prostoru zvaného PTZ časové okno - PTZ time window). Při současném přístupu dvou uživatelů se stejnou prioritou se uživatelé o kameru neperou, nýbrž se řídí pravidlem „kdo dřív přijde, ten dřív mele“. Uživatel, který začne kameru ovládat dříve, má přednost a dostává k dispozici své časové okno.

Jméno uživatele, který získal kontrolu nad ovládáním kamery, se ostatním uživatelům zobrazuje pod ovládacím prvkem pro ovládání kamer. Ostatní uživatelé, kteří nemohou kameru ovládat, mohou tak alespoň sledovat, kdo ji v dané chvíli používá a případně ověřit, že je ovládání kamery již uvolněno pro další uživatele.

Z hlediska priorit ovládání má nejnižší prioritu túra, vyšší prioritu má ruční ovládání (polohování či pohyb na preset), které túru na danou nastavitelnou dobu přeruší. Pokud je však túra spuštěna v reakci na událost, je čas přerušení této událostní túry při ručním ovládání kamery snížen na velmi krátký čas v řádu vteřin, neboť událostní túra má vyšší prioritu než běžná túra.

Podobně udává hodnota Priorita mluvení do kamery prioritu uživatele či skupiny pro funkci vysílání zvuku do kamery. Uživatel s vyšší prioritou může začít mluvit do kamery i v případě, že do kamery právě vysílá zvuk uživatel s nižší prioritou, jehož vysílání je v takovém případě automaticky ukončeno. Prioritu lze opět nastavit v rozsahu 1 – 20, přičemž vyšší číslo znamená vyšší prioritu. Pokud má uživatel prioritu nižší nebo stejnou, musí počkat, až jiný uživatel vysílání zvuku do kamery dokončí.

Priorita přístupu k záznamu udává prioritu uživatele či skupiny, v rámci které může uživatel přistupovat k intervalům záznamu s aplikovaným omezením a zároveň také sám omezení nastavovat. Má-li tedy uživatel např. prioritu 10, nemůže zobrazit data s nastaveným omezením a minimální prioritou přístupu 11 či vyšší, může však sám o sobě nastavit omezení na části záznamu a určit minimální prioritu přístupu na 10 nebo nižší. Prioritu lze opět nastavit v rozsahu 1 – 20, přičemž vyšší číslo znamená vyšší prioritu.

POZNÁMKA

Má-li uživatel nastaveno oprávnění pro příjem externích událostí, je to nutná podmínka pro to, aby mohl přijímat události generované administračním serverem systému - události zasílané pomocí ATEAS API libovolným z popsaných komunikačních kanálů a vztahené k vytvořené virtuální struktuře objektů. Není to však podmínka postačující. Pokud je pro událost vytvořen neprázdný událostní scénář, klient událost přijme pouze tehdy, pokud má přístup alespoň k jedné z kamer, které jsou jeho součástí. Tímto způsobem lze externí události inteligentně distribuovat v systému s větším počtem serverů a klientů.

Uživatele s právem přístupu do záznamu je možné dále omezit počtem hodin (položka Omezení hodin), které mohou v záznamu prohlížet. Je tedy možné např. nastavit oprávnění tak, že data starší jednoho dne budou moci zobrazovat pouze vybraní uživatelé apod. Hodnotu je možné nastavit v rozsahu 1 hodiny až 100 dní (2400 hodin).

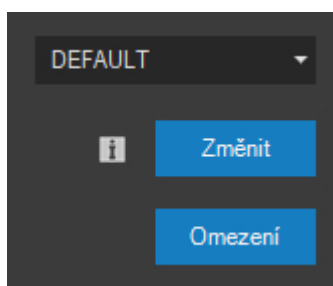
Pro skupinu je také možné aktivovat princip čtyřech očí, který je popsán dále v textu.

Pro zjednodušení nastavení oprávnění uživatelů, případně skupin je možné provádět kopírování oprávnění mezi uživateli. Chceme-li tedy nastavit oprávnění shodně či podobně jako u jiného

uživatele, je výhodné provést kopii celé sady oprávnění a později ji upravit. Pro kopírování a vkládání sady oprávnění slouží dvě tlačítka v levém dolním rohu okna.

Profily uživatelů

Aby mohl uživatel přistupovat ke kamerovému serveru (či serverům), je nutné mu zřídit profil. Profil vybraného uživatele pro vybraný server se nastavuje v části Profil uživatele.



V rozbalovacím seznamu je možné volit z několika možností s následujícím významem:

NO – Žádný profil, vybraný uživatel nebude moci přistupovat k vybranému serveru.

LOCAL – Lokální profil, vybraný uživatel bude k mediálním datům vybraného serveru (video a audio) přistupovat přes multicastové adresy a použije přitom LAN adresu kamerového serveru.

DEFAULT – Implicitní profil, vybraný uživatel bude k mediálním datům kamerového serveru přistupovat pomocí unicastových spojení a použije přitom adresu LAN kamerového serveru.

REMOTE – Vzdálený profil, vybraný uživatel bude k mediálním datům přistupovat přes unicastová spojení na adrese WAN kamerového serveru.

POZNÁMKA

Nastavení WAN adresy pro kamerové servery není v edicích HOME a PROFESSIONAL nutné. V edici UNLIMITED je nutné pouze tehdy, budou-li uživatelé přistupovat k serveru také mimo svou lokální síť. Více viz subkapitola Základní správa serverů.

Uživatelům lze tak nastavením profilu zabránit, aby ke kamerovému systému přistupovali také mimo svou lokální síť, pouze uživatelé s profilem REMOTE k danému serveru se budou moci k němu připojit. Změnu profilu lze způsobit stisknutím tlačítka **ZMĚNIT**. Po úspěšné změně se zobrazí potvrzující zpráva.

POZNÁMKA

Před provedením změny profilu zobrazí aplikace zprávu, zdali má být změna provedena pouze pro vybraný server nebo pro všechny servery v systému, ke kterým může administrátor přistupovat.

POZNÁMKA

Výchozí profil všech uživatelů k nově přidanému serveru a zároveň výchozí profil nově přidaných uživatelů ke všem serverům je NO (žádný profil). Výjimku tvoří uživatelský účet 1 (admin) jehož výchozí přístup ke všem nově přidaným serverům je DEFAULT.

POZNÁMKA

Není možné zbavit administrátora s číslem 1 přístupu k žádnému serveru. Tento účet musí mít ke všem serverům profil nastavený na LOCAL, DEFAULT nebo REMOTE. Při pokusu o nastavení na NO aplikace pokračování v akci nepovolí.

Použití profilu LOCAL pro všechny nebo vybrané uživatele může mít velmi pozitivní dopad na vytížení sítě a objem přenášených dat při přístupech více uživatelů do systému, neboť se používají multicastové přenosy. Při lokálním profilu se využívá multicastového vysílání kamerového serveru, nikoliv jednotlivých kamer, byť to umožňují. To sice může znamenat navýšení celkového síťového provozu (multicast data proudí skrz kamerový server), koncepce má však tyto výhody:

- Multicast lze využít i v případech, kdy je oddělena síť kamer a klientů a klienti nevidí adresy kamer. Při požadavku na multicast vysílání samotné kamery např. pomocí protokolu RTSP by klient musel přistoupit na adresu kamery.
- Video a audio data jsou na serveru označena časovým razítkem platným pro celý systém, není zde tedy závislost na časové synchronizaci kamery, pokud např. uživatel ukládá snímky kamery z živého obrazu.
- Multicastové vysílání lze použít i v případech, kdy ho kamera neumožňuje.

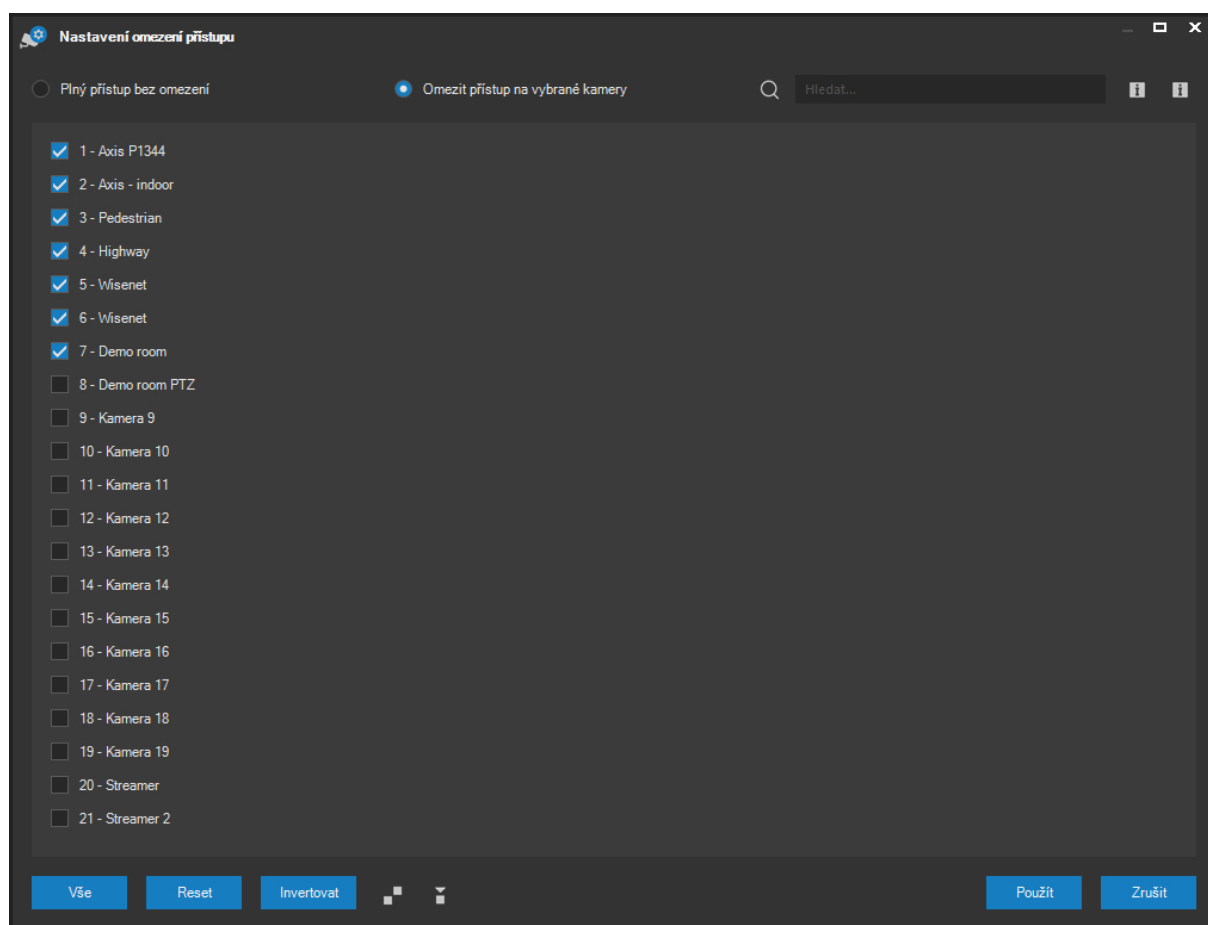
POZOR

Aby mohl přenos typu multicast fungovat ve Vaší síti, musí aktivní síťové prvky (switch) podporovat multicastové přenosy. Tuto informaci lze nalézt v dokumentaci nebo datasheetu Vašeho switchu. Podporován musí být protokol IGMP ve verzi 2. Pokud má být multicast funkční i v soustavě více propojených sítí, musí být podpora multicastu zajištěna i na síťových směrovačích (routerech). Při změně profilu na LOCAL aplikace zobrazí informační zprávu v tomto duchu.

Omezení uživatelů

Pokud je vybranému uživateli zřízen přístup k vybranému serveru (nastavením profilu na LOCAL, DEFAULT nebo REMOTE), má tento uživatel automaticky přístup ke všem kamerám na tomto serveru. Pokud chcete uživateli omezit přístupné kamery na daném serveru, je možné to provést stisknutím tlačítka **OMEZENÍ**.

Pomocí omezení je nejen možné omezovat přístup uživatele na vybrané (nebo i všechny) kamery kamerového serveru, ale také podrobně definovat kamerová oprávnění pro každou kameru samostatně. Pokud tedy chceme, aby pro uživatele platila jednotně nastavená kamerová oprávnění pomocí tlačítka **OPRÁVNĚNÍ**, nesmí mít takový uživatel vytvořeno na daném kamerovém serveru žádné omezení.



Zobrazené kamery je možné filtrovat pomocí vyhledávacího pole, do něhož lze zadat více skupin znaků, které se všechny musí vyskytovat v čísle či názvu kamery. Pro vyhledávání včetně mezer lze zadat text či frázi v uvozovkách.

Je možné volit ze dvou přepínačů Plný přístup bez omezení a Omezit přístup na vybrané kamery. S plným přístupem bude mít uživatel přístup ke všem kamerám a automaticky též ke všem kamerám, které budou v budoucnu přidány. Pokud přístup omezíte, uživatel bude moci přistupovat pouze k vybraným (zaškrtnutým) kamerám a nebude mít přístup k nově přidaným kamerám.

Pomocí tlačítek **VŠE**, **RESET** a **INVERTOVAT** lze upravit výběr kamer tak, že budou zaškrtnuty veškeré existující kamery na serveru, respektive bude zaškrtnutí všech kamer zrušeno nebo bude výběr kamer invertován.

Pokud se okno nachází v režimu nastavení omezení (je zvolený přepínač Omezit přístup na vybrané kamery), je možné pomocí pravého tlačítka myši pro libovolnou kameru, která je uživateli zpřístupněna a je zaškrtnuta, zobrazit kontextové menu a zvolit položku Oprávnění. Poté se zobrazí okno s definicí oprávnění pro danou kameru.

☐ Plný přístup bez omezení
 ☒ Omezit přístup na vybrané kamery

- ☒ 1 - Axis P1344
- ☒ 2 - Axis - indoor
- ☒ 3 - Pedestrian
- ☒ 4 - Highway
- ☒ 5 - Wisenet
- ☐ 6 - Wisenet
- ☐ 7 - Demo room
- ☐ 8 - Demo room PTZ
- ☐ 9 - Kamera 9
- ☐ 10 - Kamera 10

Oprávnění

Nastavení oprávnění - kamera 1

Kamerová oprávnění

- ☒ Živé video
- ☒ Živý zvuk
- ☒ Ovládání kamer
- ☒ Použití tury
- ☒ Nastavení presetů a tūr
- ☒ Obousměrné audio (stiskni a mluv)
- ☒ Aktivace výstupů
- ☐ Ruční nahrávání
- ☒ Zobrazení čísla
- ☒ Živá metadata
- ☒ Prohlížení záznamu
- ☒ Stahování záznamu
- ☒ Zvuk v záznamu
- ☐ Vytváření záložek
- ☐ Omezení hodin
- ☒ Příjem událostí
- ☐ Uzavírání poplachů
- ☐ Příjem transakcí
- ☐ Nastavení analýzy
- ☐ Deanonymizace videa

Obecná oprávnění

- ☐ Tvorba automatů
- ☐ Použití video stěny
- ☐ Přidávání a odebrání URL
- ☐ Aktivace externích výstupů
- ☐ Úprava lokálního nastavení
- ☐ Příjem externích událostí
- ☐ Uzavírání externích poplachů
- ☐ Úprava lokálních pohledů
- ☐ Webový obsah
- ☐ Přístup ke clusterovanému záznamu
- ☐ Rozšířené funkce událostí
- ☐ Export scén a snímků
- ☐ Uživatelská tlačítka
- ☐ Deník poplachů
- ☐ Ukazovat adresy kamer
- ☐ Editace databáze obličejů
- ☐ Tvorba osobních hlídačů
- ☐ Stažení a zobrazení map

Nastavení priorit

Priorita ovládání (PTZ) 1

Priorita přístupu k záznamu 1

Priorita mluvení do kamery 1

Princip čtyř očí

- ☐ Použít pro prohlížení záznamu
- ☐ Použít pro stažení záznamu

Pro všechny Použít Zrušit

Toto okno je podobné jako v případě nastavení uživatelských oprávnění po stisku tlačítka **OPRÁVNĚNÍ** s tím rozdílem, že není možné provádět změny v seznamu obecných oprávnění a veškeré změny v seznamu kamerových oprávnění včetně nastavení PTZ priority budou po uložení změn v okně nastavení omezení aplikována pouze na vybranou kameru.

POZNÁMKA

Pro administrátora s číslem 1 není možné toto omezení nastavovat pro žádný kamerový server.

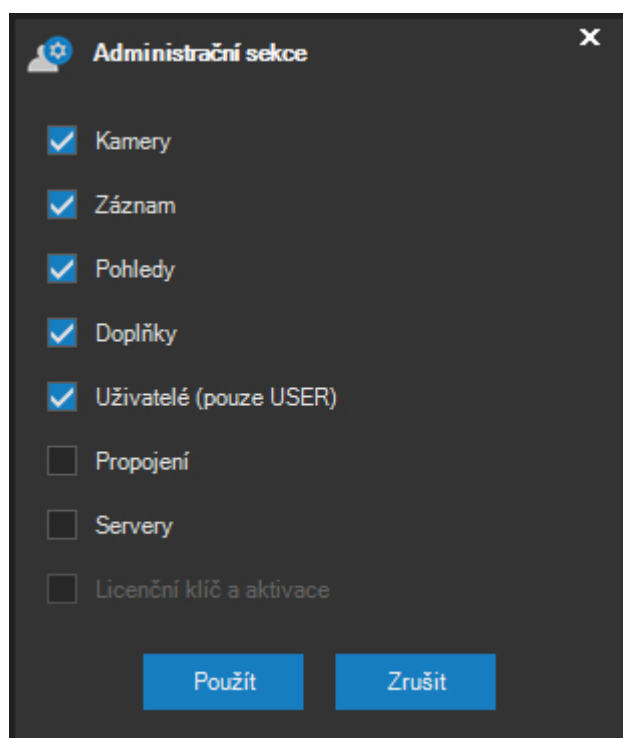
Pro zjednodušení nastavení oprávnění uživatelů, případně skupin je možné provádět kopírování oprávnění mezi jednotlivými uživateli nebo kamerami. Chceme-li tedy nastavit oprávněné shodně či podobně jako u jiného uživatele či kamery, je výhodné provést kopii celé sady oprávnění a později ji upravit. Pro kopírování a vkládání sady oprávnění slouží dvě tlačítka v levém dolním rohu okna. Stejná dvě tlačítka jsou k dispozici i v hlavním okně správy omezení, kde je možné kopírovat nastavení omezení pro všechny kamery mezi uživateli nebo skupinami uživatelů.

Velmi často také požadujeme stejné nastavení oprávnění pro určité kamery, na které jsme uživateli zřídili omezení. Přesně tento účel má tlačítko **PRO VŠECHNY**.

Řízení přístupu administrátorů - administrační sekce

Výše byl popsán způsob vytváření nových uživatelských účtů ve skupině uživatelů nebo administrátorů. Základním rozdílem mezi uživatelem a administrátorem je v přístupu k položkám nabídky v části Administrace základní nabídky, čili v přístupu do administrační sekce aplikace. Výše byla také popsána specifika administrátorského účtu s identifikací č. 1 a uživatelským jménem admin, kterého můžeme také nazvat master administrátorským účtem.

Master administrátor může v systému zřídit další administrátorské účty, na které může delegovat oprávnění spravovat kamery či záznam na jednotlivých kamerových serverech. Administrátoři tedy mohou mít rozdělenou působnost podle toho, k jakým kamerovým serverům jim byl zřízen přístup. Verze ATEAS Security 4.0.0 umožňuje nastavení působnosti administrátorů nejen podle severů, ale také podle činností na nich prováděných. K tomu slouží nástroj Administrační sekce dostupný pomocí tlačítka **SEKCE**.



Na obrázku je implicitní podoba přístupu k jednotlivým administračním sekcím, tak jak byla pevně zakotvena v systému do verze 3.9.6 včetně. Nově zřízené administrátorské účty tak měly přístup ke správě kamer, záznamu, pohledů a doplňků - samozřejmě pouze na kamerových serverech, na kterých jim byl vytvořen profil.

Pomocí tohoto nástroje může master administrátor zbavit administrátory přístupu k jednotlivým sekcím, jako jsou kamery, záznam, pohledy či doplňky, ale může také zřídit přístup do sekce uživatelů, propojení a servery.

POZNÁMKA

Pro zachování logiky fungování a kontroly master administrátora nad působností ostatních administrátorů v systému, ostatní administrátoři v systému nemohou v sekci uživatelů nijak ovlivnit uživatele ze skupiny administrátorů (ani samozřejmě účet svůj).

POZNÁMKA

Pro uživatele bez možnosti přístupu do sekce uživatelů zůstává administrační část uživatelů a serverů přístupná v režimu pouze pro čtení s možností využít některé nechráněné funkce.

Pokud je administrátorům povolen přístup do sekce Servery, budou moci vytvářet, měnit a odstraňovat kamerové servery v systému. Budou také oprávněni mezi ně rozdělovat licencovaný počet kamer. V takovém případě také uvidí v seznamu všechny servery včetně těch, ke kterým nemají zřízen žádný profil.

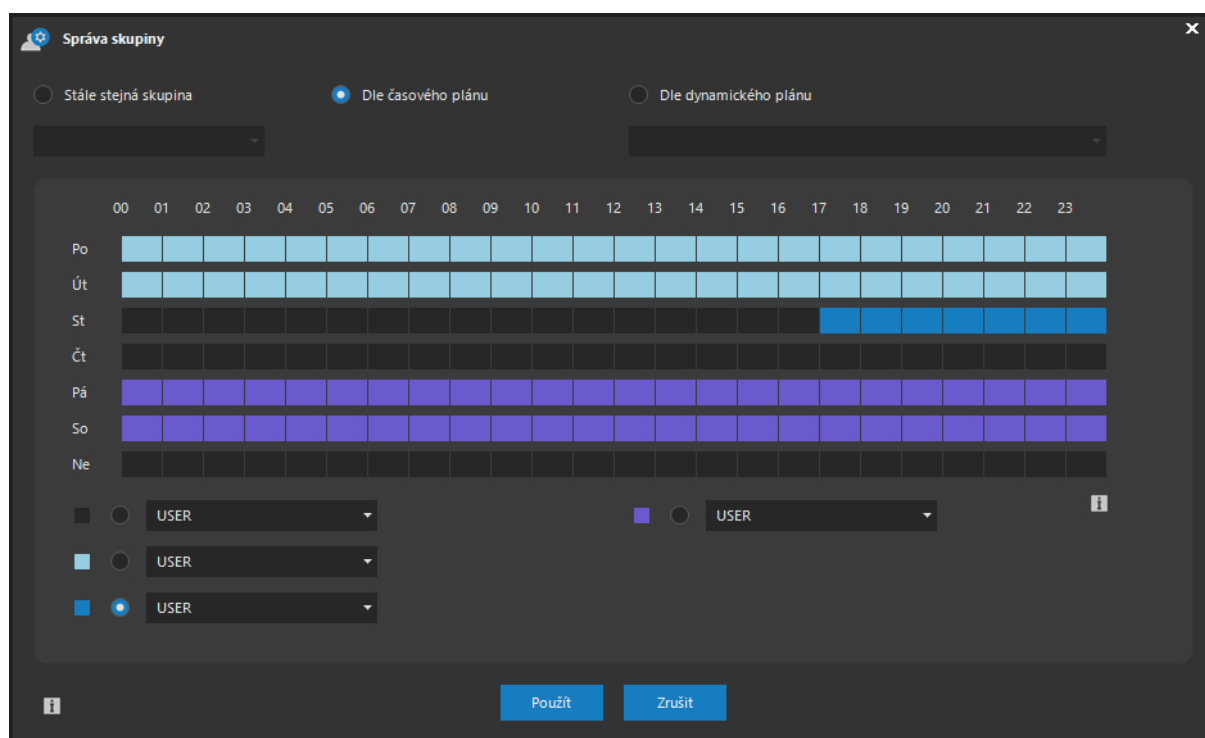
Široké a intuitivní nastavení působnosti administrátorů stále musí ponechat vybraná nastavení a činnosti v působnosti pouze master administrátora, čili administrátora s číslem 1 a uživatelským jménem admin. Jedná se o tyto činnosti:

- Master administrátor může jako jediný zřizovat, mazat a měnit nastavení uživatelských účtů ze skupiny administrátorů.
- Master administrátor může jako jediný vytvářet a mazat vlastní zdroje událostí kamer z důvodu centrální platnosti jejich názvů pro celý kamerový systém.
- Master administrátor může jako jediný provést zadání licenčního klíče a online generování aktivačního klíče včetně úvodní aktivace systému, pozdější reaktivace z důvodu přechodu na vyšší verzi systému či upgrade licenčního klíče z důvodu rozšíření licence.

Zařazení uživatelů do skupin

Každý uživatelský účet je po vytvoření součástí nějaké skupiny. Buď se jedná o předdefinovanou systémovou skupinu běžných uživatelů (USER) nebo administrátorů (ADMINISTRATOR) nebo o administrátorem definovanou skupinu s libovolným názvem. Pokud je uživatel součástí administrátorem definované skupiny, jeho oprávnění a omezení jsou vždy odvozena od oprávnění a omezení dané skupiny a nemohou být upravena individuálně, aplikace v takovém případě reaguje varovnou zprávou.

Pokud je uživatel součástí jedné jediné skupiny, hovoříme o jeho statickém zařazení do skupiny. Pokud je součástí více skupin, hovoříme o jeho zařazení do skupin jako o dynamickém. Dynamické zařazení do skupiny může být založeno na čase anebo na dynamickém plánu určeném událostí v systému. Toto nastavení může být provedeno po stisku tlačítka **SKUPINA**.



Na obrázku je vidět možnost statického nebo dynamického zařazení vybraného uživatele do skupiny či skupin. Při statickém zařazení je nutné vybrat jednu konkrétní skupinu (včetně předdefinované systémové skupiny), do které bude uživatel zařazen. Při dynamickém zařazení podle času je možné vybrat až čtyři různé skupiny uživatelů a naplánovat časové úseky, kdy bude automaticky docházet ke změně zařazení uživatele do skupiny. Při dynamickém zařazení podle dynamického plánu je nutné ze seznamu vybrat vytvořený dynamický plán a dále je možné určit a barevně odlišit dvě různé skupiny, mezi kterými bude uživatel automaticky přerazován podle toho, je-li příslušný dynamický plán neaktivní (první skupina) či aktivní (druhá skupina).

TIP

Pro rychlé označení celého dne nebo týdne lze použít dvojité resp. trojitě kliknutí.

TIP

Pro rychlé určení pracovní doby ve více dnech najednou použijte klávesu ALT.

V praxi je možné použít dynamické zařazení do skupin např. pro omezení denního dohledu do obývaných prostor, či zákazu ovládání otočných kamer v průběhu některých časových úseků apod.

POZNÁMKA

Pokud je uživatel zařazen do jedné skupiny (statické zařazení), je název skupiny zobrazen v seznamu uživatelů ve sloupci Skupina. Pokud je však zařazen do více skupin (dynamické zařazení), ve sloupci se bude zobrazovat systémová hodnota <dynamická>.

POZNÁMKA

Změna oprávnění či omezení skupiny se projeví okamžitě, a to bez rozdílu, je-li uživatel do skupiny zařazen staticky nebo dynamicky.

POZNÁMKA

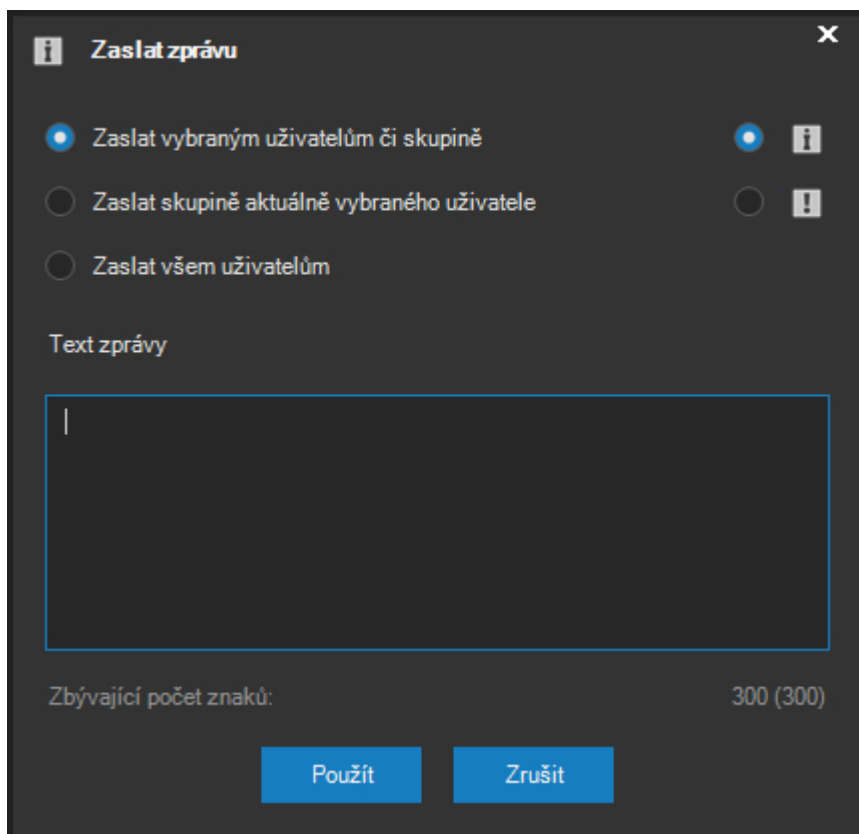
Vždy platí, že uživatelé založení v předdefinované skupině USER nebo ve skupině na ní založené, mohou být staticky či dynamicky zařazení pouze do skupin USER či skupin na ní založených. Totéž platí analogicky pro předdefinovanou skupinu ADMINISTRATOR.

Odhlášení uživatele

Pomocí tlačítka **ODHLÁSIT** je možné kdykoliv provést nucené odhlášení uživatele ze systému. To lze provést pro uživatele, který je přihlášen standardním klientem anebo jakýmkoliv jiným klientem včetně mobilních aplikací.

Zasílání zpráv

Pomocí tlačítka **ZPRÁVA** je možné vybranému uživateli či skupinám uživatelů zasílat interní zprávy. Tyto zprávy jsou uživatelům zobrazeny standardním způsobem v jejich klientských aplikacích, a administrátor je tak může např. upozornit na chystaný restart systému apod.



Pomocí přepínačů v horní části dialogu je možné určit, komu bude zpráva zaslána. První volba znamená, že zpráva bude zaslána jednomu vybranému uživateli anebo jedné vybrané skupině. Druhá volba znamená, že zpráva bude zaslána všem uživatelům, kteří jsou aktuálně ve stejné skupině jako vybraný uživatel. Přitom se nemusí jednat jen o skupiny, které administrátor vytvořil, ale také o základní skupiny USER nebo ADMINISTRATOR. Třetí volba zajistí, že zpráva bude zaslána všem aktuálně přihlášeným uživatelům systému.

POZNÁMKA

Zprávy nejsou zasílány klientům video stěny, pokud nejsou jako cíl vybráni explicitně (uživatel či vytvořená skupina).

Délka zprávy je omezena na 300 znaků a dále je možné pomocí příslušného přepínače určit závažnost (ikonu), s jakou bude zpráva uživatelům zobrazena - jako běžná informace či upozornění.

11.10.14. Správa skupin

Abychom mohli manipulovat se skupinami uživatelů, je zapotřebí zaškrtnout přepínač Skupiny. Skupiny uživatelů je možné vzestupně a sestupně třídit podle všech sloupců v seznamu. Zařazování jednotlivých uživatelů do skupin je popsáno v předchozí subkapitole.

Přidání skupiny

Pomocí tlačítka **NOVÁ** a po zadání názvu dojde k vytvoření nové skupiny uživatelů. Skupina musí být vždy založena na jedné ze dvou předdefinovaných systémových skupin - běžní uživatelé nebo administrátoři (USER nebo ADMINISTRATOR). Rozdíl je v tom, zdali členové skupiny budou mít možnost vstupovat do administrační sekce či nikoliv.

TIP

Skupinu je možné přejmenovat přímo v seznamu kliknutím na její jméno.

Odebrání skupiny

Tlačítkem **ODSTRANIT** lze vymazat libovolnou vytvořenou skupinu uživatelů.

POZNÁMKA

Pokud jsou ve skupině nějací uživatelé, jejich příslušnost do skupiny bude po odstranění skupiny na úrovni předdefinované systémové skupiny USER nebo ADMINISTRATOR. Jejich základní oprávnění budou ponechána na oprávněních skupiny a jejich omezení budou obnovena ve stavu před vytvořením skupiny. To se týká nejen situace, kdy je uživatel zařazen pouze do jedné skupiny, která je poté odstraněna, ale i situace, kdy je uživatel zařazen do více skupin a v daném čase je zrovna součástí odstraňované skupiny.

Oprávnění a omezení skupin

Nastavení základních oprávnění a omezení pro vybranou skupinu je zcela analogické jako nastavení oprávnění a omezení pro konkrétního uživatele.

POZNÁMKA

Při změně oprávnění či omezení skupiny se tato změna ihned projeví u všech uživatelů, kteří jsou v daném čase její součástí.

Profily skupin

Vytvořeným skupinám uživatelů je možné vytvářet, měnit nebo rušit profily u jednotlivých kamerových serverů, přičemž platí vše, co bylo výše zmíněno v odstavci Profily uživatelů. Určení profilu vybrané skupině však umožňuje změnu profilu všech uživatelů ve skupině najednou.

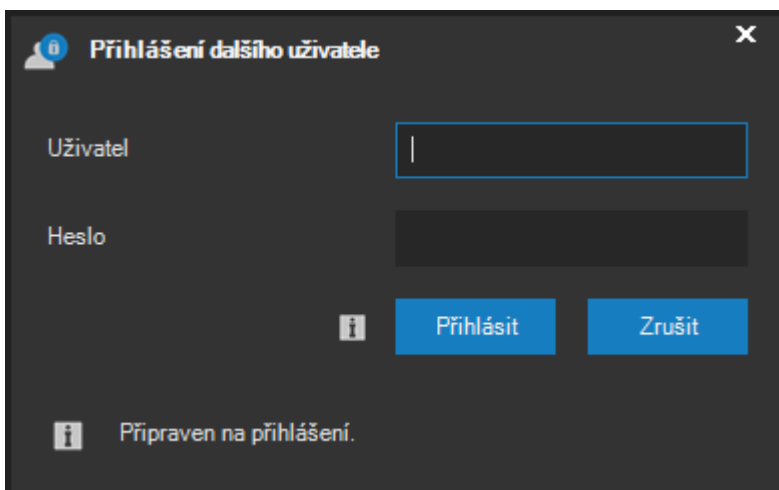
POZNÁMKA

Jelikož skupina sama o sobě není nositelem profilu k serverům, je změna profilu provedena přímo u všech uživatelů staticky zařazených ve vybrané skupině. Profily jednotlivých uživatelů pak mohou být dodatečně modifikovány.

11.10.15. Princip čtyř očí

V dialogu oprávnění skupiny je možné aktivovat tzv. princip čtyř očí, který lze použít pro stažení anebo už i pouhé prohlížení záznamu. Tento princip zajišťuje, že pro přístup k záznamu se budou muset na jednom počítači přihlásit vždy dva uživatelé z dané skupiny. Pokud je tento princip aktivován, žádný z uživatelů nebude moci přistupovat k záznamu samostatně.

Je-li princip aktivován a uživatel se pokusí přistoupit k záznamu či jeho stažení, bude automaticky vyvolán dialog pro přihlášení dalšího uživatele.



Teprve po přihlášení dalšího uživatele ze stejné skupiny a s vytvořeným profilem na daném kamerovém serveru bude zpřístupněna daná funkce. Jakmile se druhý uživatel odhlásí, funkci již nebude možné využít.

POZNÁMKA

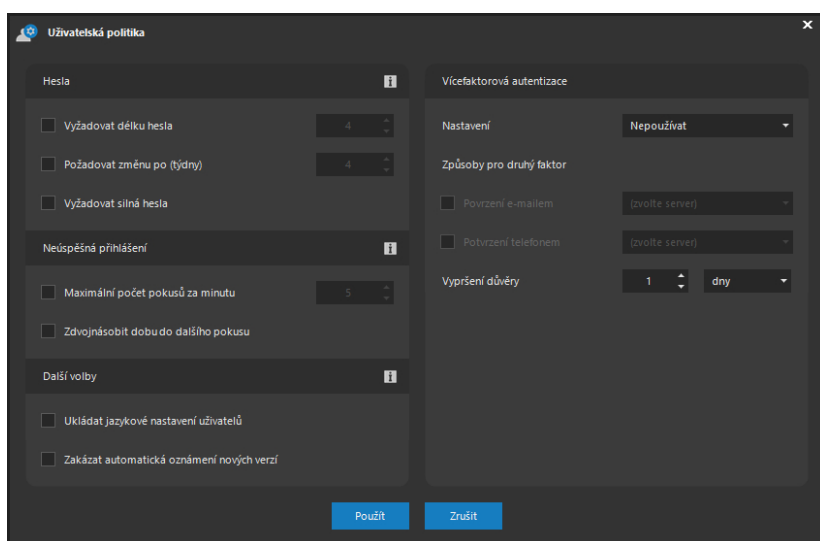
Dodatečné přihlášení uživatele nekoliduje s jeho plným přihlášením do systému, není tedy vyvolán chybový stav duplicitního přihlášení.

POZNÁMKA

Přístup k záznamu v režimu čtyř očí je logován spolu s informací o obou přihlášených uživateli.

11.10.16. Uživatelská politika

Administrátor má kromě možnosti nastavení oprávnění a omezení jednotlivých uživatelů či skupin také možnost nastavení některých globálních parametrů týkající se všech uživatelů v systému. Soubor těchto nastavení se nazývá uživatelská politika. Přístup k těmto nastavením vede přes tlačítko **POLITIKA**.



V části Hesla je možné provést globální nastavení minimálního požadovaného počtu znaků pro hesla jednotlivých uživatelů. Dále je také možné zaškrtnout volbu Vyžadovat silná hesla, která u uživatelů vynutí silný tvar hesla, což znamená, že heslo musí obsahovat alespoň jedno malé písmeno, jedno velké písmeno a alespoň jednu číslici.

POZNÁMKA

Po aktivaci nových pravidel uživatelské politiky hesel budou noví i stávající uživatelé při příštím přihlášení nuceni změnit svá hesla, pokud tato neodpovídají nastavené politice.

Dále je zde možné aktivovat časové omezení platnosti hesel uživatelů. Pokud je tato funkce v rámci uživatelské politiky aktivována, budou všichni uživatelé po uplynutí daného počtu týdnů od jejich poslední změny hesla vyzváni k zadání hesla nového.

POZNÁMKA

Nové heslo se nesmí shodovat s heslem platným před touto změnou.

V části Neúspěšná přihlášení jsou k dispozici z bezpečnostního hlediska důležité volby pro chování systému v případě neplatného přihlášení. Aktivací těchto voleb je možné efektivně zamezit útokům hrubou silou na uživatelské heslo. První volba umožňuje určit maximální počet povolených neúspěšných přihlášení za minutu (veškeré pokusy jsou spolu s IP adresou logovány). Druhá volba umožňuje tuto ochranu ještě zesílit zdvojnásobením doby do povolení dalšího pokusu.

Již tedy po relativně malém počtu neúspěšných pokusů je možné dosáhnout až maximální doby uzamčení účtu, která činí jeden rok. Jediným způsobem pro reset této doby je reset uživatelského hesla do výchozí podoby. Pro administrátorský účet s číslem jedna lze dobu resetovat pouze restartem služby administračního serveru.

V části Další volby je možné aktivovat volbu ukládání jazykového nastavení uživatelů. Pokud je tato volba aktivována, systém si bude pamatovat jazyková nastavení všech uživatelů a automaticky provede přepnutí příslušného jazyka po přihlášení uživatele z kterékoliv stanice.

POZNÁMKA

Toto nastavení jazyka má vyšší prioritu než nastavení jazyka v lokálním nastavení stanice.

Také je zde možné zakázat automatické oznamování aktualizací systému v klientské aplikaci, které provádí přímo klient pomocí komunikace s webovými servery ATEAS.

V části Vícefaktorová autentizace lze aktivovat možnost či povinnost vícenásobného ověření uživatele při přihlášení do systému. Podporované způsoby pro další faktor (tj. kromě znalosti přihlašovacích údajů) jsou přístup k nastavené e-mailové schránce anebo k mobilnímu telefonu.

V případě e-mailové adresy je nutné vybrat server odchozí pošty, který bude zasílat ověřovací e-maily. V případě mobilního potvrzení je nutné vybrat server, který je konfigurován jako brána pro zasílání ověřovacích notifikací na mobilní zařízení podporující protokol Firebase.

Klientská aplikace, ze které je provedeno vícefaktorové ověření, se může při příštím přihlášení se stejným účtem přihlásit rychleji, pokud ji systém důvěřuje. Důvěra pro aplikaci vyprší, pokud je účet v dané klientské aplikaci mimo systém po dobu nastavenou v položce Vypršení důvěry.

POZNÁMKA

Je-li interval nastavený na hodnotu nula, bude muset uživatel vícefaktorové ověření absolvovat vždy.

Není-li uživatel schopen absolvovat vícefaktorové ověření, musí následovat proces resetu uživatelského hesla. To může nastat v případě ztráty přístupu k e-mailové adrese, ke spárovanému mobilnímu zařízení či při odinstalaci mobilní aplikace ATEAS.

POZNÁMKA

V případě použití e-mailového ověření musí být pro uživatele dostupný administrační server systému, kam směřuje ověřovací odkaz. V případě mobilního ověření musí být administrační server systému připojen k internetu pouze pro odchozí spojení, mobilní zařízení musí být také online.

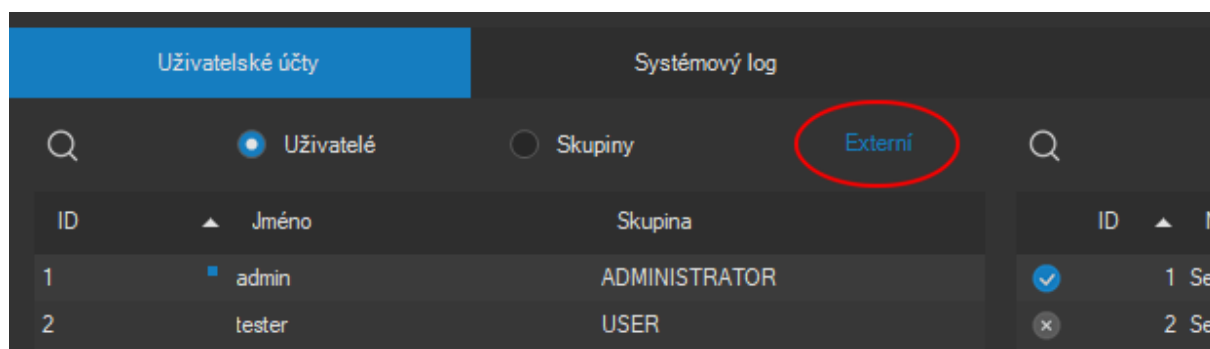
11.10.17. Integrace uživatelů s externími zdroji

Integrace správy uživatelů s externím zdrojem slouží jako alternativa k ruční správě uživatelů, u které je nutné všechna uživatelská jména do systému přidat případně odebrat ručně. Pomocí nástroje integrace s externím zdroji je možné provést hromadné přidání či odebrání uživatelů systému na základě načtení informací o uživateli z externího zdroje. Aktuálně tato funkce podporuje připojení ke službě Active Directory pomocí protokolu LDAP (Lightweight Directory Access Protocol).

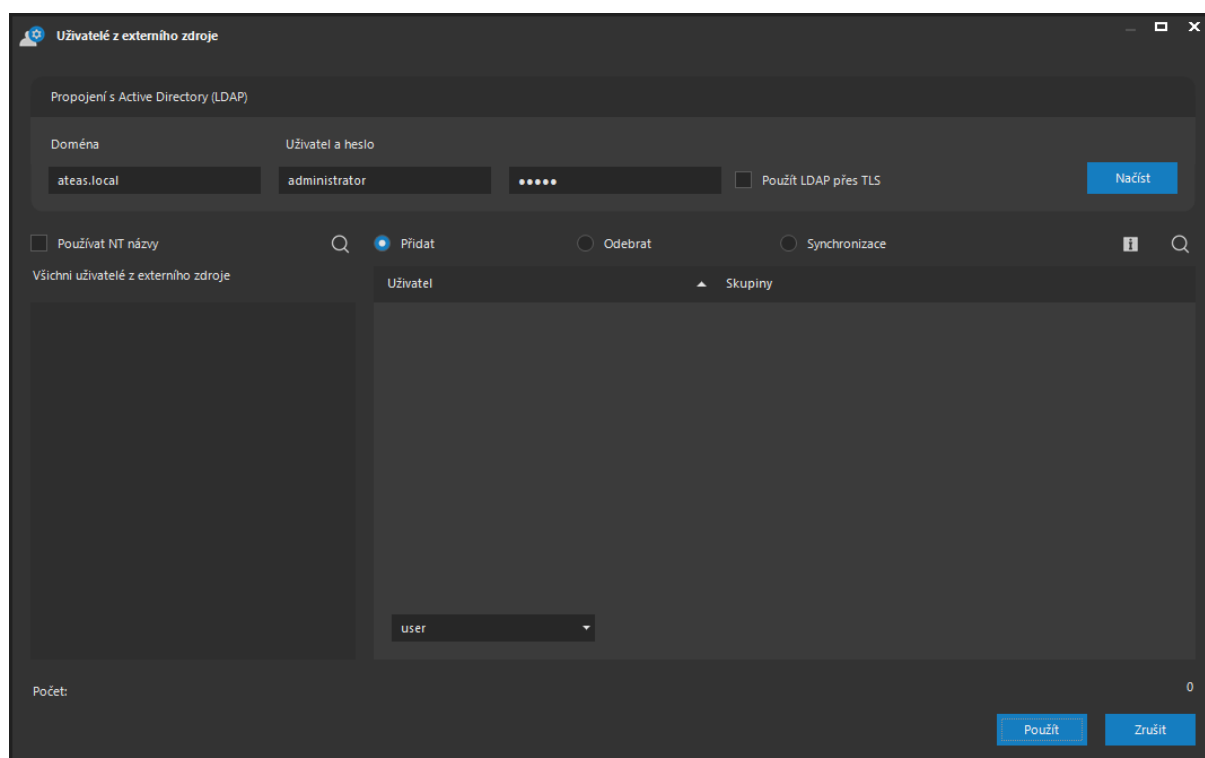
POZNÁMKA

Možnost integrace s Active Directory je k dispozici až od edice ATEAS Security PROFESSIONAL.

Nástroj lze aktivovat kliknutím na odkaz Externí vedle přepínačů uživatelů a skupin.



V horní části následujícího dialogu je možné zadat údaje pro připojení ke službě Active Directory. Vyžadováno je zadání domény, uživatele a hesla pro přihlášení do domény. Pomocí tlačítka **NAČÍST** je možné se připojit do domény a získat aktuální seznam všech uživatelských účtů, který je zobrazen v seznamu vlevo.



POZNÁMKA

Aby mohl být seznam získán, je nutné, aby administrační server systému ATEAS uměl vyhodnotit doménový název. Administrační server ATEAS musí být tedy součástí domény nebo do ní musí mít umožněn přístup.

POZNÁMKA

Po úspěšném načtení uživatelských účtů v doméně jsou použitý název domény a uživatelské jméno uloženy a automaticky zobrazeny při příštím otevření tohoto dialogu. Heslo je však nutné zadat vždy.

Pokud je aktivována volba Použít LDAP přes TLS, bude vytvořeno zabezpečené připojení. Namísto výchozího LDAP portu 389 bude využit LDAP port 636. Pro použití TLS musí mít doménový řadič řádně nainstalován správný certifikát. Zabezpečené připojení pak bude využito automaticky i při externí autentizaci uživatelů.

Na základě porovnání načtených uživatelských účtů z externího zdroje a uživatelských účtů vytvořených v ATEAS systému je možné pomocí přepínačů Přidat a Odebrat generovat rozdílové

seznamy. Volba Přidat zobrazuje seznam všech uživatelských účtů z externího zdroje, které ještě nejsou vytvořeny v ATEAS Security. Volba Odebrat zobrazuje seznam všech uživatelských účtů v ATEAS Security, které nejsou vytvořeny v externím zdroji.

Ve všech seznamech v dialogu je možné aktivovat vyhledávání pomocí příslušných tlačítek. Zejména to může být vhodné v seznamu přidávaných účtů domény, kde lze hledat a filtrovat dle příslušnosti ke skupinám.

Tlačítkem **POUŽÍT** lze provést hromadné přidání nebo odebrání všech vybraných uživatelských účtů a provést tak jedním kliknutím synchronizaci uživatelských účtů vytvořených v externím zdroji a v ATEAS Security. Při přidávání uživatelů do ATEAS Security je možné také vybrat skupinu uživatelů, do které budou uživatelé přidáni.

POZNÁMKA

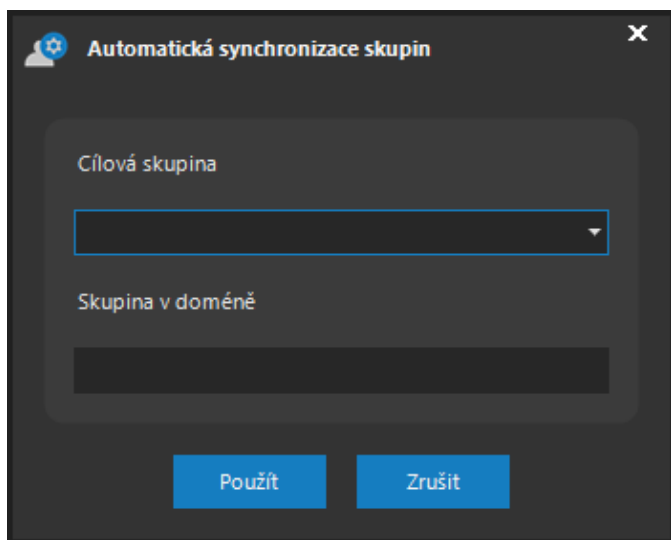
Použití vlastní skupiny uživatelů při přidávání uživatelů z externího zdroje je výhodné, protože je následně možné celé skupině nastavit profily ke kamerovým serverům a hromadně řídit jejich oprávnění a omezení v systému.

POZNÁMKA

Z hromadných operací pomocí této funkce je vyjmut master administrátorský účet admin.

Automatická synchronizace

Pomocí přepínače Synchronizace je možné zobrazit aktuální seznam pravidel pro synchronizaci skupin ATEAS a skupin v doméně. Tlačítkem **PŘIDAT** je možné doplnit nové pravidlo.



Jakmile jsou uložena nějaká pravidla pro synchronizaci skupin, bude tato synchronizace automaticky probíhat vždy po několika minutách. Interval je možné nastavit v pravé spodní části okna a potvrdit tlačítkem **ULOŽIT**. Výchozí hodnota je 5 minut. Tlačítkem **ODEBRAT** lze libovolné pravidlo odstranit.

POZNÁMKA

Synchronizace se bude týkat všech uživatelů, kteří jsou součástí skupiny v doméně, i pokud jsou zároveň součástí i jiných skupin.

Tvary uživatelských jmen

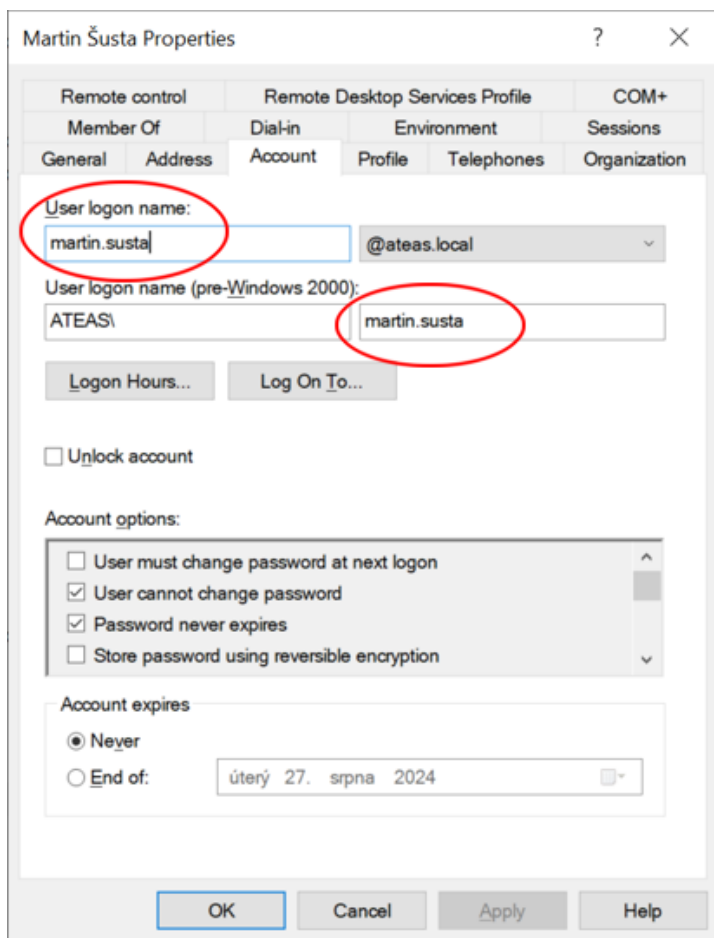
V prostředí správy uživatelských účtů v AD je možné pracovat se dvěma typy uživatelských jmen. Historicky byla uživatelská jména tvořena příjmením a úvodním písmenem křestního jména, které se uvádělo za označení domény, např.

ATEAS\NovakJ

Postupem času se začal více prosazovat tvar e-mailové adresy, kde doména následuje za znakem zavináče, např.

jan.novak@ateas.net

V nastavení AD se jedná o tyto dvě položky:



Martin Šusta Properties

Remote control Remote Desktop Services Profile COM+

Member Of Dial-in Environment Sessions

General Address Account Profile Telephones Organization

User logon name: martin.susta @ateas.local

User logon name (pre-Windows 2000): ATEAS\martin.susta

Logon Hours... Log On To...

☐ Unlock account

Account options:

- ☐ User must change password at next logon
- ☒ User cannot change password
- ☒ Password never expires
- ☐ Store password using reversible encryption

Account expires

☒ Never

☐ End of: úterý 27. srpna 2024

OK Cancel Apply Help

POZOR

ATEAS při externí autentizaci doménu doplňuje vždy automaticky, uživatel ji při přihlášení nepoužívá.

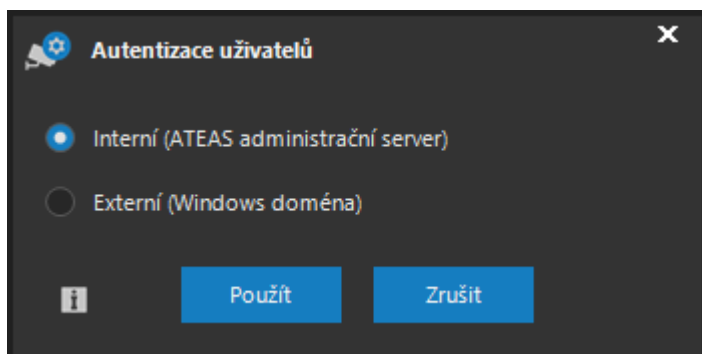
Pokud daná organizace používá různé tvary uživatelských jmen očištěné od doménové části, je nutné pro ruční a automatickou synchronizaci uživatelských účtů zvolit jednu z forem. To se provádí volbou Používat NT názvy. Jejím zaškrtnutím se aktivuje použije starších (NT) uživatelských názvů.

11.10.18. Způsoby autentizace

Výchozím způsobem autentizace uživatele v ATEASu je autentizaci interní, která znamená, že uživatelské jméno a heslo budou ověřeny ATEAS administračním serverem. Pro potřeby prohloubení integrace s Windows doménami je ovšem možné přepnout režim autentizace na externí. Změna se provede pomocí tlačítka **AUTENTIZACE**.

POZNÁMKA

Možnost externí autentizace je k dispozici až od edice ATEAS Security PROFESSIONAL.

**POZNÁMKA**

Změnu lze provést jak pro uživatele, tak pro celou skupinu.

Po přepnutí autentizace na externí, bude uživatelské jméno a heslo ověřeno přímo ve Windows doméně, která je nastavena jako externí zdroj uživatelských účtů. Vytvoření tohoto externího zdroje bylo popsáno v předchozí subkapitole.

POZNÁMKA

Ověření uživatelského účtu při externí autentizaci probíhá implicitně prostřednictvím administračního serveru, tudíž je možné externí autentizaci použít též pro mobilní či webové klienty systému.

POZNÁMKA

Funkce externí autentizace nemůže být použita pro administrátorský účet s číslem 1.

POZNÁMKA

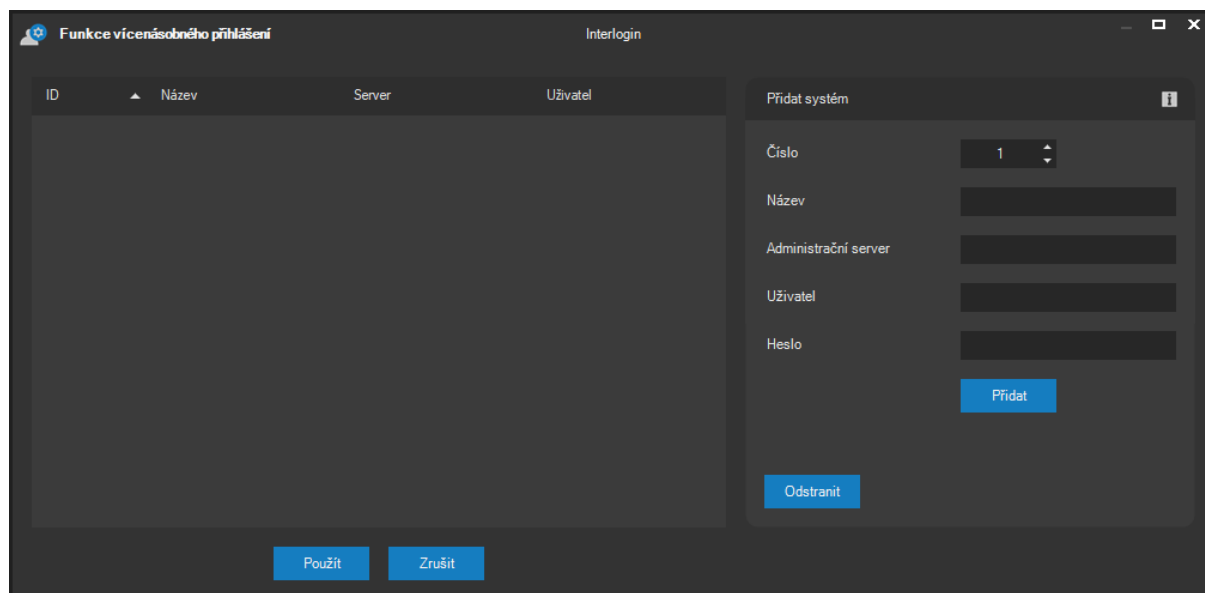
Při externí autentizaci nelze využít funkcí automatického přihlášení do systému.

11.10.19. Funkce ATEAS Interlogin

Běžně se uživatelé přihlašují vždy k jednomu kamerovému systému. Tento kamerový systém může pochopitelně sestávat z libovolného počtu kamerových serverů v rámci edice ATEAS Security UNLIMITED. Relativně často však vzniká potřeba, aby se uživatel mohl přihlásit současně k více kamerovým systémům ATEAS. Např. bezpečnostní agentury mohou od vlastníků licencí ATEAS obdržet účet s omezenými oprávněními pro možnost vzdáleného dohledu. Nastavení funkce vícenásobného přihlášení lze provést pomocí tlačítka **INTERLOGIN**.

POZNÁMKA

Použití této funkce nevyžaduje instalaci žádných dodatečných komponent, je nativní součástí platformy ATEAS.



Funkci Interlogin lze aktivovat jak pro jednotlivé uživatele, tak pro celou skupinu uživatelů. V předchozím dialogu je možné zadat jednoznačné číslo, uživatelský název, adresu či síťový název administračního serveru ATEAS a údaje pro přihlášení. Tlačítkem **PŘIDAT** lze kamerový systém přidat do seznamu a uživatel bude po příštím přihlášení (primární přihlášení) automaticky přihlášen i

k dalším kamerovým systémům (sekundární přihlášení) s přístupem k jeho kamerám, záznamu a událostem dle oprávnění.

POZNÁMKA

Před přidáním účtu v tomto dialogu je nutné nejprve provést primární přihlášení uživatele a změnu jeho hesla.

POZNÁMKA

Funkce ATEAS Interlogin je k dispozici pouze v edici ATEAS Security UNLIMITED. Všechny systémy přidané v rámci předchozího dialogu musí být edice PROFESSIONAL nebo UNLIMITED.

V porovnání s propojením všech serverů v systému v rámci jedné UNLIMITED licence, se funkce vícenásobného přihlášení liší v těchto směrech:

- Všechny systémy zůstávají nezávislé s vlastní licencí a správou.
- Nelze vytvářet událostní scénáře se zapojením serverů z různých systémů.
- Profil uživatele nemůže být LOCAL (je automaticky změněn na DEFAULT).
- Kamery v pohledech musí být vždy jen z jednoho kamerového systému.
- Pohledy s kamerami z jiného než primárního kamerového systému nelze sdílet.

POZNÁMKA

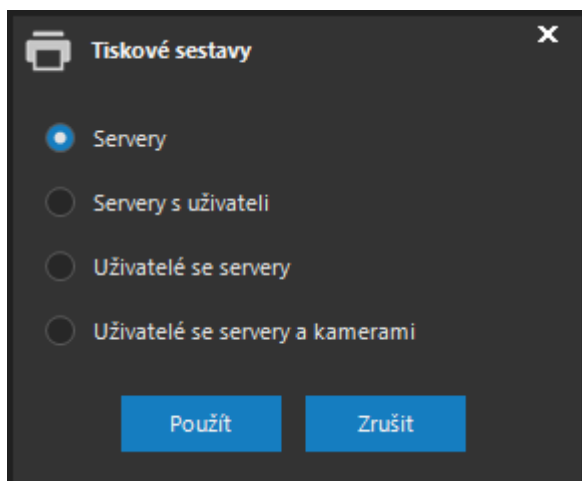
Funkci ATEAS Interlogin nelze řetězit. Pokud je funkce aktivována pro uživatele, který je již ovšem přihlášen do systému sekundárně, není nastavení účinné.

POZOR

Verze systémů pro vícenásobné přihlášení může být nižší než verze systému, kam je uživatel přihlášen primárně, musí však být minimálně 4.5.0.

11.10.20. Tiskové sestavy

Pro kamerové servery je možné pomocí tlačítka tisku v pravém horním rohu okna vytvořit několik tiskových sestav, jak ukazuje následující obrázek.



První sestava zobrazuje přehled všech kamerových serverů spolu s jejich základními údaji. Druhá sestava ke každému serveru přiřazuje uživatelské účty všech uživatelů, kteří mají k danému serveru zřízení přístup. Třetí sestava naopak zobrazuje seřazený seznam uživatelů a k nim přiřazené servery, ke kterým má uživatel zřízení přístup. Čtvrtá sestava pak k té předchozí přidává ještě informace o kamerách, ke kterým má uživatel zřízení přístup.

POZOR

Je-li uživatel součástí více skupin s různými oprávněními a jeho zařazení do skupiny je řízeno časem nebo událostí, výpis konkrétních kamer není možné pořádit a bude zobrazen výchozí stav bez zařazení do skupiny.

11.10.21. Systémový log

Systém (přesněji administrační server) provádí ukládání důležitých událostí v systému do systémového logu. Je tedy například možné kontrolovat, který uživatel a kdy pohyboval kamerou, který z uživatelů se do systému přihlásil a stáhnul nějakou záznamovou sekvenci apod. Náhled systémového logu je dostupný v části administrace uživatelů na kartě Systémový log.

Administrace uživatelů

Uživatelské účty **Systémový log**

pátek 10. března 2023

PO ÚT ST ČT PÁ SO NE

27 28 1 2 3 4 5

6 7 8 9 10 11 12

13 14 15 16 17 18 19

20 21 22 23 24 25 26

27 28 29 30 31 1 2

3 4 5 6 7 8 9

(všechni uživatelé) ▼

(všechny akce) ▼

(všechny servery) ▼

(všechny kamery) ▼

Hledat

Live Stream

Systém

Tisk

Datum	Uživatel	Akce	Adresa
9.3.2023 08:46:36	admin	Přihlášení	adresa 10.0.0.1
9.3.2023 08:47:20	admin	Živý obraz	server 1 kamera 1
9.3.2023 08:47:20	admin	Živý obraz	server 1 kamera 2
9.3.2023 08:47:20	admin	Živý obraz	server 1 kamera 3
9.3.2023 08:47:20	admin	Živý obraz	server 1 kamera 4
9.3.2023 08:47:35	admin	Živý obraz	server 1 kamera 1
9.3.2023 08:47:39	admin	Změna zařízení	server 1 kamera 1,2
9.3.2023 08:47:40	admin	Živý obraz	server 1 kamera 1
9.3.2023 08:47:42	admin	Živý obraz	server 1 kamera 2
9.3.2023 08:47:42	admin	Živý obraz	server 1 kamera 3
9.3.2023 08:47:42	admin	Živý obraz	server 1 kamera 4
9.3.2023 08:47:44	admin	Přehrávání záznamu	server 1 kamera 1 od 9.3.2023 08:47:43
9.3.2023 08:47:44	admin	Přehrávání záznamu	server 1 kamera 2 od 9.3.2023 08:47:43
9.3.2023 08:47:49	admin	Živý obraz	server 1 kamera 2
9.3.2023 08:47:51	admin	Přehrávání záznamu	server 1 kamera 2 od 9.3.2023 08:47:43
9.3.2023 08:47:54	admin	Živý obraz	server 1 kamera 2
9.3.2023 08:47:56	admin	Živý obraz	server 1 kamera 1
9.3.2023 08:47:59	admin	Přehrávání záznamu	server 1 kamera 2 od 9.3.2023 08:47:43
9.3.2023 08:47:59	admin	Přehrávání záznamu	server 1 kamera 1 od 9.3.2023 08:47:43
9.3.2023 08:51:13	admin	Přehrávání záznamu	server 1 kamera 2 od 9.3.2023 08:48:03
9.3.2023 08:51:13	admin	Přehrávání záznamu	server 1 kamera 1 od 9.3.2023 08:48:03
9.3.2023 08:51:20	admin	Živý obraz	server 1 kamera 1
9.3.2023 08:51:31	admin	Změna zařízení	server 1 kamera 1,2
9.3.2023 08:51:31	admin	Živý obraz	server 1 kamera 1

Archivační doba v měsících

Systémový log 2 **Změnit** Deník poplachů 4 **Změnit** Metadata **Změnit**

Hlavní seznam akcí zaznamenaný v logu obsahuje přesný čas akce, jméno uživatele a popis a detaily akce. Při požadavku na živý obraz je možné v doplňujících údajích zjistit, o jaký kamerový server a jakou kameru se jednalo. Při stahování záznamu, je možné kromě informací o kameře navíc dohledat také časové vymezení stahované sekvence, u pohybových akcí číslo presetu apod.

POZNÁMKA

Pro akci Přihlášení uživatele lze dohledat i IP adresu, ze které uživatel do systému přistoupil.

POZNÁMKA

Některé akce v logu nemusí mít nutně přiřazeného uživatele, např. pokud je zaznamenan neplatný pokus o přihlášení do systému.

Filtrování logu

V levé části okna máte možnost výběrem dne z ovládacího prvku kalendáře zobrazit náhled systémového logu ve vybraných dnech. V kalendáři se lze pohybovat mezi jednotlivými měsíci, při spuštění okna je datum nastaveno na aktuální. Pod kalendářem je dále možné filtrovat systémový log podle uživatele, typu akce, kamerových serverů a jednotlivých kamer.

POZNÁMKA

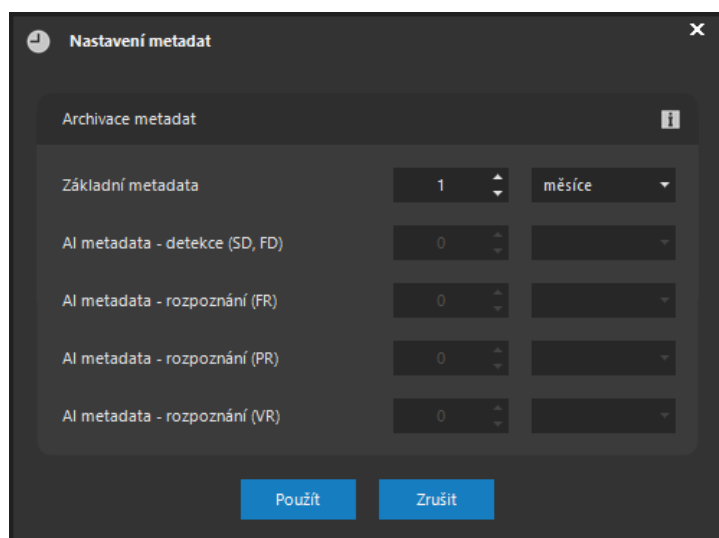
Pokud je událostí ve vybraném dni příliš mnoho, jsou pro lepší přehlednost aktivována listovací tlačítka pod seznamem, která umožní stránkovaný pohyb po systémovém logu.

Systémový log je pravidelně čištěn, aby s dobou provozu systému nenarůstal do zbytečně velkých rozměrů. Dobu archivace systémového logu můžete nastavit ve spodní části okna, po nastavení je třeba stisknout tlačítko **ZMĚNIT**. Implicitní doba archivace systémového logu jsou dva měsíce, lze nastavit v rozmezí od jednoho měsíce až do jednoho roku.

Vedle možnosti změnit dobu archivace systémového logu je možné ve spodní části okna též změnit výchozí dobu archivace deníku poplachů. Vlastní změna se provede stisknutím tlačítka **ZMĚNIT**. Implicitní doba archivace deníku poplachů jsou čtyři měsíce, lze nastavit v rozmezí od jednoho měsíce do čtyř let.

Archivace metadat

Podobně jako pro každý kamerový server lze i v případě aktivované centralizace metadat na administračním serveru nastavit dobu archivace jednotlivých skupin metadat pomocí tlačítka **ZMĚNIT**. V kontextu administračního serveru však lze měnit archivaci pouze u těch skupin metadat, které mohou být centralizovány.



Archivace metadat		
Základní metadata	1	měsíce
AI metadata - detekce (SD, FD)	0	měsíce
AI metadata - rozpoznání (FR)	0	měsíce
AI metadata - rozpoznání (PR)	0	měsíce
AI metadata - rozpoznání (VR)	0	měsíce

Použít Zrušit

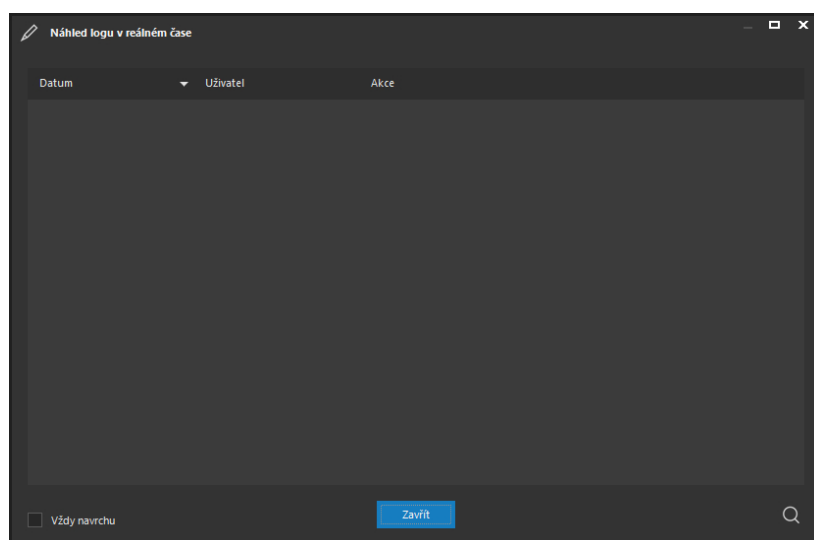
Tisk logu

Systémový log lze vytisknout na libovolnou tiskárnu včetně tisku do PDF souboru pomocí tlačítka **TISK** v pravém horním rohu okna. Po zobrazení tiskové sestavy lze v logu provádět stránkování pomocí kláves Page up a Page down.

POZNÁMKA

Vzhledem k tomu, že log může být pro daný výběr velmi rozsáhlý, je vždy vytištěna pouze jeho aktuální sekce zobrazená v okně. Pro vytištění další části je nutné tisk opakovat. Část logu a jejich celkový počet je součástí nadpisu v tiskové sestavě.

Zobrazení systémového logu v základním okně je statické, není tedy automaticky aktualizováno s výskytem nových akcí v systému zapisovaných do systémového logu (pro obnovu údajů je vždy třeba znovu kliknout na vybraný den kalendáře nebo zvolit uživatele). Pro online náhled systémového logu s dynamickou aktualizací slouží funkce dostupná přes tlačítko **LIVE ŠPEH**.



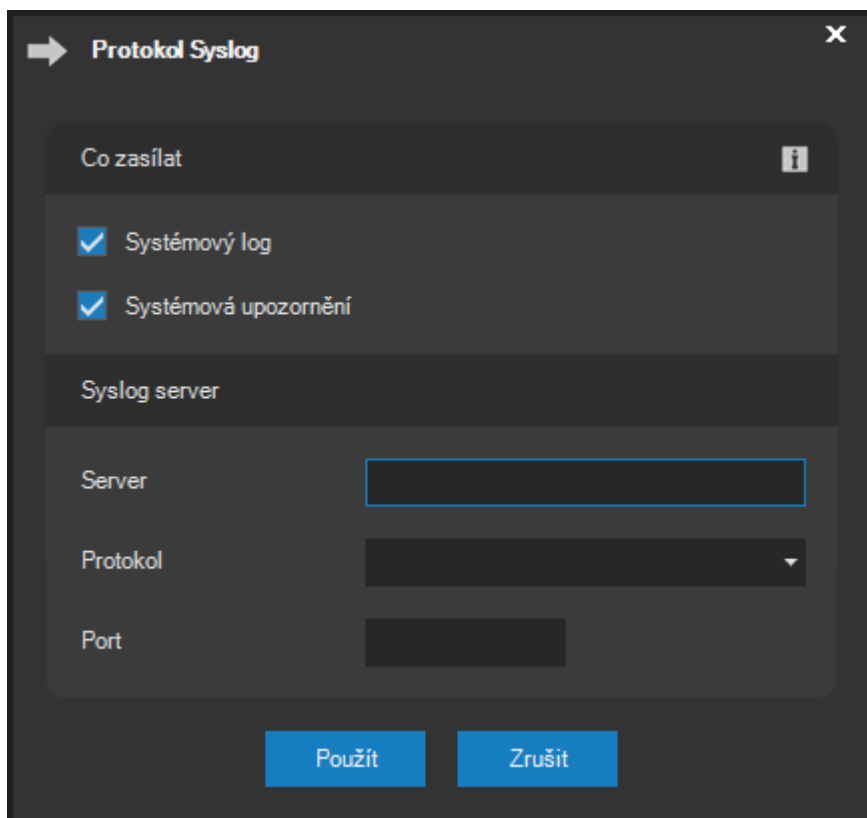
Toto okno si může administrátor nechat otevřené i po skončení práce v administrační části. V tomto okně je k dispozici živý a automaticky aktualizovaný náhled akcí zapisovaných do systémového logu, opět s možností zobrazit detailní či doplňující informace k akci. Zaškrtnutí políčko Vždy navrchu navíc zajistí, že tento špeh nebude překryt jinými okny systému Windows.

POZNÁMKA

V okně špeha systémového logu je určena maximální délka historie, při jejímž dosažení budou nejstarší zobrazené akce ze seznamu odstraňovány, aby nedošlo k neúměrnému růstu seznamu. Odstraňované události jsou samozřejmě nadále dohledatelné v historickém náhledu logu.

11.10.22. Podpora standardu Syslog

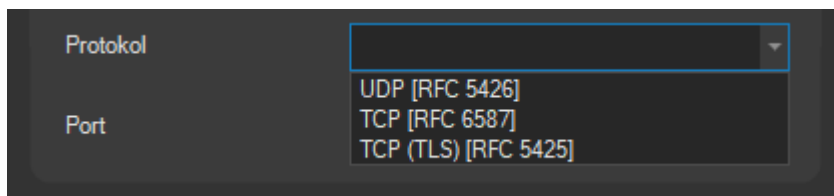
ATEAS podporuje protokol Syslog, který slouží pro standardizované zasílání zpráv z libovolného systému na Syslog servery, které sdružují zprávy z celé řady systémů a umožňují jejich filtrování, vyhledávání apod. Nastavení propojení na Syslog server lze provést po stisku tlačítka **SYSLOG**.



ATEAS implementuje protokol Syslog dle RFC 5424, což je novější verze protokolu než původně definovaný standard.

V dialogu je možné zvolit, zdali budou zasílány pouze položky systémového logu, tak jak je možné je vidět přímo v ATEAS systémovém logu, anebo také systémová upozornění jako je např. odpojení kamerového serveru, selhání záznamové oblasti anebo půlnoční informační zprávy.

V části Syslog server je možné zadat adresu či název Syslog serveru, vybrat přenosový protokol a případně také určit port. Pro výběr protokolu jsou k dispozici následující volby, z nichž každá je upravena jiným dokumentem RFC.



Váš Syslog server tedy musí vybraný protokol plně podporovat, aby mohl zprávy přijímat.

POZOR

Volby se liší nejen použitým transportním protokolem, ale také způsobem oddělení jednotlivých Syslog zpráv dle příslušných RFC, takže pokaždé jsou přenášena mírně odlišná data.

Při volbě UDP protokolu je automaticky přednastaven standardní Syslog port 514, který však můžete změnit.

Při volbě TCP přes TLS je automaticky přednastaven standardní Syslog port 6514, který však můžete opět změnit.

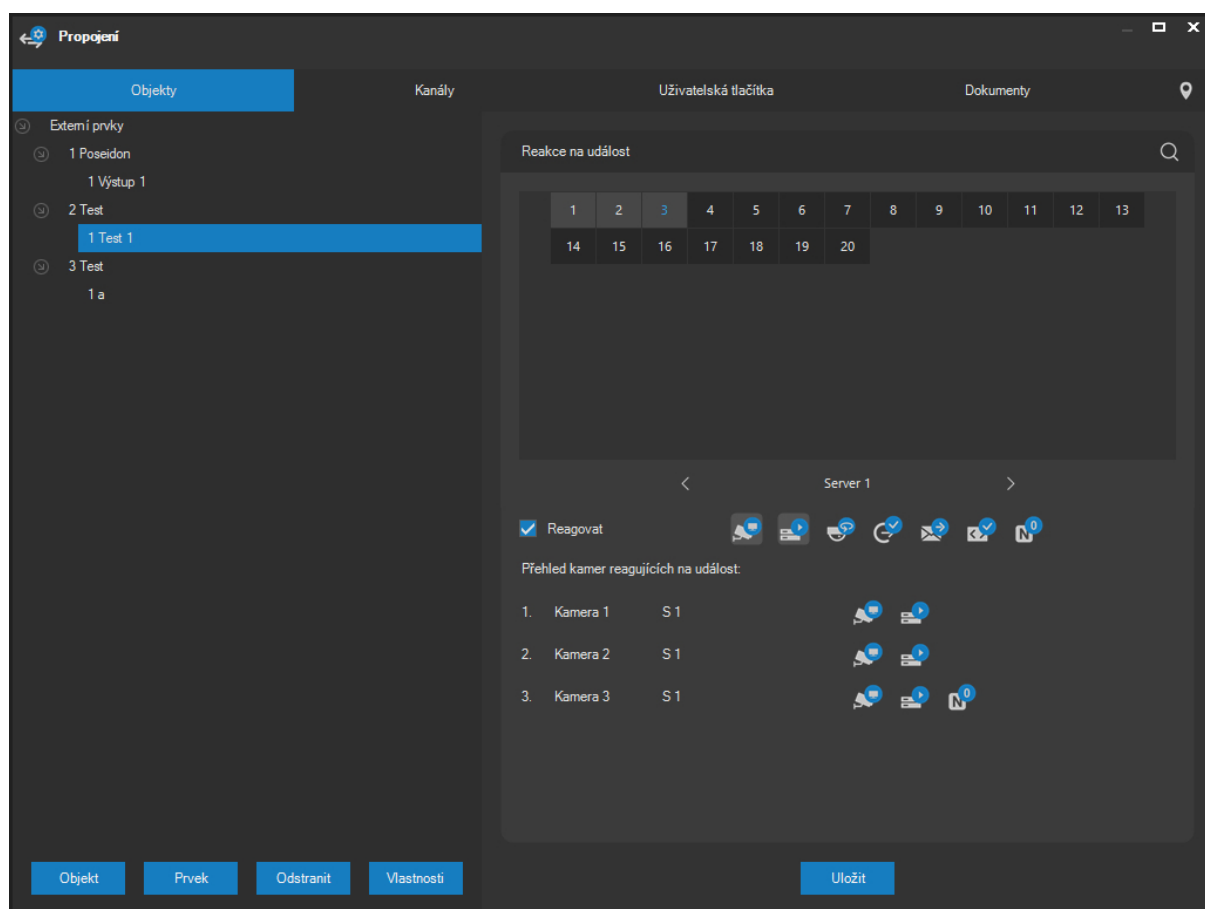
Při volbě TCP není standardem určený žádný port. Nicméně je přednastaven port 1514, který se (stejně jako další hodnoty jako je 2514 či 3514) nejčastěji používá.

11.11. Propojení

Volba propojení z hlavní nabídky Administrace slouží k otevření části, na kterém je možné vytvářet a editovat virtuální strukturu objektů a jejich prvků. Na základě přijímaných zpráv obsahující identifikaci těchto objektů je možné spouštět připravené kamerové událostní scénáře. Tímto způsobem je možné vynutit reakci uvnitř kamerového systému v závislosti na externí události v jiném systému.

11.11.1. Virtuální struktura objektů

Virtuální strukturu objektů lze vytvářet na kartě Objekty. Její struktura je dvoustupňová, jak je patrné z následujícího obrázku.

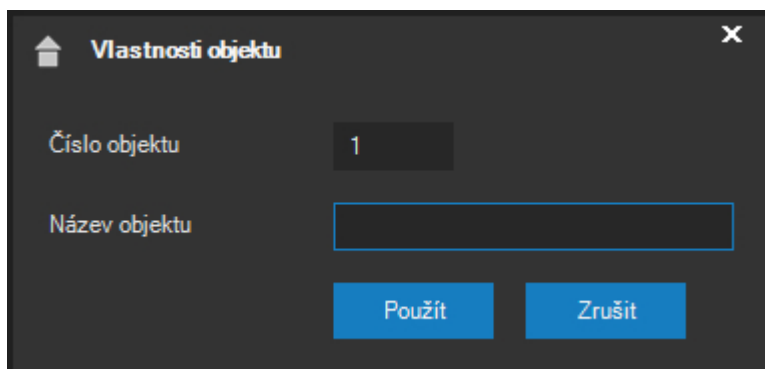


Terminologie používaná v ATEAS Security nazývá první úroveň termínem objekt či skupina a druhou úroveň termínem prvek. Struktura externích objektů může být vztažena na libovolný systém vzdáleného zabezpečení, zabezpečení objektů pomocí ústředí atd.

Přidání nového objektu (skupiny) lze provést odpovídajícím tlačítkem pod seznamem objektů.



V následujícím dialogu je zapotřebí vyplnit číslo objektu a jeho název.



Systém Vám automaticky navrhne nejmenší kladné volné číslo skupiny. Toto číslo samozřejmě nemusíte akceptovat a lze ho přepsat. Podmínkou je však použití jedinečného identifikátoru (systém kontroluje a reaguje varovnou zprávou pokud je zjištěna duplicita). Systém také pracuje s vnitřním omezením počtu skupin a prvků. Maximální počet skupin je 10 tisíc s maximálním počtem 99 prvků v jedné skupině, přičemž maximální hodnota čísla prvku může být pětimístné číslo. Při překročení těchto limitů bude aplikace reagovat varovnou zprávou.

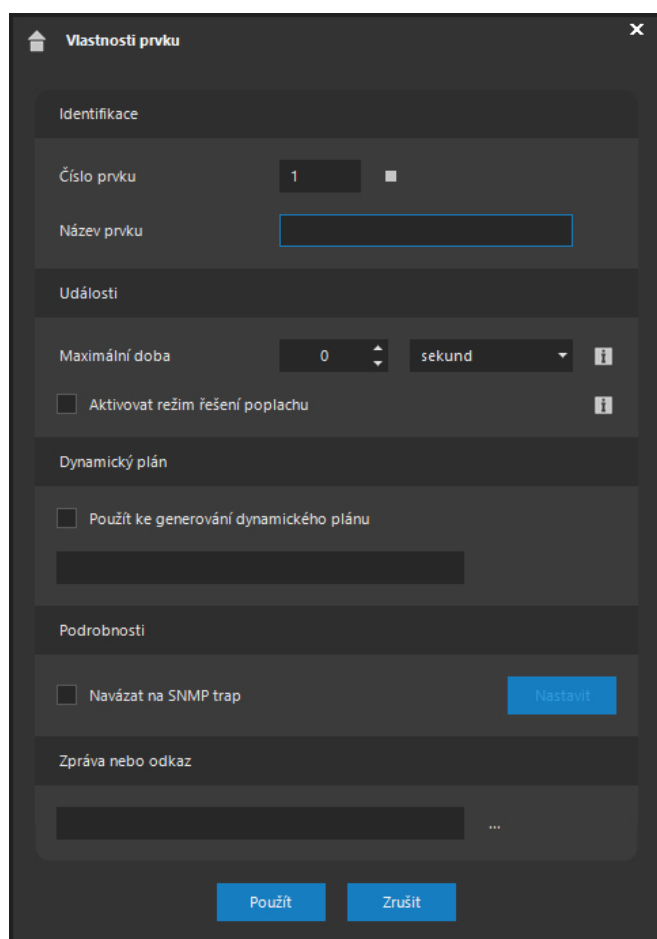
Vytvoření nového prvku se provede kliknutím na příslušné tlačítko.



Při použití tohoto tlačítka však musí být vybrána skupina (nebo její prvek), ve které má být nový prvek vytvořen, jinak se zobrazí varování a nebude možné nový prvek vytvořit. V následujícím dialogu je opět nutné vyplnit (nebo akceptovat navržené) číslo identifikující prvek, jeho název a maximální dobu trvání události v minutách. Tento parametr má shodný význam jako u nastavování událostních vstupů kamer. Parametr udává maximální dobu trvání události, pokud není událost ukončena pomocí ATEAS API rozhraní nebo SNMP zprávou.

Prvek je možné navázat na libovolný SNMP trap zaškrtnutím příslušné volby. O SNMP pojednává samostatná subkapitola dále v textu.

Po potvrzení tlačítkem **POUŽÍT** bude prvek přidán do určené skupiny.



Vedle čísla prvku je zobrazena aktuálně přiřazená barva. Barvu je možné změnit kliknutím na barevný symbol a vybrat jakoukoliv uživatelsky definovanou barvu. Tato barva je pak použita u událostí zobrazených na časové ose při přehrávání záznamu.

TIP

K původní výchozí barvě se lze rychle vrátit kliknutím pravým tlačítkem myši.

Zaškrtnutím volby Aktivovat režim řešení poplachu je možné pro daný zdroj události aktivovat rozšířený mód řešení poplachů. Více viz samostatná subkapitola Režim řešení poplachů.

Podobně jako u kamerové události může být událost objektu doprovazena zprávou pro uživatele, kterou je možné zapsat v části Zpráva nebo odkaz. Ke každému prvku lze přidat jinou textovou zprávu, případně – pomocí tlačítka vedle zprávy - také celý dokument ve formátu PDF nebo hypertextový odkaz (musí začínat protokolem http nebo https). Způsob vložení dokumentu a syntaxe

připojení dokumentu jsou shodné jako u kamerových událostí, kde je způsob vložení dokumentu popsán.

Libovolný prvek či celý objekt lze odstranit tlačítkem se symbolem odstranění. Před odstraněním prvku či objektu je ještě nutné potvrdit zprávu o odstranění. V případě odstranění objektu jsou nenávratně odstraněny také všechny jeho prvky.



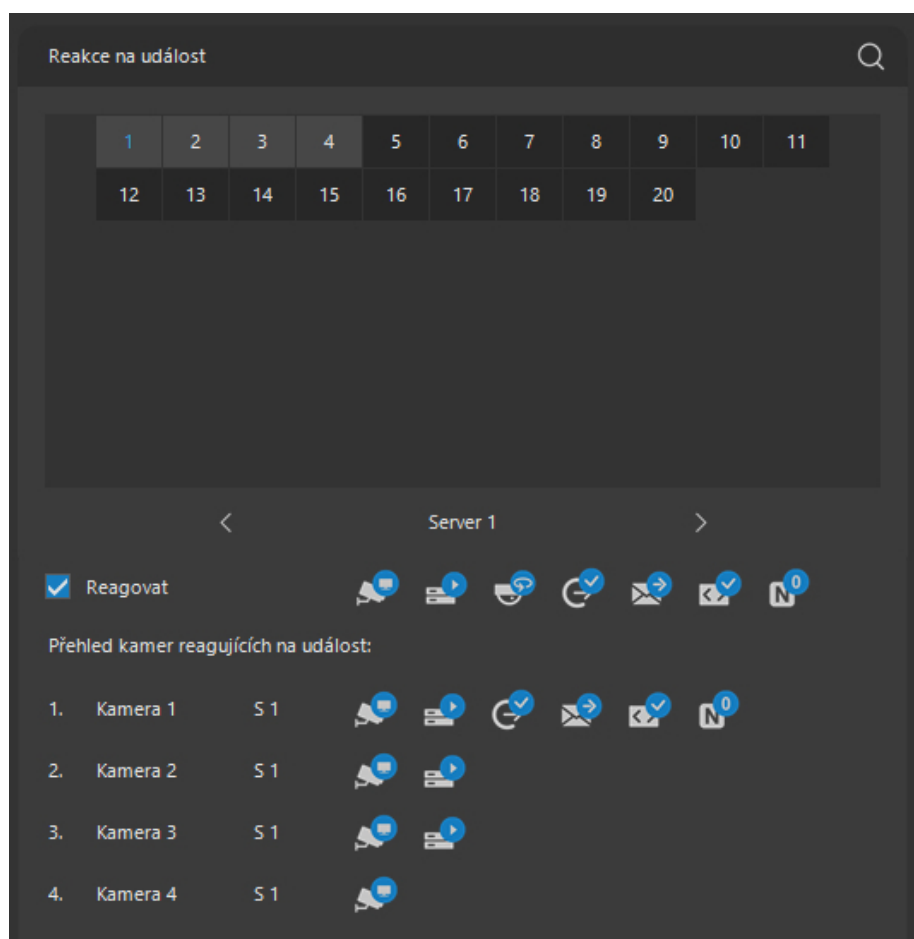
Pomocí tlačítka s popiskem Vlastnosti lze pro vybraný objekt či prvek upravit základní parametry.

POZNÁMKA

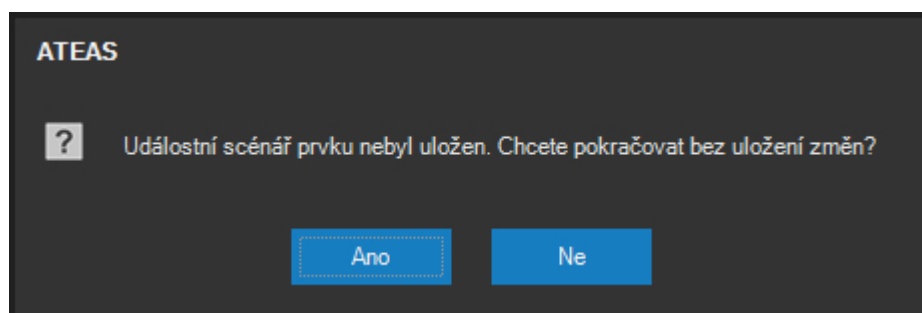
Dialog úpravy základních vlastností je shodný s dialogem vytváření nového objektu či prvku, pouze s vyloučením možnosti změnit některé údaje.

11.11.2. Vytváření událostních scénářů

Stejně jako u událostních vstupů z kamer (detekce pohybu, poplachové vstupy, výpadek, uživatelem definované události jako sabotáž či detekce zvuku) je možné pro jednotlivé prvky rozřazené do skupin vytvářet událostní scénáře. Při poplachu na čidle připojeného pomocí ústředny a PCO je tak možné automaticky přepínat vybrané kamery na monitor obsluhy, zahájit poplachové nahrávání, polohovat kamery či přepnout do poplachové tůry, odeslat e-mail, aktivovat výstupy atd. a to vše na více kamerových serverech. Nastavení událostního scénáře je zcela analogické jako u samotných kamer, tento popis je uveden v subkapitole o správě kamer.

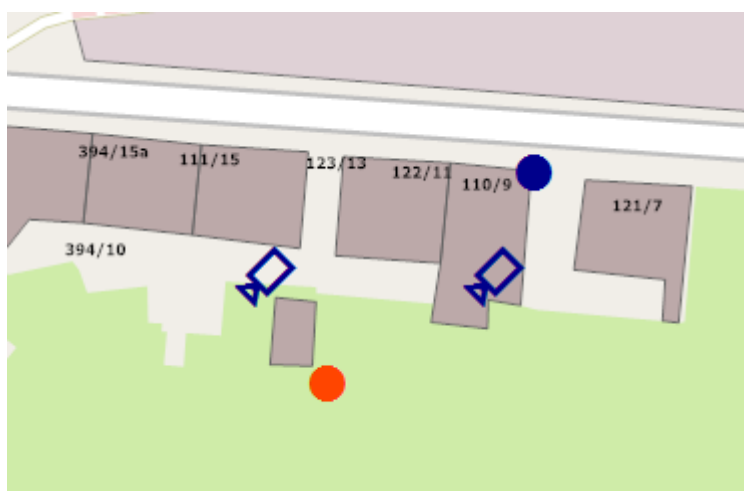


Jediným patrným rozdílem je tlačítko **ULOŽIT**, které se nachází pod virtuální strukturou objektů. Toto tlačítko slouží k explicitnímu uložení změn provedených v událostním scénáři. Pokud byste chtěli uzavřít formulář nebo provést přepnutí na jiný prvek, při existenci neuložených změn aplikace zobrazí zprávu. Stiskem tlačítka **NE** způsobíte, že aplikace nebude pokračovat v započaté akci, a budete tak mít možnost provedené změny uložit.



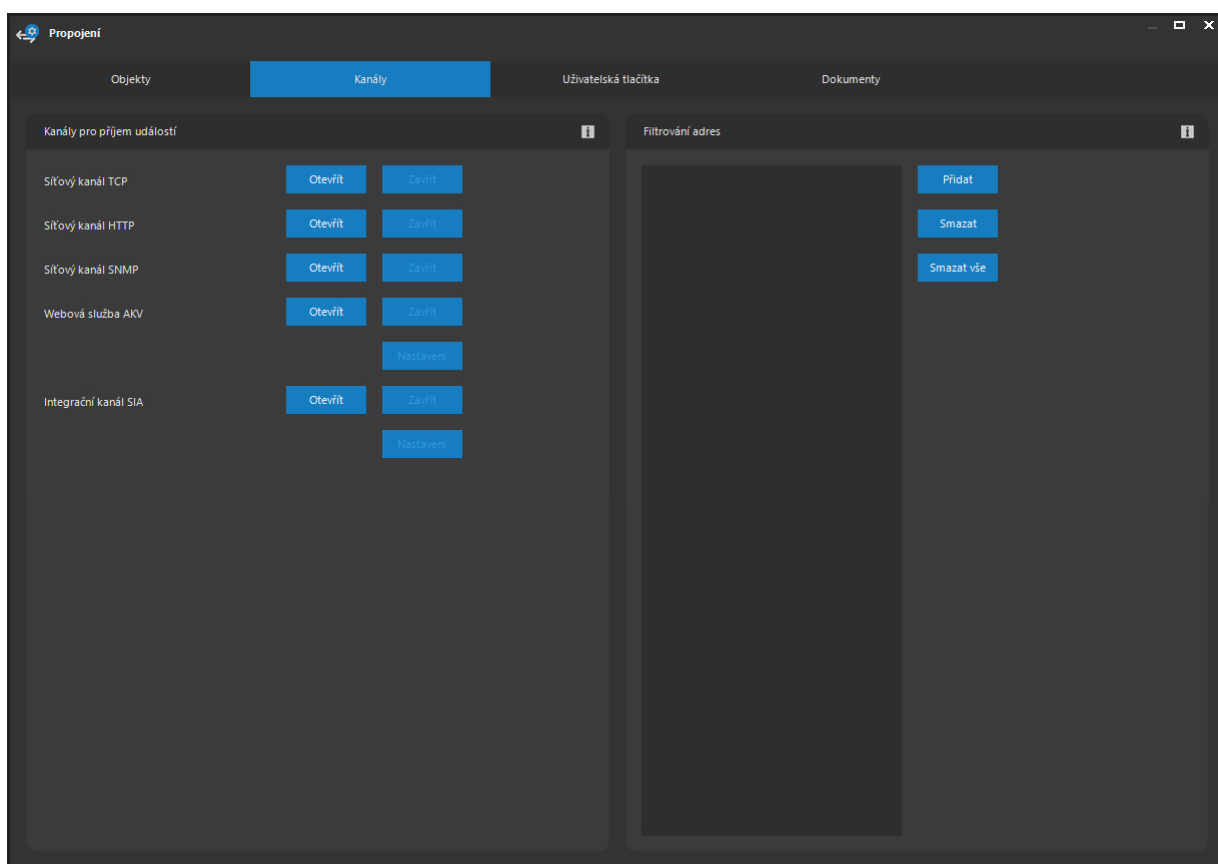
11.11.3. Umístění prvku do mapy

Podobně jako kamery mohou být i externí prvky lokalizovány v mapových podkladech. Postupy a techniky pro umístění prvku do mapy jsou obdobné jako v případě kamer a jsou popsány v kapitole Umístění kamery do mapy.



11.11.4. Komunikační kanály

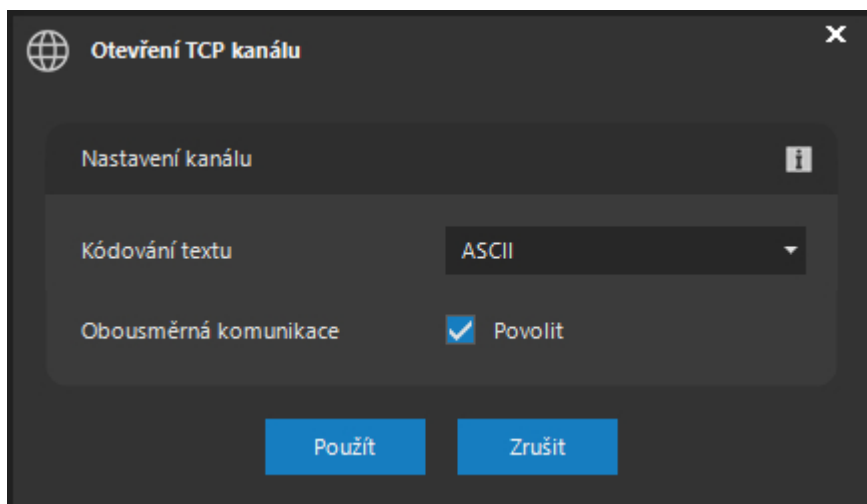
Pomocí ATEAS API je možné předat systému ATEAS Security informaci o události (poplachu) na některém z prvků, případně také informaci o jejím ukončení (není nutné, pokud je správně nastaven parametr maximální doby trvání události). Externí systémy mohou k předání těchto informací v textovém tvaru použít různé komunikační kanály. Komunikační kanály se spravují na kartě Kanály.



11.11.5. Síťový kanál TCP a HTTP

Kanály TCP a HTTP používají ATEAS API popsané v příloze této dokumentace. Kanál SNMP využívá SNMP trapů a je popsán dále v této kapitole. Všechny kanály jsou po instalaci administračního serveru zavřeny a musí být otevřeny pomocí tlačítka **OTEVŘÍT**.

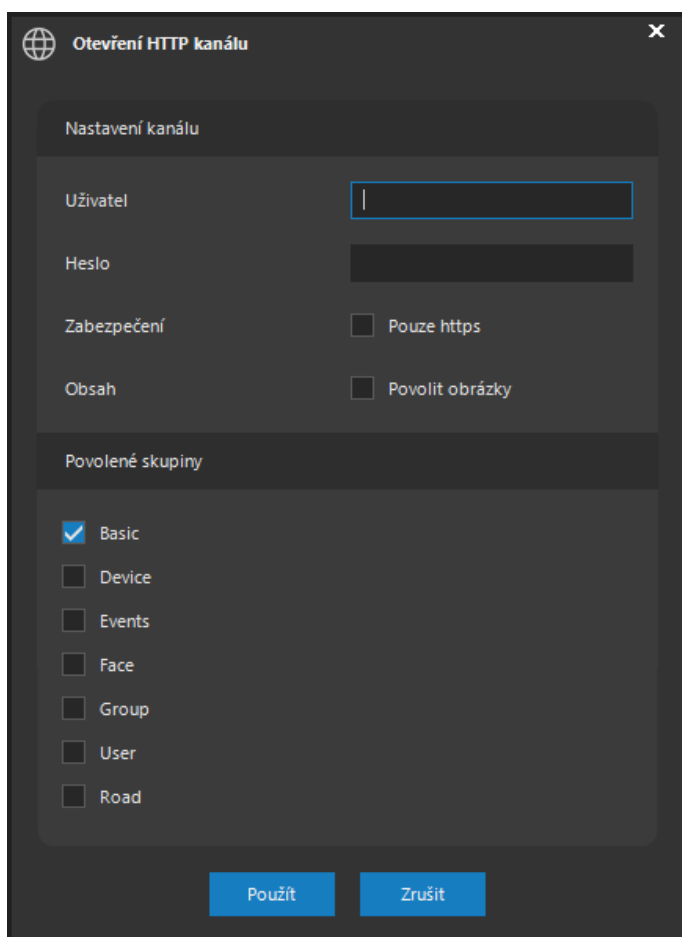
Pro TCP kanál je při otevření nutné zvolit kódování textu a případně povolit obousměrnou komunikaci.



TIP

Pokud je obousměrná komunikace zakázána, bude možné pomocí spojení pouze přijímat data, nikoliv zasílat příkazy.

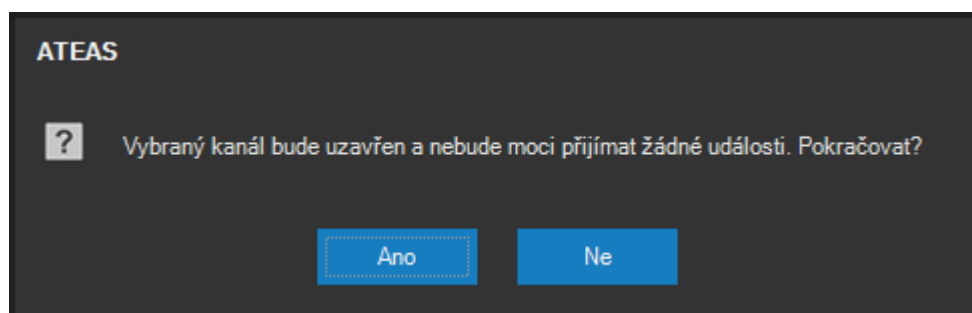
Pro HTTP kanál je při otevření možné zvolit přihlašovací údaje, které, pokud budou zadány, budou nutné pro HTTP autentizaci požadavku. Je také možné vynutit šifrovanou podobu spojení pomocí protokolu TLS. Volba Povolit obrázky aktivuje připojení přehledových či detailních obrazových dat (výřezů) do HTTP rozhraní. To se týká např. možnosti připojit přehledový snímek a výřez registrační značky při jejím rozpoznání.



V části Povolené skupiny je možné omezit skupiny API jen na skutečně používané skupiny, a zabránit tak používání jiných citlivých skupin.

U úspěšně otevřených kanálů bude k dispozici informační tlačítko, které po stisknutí zobrazí informace o komunikačních parametrech kanálu.

Zároveň bude také k dispozici tlačítko **ZAVŘÍT**, pomocí kterého je možné po potvrzení zprávy daný komunikační kanál uzavřít. Na uzavřeném komunikačním kanálu nadále není možné přijímat události.



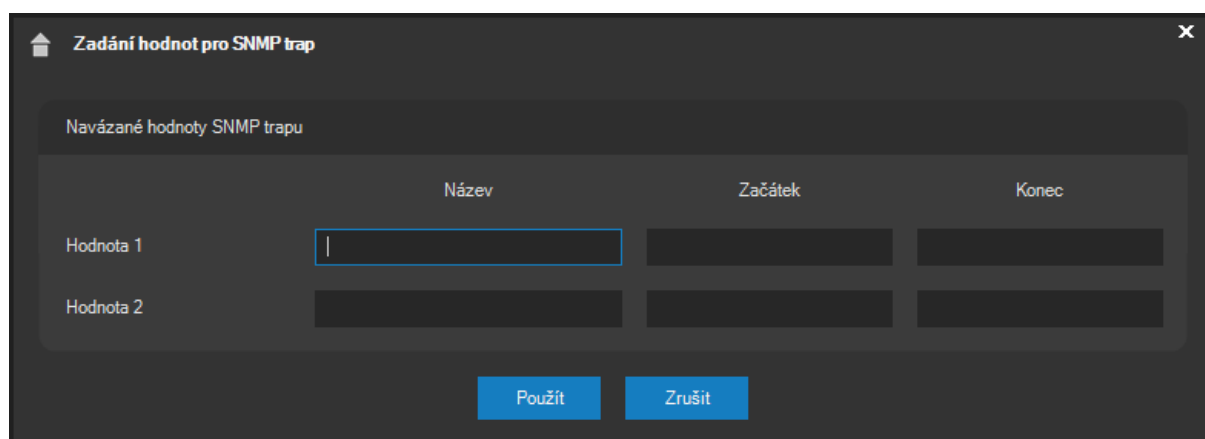
POZNÁMKA

Příjem příkazů po TCPIP kanálu lze omezit nástrojem filtrování IP adres, viz samostatná subkapitola.

11.11.6. Síťový kanál SNMP

Administrační server může přijímat externí události a reagovat na ně komplexními kamerovými scénáři. Externí zařízení poskytující události mohou být libovolného typu za předpokladu, že jsou schopna vyslat informaci o události jedním z podporovaných způsobů. V současné době se může jednat o příjem událostí pomocí vytvořeného TCP spojení, HTTP příkazů nebo pomocí protokolu SNMP. Příjem událostí pomocí SNMP je založen na standardech SNMP, a událost je tak přijata v podobě nevyžádané SNMP zprávy (SNMP trapu) standardně na portu 162.

Libovolnému objektu a jeho prvku lze přiřadit hodnoty SNMP zprávy, která bude tento prvek aktivovat, a dojde tak ke vzniku události. Pro navázání prvku na SNMP zprávu je nutné v okně prvku aktivovat volbu Navázat na SNMP trap a zvolit tlačítko **NASTAVIT**, které zpřístupní následující dialog.



	Název	Začátek	Konec
Hodnota 1			
Hodnota 2			

POZNÁMKA

Možnost navázání prvků na libovolné SNMP zprávy je k dispozici až od edice ATEAS Security PROFESSIONAL.

V tomto dialogu je nutné zadat název alespoň první hodnoty a vyplnit pole Začátek. Pokud se hodnota uvedená v poli Začátek s názvem uvedeným v poli Název vyskytne v přijaté SNMP zprávě, dojde ke vzniku události. Pokud je zařízení schopno informovat SNMP zprávou také o ukončení události, je možné zadat očekávanou hodnotu konce události do pole Konec.

POZNÁMKA

Pokud zařízení události neukončuje pomocí samostatných SNMP zpráv, lze doporučit nastavení maximální doby trvání událostí v nastavení prvku. Tím dojde k ukončení události po vypršení zadaného časového intervalu.

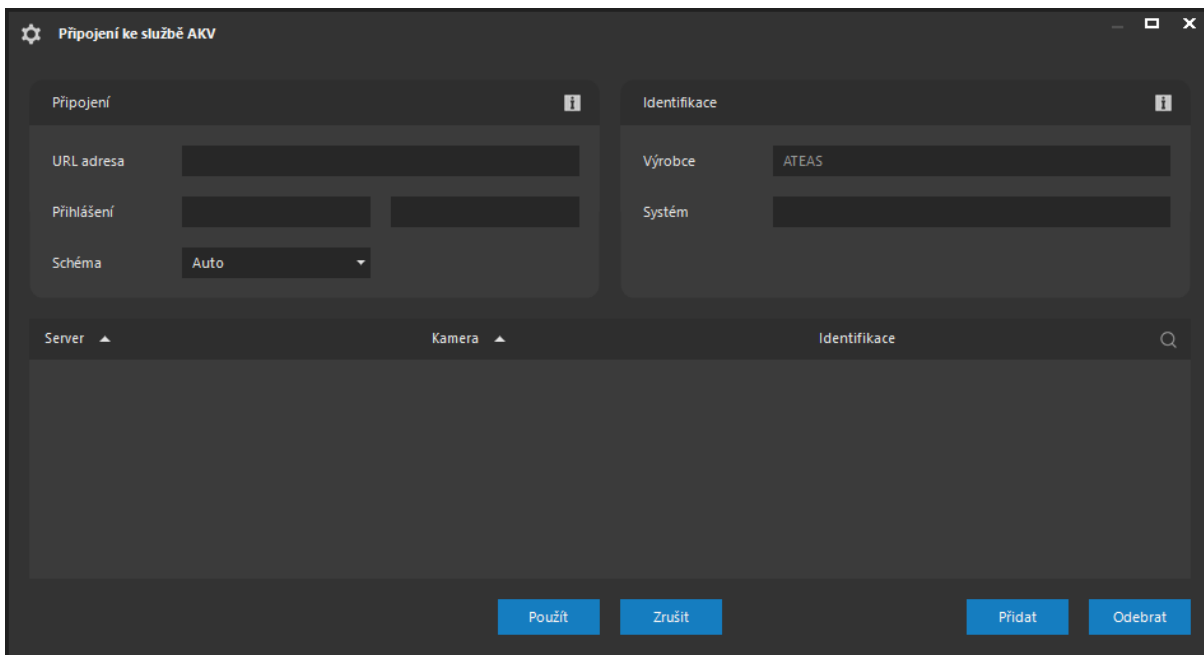
SNMP zprávy některých zařízení mohou být složeny z mnoha hodnot a nemusí být vždy možné vyhodnotit začátek události pouze na základě jedné hodnoty SNMP zprávy. Proto je možné zadat dvě hodnoty. Aby při použití dvou hodnot událost vznikla (resp. skončila) musí SNMP zpráva obsahovat vždy oba názvy s hodnotami Začátek (resp. Konec).

POZNÁMKA

Při použití obou hodnot nezáleží na tom, v jakém pořadí se hodnoty vyskytují v SNMP zprávě, ani na tom, zdali se jedná o dvě bezprostředně po sobě následující hodnoty.

11.11.7. Webová služba AKV

Webová služba AKV je provozována orgány státní správy České republiky a slouží k centralizaci informací o detekci a rozpoznání RZ vozidel.



Pro připojení služby je nutné obdržet adresu, kde služba běží, přihlašovací údaje a také identifikaci systému a kamer, které budou mít možnost údaje zasílat. Pomocí tlačítka **PŘIDAT** je možné zobrazit okno s možností vyhledat kameru pro přiřazení ke službě. Po přiřazení je nutné doplnit ještě přidělenou identifikaci dané kamery do sloupce Identifikace. Kameru je možné kdykoliv odstranit pomocí tlačítka **ODEBRAT**.

POZNÁMKA

Příslušný orgán musí zavést položku ATEAS jako podporovaný systém pro zasílání údajů.

Webové službě budou poté zasílány údaje o kameře a čase rozpoznání, RZ v textovém tvaru, obrázek výřezu RZ a celkový obrázek z kamery.

POZOR

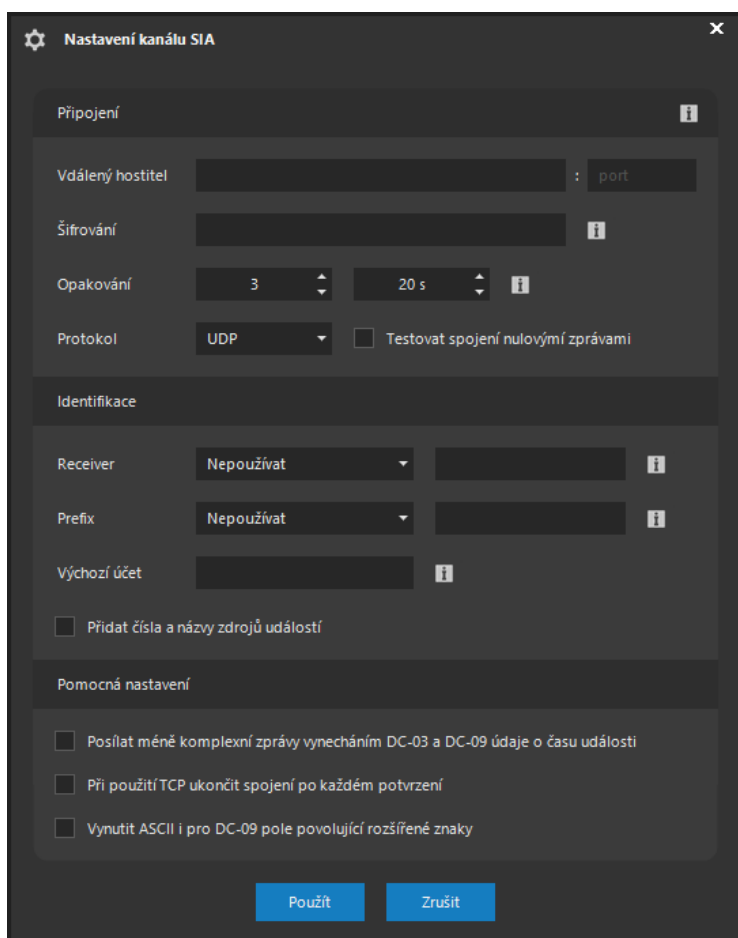
Zasílání obrázků bude aktivní, i pokud není povolena volba zasílání obrazových dat u HTTP komunikačního kanálu.

11.11.8. Integrační kanál SIA

Tento kanál umožňuje zasílat informace o poplachu pomocí SIA protokolu, který je průmyslovým standardem pro zařízení sdružující poplachy s různých systémů z důvodu jejich centralizovaného příjmu, zpracování a odbavování. ATEAS podporuje standardy DC-03, DC-07 a DC-09 pro přenos po IP.

POZNÁMKA

Možnost otevření SIA integračního kanálu je k dispozici až od edice ATEAS Security PROFESSIONAL.



Napojení na vzdáleného hostitele lze provést zadáním jeho názvu či adresy a portu, případně síťového protokolu a šifrování.

POZNÁMKA

SIA používá AES šifrování s délkou klíče 128, 192 nebo 256 bitů. Na obou stranách je tedy nutné zadat příslušný klíč s délkou 32, 48 nebo 64 znaků v hexadecimálním tvaru.

Dle SIA standardu jsou nepotvrzené zprávy několikrát zopakovány, počet opakování a časový rozestup jsou nastavitelné. U TCP spojení pak může být vhodné spojení testovat nulovými SIA zprávami, a zajistit si tak nižší latenci příjmu poplachu po výpadku spojení.

V části Identifikace je nutné vyplnit výchozí účet (objekt), který bude použit k identifikaci systému v místě centrálního příjmu poplachů. Jedná se o 16-bytovou hodnotu. Volitelně lze přidat též identifikaci a název zdroje události.

TIP

Hodnotu pro účet lze zadat také v hexadecimálním tvaru pomocí prefixu 0x.

Pokud je to vyžadováno místem centrálního příjmu poplachů, je možné identifikaci systému rozšířit o identifikaci v poli Receiver (nejméně specifické určení) a Prefix. ATEAS zde nabízí i možnost automatického použití jiných identifikátorů (ATEAS ID, ID serveru).

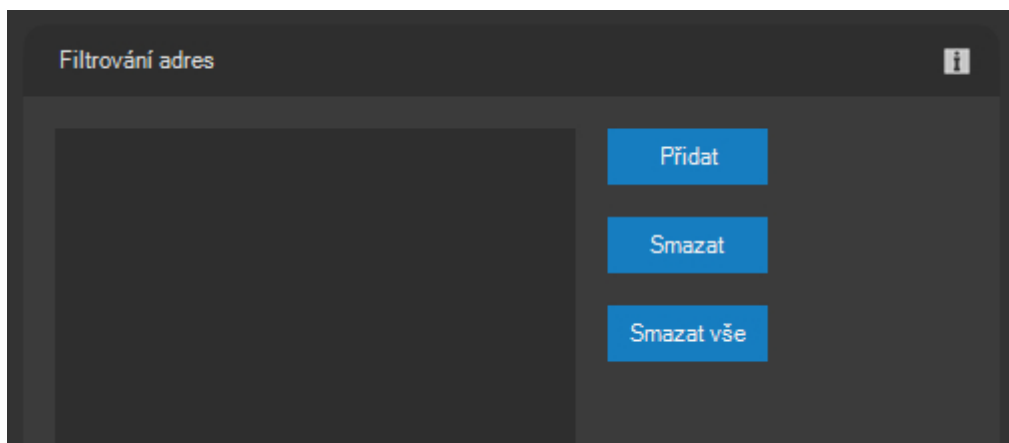
V části Pomocná nastavení je možné upravit chování tak, aby více vyhovovalo některým zařízením. Například je možné vynechat údaj o čase události (bude použit čas odeslání zprávy), vytvářet nové TCP spojení pro každou zprávu nebo vynutit ASCII znaky i v částech zprávy, kde standard DC-09 umožňuje rozšířené kódování.

POZNÁMKA

Identifikaci kamer lze dále samostatně upravit pro každou kameru v nastavení SIA identifikace kamery.

11.11.9. Filtrování IP adres

Jelikož TCP kanál není nijak zabezpečen, je možné pro něj použít nástroj filtrování IP adres, a omezit tak možnost komunikace jen na vybrané adresy.



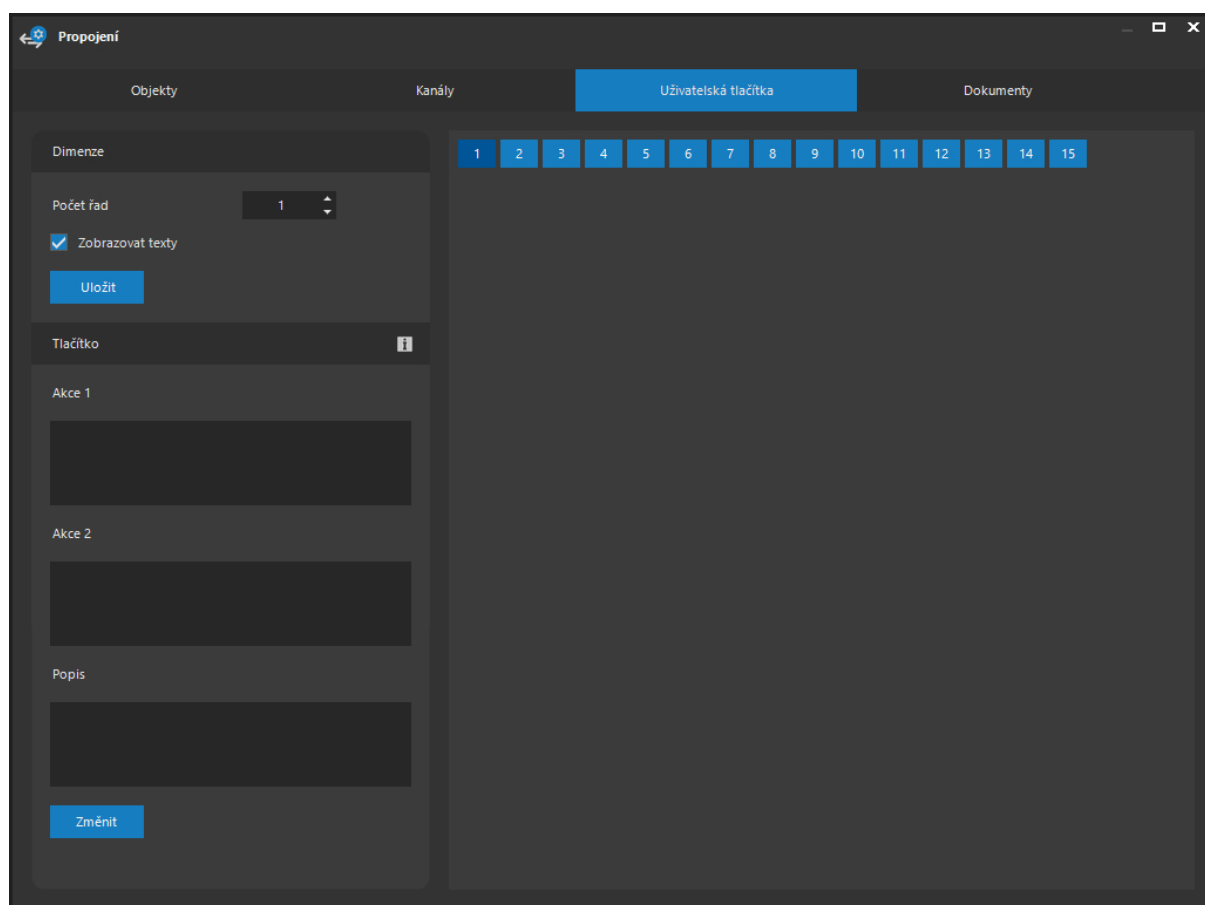
Pokud je pomocí tlačítka **PŘIDAT** do seznamu povolených adres vložena alespoň jedna IP adresa, bude administrační server akceptovat externí události, pouze pokud budou zaslány pomocí TCPIP spojení z dané IP adresy. Do seznamu je možné přidat libovolné množství adres, vybranou adresu lze odstranit pomocí tlačítka **SMAZAT**, celý seznam lze vymazat tlačítkem **SMAZAT VŠE**.

POZOR

Pokud není v seznamu žádná IP adresa, budou události či jiné příkazy ATEAS API zasílané po TCPIP akceptovány z libovolné adresy v síti bez její jakékoliv kontroly.

11.11.10. Uživatelská tlačítka

Na třetí kartě v okně administrace v části Propojení je možné provést nastavení uživatelských tlačítek. Uživatelská tlačítka jsou poté oprávněným uživatelům zobrazena v samostatném okně a mohou pomocí nich spouštět předdefinované příkazy pomocí protokolu http nebo https. Tyto příkazy mohou ovlivňovat funkce IP kamer, které by nebylo možné ovládat jiným způsobem, anebo mohou ovlivňovat jakákoliv externí zařízení dostupná přes protokol http.



V prvním kroku je nutné nastavit počet řad uživatelských tlačítek, která se budou uživatelům zobrazovat. Po stisknutí tlačítka **ULOŽIT** je v hlavní ploše okna zobrazen náhled uživatelských tlačítek.

POZNÁMKA

Při změně počtu řad jsou v otevřených oknech s uživatelskými tlačítky u uživatelů změny reflektovány okamžitě a to včetně situace vynulování počtu řad, po kterém je okno u uživatelů automaticky zavřeno.

POZNÁMKA

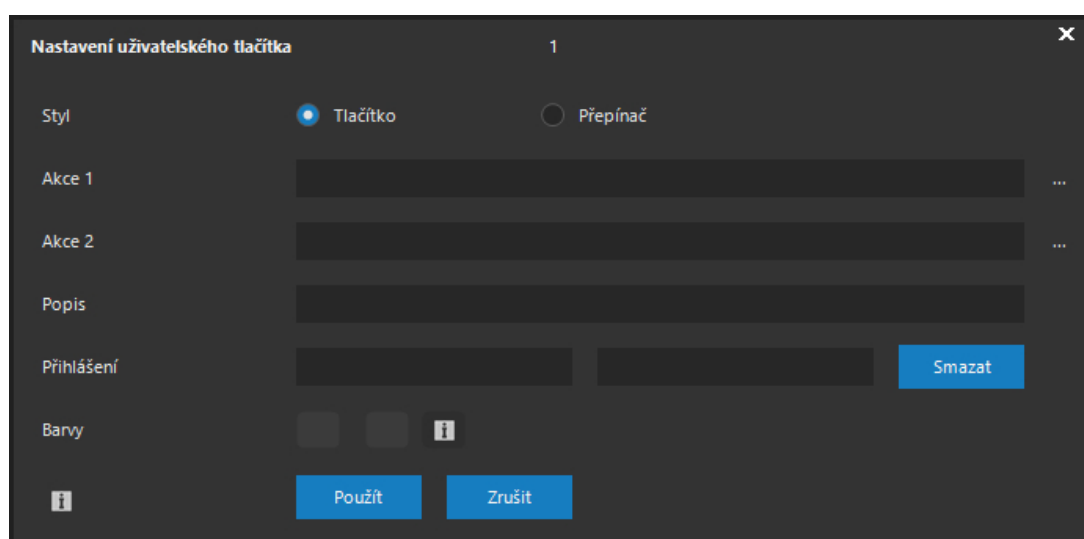
Okno s uživatelskými tlačítky může zobrazit pouze uživatel, který má nastaveno příslušné oprávnění nebo je součástí skupiny, která toto oprávnění má přiřazeno.

POZNÁMKA

Použití uživatelských tlačítek je automaticky zapisováno do systémového logu.

Aby uživatelské tlačítko mělo nějakou funkci, je nutné pro něj definovat styl, konkrétní akce a popis pomocí tlačítka **ZMĚNIT**. Volitelně je možné vyplnit přihlašovací údaje, pokud daná akce bude vyžadovat přihlášení.

Pokud je aktivována volba Zobrazovat texty, budou uživatelé namísto čísel tlačítek s popisem v podobě bubliny nad nimi vidět texty přímo na zvětšených tlačítkách.



Uživatelské tlačítko může být konfigurováno jako skutečné tlačítko nebo jako přepínač. Tlačítko slouží pro jednorázové spuštění jedné akce, zatímco přepínač zůstává po prvním stisku ve stisknutém stavu a při jeho uvolnění může být spuštěna samostatná akce. Uživatelské tlačítko ve stylu přepínače je tak ideální pro ovládání externích zařízení, které mají stav zapnuto a vypnuto.

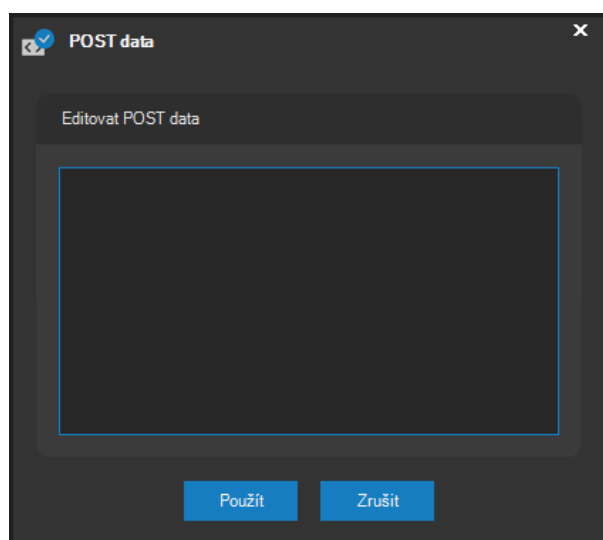
POZNÁMKA

Administrační server ATEAS udržuje stavy všech uživatelských tlačítek typu přepínač, ostatním právě přihlášeným uživatelům je tak zobrazení přepínačů automaticky synchronizováno.

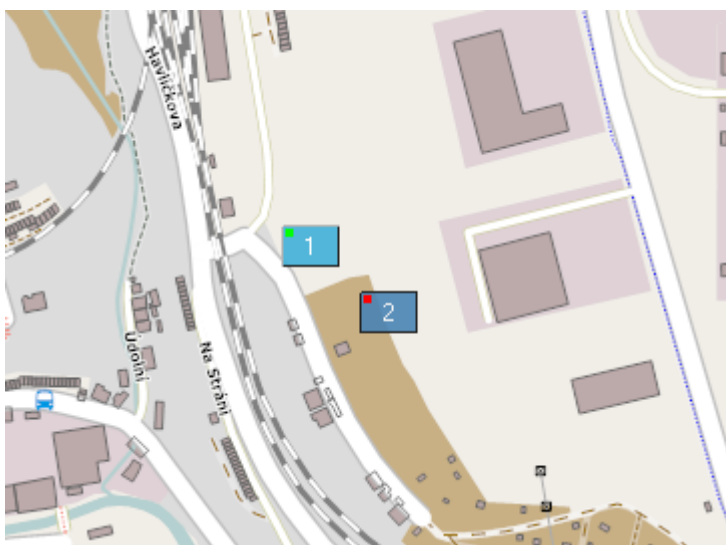
Po vyplnění dialogu pro jednotlivá tlačítka, jsou akce a popisy zobrazovány v příslušných textových polích v hlavním administračním okně.

Součástí akce mohou být také nejvýše čtyři parametry. Chcete-li do příkazu vložit parametr, použijte tvar <P1> až <P4>. Tyto části příkazu jsou variabilní a mohou být vyplněny konkrétní hodnotu až při samotném použití uživatelského tlačítka. Parametry lze s výhodou použít u příkazů, kde chceme dát uživateli volnost v nějaké z jeho částí (např. určení doby aktivace nějakého zařízení apod.).

Přestože zapsaná URL mohou obsahovat příkazy včetně např. parametrů pro CGI skripty, některá zařízení mohou vyžadovat zaslání dat jinou než HTTP GET metodou. Pomocí tlačítka za textovým polem lze otevřít dodatečný dialog pro zadání dat pro HTTP POST.



Uživatelská tlačítka mohou být lokalizována v mapě. To je výhodné všude tam, kde uživatelská tlačítka ovládají externí zařízení, která jsou lokalizovatelná v mapových podkladech, a uživatel tak může externí zařízení ovládat přímo pomocí tlačítka v mapě. Jiným možným využitím lokalizovaných uživatelských tlačítek je spouštění událostní scénářů připojených k tomuto tlačítku (např. natočení PTZ kamer na dané místo prostřednictvím presetů). V tomto případě musí být pro některou kameru vytvořena vlastní událost se systémovým názvem ATSBUTTON<n>, více viz kapitola o vlastních událostech.



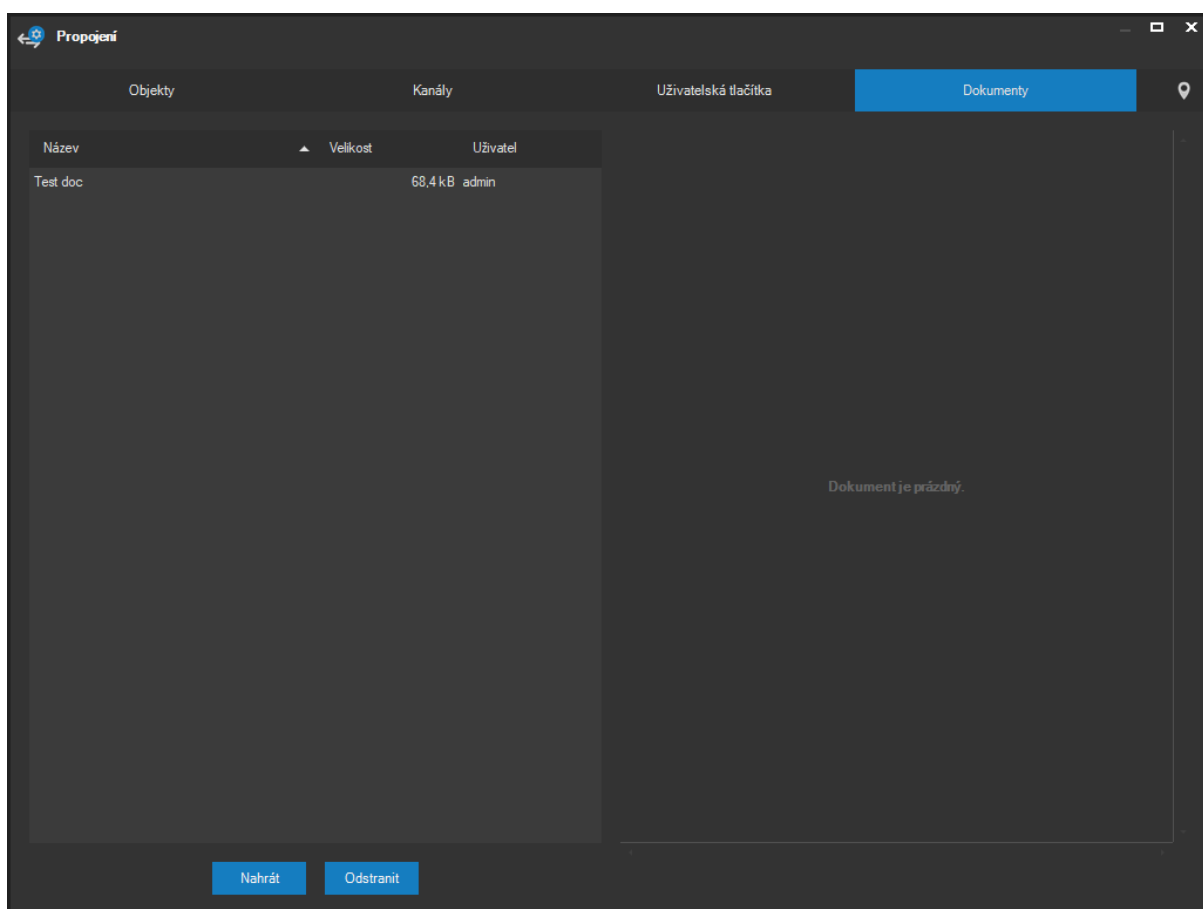
POZNÁMKA

Lokalizace uživatelských tlačítek probíhá zcela shodně jako v případě lokalizace kamer.

Ve výchozím nastavení jsou u tlačítek umístěných v mapě použity základní barvy pro odlišení stavů u tlačítka typu přepínač. Tyto barvy lze změnit a zároveň také vynutit jejich použití i v okně uživatelských tlačítek nastavením barev u položky Barvy. Samostatně lze nastavit barvu pro nesepnutý a sepnutý stav tlačítka.

11.11.11. Integrace dokumentů

Na kartě Dokumenty je možné do systému nahrát dokumenty, které lze poté použít v nejrůznějších situacích podporujících procesy kamerového zabezpečení. Např. lze uživatelům při řešení konkrétních poplachových situací namísto jednoduché uživatelské zprávy zobrazit dokument obsahující podrobnější instrukce, schéma objektu či jakékoliv další informace.



V levé části okna je zobrazen seznam všech vložených dokumentů včetně jejich názvu, velikosti a uživatele, který dokument do systému nahrál. Kliknutím na dokument lze zobrazit jeho náhled v pravé části okna.

POZNÁMKA

Podporován je formát PDF, dokument tedy může obsahovat různě formátovaný text, obrázky, schémata, tabulky apod.

POZNÁMKA

Pro manipulaci s dokumenty PDF není nutná instalace žádné dodatečné komponenty pro práci s PDF formátem, ATEAS podporuje PDF formát nativně, a proto vždy postačí jen nainstalovat klienta kamerového systému.

Pro nahrání nového dokumentu do systému lze použít tlačítko **NAHRÁT**. Po zadání názvu dokumentu bude možné dokument vyhledat pomocí dialogu otevření souboru a nahrát. Tlačítkem **ODSTRANIT** lze dokument smazat.

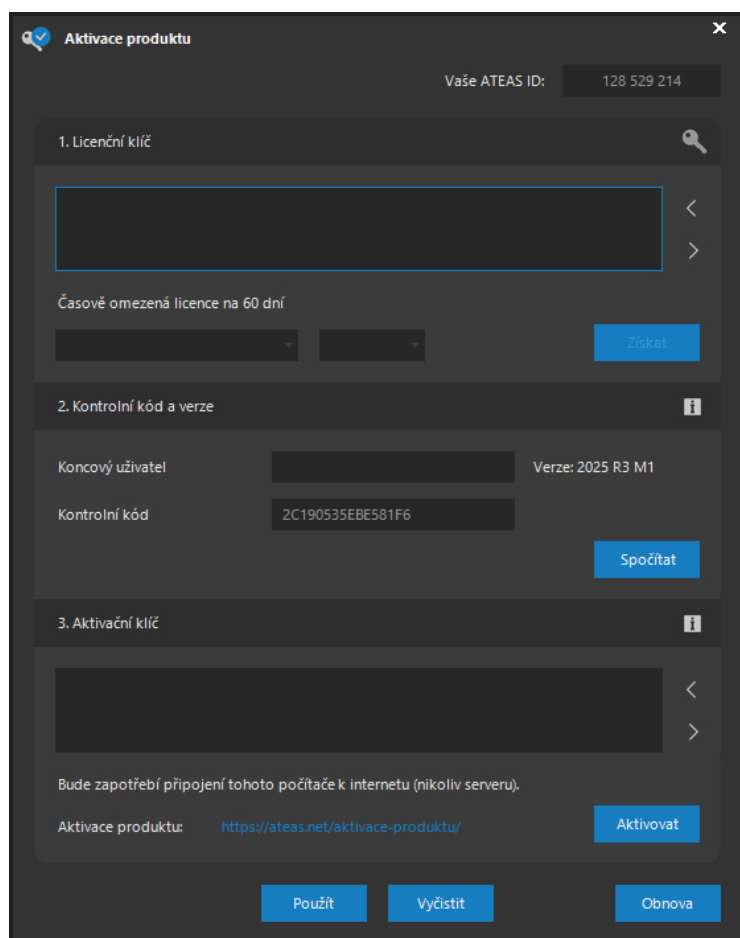
POZOR

Velikost nahrávaného dokumentu je omezena.

11.12. Licence a aktivace

11.12.1. Licenční klíče a jejich aktivace

Po úvodní instalaci systému (administračního serveru) nebo kdykoli během práce se systémem je možné provést zadání licenčního klíče, které povede k počátečnímu nastavení nebo povýšení edice produktu a nastavení nebo rozšíření počtu kamer a současných přístupů do systému. Každé licenční číslo je nutné aktivovat přes servery ATEAS.



Při upgrade licenčního klíče se na administračním serveru zvýší počet kamer, který je možné připojit do systému. Tento počet je u edic HOME či PROFESSIONAL automaticky navýšen pro vytvořený kamerový server, který je součástí systému. Pro edici UNLIMITED, kde je možné vytvářet více kamerových serverů, však platí, že distribuce licencí musí být provedena ručně.

Do části Licenční klíč je nutné zadat Vámi zakoupené licenční číslo produktu. Toto licenční číslo je možné zkopírovat nebo vložit přímo z licenčního souboru, který byl přiložen k aktivačnímu e-mailu. Vložení licenčního klíče přímo ze souboru lze provést pomocí tlačítka s bílou šipkou. Licenční klíč je automaticky dešifrován a označení edice a počet kamer se objeví nad ním.

Nemáte-li zakoupené licenční číslo, je možné automaticky získat zkušební licenci na 60 dní. K tomu postačí vybrat edici, počet kamer a použít tlačítko **ZÍSKAT**. Z testovací licence je možné kdykoliv přejít na zakoupenou licenci bez časového omezení.

POZOR

Licenci v systému není možné ponížít na nižší edici nebo nižší počet kamer. Na to je třeba pamatovat, pokud plánujete pozdější přechod na zakoupenou licenci.

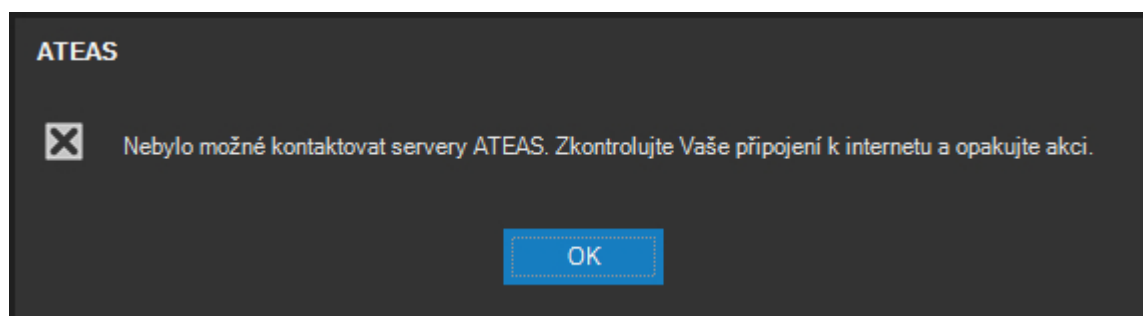
Část kontrolní kód obsahuje číslo jednoznačně svázané s Vaším systémem. Toto číslo je nutné použít, pokud aktivujete systém ručně přes webové stránky výrobce ateas.net.

Kontrolní kód je kromě základních vlastností počítače také svázán s názvem koncového uživatele zakoupené licence, který je nutné při aktivaci vyplnit a použít tlačítko **SPOČÍTAT** pro vygenerování kontrolního kódu.

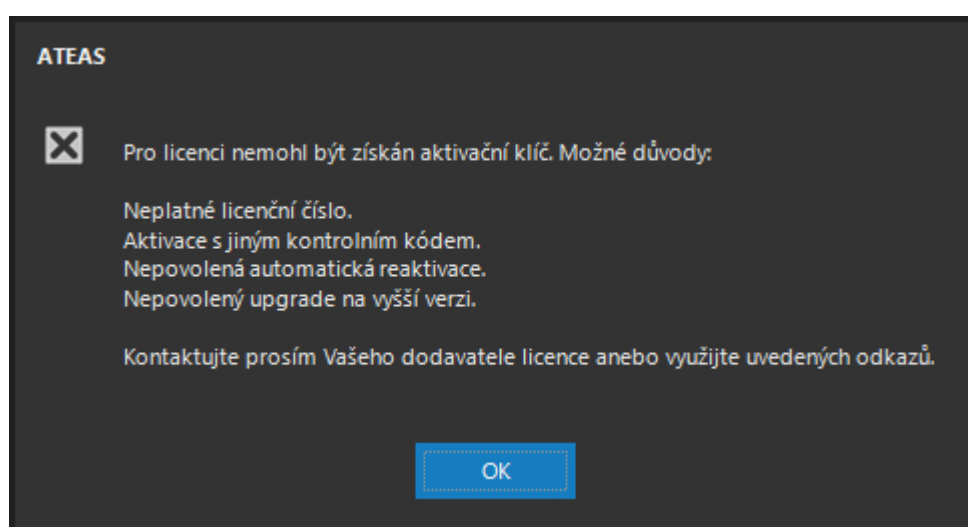
POZOR

Název koncového uživatele musí být uveden dle skutečnosti. Název si mohou uživatelé systému zobrazit a v případě nesouladu by měli žádat o zjednání nápravy. Systém s nepravdivým označením koncového uživatele je považován za nesprávně licencovaný.

Každé licenční číslo je nutné aktivovat. Pokud je Váš počítač (klient kamerového systému) připojen k internetu, můžete aktivační klíč získat během několika vteřin pouhým kliknutím na tlačítko **AKTIVOVAT**. Pokud není možné se připojit k internetu a serverům ATEAS, zobrazí se následující zpráva.



Pokud se připojení podaří, ovšem selže pokus o aktivaci Vaší licence, bude varovná zpráva vypadat následovně.



V prvním případě je nutné zkontrolovat Vaše připojení k internetu a případně pro aktivaci licence použít webovou stránku. Ve druhém případě byl pokus o aktivaci licence aktivně odmítnut. Může se jednat o pokus opětovné aktivace stejného licenčního čísla ovšem s jiným kontrolním kódem, nebo jste licenční číslo zadali chybně. Případně se také může jednat o nepovolený upgrade na vyšší verzi, pokud nemáte již žádné volné aktualizace k dispozici, nemůže být Vaše licenční číslo aktivováno s novou verzí produktu. Pokud se aktivace nedaří, můžete vyzkoušet aktivaci přímo na webové stránce výrobce, kde se můžete dozvědět více o příčinách Vašeho chybového stavu.

POZNÁMKA

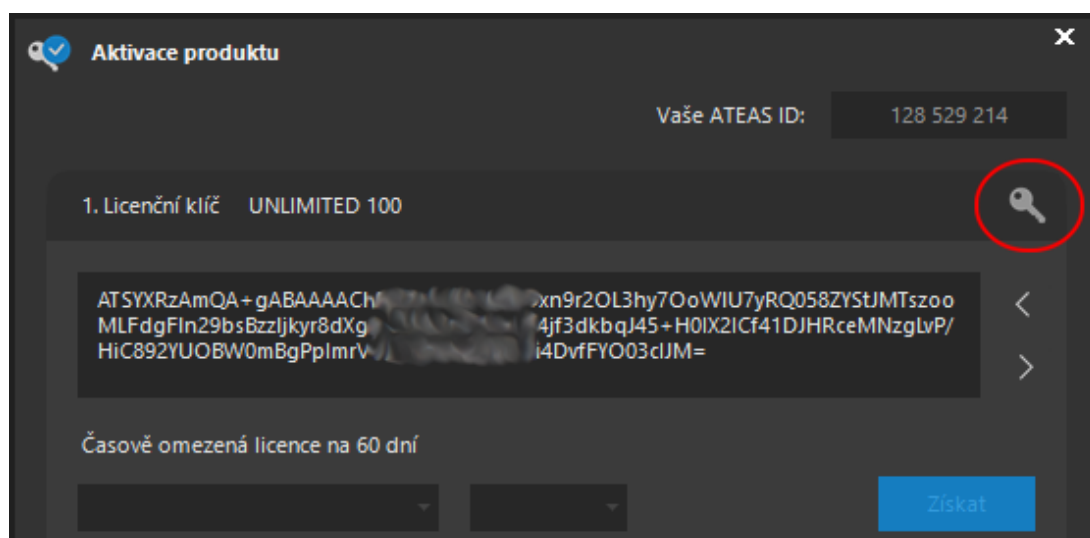
Při kompletní reinstalaci ATEAS ve stávajícím prostředí Vašeho počítače a operačního systému je samozřejmě bez problémů možné Vaši licenci aktivovat kdykoliv znovu.

U aktivovaných systémů vyjma systémů se zkušební licenci se v licenčním dialogu zobrazí také hodnota ATEAS ID, která jednoznačně identifikuje Váš systém a je nutné ji uvádět při většině úkonů spojených s danou instalací, jako je např. rozšíření systému apod.

11.12.2. Rozšiřování systému

V případě rozšíření systému o další kamery či přechodu na vyšší edici je do systému nutné vložit nový licenční klíč a ten potom aktivovat. Vložení licence lze provést způsoby popsány výše, zkopírováním do pole Licenční klíč nebo importem ze souboru.

Pokud je Váš kamerový klient online, je nová licence pro Váš systém rozpoznána automaticky a tento stav bude indikován blikajícím symbolem licenčního klíče.



Po kliknutí na tento symbol budete vyzváni k potvrzení vložení nového klíče, který se automaticky objeví v poli Licenční klíč. Následně už bude stačit provést pouze jeho aktivaci.

11.12.3. Aktivace nových verzí

Po aktualizaci na novou verzi bude nutné opět aktivovat Vaši stávající licenci. Aktivace je možná bez omezení, pokud daný systém využívá zkušební licenci. V případě zakoupené licence musí mít systém aktivní ATEAS PMA, které umožňuje instalaci všech nových verzí ATEAS.

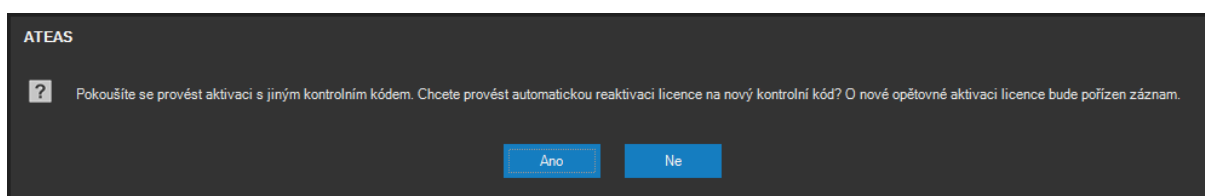
Více k tomuto tématu naleznete v kapitolách dokumentace Informace o verzi a Informace o PMA.

11.12.4. Automatická reaktivace licencí

Jakmile je systém aktivován, aktivaci licence není již možné provést na jiném počítači, přesněji v situaci, kdy by byl administrační server systému instalován na počítači s jiným kontrolním kódem. Pokud by byla druhá či jakákoliv další aktivace stejné licence na jiných počítačích v souladu s licenčními podmínkami (např. po selhání hardware, reinstalaci OS apod.), lze deaktivaci licence vyřešit čestným prohlášením prostřednictvím dodavatele licencí.

Zákazníci, kteří mají aktivovanou službu PMA (neomezený přístup k novým verzím produktu) však mohou využít funkce automatické reaktivace licence na novém stroji bez součinnosti s dodavatelem licence a bez vyplnění čestného prohlášení o deaktivaci.

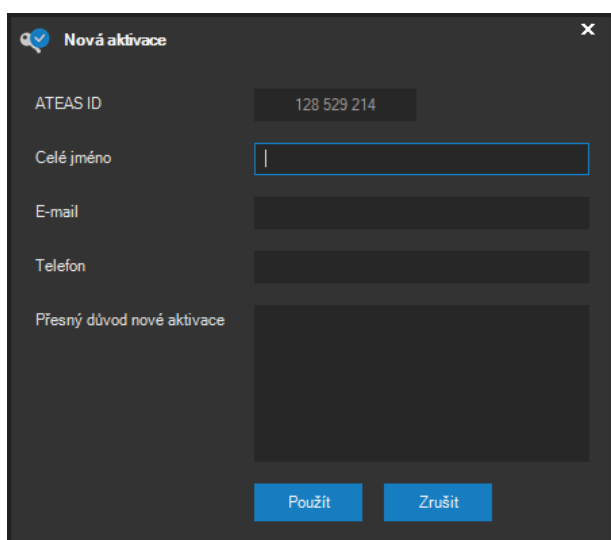
Systém tento případ automaticky rozpozná a při pokusu o opětovnou aktivaci licence nabídne po potvrzení dotazu následující dialog.



ATEAS

? Pokoušíte se provést aktivaci s jiným kontrolním kódem. Chcete provést automatickou reaktivaci licence na nový kontrolní kód? O nové opětovné aktivaci licence bude pořízen záznam.

Ano Ne



Nová aktivace

ATEAS ID 128 529 214

Celé jméno

E-mail

Telefon

Přesný důvod nové aktivace

Použít Zrušit

Pro provedení nové aktivace licence je nutné přesně vyplnit všechna pole v reaktivačním dialogu a potvrdit tlačítkem **POUŽÍT**.

POZNÁMKA

Pro jedno ATEAS ID může být automatická reaktivace licence provedena pouze jednou za několik dní, častější pokusy jsou blokovány.

POZOR

O opětovné deaktivaci je pořízen záznam a je automaticky informován příslušný dodavatel licence. Pokud vzniknou pochyby o správnosti vyplněných údajů anebo bude detekována situace odporující licenčním podmínkám, budou další pokusy o automatickou reaktivaci licence blokovány.

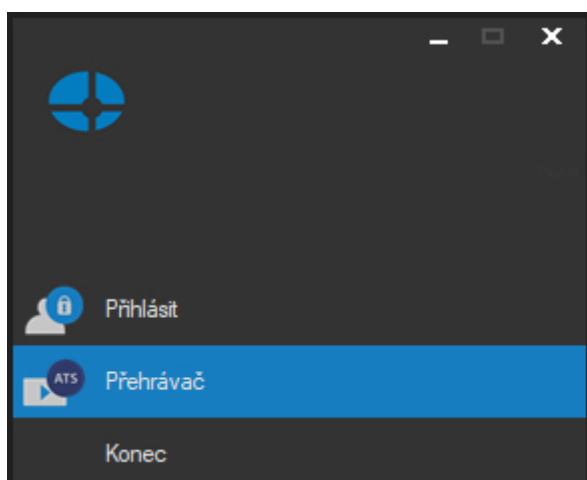
Kapitola 12 - Přehrávač

12.1. Spuštění přehrávače

Aplikace Přehrávač je jednoduchý a intuitivní přehrávač, který podporuje formát ATS, do něhož lze exportovat video a zvuk z kamer. Přehrávač umožňuje také export snímků ve formátu JPEG. Kromě formátu ATS je možné z klientské aplikace provést export videa i do formátu AVI či MP4, které je podporovány velkým množstvím jiných přehrávačů. Naproti tomu má však export do formátu ATS některé výhody:

- Export je násobně rychlejší, neboť nedochází k rekompresi videa pomocí zvoleného kodeku.
- Výsledný soubor může obsahovat až 16 kamer včetně zvuku.
- Výsledný soubor může obsahovat video komprimované různými formáty videa a zvuku.
- Exportované video podporuje dynamické změny snímkové frekvence a rozlišení videa.
- Pomocí integrovaného nástroje lze ATS soubory digitálně podepsat.
- Soubor může být šifrován a ochráněn heslem.

Spuštění přehrávače je možné provést několika způsoby. Pokud máte spuštěnu klientskou aplikaci ATEAS Observer, je možné zvolit položku Přehrávač přímo z hlavní nabídky aplikace. Tato volba je dostupná také ještě před přihlášením do systému.



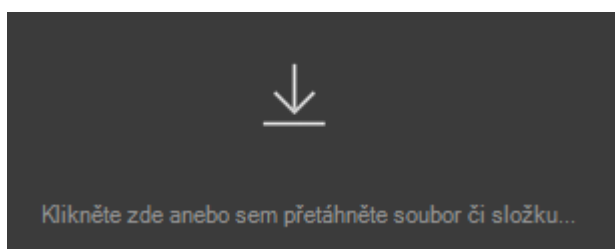
Pokud nemáte spuštěnu klientskou aplikaci, můžete přehrávač spustit také dvojím kliknutím na soubor s koncovkou ATS kdekoliv v systému Windows. Koncovka souboru ATS je po instalaci ATEAS Security rozpoznána jako registrovaný typ souborů a přehrávač bude spuštěn automaticky.

Kromě toho je také možné přehrávač spustit na počítači bez instalace klienta ATEAS přímo spustitelným souborem přehrávače. Tento soubor je dostupný jako součást instalačního obrazu ATEAS a také na webu Vašeho administračního serveru. Pokud byl přehrávač exportován spolu s daty, je přehrávání spuštěno automaticky.

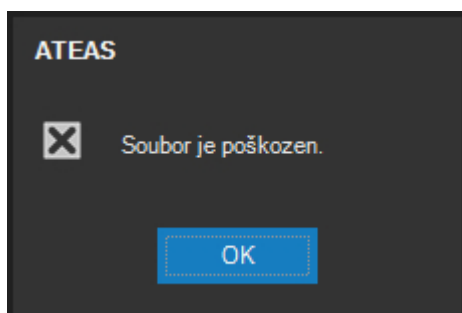
12.2. Přehrávání videa ve formátu ATS

12.2.1. Otevření složky

Pokud byl přehrávač spuštěn automaticky výběrem ATS souboru přímo v operačním systému, dojde k automatickému otevření tohoto souboru. Soubor je také možné otevřít pomocí seznamu souborů v pravé části okna přehrávače, který je popsán v samostatné subkapitole. Dalším a mnohdy nejrychlejším způsobem otevření složky anebo souboru v přehrávači je jejich přetažení přímo ze složky do seznamu souborů. Aktivní oblast pod seznamem souborů a složek po kliknutí zároveň také zobrazí dialog s výběrem složky.

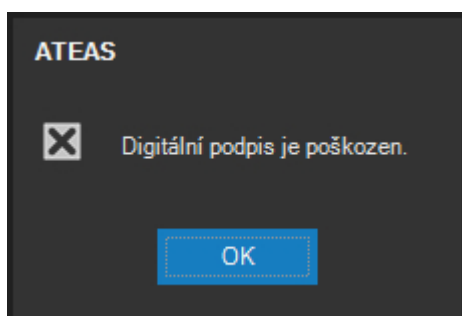


Při otvírání souboru může nastat několik případů. Pokud soubor nemá odpovídající formát, nebude otevřen a bude zobrazena varovná zpráva.



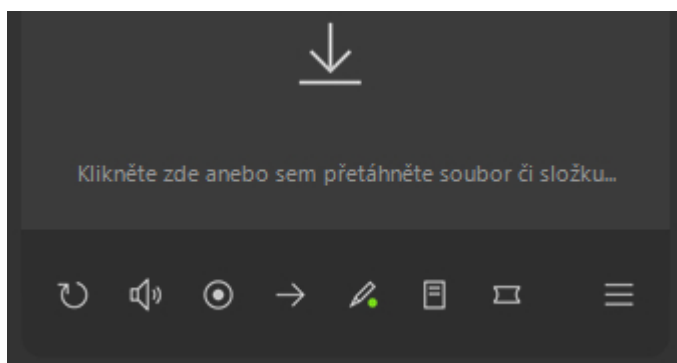
Pokud je struktura souboru v pořádku, zjišťuje se přítomnost digitálního podpisu. Pokud přehrávaný soubor neobsahuje digitální podpis, automaticky začne přehrávání souboru. Indikátor digitálního podpisu umístěný v pravém dolním rohu přehrávače bude v tomto případě zobrazen šedivou barvou. Pokud je soubor digitálně podepsán, bude digitální podpis ihned automaticky ověřen. Zde mohou nastat tři případy.

Prvním případem je situace, kdy bude digitální podpis vyhodnocen jako neplatný. To znamená, že s daty souboru po jeho podpisu někdo manipuloval (v libovolně velkém souboru postačí změna jednoho jediného bitu) a jeho obsah není možné považovat za pravý. Aplikace tuto situaci indikuje uživateli zprávou a indikátor digitálního podpisu bude zobrazen červenou barvou.

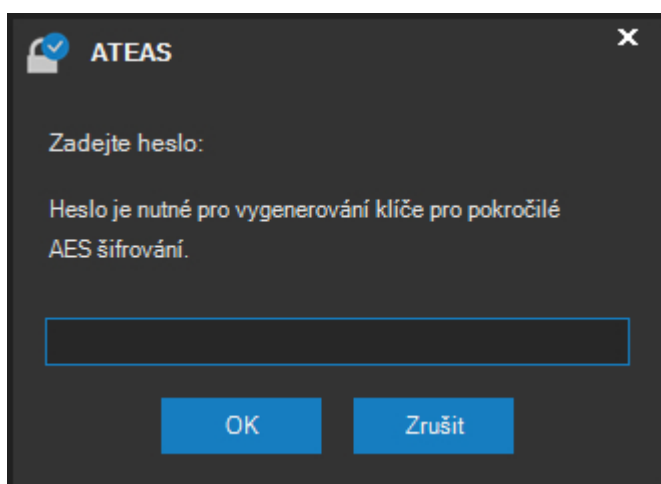


Ve druhém případě je digitální podpis ověřen pozitivně, na straně příjemce však není možné obsah souboru označit za důvěryhodný, neboť nejsou k dispozici všechny potřebné certifikáty nebo cesta k certifikátu podpisu na straně příjemce nekončí u kořenového certifikátu, který je nainstalován v úložišti důvěryhodných kořenových certifikačních úřadů. V tomto případě je možné na straně příjemce provést potřebné instalace certifikátů (buď přímo z podpisu souboru nebo externě). Indikátor digitálního podpisu bude v tomto případě zobrazen oranžovou barvou.

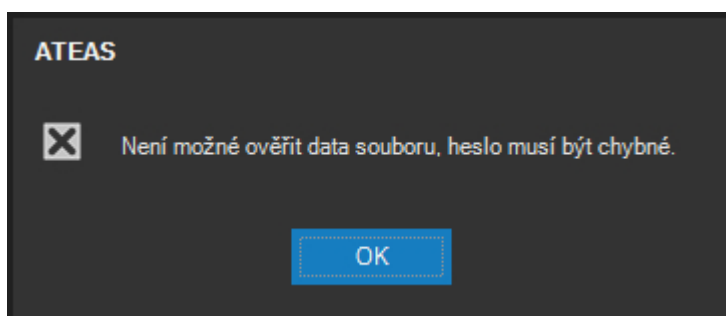
Třetí možností je situace, kdy bude digitální podpis vyhodnocen jako platný a certifikát podpisu jako důvěryhodný. V tomto případě bude indikátor digitálního podpisu zobrazen zelenou barvou.



Pokud byl ATS soubor při exportu ochráněn pomocí pokročilého šifrování AES, bude po verifikaci digitálního podpisu vyžadováno heslo pro otevření souboru, které je vstupem pro jednocestné matematické funkce, pomocí kterých je získán klíč pro dešifrování dat souboru. Pokud jsou data souboru šifrována, bude automaticky zobrazen následující dialog.



Je-li zadáno správné heslo, bude zahájeno přehrávání souboru. V opačném případě není možné získat přístup k datům souboru a aplikace zobrazí kritickou zprávu.

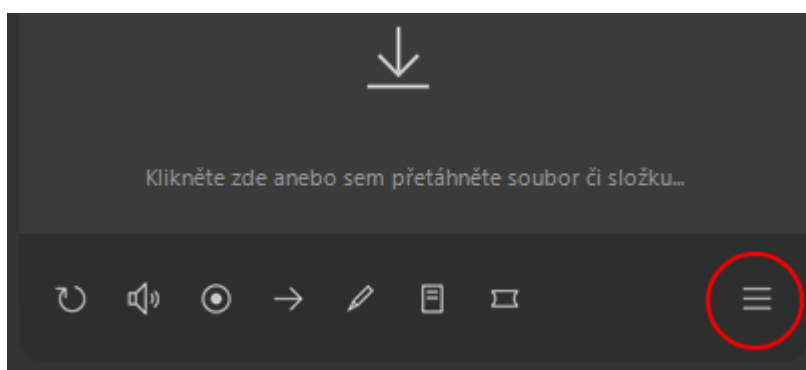


POZNÁMKA

Bez znalosti správného hesla a za použití dnešních technologií není v rozumném čase v žádném případě možné získat přístup k dešifrovaným datům souboru a přehrát jeho obsah.

12.2.2. Seznam souborů

Po otevření libovolné složky přehrávač automaticky vytvoří seznam všech ATS souborů v dané složce. Tento seznam je možné zobrazit anebo schovat pomocí tlačítka v pravém spodním rohu okna přehrávače. Automaticky jsou prohledány také všechny podsložky, a vytvoří se tak přehledná stromová struktura.

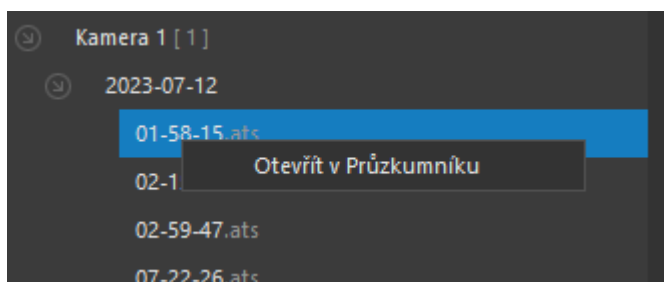


Otevření libovolného souboru pak lze provést jednoduchým kliknutím do seznamu souborů. Při spodním okraji seznamu souborů je k dispozici tlačítko pro aktivaci automatického přehrávání. Pokud je tato volba aktivována, přehrávač postupně automaticky přehraje všechny soubory v seznamu.

Vpravo nad seznamem souborů jsou k dispozici tlačítka pro obnovení seznamu a vyhledávání.

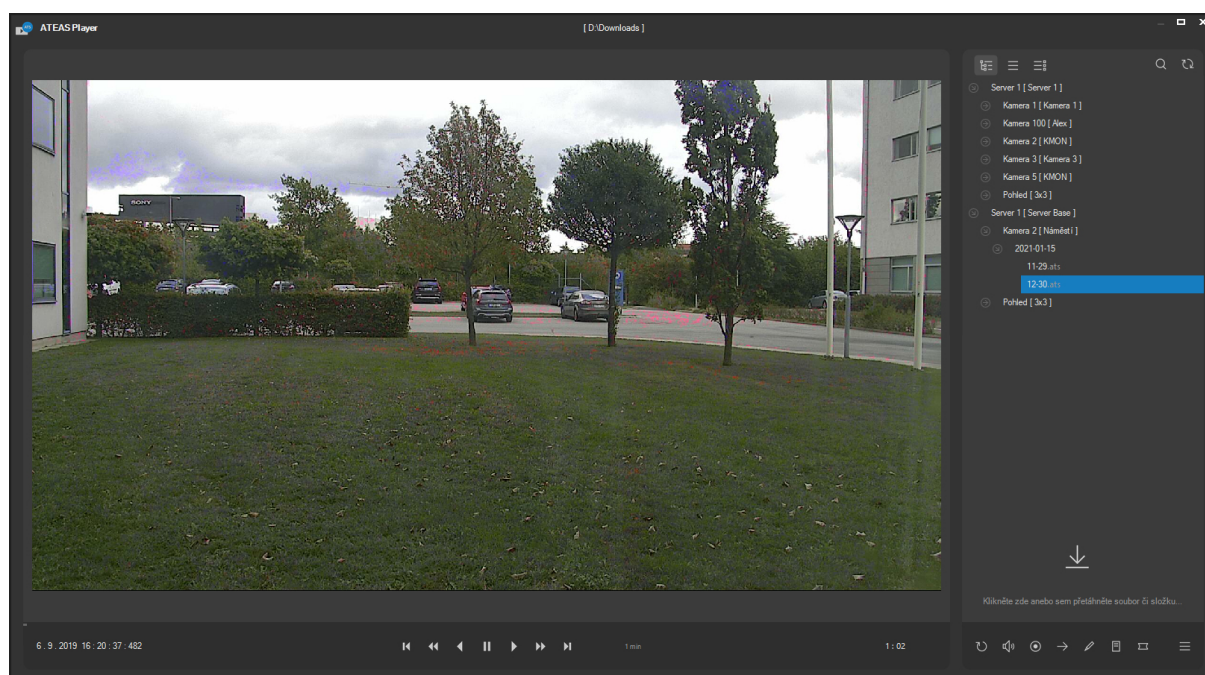
Rozdělení plochy přehrávače mezi oblast pro přehrávání a seznam souborů lze provést umístěním kurzoru myši mezi tyto plochy a přetažením. Dvojitým kliknutím se lze vrátit k výchozímu rozdělení.

U každého souboru je možné pomocí kontextové nabídky provést rychlý přechod do složky se souborem.

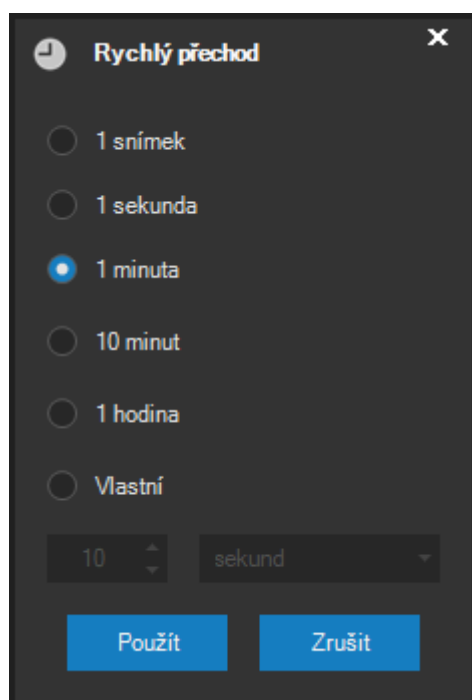


12.2.3. Přehrávání souboru

Během přehrávání lze měnit rychlost a směr přehrávání a provádět jednorázové posuny pomocí ovládacího prvku přehrávání umístěného uprostřed ve spodní části okna přehrávače.



Skupina dvou tlačítek vlevo na tomto ovládacím prvku slouží ke změně rychlosti přehrávání v rozmezí šestnáctinásobného zpomalení až šestnáctinásobného zrychlení. Skupina třech větších tlačítek uprostřed ovládacího prvku slouží ke změně směru či zastavení přehrávání. Dvě tlačítka vpravo mohou být použita pro rychlý přesun o daný časový interval vpřed či vzad. Tento časový interval je nastavitelný po kliknutí na jeho aktuální hodnotu. V následujícím okně lze pak zvolit předdefinovaný nebo nastavit vlastní časový interval, který po stisku tlačítka **POUŽÍT** bude přiřazen tlačítkům rychlého přechodu. Hodnota 1 snímek je časově nezávislá a umožňuje přechod mezi jednotlivými snímky.

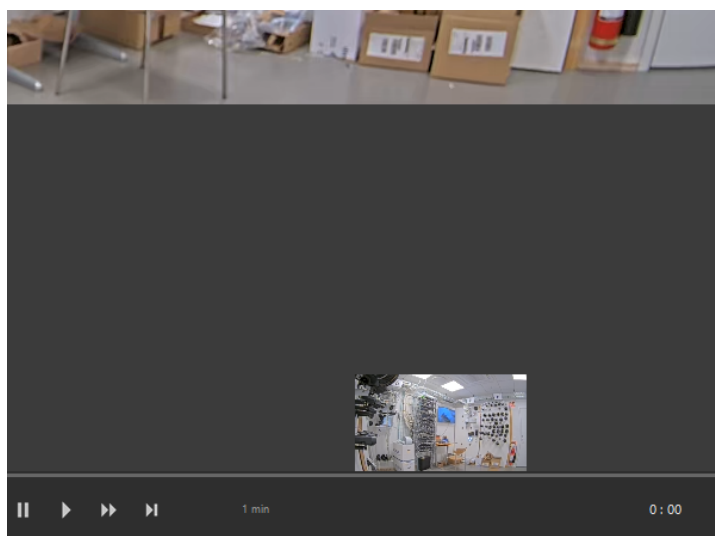


POZNÁMKA

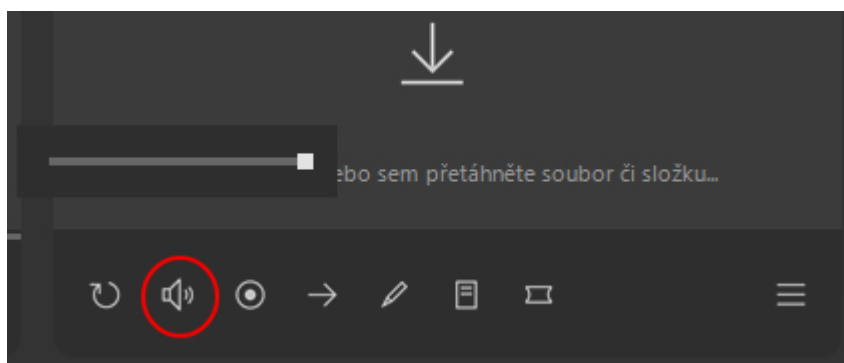
Pokud otevřený ATS soubor obsahuje více kamer, musí být před zahájením krokování po jednotlivých snímcích vybrána nějaká kamera. Ostatní kamery v pohledu jsou časově synchronizovány s vybranou kameru po celou dobu krokování.

Při přehrávání je levém dolním rohu zobrazena informace o čase přehrávání, v pravém dolním rohu informace o zbývajícím čase do konce souboru. Pod oknem s přehrávanou sekvencí se dále nachází ovládací prvek, který ukazuje průběh přehrávání, po dosažení pravého dorazu (respektive levého při přehrávání zpět) je přehrávání automaticky zastaveno. Do ovládacího prvku, který ukazuje průběh přehrávání, je možné také klikat a táhnout myší, což vede k rychlému přesunu do daného místa scény. To lze provádět jak při spuštěném tak pozastaveném přehrávání.

Pokud se ukazatel myši pohybuje nad tímto prvkem, je automaticky zobrazován zmenšený náhled videa pro daný čas.



Pokud je součástí scény též zvuk, je automaticky přehráván spolu s videem. Hlasitost přehrávaného zvuku je možné regulovat příslušným ovládacím prvkem.



POZNÁMKA

Pokud otevřený ATS soubor obsahuje více kamer, bude zvuk vždy přehráván pro vybranou kameru.

POZNÁMKA

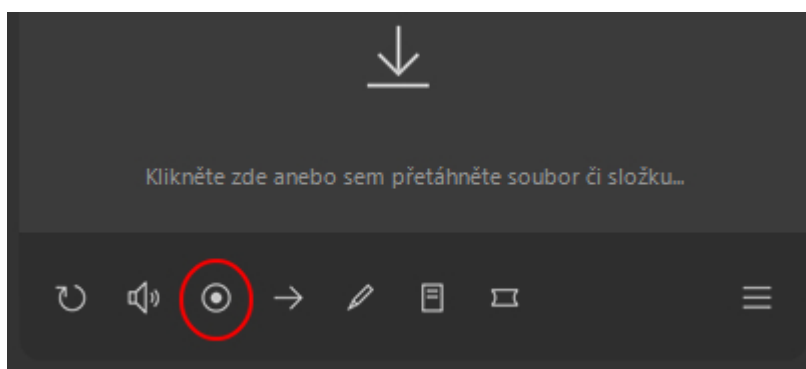
Pomocí pravého tlačítka lze provést rychlé ztlumení zvuku a obnovu na poslední nastavenou úroveň hlasitosti.

Během přehrávání jsou automaticky detekovány mezery v záznamu a přehrávač automaticky přeskakuje prázdná místa, což činí přehrávání pohodlnějším.

Během přehrávání je možné kdykoliv použít tlačítko pro uložení snímku. Nezávisle na formátu přehrávaného videa je po stisku tohoto tlačítka vytvořen snímek a vložen do nového okna nad přehrávané video.

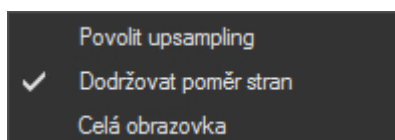
POZNÁMKA

Pokud otevřený ATS soubor obsahuje více kamer, musí být před uložením snímku vybrána kamera, pro kterou bude snímek uložen.



V okně jsou k dispozici dvě tlačítka. Tlačítkem **ULOŽIT** lze vyvolat dialog s možností exportu snímku do formátu JPEG. Tlačítkem **ZAVŘÍT** je okno se snímkem uzavřeno, aktivním oknem se stane opět přehrávač ATS souborů.

Kdykoliv během přehrávání je možné pomocí pravého tlačítka myši v ploše pro zobrazení videa vyvolat kontextovou nabídku s několika rozšiřujícími možnostmi týkající se přehrávání.



Volba Povolit upsampling je implicitně vypnuta a pokud ji zapnete, bude video zobrazeno v maximální možné velikosti, kterou umožňuje okno přehrávače. Pokud je volba vypnuta, šířka i výška videa nikdy nepřesáhnou nativní rozlišení videa, tj. přehrávač nebude při přehrávání dopočítávat žádné pixely.

Volba Dodržovat poměr stran je implicitně zapnuta a vynucuje dodržení poměru šířky a výšky zobrazovaného videa podle nativního rozlišení, nebude tedy docházet k deformaci zobrazovaných osob či objektů.

Volba Celá obrazovka umožňuje přepnout přehrávač do režimu celé obrazovky a zpět.

POZNÁMKA

Režim celé obrazovky se dokáže inteligentně přizpůsobit rozvržení monitorů, pokud jich je ke stanici připojeno více.

POZNÁMKA

Režim celé obrazovky lze opustit také pomocí klávesy Escape.

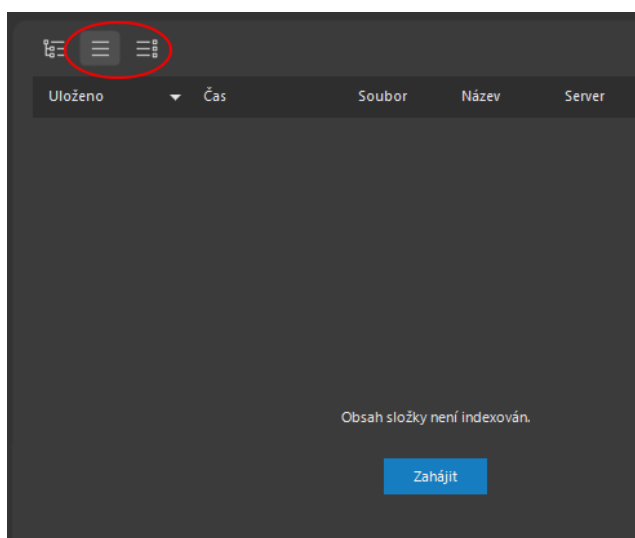
POZNÁMKA

Při přepnutí do režimu celé obrazovky je automaticky aktivována volba Povolit upsampling, jejíž použití je v režimu celé obrazovky logické.

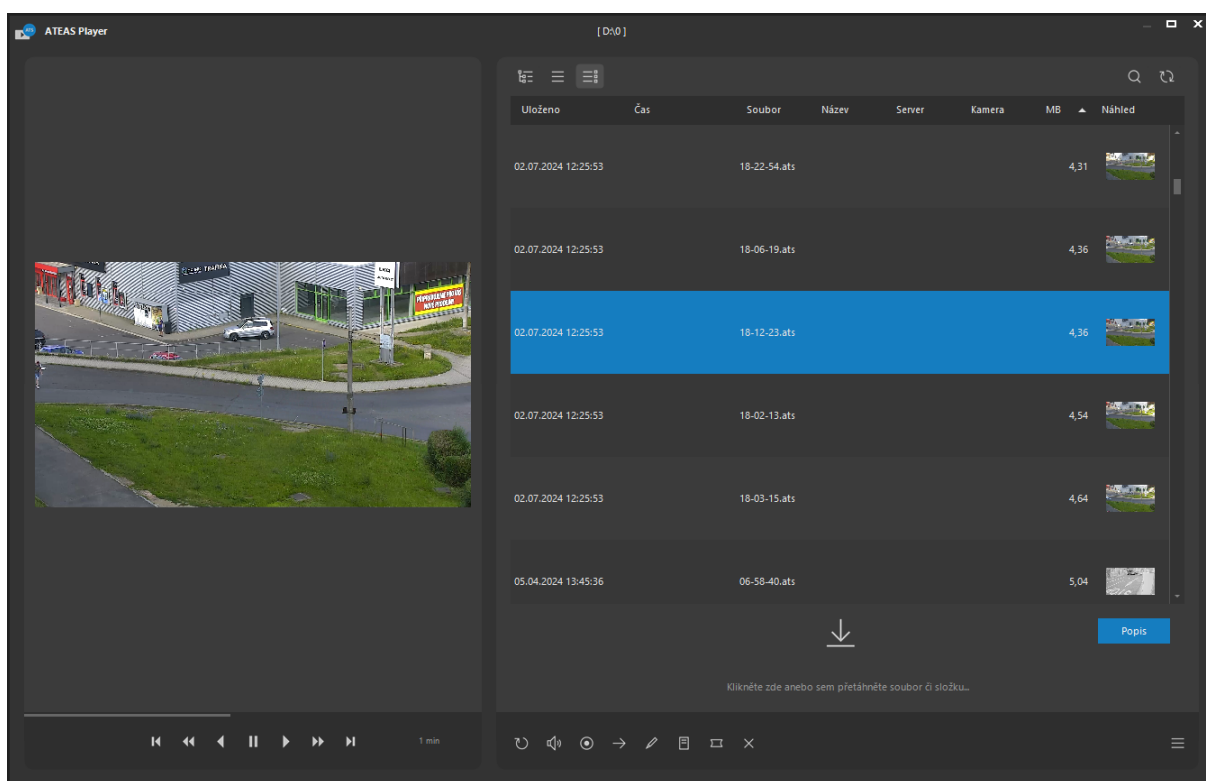
Během přehrávání v režimu celé obrazovky je možné používat některé klávesy pro kontrolu přehrávání. Tlačítko mezerníku provádí střídavě pozastavení přehrávání (pauza) a přehrávání směrem vpřed. Stejnou funkci má i tlačítko pauzy a spuštění přehrávání ve skupině tlačítek ovládání médií na klávesnici, pokud je jimi klávesnice vybavena. Přehrávání směrem zpět je možné aktivovat pomocí klávesy Backspace. Klávesami plus a minus na numerické klávesnici lze zvyšovat či snižovat rychlost přehrávání.

12.2.4. Indexované složky

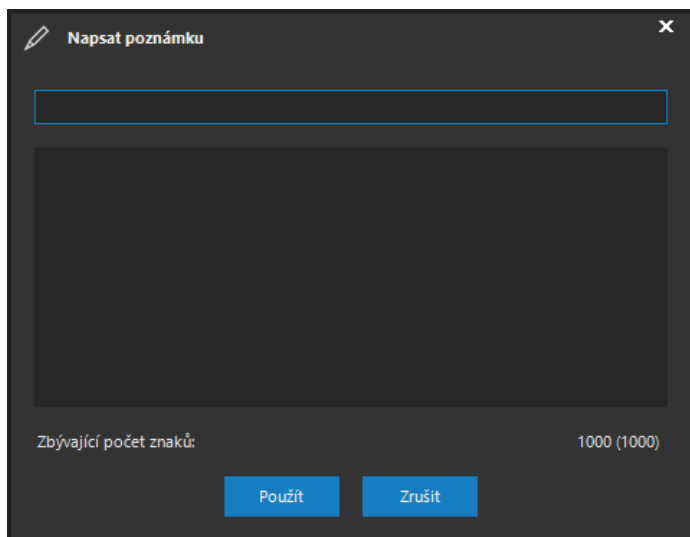
Ve výchozím stromovém zobrazení vybrané složky je možné provádět základní vyhledávání. Není však možné provádět třídění podle všech kritérií či doplňovat dlouhé komentáře. Pro tyto funkce je nutné přepnout do režimu zobrazení seznamu či náhledu a pokud není složka již indexována, její indexování zapnout tlačítkem **ZAHÁJIT**.



Indexovaný obsah složky poté umožní třídění podle všech záhlaví sloupců, doplnění názvu a delšího popisu tlačítkem **POPIS**, vyhledávání nebo zobrazení náhledu videa při najetí kurzorem myši. V režimu náhledu jsou pak náhledy zobrazeny automaticky u všech souborů.

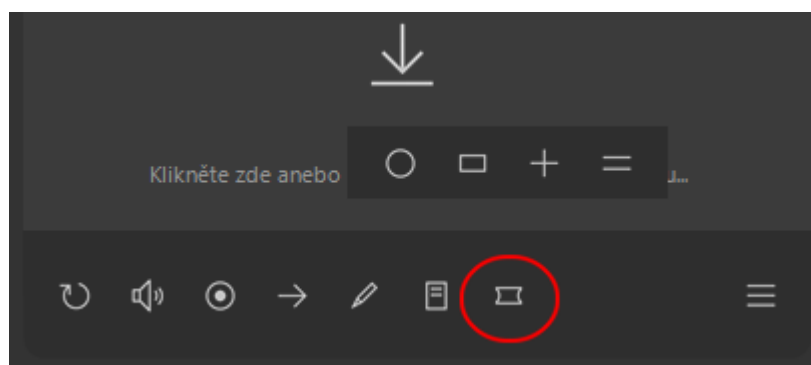


Po doplnění názvu či popisu tlačítkem **POPIS** je následně možné vyhledávat podle libovolného textu v nich obsaženém.



12.2.5. Korekce obrazu typu rybí oko

Pro exportované soubory z kamer, které byly administrátorem systému konfigurovány jako kamery s obrazem typu rybí oko, lze při přehrávání zobrazit anebo skrýt dodatečná tlačítka pro volbu režimu korekce obrazu.



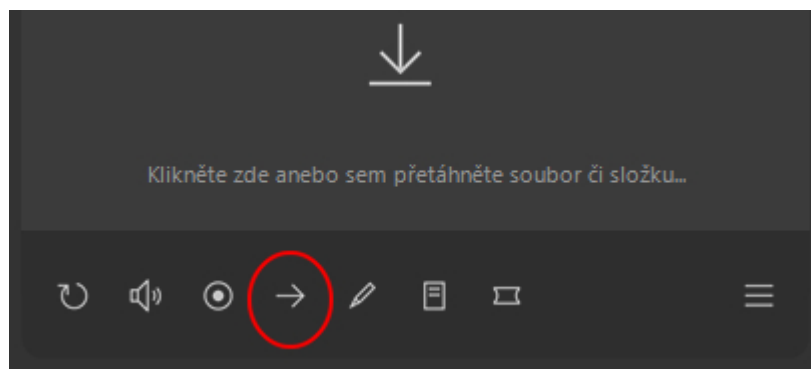
Funkce korekce obrazu typu rybí oko a jednotlivé režimy korekce zde fungují zcela shodně jako v dohledovém okně a jsou popsány v subkapitole Korekce obrazu typu rybí oko v subkapitole Funkce vybrané kamery.

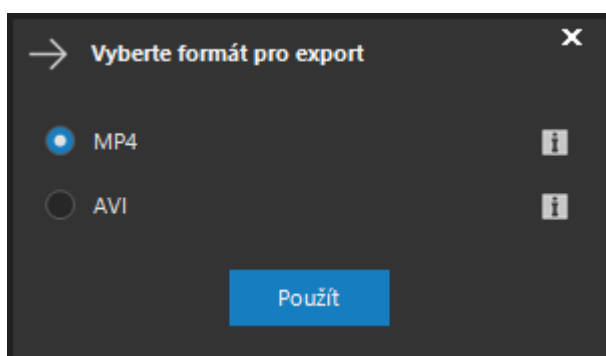
12.2.6. Export videa

Aktuálně vybrané soubory ATS je možné exportovat do jiných formátů. Výběr souborů není omezen jednou složkou, je možné vybrat více souborů z více různých složek. Po stisku tlačítka pro export videa a výběru formátu pro export se zobrazí dialog exportu videa v kompaktním zobrazení. Tlačítkem **VÍCE** je možné zobrazit dodatečné možnosti exportu. Při exportu jednoho souboru bude možné vybrat cílovou složku a zadat název exportovaného souboru, při výběru více souborů bude možné určit cílovou složku, názvy exportovaných souborů a jejich organizace do podsložek bude automaticky odpovídat vstupním souborům.

POZNÁMKA

Při exportu jednoho souboru, který obsahuje více kamer, musí být před zahájením exportu vybrána kamera, která bude exportována.





Formát AVI je široce používaný univerzální formát na všech platformách se snadnou přenositelností, nevýhodou při exportu však bude nižší rychlost (nutnost rekomprese videa) a nemožnost změny rozlišení či formátu videa a zvuku v souboru. Změny snímkové frekvence jsou automaticky vyhlazeny exportním modulem.

Formát MP4 je podobně jako formát AVI bez problémů přenositelný. Při exportu do MP4 se využívá exportu bez rekomprese videa, jeho rychlost je tak srovnatelná s exportem do formátu ATS.

Pro formát MP4 je zejména vhodná vyšší snímková frekvence, která zajistí přehrávání i v méně robustních přehrávačích třetích stran.

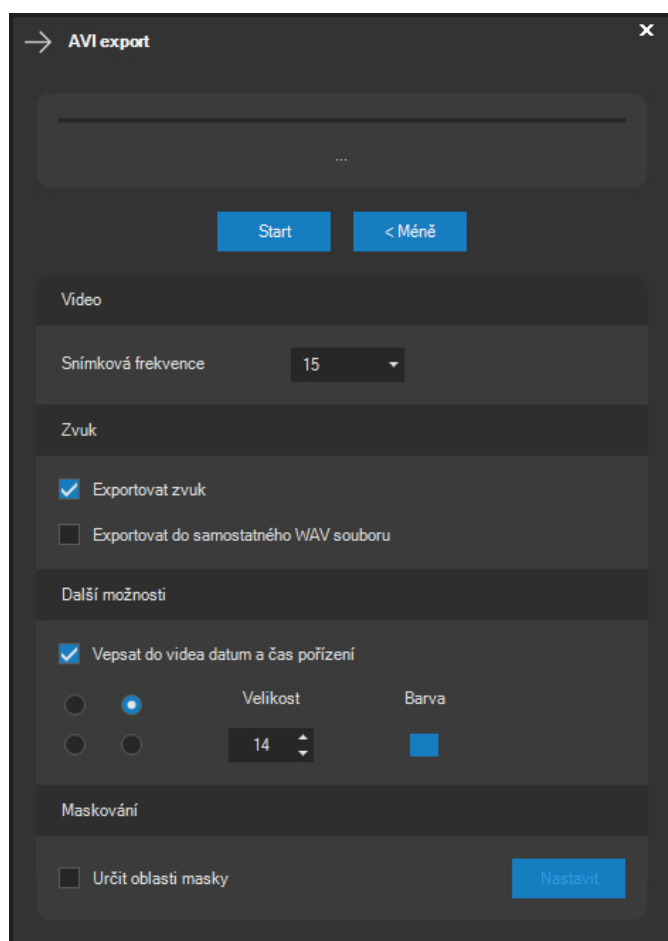
POZOR

Formát AVI a MP4 nepodporují vestavěnou bezpečnost v ATEAS Security, jejich obsah tak není při exportu šifrován a data nelze opatřit digitální podpisem.

12.2.7. Export videa do AVI

Základní nastavení

Po stisku tlačítka pro export videa a výběru AVI formátu se zobrazí dialog exportu videa do AVI v kompaktním zobrazení. Tlačítkem **VÍCE** je možné zobrazit dodatečné možnosti exportu.



Po stisknutí tlačítka **START** se zobrazí dialog, ve kterém je nutné vybrat umístění a zadat název pro nově vytvořený soubor AVI.

POZNÁMKA

Pokud je před zahájením exportu vybráno více lokálně uložených scén, nemá smysl zadávat konkrétní název souboru, ale bude možné vybrat cílovou složku. Názvy jednotlivých souborů se poté utvoří v obecné podobě (např. Scena1, Scena2) nebo bude pro výsledný název souboru použit název scény, pokud byl uživatelem vytvořen.

Po zahájení exportu se tlačítko **ZAVŘÍT** změní na tlačítko **ZRUŠIT**, kterým je možné předčasně ukončit export videa. Ovládací prvek vedle tlačítka **START** informuje o průběhu exportu videa, po jeho dokončení se zobrazí potvrzovací zpráva.

Před zahájením exportu je možné zvolit ještě některé doplňkové volby pro export:

POZNÁMKA

Tyto doplňkové volby budou při příštím otevření dialogu automaticky nastaveny na naposledy použité hodnoty.

V rozbalovacím seznamu Snímková frekvence je možné určit exportní snímkovou frekvenci. Pokud nechcete, aby byly při exportu vynechány nějaké snímky, vždy zvolte takovou snímkovou frekvenci, která je vyšší než nejvyšší snímková frekvence v exportované sekvenci. Při nižší snímkové frekvenci bude (v závislosti na kodeku) výsledná velikost souboru nižší.

Zvuk

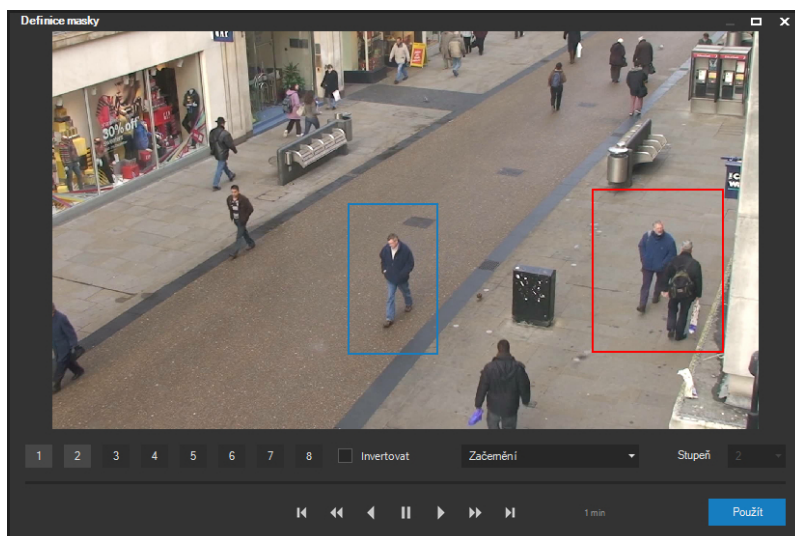
Je možné zaškrtnout volbu Exportovat zvuk případně též Exportovat do samostatného WAV souboru. Při zaškrtnutí pouze volby Exportovat zvuk bude zvuková stopa uložena spolu se stopou videa do výsledného AVI souboru. Pokud navíc zaškrtnete ještě volbu Exportovat do samostatného WAV souboru, bude vedle souboru AVI vytvořen stejnojmenný soubor s koncovkou WAV, který bude obsahovat zvukový záznam.

Další možnosti

V části Další možnosti je možné aktivovat volbu Vepsat do videa datum a čas pořízení. Touto možností se provede vykreslení data a času přímo do exportovaného souboru. Při zaškrtnutí této možnosti lze dále určit jeden ze čtyř rohů, ve kterém se datum a čas v exportovaném videu objeví. V případě potřeby je také možné změnit barvu a velikost písma, které bude použito. Velikost písma lze nastavit v rozmezí 8 – 60 bodů, barvu lze vybrat nebo vytvořit v dialogu výběru barvy po stisknutí na tlačítko vedle aktuálně zvolené barvy.

Maskování

Po aktivaci volby Určit oblasti masky je možné pomocí tlačítka **NASTAVIT** zobrazit dialog s náhledem videa, ve kterém je možné vytvořit masku.



Je možné vytvořit až osm nezávislých dynamických masek, které je možné v průběhu přehrávání přesouvat či postupně skrývat a znovu zobrazit. Také je možné měnit jejich rozměry. Tímto způsobem lze při exportu snadno anonymizovat např. vybrané osoby či jejich obličeje v záznamu, i pokud se pohybují.

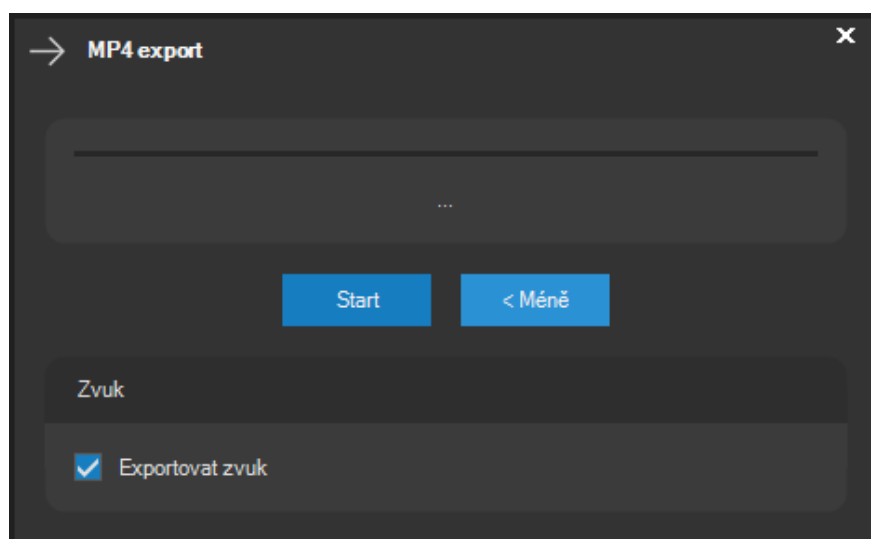
Maskám může být přiřazen efekt kompletního začernění nebo efekt pixelizace a rozostření, u kterých je též možné zvolit sílu efektu na stupnici od 1 do 3 (nejsilnější).

Masky lze nastavit také s aktivovanou volbou Invertovat, kdy bude maska aplikována vně označené oblasti. Tím lze rychleji docílit situace, kdy bude v exportovaném videu ponechán bez masky např. jen jeden či více konkrétních pohybujících se objektů.

12.2.8. Export videa do MP4

Základní nastavení

Po stisku tlačítka pro export videa a výběru MP4 formátu se zobrazí dialog exportu videa do MP4 v kompaktním zobrazení. Tlačítkem **VÍCE** je možné zobrazit dodatečné možnosti exportu.



Po stisknutí tlačítka **START** se zobrazí dialog, ve kterém je nutné vybrat umístění a zadat název pro nově vytvořený soubor MP4.

POZNÁMKA

Pokud je před zahájením exportu vybráno více lokálně uložených scén, nemá smysl zadávat konkrétní název souboru, ale bude možné vybrat cílovou složku. Názvy jednotlivých souborů se poté utvoří v obecné podobě (např. Scena1, Scena2) nebo bude pro výsledný název souboru použit název scény, pokud byl uživatelem vytvořen.

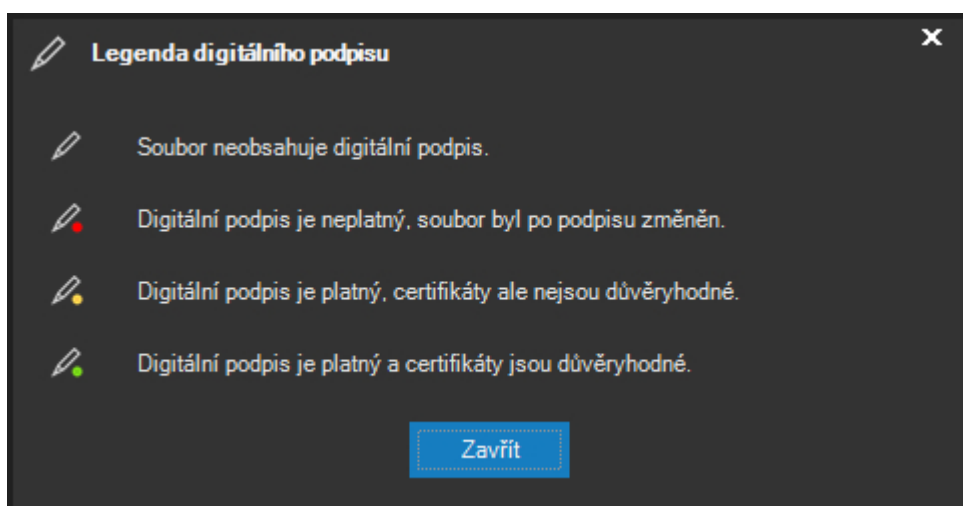
Před zahájením exportu je možné zvolit, zdali bude výsledný soubor obsahovat zvukovou stopu, nebo bude-li při exportu odstraněna.

POZNÁMKA

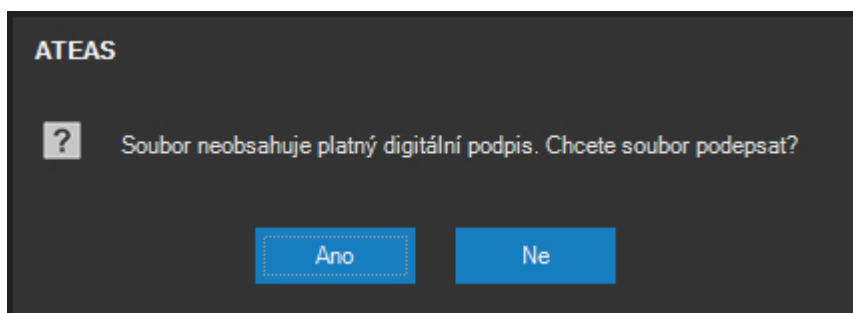
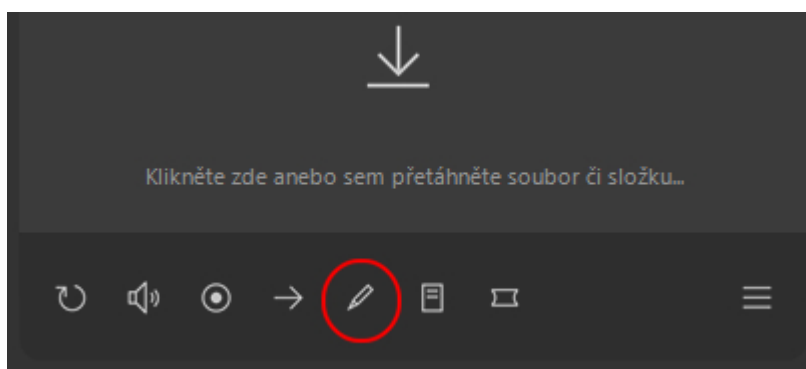
Tyto doplňkové volby budou při příštím otevření dialogu automaticky nastaveny na naposledy použité hodnoty.

12.3. Digitální podpis

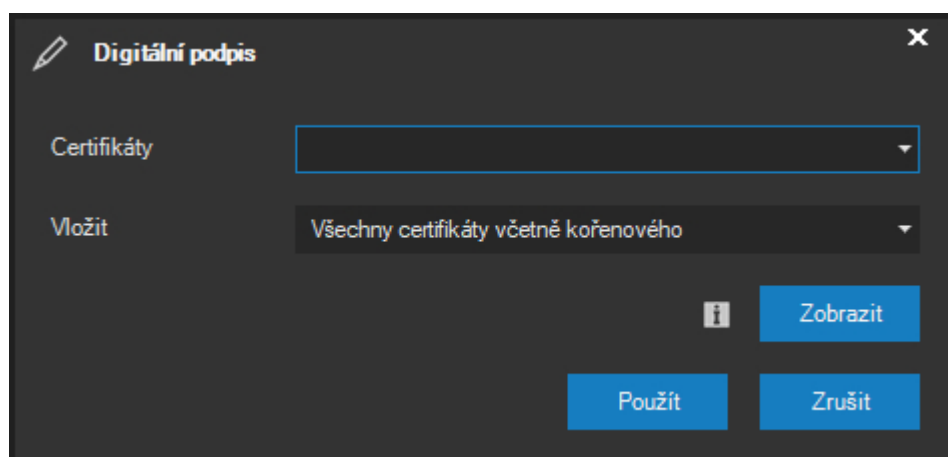
Výsledek ověření digitálního podpisu u souborů videa a snímků je zobrazen pomocí indikátoru digitálního podpisu. Pokud na tento barevný indikátor klikneme pravým tlačítkem, bude zobrazen dialog s legendou všech stavů digitálního podpisu, jak ukazuje následující obrázek.



Pokud ještě není soubor podepsán, je možné tak učinit pomocí tlačítka pro podpis.



Pokud na tuto otázku odpovíme tlačítkem **ANO**, bude možné soubor podepsat. V následujícím dialogu je možné vybrat certifikát podpisu a způsob vložení.

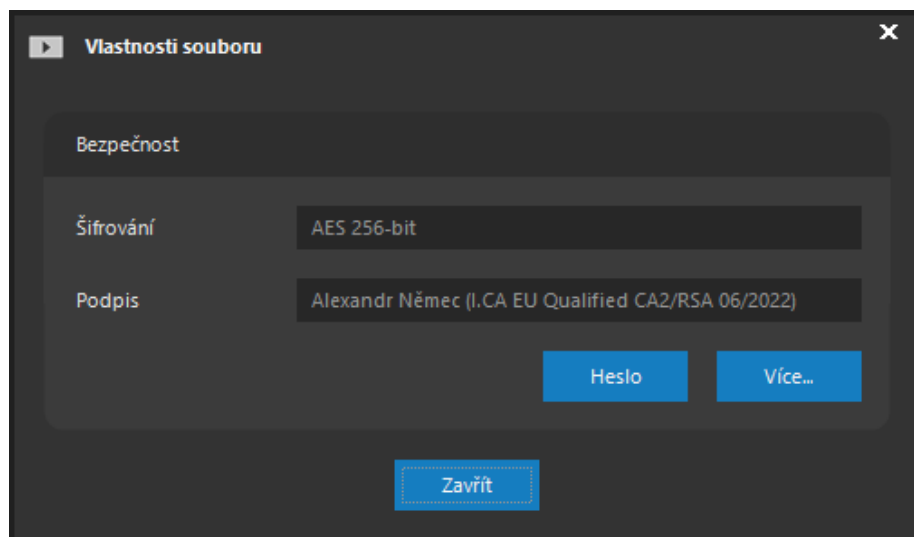


Platí, že je možné k podpisu použít libovolný certifikát nainstalovaný ve Vašem úložišti certifikátů v systému Windows (odkud je ATEAS Observer načítá).

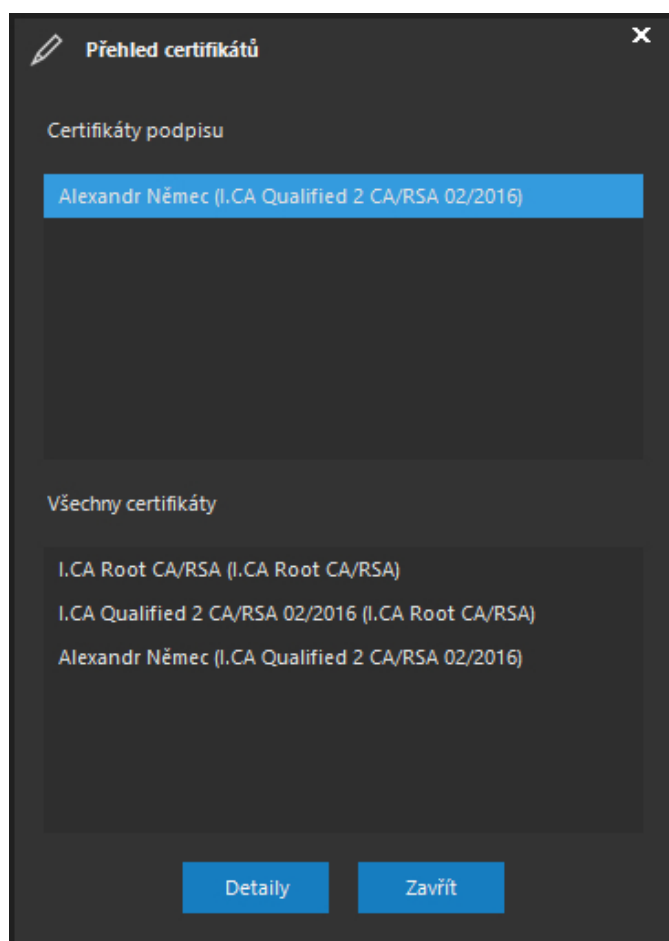
Pokud je soubor již podepsán, je možné pomocí tlačítka Vlastnosti zobrazit připojené digitální podpisy a příslušné certifikáty.

12.4. Vlastnosti souboru

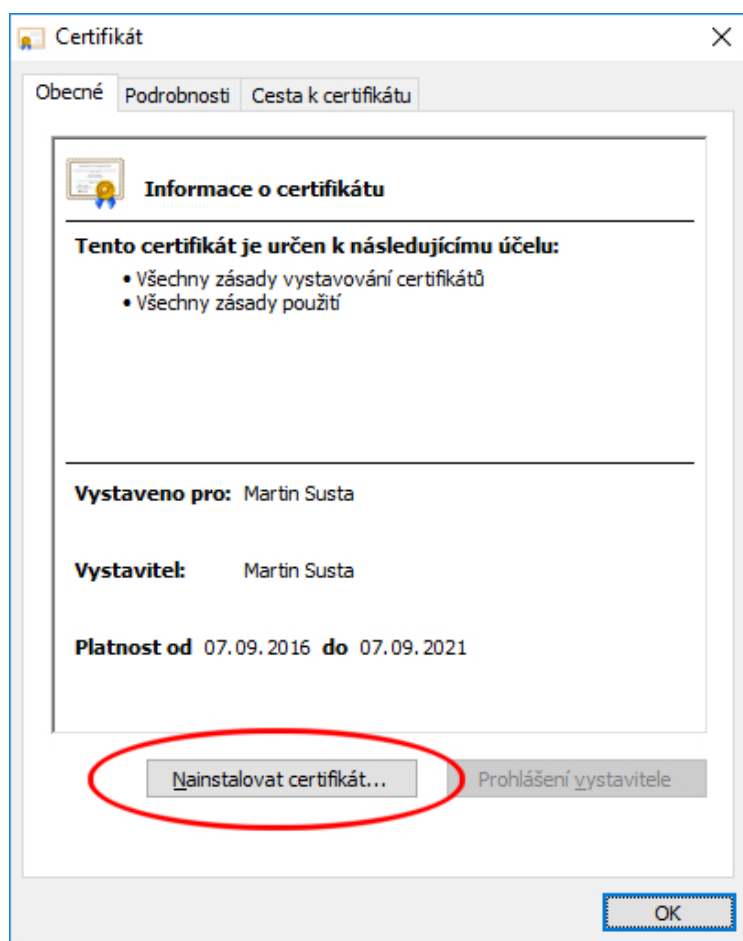
Tlačítkem Vlastnosti lze otevřít dialog s doplňujícími informacemi o souboru.



V části Bezpečnost je zobrazen způsob šifrování (tedy zdali je pro otevření souboru nutné heslo) a certifikát podpisu. Pokud je soubor podepsaný, tlačítkem **VÍCE** je možné zobrazit podrobný seznam certifikátů v souboru.



V horní části okna jsou uvedeny certifikáty podpisu, ve spodní části jsou uvedeny všechny certifikáty vložené do podpisu. Tlačítkem **DETAILY** lze kterýkoliv vybraný certifikát zobrazit ve standardním okně Windows s detailními informacemi o certifikátu včetně zobrazení cesty a důvodu nedůvěryhodnosti. Automaticky také bude k dispozici tlačítko pro import certifikátu do certifikátů třetích stran či do důvěryhodných kořenových certifikačních úřadů. Tlačítkem **NAINSTALOVAT CERTIFIKÁT** lze spustit automatického průvodce přidáním certifikátu do systému Windows.



Tlačítkem **HESLO** je možné zrušit anebo změnit heslo souboru. To se hodí např. v případě, kdy administrátor systému aktivoval ochranu stahování a tento soubor se rozhodl odemknout či povolit jeho otevření dalšími osobami.

POZOR

Změnou hesla dojde k zneplatnění a automatickému odstranění digitálního podpisu, soubor tedy bude nutné v případě potřeby podepsat znovu.

Kapitola 13 - Mapové okno

13.1. Základy mapového okna

Mapové okno je inteligentní integrovanou komponentou vestavěnou v systému ATEAS Security pro vizualizaci geografického kontextu Vašeho systému. Souřadnicová orientovanost umožňuje veškeré skutečně mapové funkce včetně mapového zoomu, centrování podle souřadnic, centrování na definované výřezy, vytváření a přepínání jednotlivých úrovní mapy a mnoho dalších. S využitím této komponenty tak získáte možnost integrovat Vaše mapové podklady (mapy, výkresy, plány) s bezpečnostním a kamerovým systémem. Následující obrázky ukazují příklady importovaných map.

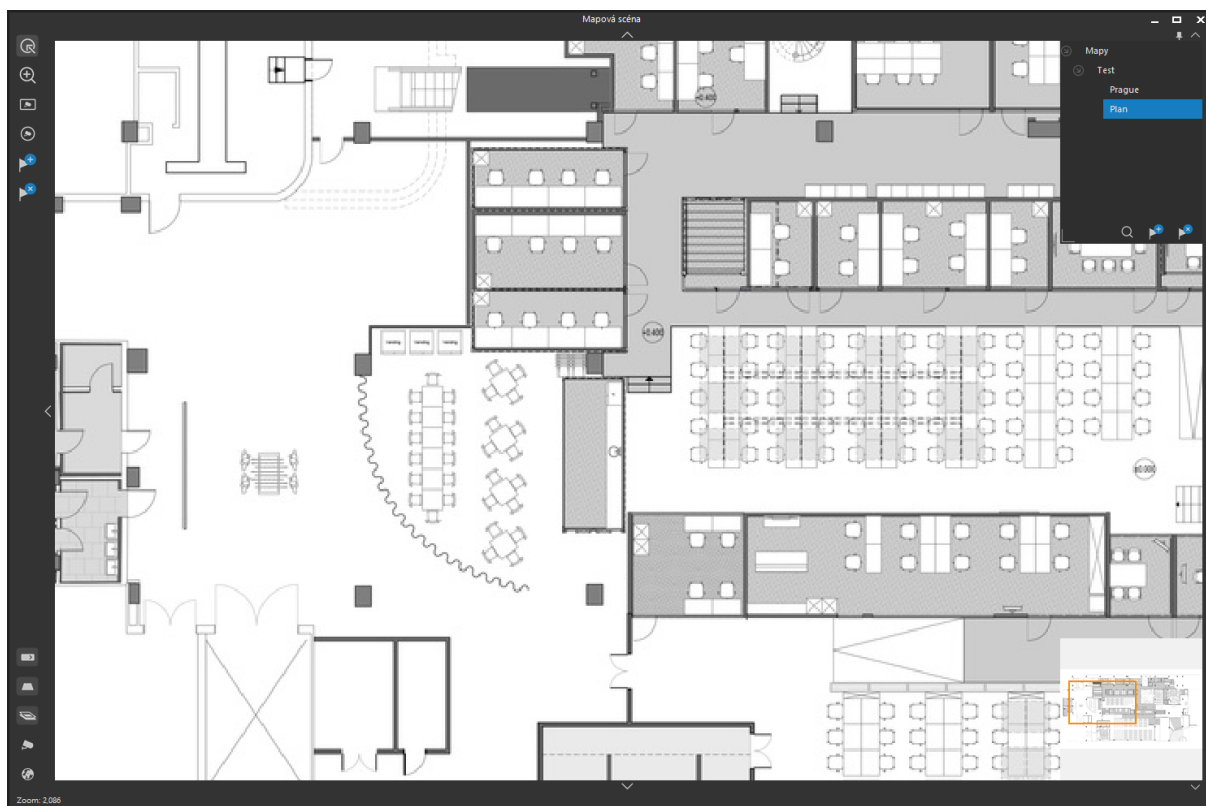
Mapové okno je také kompatibilní s mapovými podklady OpenStreetMap. Mapové podklady, které Vám mohou být dodány, tedy mohou obsahovat volná mapová data z tohoto zdroje. Jedná se o reálné, přesné, vícevrstvé, georeferencované mapy, které nabízí možnost mapového zoomu až do nízkých mapových měřítek (podrobná úroveň budov) a vysoký výkon. Základní výhodou je jejich volná dostupnost a nezávislost na mapových podkladech třetích stran. Jednoduše Vám tak mohou být do systému přidány podrobné mapy pro celé město či kraj.

POZNÁMKA

Mapové okno plynule podporuje různé maximální úrovně přiblížení pro různé části mapy, lze tak do systému připojit mapu např. s celým regionem na přehledové úrovni a vybrané jeho části či města v maximální podrobnosti.

POZNÁMKA

Možnost použití mapy ze zdrojů OpenStreetMap je k dispozici až od edice ATEAS Security PROFESSIONAL.



POZNÁMKA

V této kapitole je popsáno základní ovládání mapy. Některé funkce dotýkající se mapového okna jsou však také součástí ostatních kapitol. Viz například umístění kamery na souřadnice (v části nastavení kamer), nastavení chování mapy, historie událostí v mapě, výběry (v části lokální nastavení) či zobrazení událostních symbolů (v části o dohledovém okně a příjmu událostí).

13.2. Distribuce mapových podkladů

Distribuce mapových podkladů v systému je automatická. Administrátor s přístupem k administračnímu serveru systému vytváří a upravuje strukturu mapových podkladů a zveřejňuje ji pro distribuci klientům, kteří si strukturu map synchronují u sebe.

POZNÁMKA

Aby si klient mohl synchronizovat mapy, musí mít přiděleno příslušné oprávnění.

Administrátor systému vytváří mapovou strukturu ve složce `httproot\maps` na administračním serveru systému. Tam může vytvořit až tři vnořené úrovně mapových podkladů v podobě podsložek. Každá složka může obsahovat rastrový podklad ve formátu JPG, TIF, PNG či BMP anebo OSM mapový model. OSM mapový model vychází z volně dostupných dat OpenStreetMaps, které jsou k dispozici pro celý svět, a můžete si tak vyexportovat libovolný region. Existuje více nástrojů a způsobů exportu, jeden z nich je popsán v příloze této dokumentace.

TIP

Rastrové podklady s velmi vysokým rozlišením je vhodné převést do OSM mapového modelu způsobem popsaným v příloze neboť práce s rastry s extrémním rozlišením může být pomalá.

Název složky obsahuje jednoznačné ID mapové vrstvy a název za pomlčkou, např.

10-Prague

Pořadí mapových složek na jedné úrovni je implicitně dáno použitým ID. Pokud takové pořadí nevyhovuje, je možné doplnit za název číslo v hranatých závorkách určující pořadí, např.

10-Prague[1]

Mapové složky na dané úrovni budou poté seříděny prioritně podle těchto dodatečných pořadových čísel. Pořadová čísla nemusí tvořit souvislou řadu, pro jednoznačné určení pořadí by se však na jedné úrovni neměly vyskytovat duplicitní hodnoty.

POZOR

Mapová struktura by však nikdy neměla obsahovat duplicitní hodnoty ID pro mapové vrstvy. Jejich označení musí být jednoznačné nejen na dané úrovni, ale v celé mapové struktuře.

Aby se provedené změny v mapové struktuře začaly distribuovat klientům, je třeba zvýšit číslo verze mapových podkladů v soubor `maps.ini`, který je umístěn v kořenové mapové složce, zbytek je zcela automatický. Číslo verze je nutné změnit vždy po jakékoliv změně v mapové struktuře či obsahu, jinak nemusí být zajištěno její promítnutí u klientů.

TIP

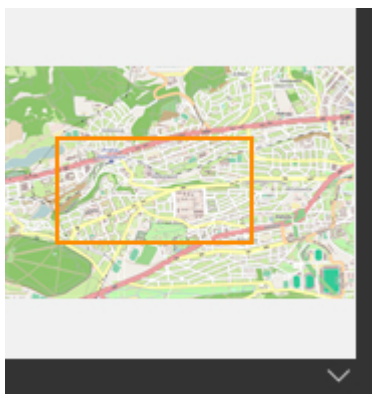
Součástí instalace jsou testovací mapové podklady, se kterými je možné začít okamžitě experimentovat.

13.3. Základní práce s mapou

13.3.1. Posuny a zoomování mapy

Mapové okno podporuje plynulé posouvání mapy pomocí přetažení myši. Kdekoliv stiskneme levé tlačítko myši a provedeme pohyb, mapa se bude posouvat spolu s ukazatelem myši. Jedná se o nejrychlejší a maximálně intuitivní způsob posunu mapy. Mapu lze dále posouvat také pomocí šipek, které jsou umístěny ve středu všech čtyřech stran mapové oblasti.

Během práce s mapou je v pravém dolním rohu k dispozici náhledové okno s maximalizovanou podobou mapy (přesněji dané mapové úrovně – patra). V ní je vyznačen rámeček, který koresponduje s právě aktuálním výřezem mapy. Pomocí šipky pod pravým dolním rohem tohoto prvku lze náhledové okno kdykoliv skrýt nebo opět zobrazit.



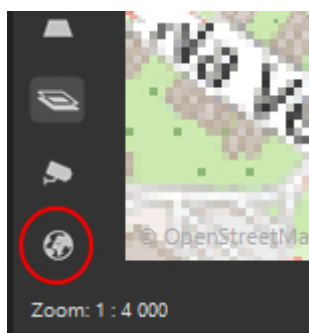
Dalším způsobem, jak provádět rychlé posuny v mapě, je uchopení vyznačeného rámečku (stisknutí levého tlačítka myši kdekoli uvnitř rámečku) a jeho posouvání po náhledovém okně. Hlavní mapová plocha bude zobrazovat obsah dle aktuální pozice rámečku.

Mapový zoom (přiblížení či oddálení mapy) lze nejjednodušší provádět pomocí kolečka myši, které provádí plynulé přiblížení či oddálení mapy. Při použití kolečka myši pro ovládání mapového zoomu je střed operace přiblížení nebo oddálení mapy určen pomocí aktuální pozice kurzoru myši. Pokud není myš kolečkem vybavena (samozřejmě i pokud je), je možné provést přiblížení mapy pomocí funkce Zoom oblasti.



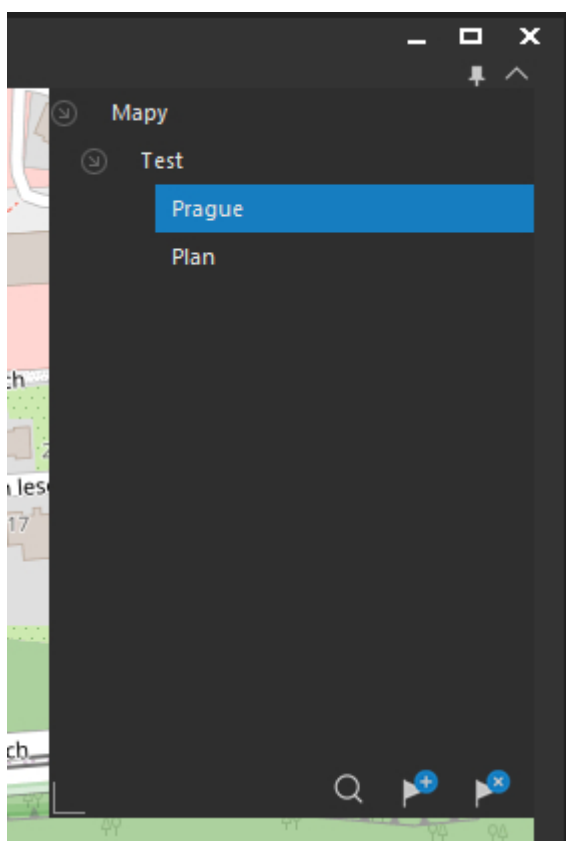
Po stisku tohoto tlačítka je vybraná funkce aktivní a je možné tažením myši při stisknutém levém tlačítku vytvořit výřez, na který bude po uvolnění tlačítka myši vytvořen zoom. Pravé tlačítko myši kdekoli v mapovém rámu provede oddálení mapy. Údaje o aktuálním přiblížení mapy jsou průběžně zobrazovány ve stavovém řádku mapového okna.

V levém dolním rohu mapového okna se nachází tlačítko pro rychlé zobrazení maximalizovaného pohledu na mapu (maximální oddálení mapy vzhledem k rozsahu mapových podkladů).



13.3.2. Přepínání úrovní

Mapové podklady dostupné v mapovém okně mohou být rozděleny do jednotlivých úrovní. Mapovými úrovněmi máme na mysli třetí rozměr mapy a je využit například všude tam, kde je zapotřebí integrovat plány pro víceposchodové budovy nebo v případě potřeby rozdělení rozsáhlejšího území na jednotlivé části. K přepínání úrovní slouží nástroj Legenda, která se nachází v pravém horním rohu mapového okna a pomocí přidružené šipky může být kdykoliv skryt nebo opět zobrazen.



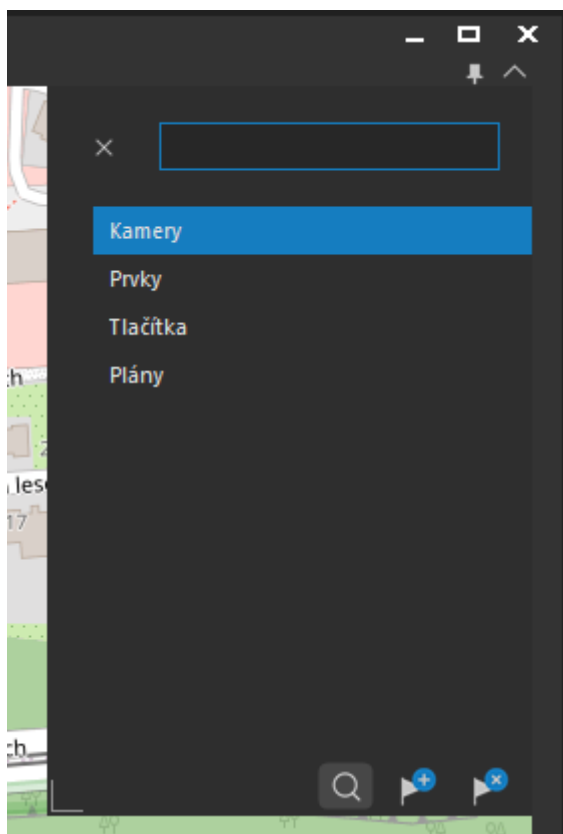
Ovládání legendy je velmi jednoduché. Aktivaci požadované mapové úrovně provedeme jednoduše tak, že ji vybereme ve stromové struktuře map. Rozměry legendy s uložením konečné pozice pro další spuštění mapy lze provést pomocí přetažení levého spodního rohu legendy.

POZNÁMKA

Přepínání mezi jednotlivými mapovými úrovněmi (patry budovy) lze provádět ručně zde popsaným způsobem, může však být také provedeno automaticky aplikací při zapnutí automatické synchronizaci (plné či událostní), pokud se výběr či událost vztahuje k jiné mapové úrovni.

13.3.3. Vyhledávání v mapě

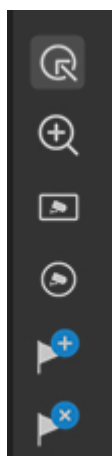
Do mapy mohou být lokalizovány kamery ze všech kamerových serverů, jejich zóny, uživatelská tlačítka, externí objekty a jejich prvky či plány. Pomocí integrovaného vyhledávání lze mezi všemi těmito entitami vyhledávat podle názvu. K aktivaci vyhledávání použijeme vyhledávací tlačítko pod legendou.



Vyhledávání probíhá v reálném čase a výsledky jsou ihned viditelné v seznamu. Kliknutím na libovolný prvek lze provést vyhledání a vycentrování v mapě.

13.4. Další mapové funkce

Panel nástrojů v mapovém okně obsahuje některé další funkce pro činnosti s mapou. Zde si uvedeme jejich stručný popis.



Funkce posunu a výběru. Pokud je aktivována tato funkce, je možné provádět plynulé posuny mapy způsobem popsaným výše. Přestože panel nástrojů obsahuje funkce pro výběr prvků (kamer), je možné tuto funkci použít též jako výběrovou. Důvod spočívá v tom, aby bylo možné při rychlých posunech či hledání v mapě provést také rychlý výběr kamer bez nutnosti volby jiné funkce z panelu nástrojů. Pokud při použití této funkce stiskneme a podržíme klávesu CTRL, bude funkce fungovat stejně jako funkce Výběr obdélníkem popsaná níže.



Funkce zoomování oblasti. Při použití této funkce můžeme v mapě vytvořit výřez (vymezit obdélníkovou oblast), na kterou bude vytvořeno přiblížení.



Funkce výběru obdélníkem (stejnou funkci má tlačítko posunu při současném stisku klávesy CTRL). Pokud je aktivována tato funkce, můžeme v mapě vytvořit obdélníkovou oblast, v jejímž rámci budou vybrány všechny kamerové body a poté dojde k jejich zobrazení v některém z dohledových oken (dle lokálního nastavení). Při úvodním stisku myši je určen jeden z rohů obdélníkové oblasti.



Funkce výběru kruhem. Pokud je aktivována tato funkce, můžeme v mapě vytvořit kruhovou oblast, v jejímž rámci budou vybrány všechny kamerové body a poté dojde k jejich zobrazení v některém z dohledových oken (dle lokálního nastavení). Při úvodním stisku myši je určen středový bod kruhu.



Funkce umístění prvku. Pomocí této funkce lze do mapy umístit jednotlivé prvky (např. kamerové body). Funkce bude aktivována (nebo vyvolá příslušnou akci), pouze pokud se nacházíte v administrační sekci a máte pak příslušná oprávnění.



Funkce výmazu prvku. Pomocí této funkce lze z mapy odebírat již lokalizované prvky (např. kamerové body). Funkce bude aktivována (nebo vyvolá příslušnou akci), pouze pokud se nacházíte v administrační sekci a máte pak příslušná oprávnění.

Kromě těchto funkcí jsou v levém dolním rohu k dispozici funkce pro zobrazení či skrytí aktivního dynamického obsahu. To se týká tlačítek, zón, map a videa z kamer.

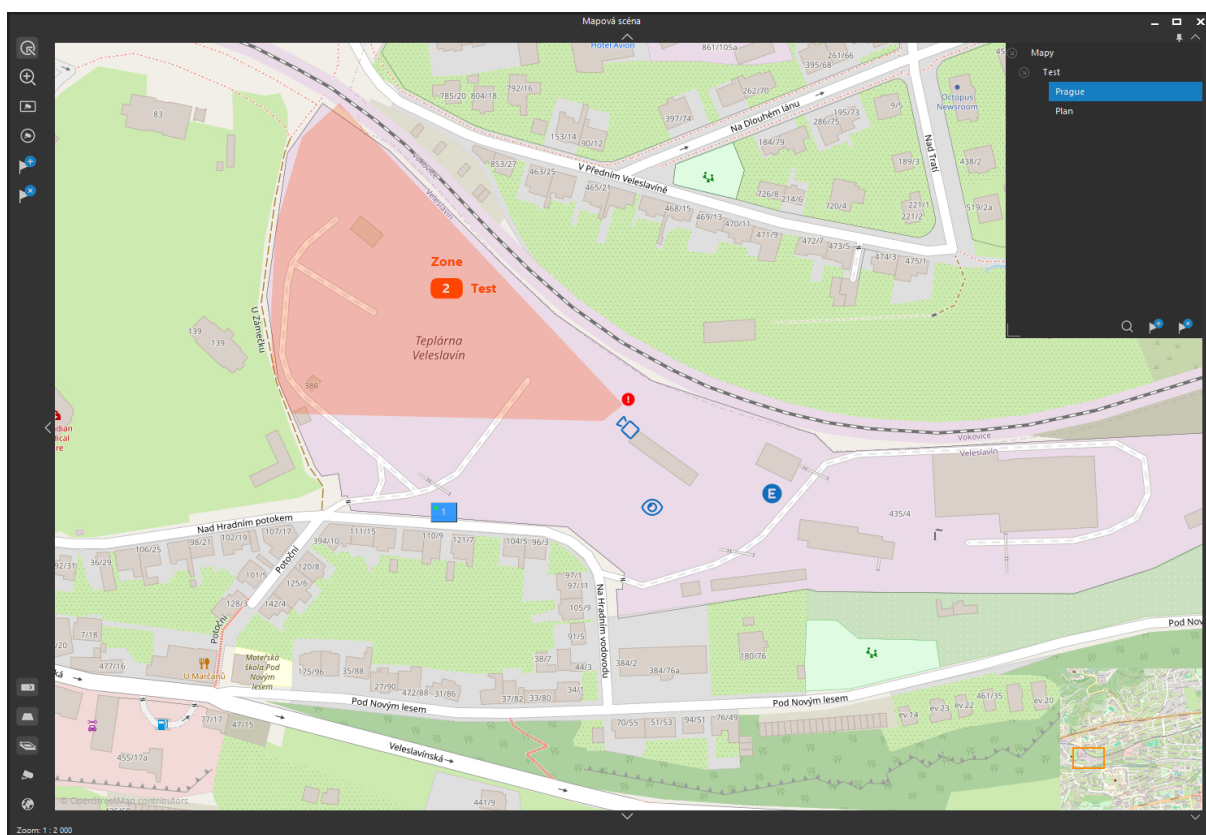


13.5. Dynamická mapová vrstva a náhled videa v mapě

Nad každou mapovou úrovní je mapovým oknem vždy vykreslena dynamická vrstva obsahující např.:

- symboly kamer,
- zóny kamer,
- automatické zónové čítače,
- symboly externích prvků,
- události s odlišením jejich stáří,
- uživatelská tlačítka,
- živé video kamer,
- propojení na jiné mapové úrovně.

Tato vrstva se neustále mění (automaticky u všech uživatelů) v závislosti na výskytu událostí v systému či přidávání, odebírání a změny lokalizace kamer nebo uživatelských tlačítek, úpravách barvy a podoby symbolu, lokální definice velikosti symbolů atd.



Kamery a uživatelská tlačítka jsou při implicitním nastavení v rastrové mapě zobrazena vždy a ve vícevrstvé mapě (ze zdroje OpenStreetMap) pro měřítko 1:35 000 a nižší. Ve vyšším měřítku (nižší podrobnosti mapy) by mohly tyto prvky nevhodně zakrývat velkou část mapových podkladů a ztížit orientaci v mapě.

POZNÁMKA

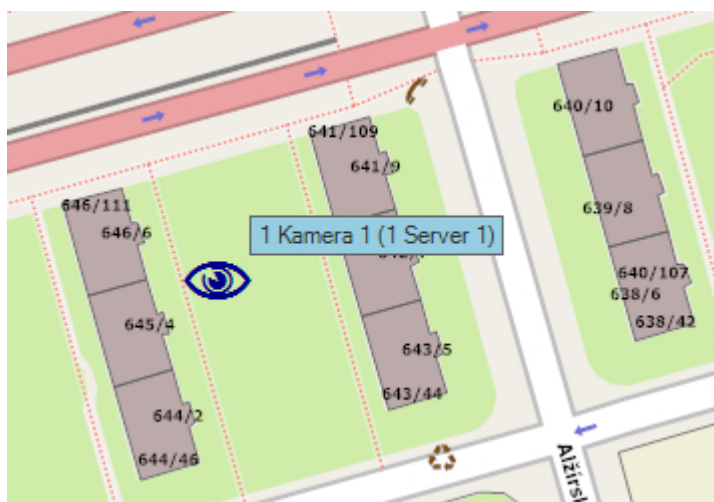
Změnu nastavení tohoto měřítko a další nastavení lze provést v lokálním nastavení Vaší klientské aplikace.

Mapa je dále vybavena funkcí inteligentního sdružování prvků stejného typu (kamery, externí prvky, události) do jednoho zástupného prvku, pokud by vzhledem k aktuálně zvolenému mapovému měřítku byly symboly překresleny přes sebe. Na sdruženém symbolu je pak vždy zobrazeno číslo udávající počet prvků, které zastupuje.

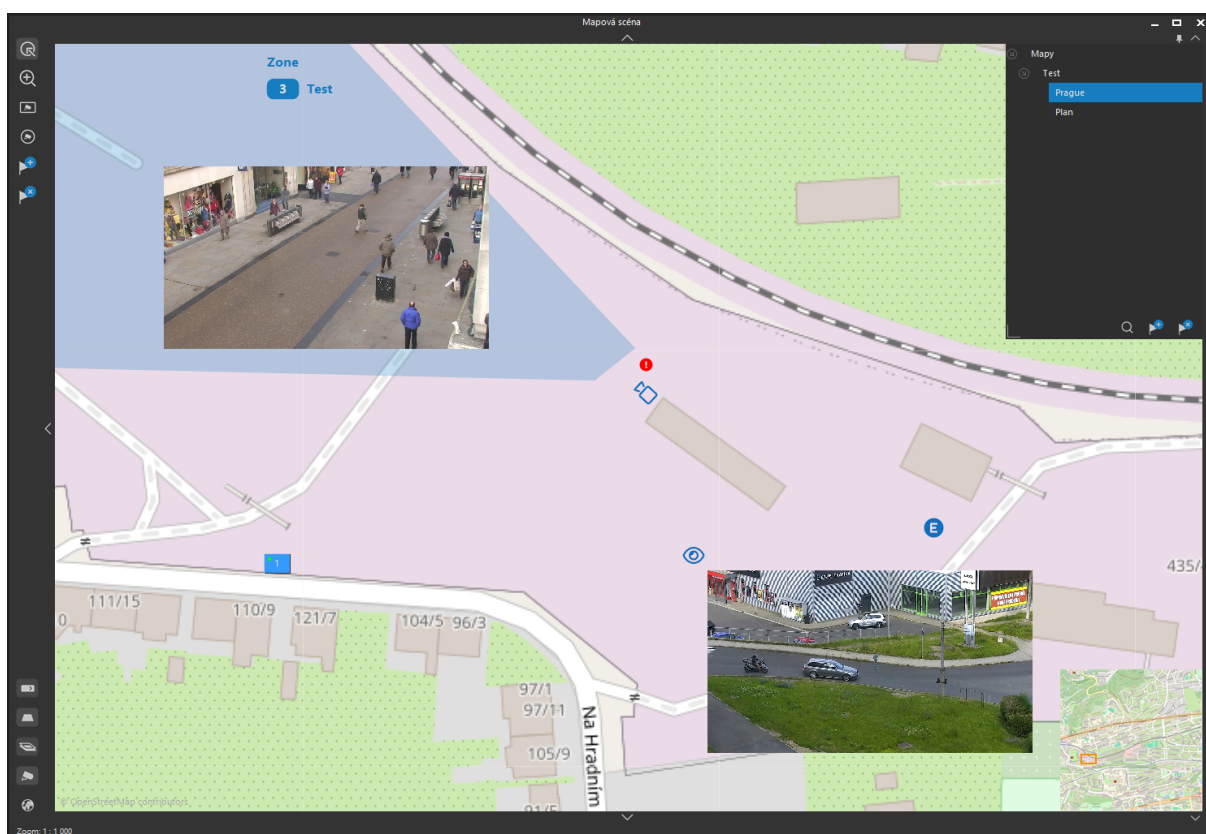


Uživatelská tlačítka je možné zobrazovat a skrývat také nezávisle na aktuálním přiblížení mapy pomocí tlačítka v levém spodním rohu mapového okna (nad symbolem kamery).

Pokud není zapnuta funkce video náhledu, je pro každou kameru, nad kterou setrváte nepatrnou dobu ukazatelem myši generován text s identifikací kamery.



Na panelu nástrojů mapového okna se dále nachází funkce, pomocí které je možné aktivovat video náhled přímo v mapovém okně, toto tlačítko má symbol kamery a je umístěno ve spodní části nástrojové lišty (nad funkcí celkový pohled). Pokud je tento nástroj aktivován, bude kromě textového rámečku s identifikací kamery k dispozici přímo v mapovém okně také náhled videa pro danou kameru.



Při setrvání myši postupně nad více kamerami se video náhled zobrazí až pro 5 kamer současně, poté se při dalším setrvání nad jinou kamerou začnou nejdříve otevřená okna automaticky zavírat.

TIP

Umístění kurzoru do zóny má stejný efekt v podobě zobrazení videa z kamery navíc rozšířený o možnost pohybu kamery na preset, pokud je s ním zóna svázána.

Pokud chcete některý video náhled vypnout ručně, stačí do něj kliknout myší. Veškeré video náhledy také budou zavřeny, pokud je na nástrojové liště deaktivována funkce zobrazování video náhledu. Video náhledy také budou uzavřeny pokud je nutné z libovolného důvodu (ruční či automatické přepnutí) nutné změnit mapovou úroveň (nikoliv mapové vrstvy).

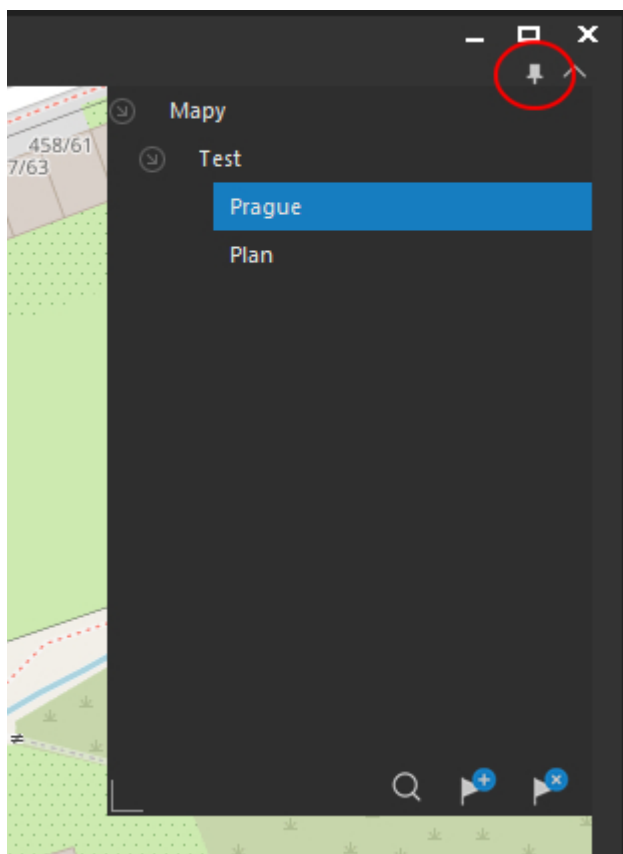
POZNÁMKA

Náhledy videa jsou v mapě umístěny geograficky. To znamená, že při posunu či zoomu mapy se budou náhledy videa posouvat ve stejném smyslu jako symboly kamer. Při nedostatečném zlomu mapy se tedy mohou náhledy videa překrývat. Přiblížením mapy lze překrytí eliminovat.

13.6. Zobrazení mapy přímo v dohledovém okně

Nejčastějším způsobem pro zobrazení mapy je zobrazení v samostatném mapovém okně. Tato konfigurace je nejvýhodnější pro vícemonitorové pracoviště. Pokud máte k dispozici jen jeden monitor anebo chcete mít všechny Vaše monitory obsazeny dohledovými okny, můžete mapu integrovat přímo do dohledového okna. Mapa může být v takovém případě zobrazena na libovolném místě pohledu.

Zapojení mapy do pohledu se provede tak, že v mapovém okně kliknete na symbol špendlíku v pravém horním rohu. Aplikace Vám napoví, že v dalším kroku je nutné vybrat prázdné místo v pohledu v libovolném dohledovém okně. Po tomto výběru dojde ke změně zobrazení mapy, která se od této chvíle bude zobrazovat přímo v dohledovém okně na zvoleném místě. Uvolnění mapy z pohledu se provede opět kliknutím na symbol špendlíku, který se nyní zobrazuje v levém horním rohu.



POZNÁMKA

Pokud je mapa umístěna přímo v dohledovém okně, toto nastavení bude uloženo také spolu s pracovním prostorem.

POZNÁMKA

Umístění mapy je svázáno s dohledovým oknem a pozicí v něm, nikoliv přímo s konkrétním pohledem složeným z kamer. Při přepínání pohledů se tedy mapa neztrácí a inteligentně se zobrazuje na správném místě v pohledu.

POZNÁMKA

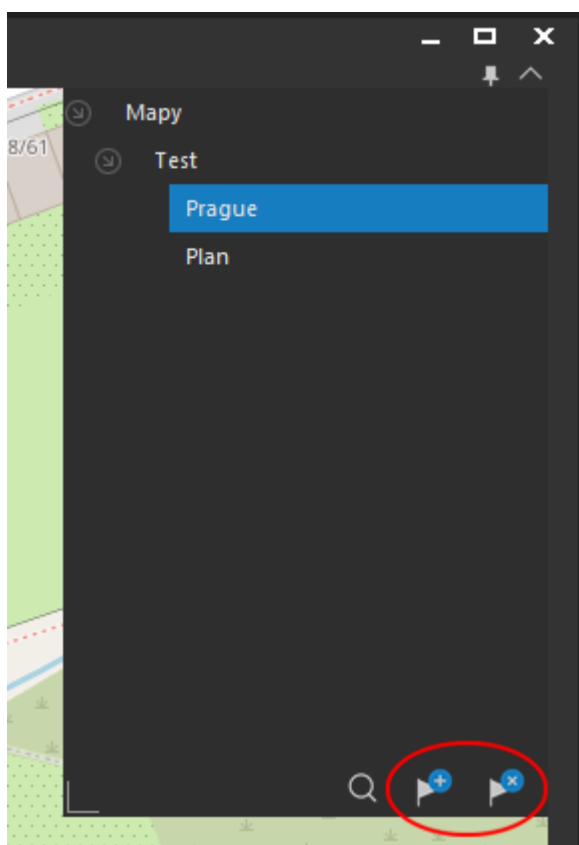
Pokud je mapa zobrazena přímo v dohledovém okně, výběr kamer v mapě je automaticky přesměrován do jiného dohledového okna.

13.7. Geografické propojení mapových úrovní

Jednotlivé mapové úrovně uspořádané v přehledné stromové struktuře poskytují dobrý přehled o všech importovaných mapových podkladech. Tyto úrovně jsou samozřejmě automaticky vybírány v závislosti na výběru kamer či výskytu událostí v systému.

Máme-li však v systému použité jak mapové podklady ze zdrojů OpenStreetMap, tak např. plány budovy, budeme intuitivně očekávat, že při maximálním přiblížení městské mapy bude možné automaticky „vstoupit“ do budovy a zobrazit její plán. Tohoto fungování lze docílit pomocí geografické lokalizace mapových podkladů, kdy plán budovy lokalizujeme do podkladu OpenStreetMap.

Lokalizaci mapy provádíme velmi podobně jako v případě lokalizace kamer. Pro určení lokalizace (či její zrušení) je nutné vybrat mapu či plán, který chceme umístit, použít jedno z tlačítek určení lokalizace mapy (pod nástrojem legenda) a provést přepnutí do cílové mapy následované určením bodu, kde bude mapa umístěna.



V místě, kde je mapa vložena, bude zobrazen symbol dveří, pomocí kterých je možné virtuálně „vstoupit“ do geograficky orientovaného plánu budovy.

POZNÁMKA

Alternativním a rychlejším způsobem lokalizace mapových podkladů je možnost použití přetažení mapové úrovně z legendy přímo do cílové mapové úrovně pomocí myši.

**POZNÁMKA**

Geograficky orientovaný plán lze také opustit bez toho, aniž bychom museli nadřazenou mapovou úroveň vybírat pomocí nástroje Legenda. Postačí použít kolečko myši a po úplném oddálení vnořené mapy pokračovat v oddálení. Další oddálení totiž provede automatické přepnutí do nadřazené mapové úrovně.

Kapitola 14 - Přístup ze zařízení Apple

14.1. Podporované funkce

Aplikace pro platformu Apple iOS je určená pro zařízení iPhone a iPad a je vybavena mimo jiné těmito funkcemi:

- výkonné zobrazování plynulého videa (podporovaný formát MJPEG, H264, H265 a AV1),
- hardwarová akcelerace videa,
- zobrazení mobilních pohledů až do 16 kamer současně,
- podpora sekundárního streamu ve sdílených pohledech,
- současné přehrávání všech kamer v pohledu s náhledem časové osy,
- přehrávání zvuku (podporovaný formát G711),
- vysílání zvuku do kamery,
- digitální zoom a digitální PTZ pro všechny kamery včetně záznamu,
- vysoce citlivé ovládání otočných kamer dle nastavených PTZ priorit v systému a oprávnění,
- přechod na preset body otočných kamer,
- možnost aktivace výstupů kamer dle oprávnění,
- intuitivní prohlížení záznamu a jeho přehrávání včetně zvuku,
- náhled a přehrávání událostí,
- možnost lokálního nastavení zobrazení videa,
- možnost exportu snímků,
- vysílání videa (a zvuku) z kamery mobilního zařízení do systému včetně GPS souřadnic,
- zobrazování metadat z neuronových sítí živě i ze záznamu,
- možnost detekce RZ přímo na displeji zařízení,
- možnost rozpoznání obličeje přímo na displeji zařízení,
- zobrazení a odbavení požadavku vícefaktorové autentizace.

14.2. Spuštění a přihlášení

Do kamerového systému je možné vstoupit pouze se znalostí přihlašovacích údajů.

11:09

Zadejte přihlašovací údaje:

Jméno

Heslo

10.0.0.1

Vstup

Přehled Živý pohled Záznam Pohledy Nastavení

11:39 dop. pá 10. 3. 100 %

Zadejte přihlašovací údaje:

Podržte tlačítko pro přejmenování.

 Přehled  Živý pohled  Záznam  Pohledy  Nastavení  EN

POZNÁMKA

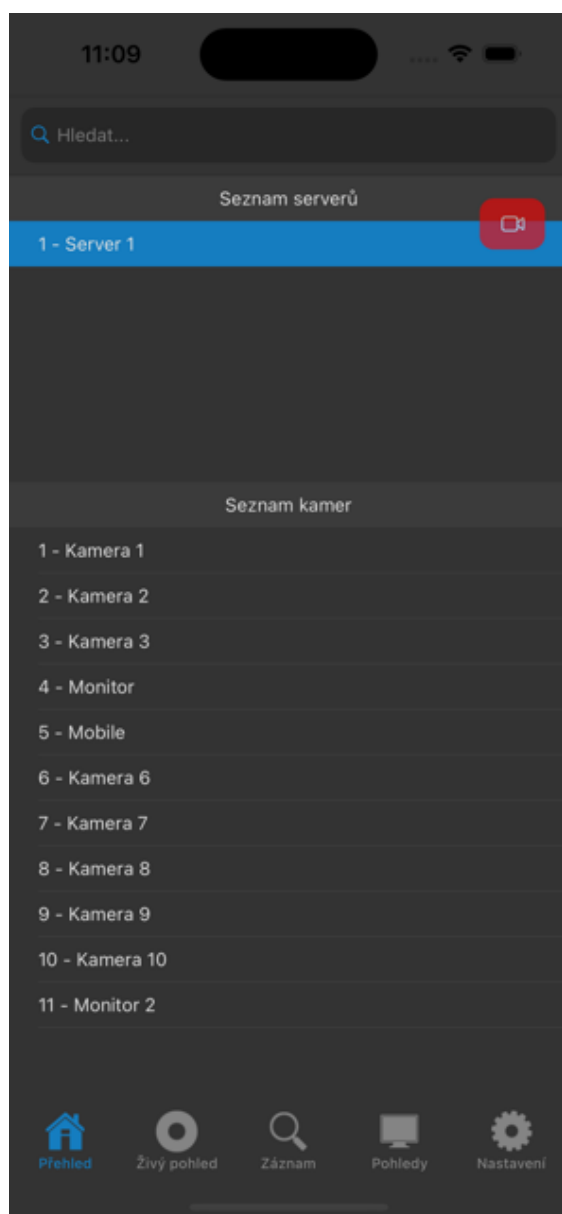
Aplikace si zapamatuje poslední přihlášení a pokud tuto funkci nedeaktivujete v nastavení aplikace, budou opakovaná přihlášení již zcela automatická.

Při přihlašování k více kamerovým systémům se jejich adresy ukládají do historie, kterou je možné zobrazit a provést výběr kamerového systému přímo z ní.

TIP

Jednotlivé položky historie lze pojmenovat a lépe se tak v historii orientovat.

14.3. Seznam kamer a živé video



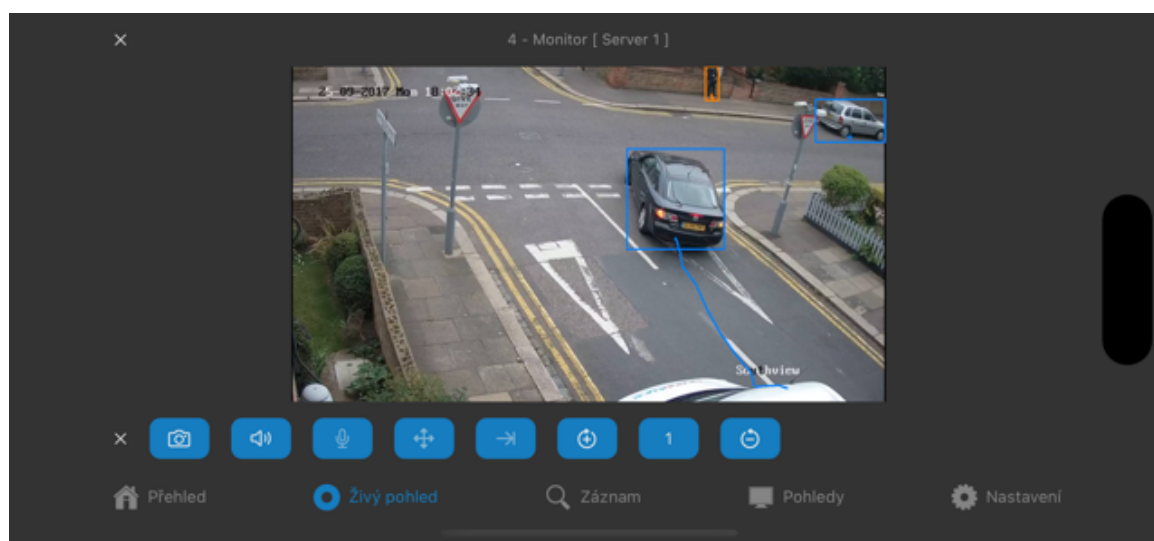
Po přihlášení se aplikace automaticky připojí ke všem dostupným kamerovým serverům. Výběrem serveru lze zobrazit seznam dostupných kamer. Mezi kamerami lze vyhledávat za pomoci pole pro vyhledávání nad seznamem serverů. Vyhledávání je vždy prováděno na vybraném kamerovém serveru.

TIP

Opakovaným dotykem kamerového serveru dojde ke zrušení jeho výběru, a lze tak provádět vyhledávání kamer na všech serverech současně.

Výběrem kamery je možné se přepnout do režimu živého videa.





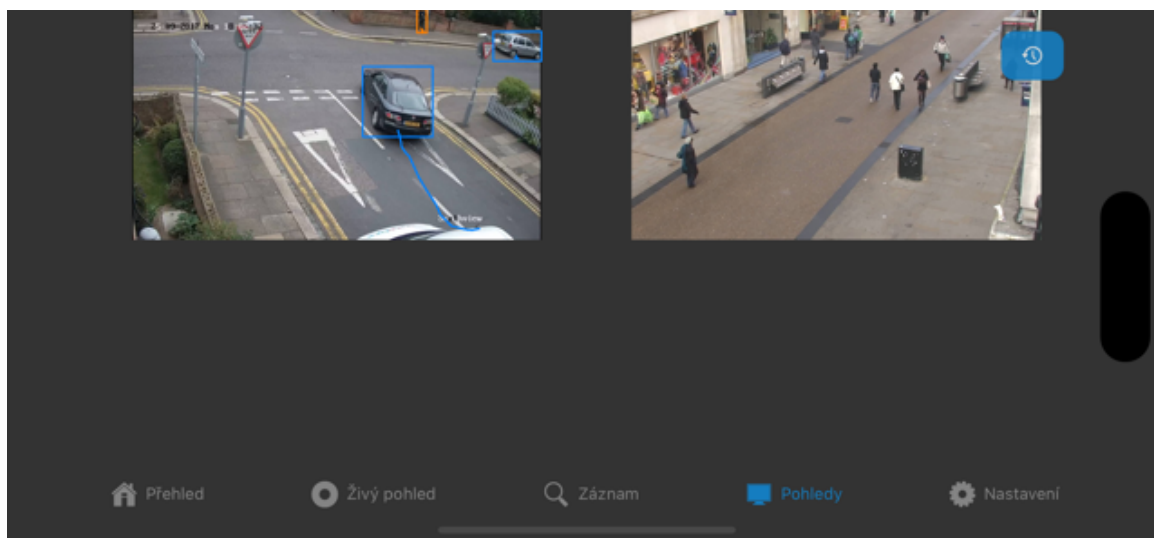
V režimu živého videa jsou k dispozici následující tlačítka:

- tlačítko pro uložení snímku,
- tlačítko pro připojení či odpojení zvuku,
- tlačítko pro aktivaci či deaktivaci vysílání zvuku do kamery,
- tlačítko pro aktivaci PTZ ovládání kamery,
- tlačítko pro zobrazení seznamu presetů,
- tlačítko pro aktivaci výstupu,
- tlačítko pro změnu čísla výstupu,
- tlačítko pro deaktivaci výstupu.

V režimu živého videa lze kamery jednoduše přepínat pomocí gesta swipe (přejetí po displeji). Pokud byla kamera vybrána ze seznamu kamer, bude přepínání prováděno mezi kamerami serveru. Pokud byla zvolena v pohledu, bude přepínání prováděno mezi kamerami daného pohledu.

14.4. Pohledy více kamer

V části Pohledy lze zobrazit seznam pohledů, které administrátor umístil do skupiny pohledů s názvem Mobile. Může se jednat o pohledy sestávající z matice 4, 9 nebo 16 kamer. Výběrem pohledu je pohled přepnut do režimu živého náhledu. Pohledy zohledňují sekundární streamy, pokud jsou v pohledu použity.

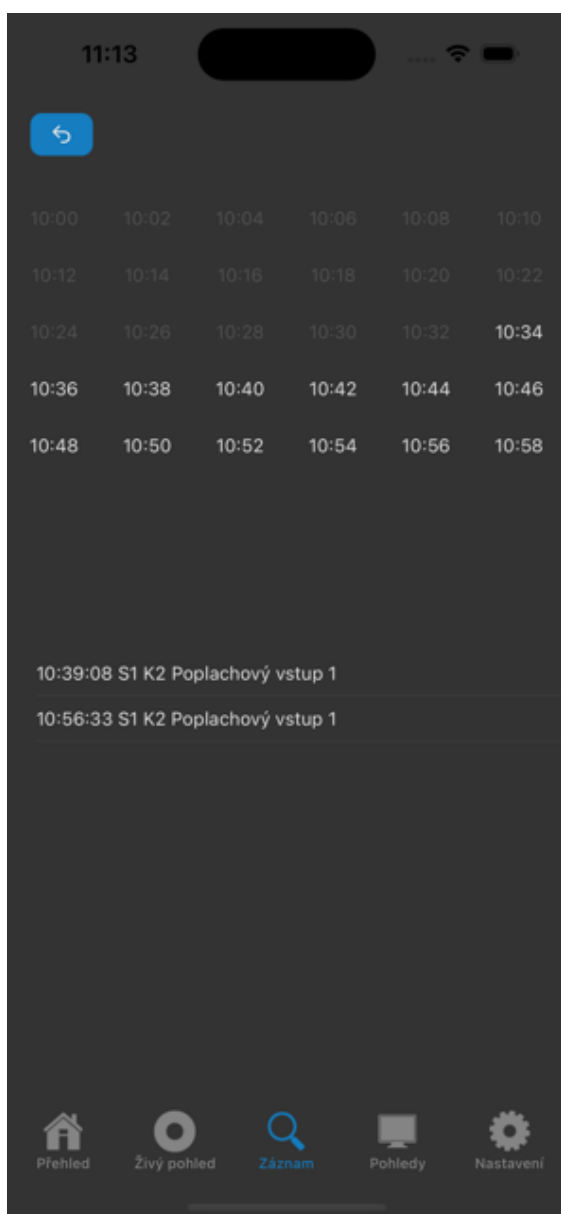


14.5. Přehrávání záznamu

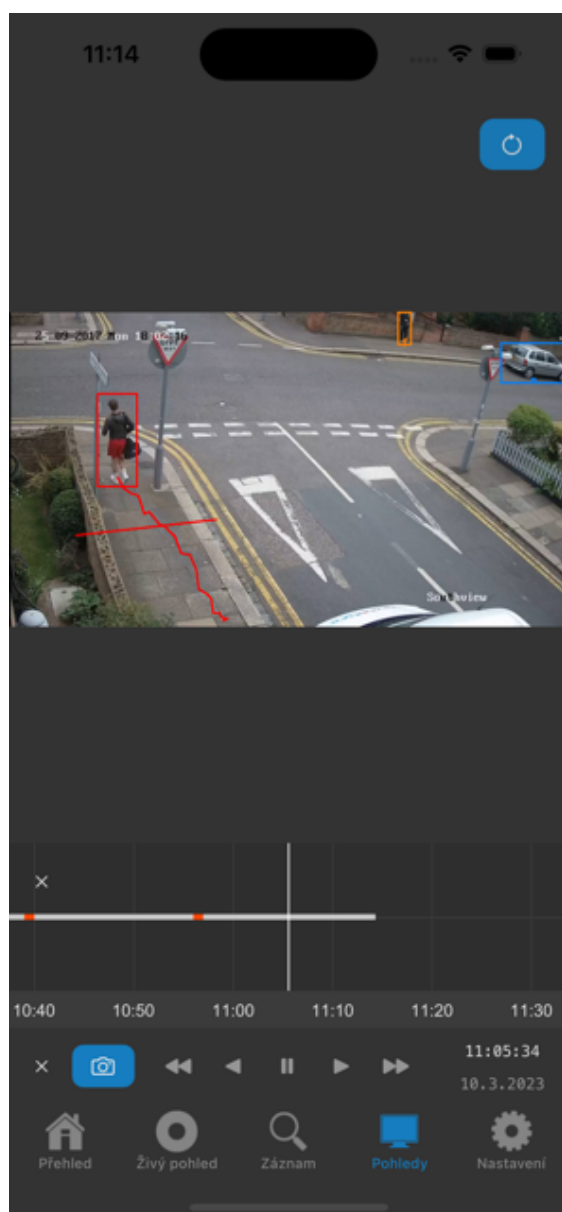
Do přehrávání záznamu vybrané kamery je možné vstoupit přímo z hlavního menu aplikace anebo přepnutím pohledu do režimu přehrávání. Pokud platí první možnost, bude pro vybranou kameru zobrazen nejprve časový přehled, kde je možné postupným výběrem dospět až k podrobnému hodinovému přehledu s výpisem událostí.

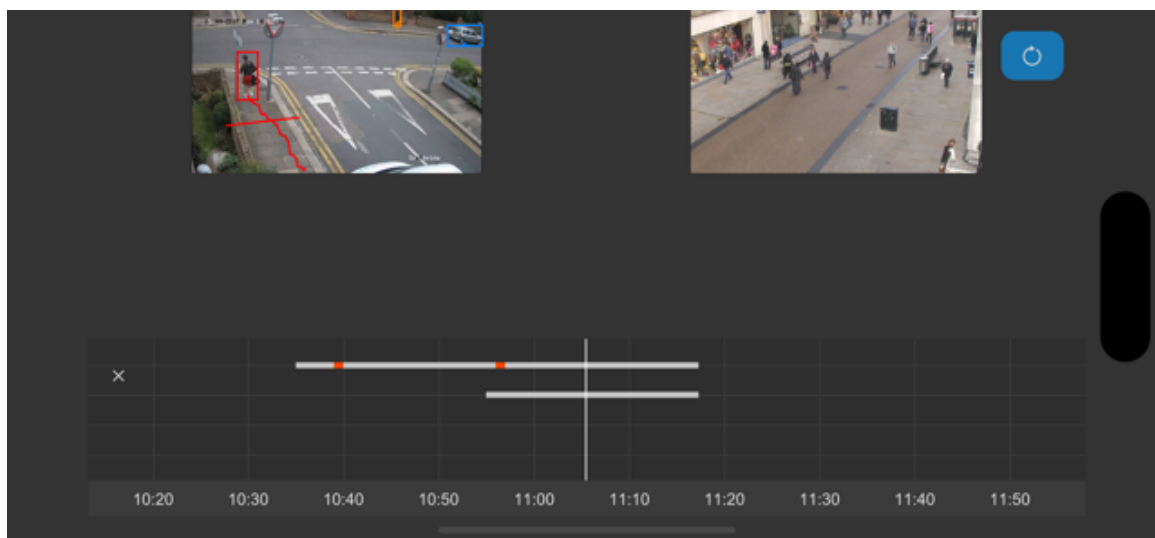
POZNÁMKA

V přehledu jsou vizuálně odlišeny údaje o dnech či hodinách, ve kterých se vyskytují nějaké události.



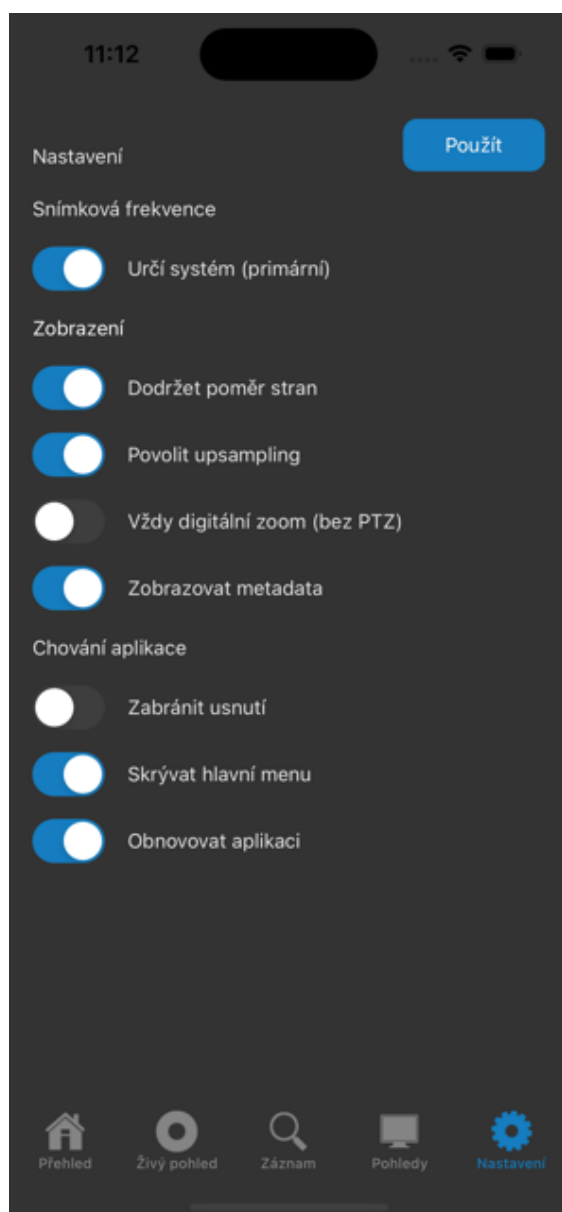
V samotném přehrávání jsou pak dispozici dvě ovládací lišty s náhledem časové osy a s ovládáním přehrávání, ve kterém je možné měnit směr a rychlost přehrávání.





14.6. Nastavení

Část Nastavení obsahuje možnosti uzpůsobení zobrazení či chování aplikace, jak ukazuje následující obrázek.



Volba Skrývat hlavní menu inteligentně zvětšuje obraz zobrazovaného videa, pokud není zaznamenán po určitou dobu žádný dotyk na obrazovce. Tuto lištu je možné opět zobrazit dvojitým dotykem. Podobný princip je použit i u ostatních ovládacích lišt (funkce živého náhledu, přehrávání, časová osa). Dvojitý dotyk vždy postupně zobrazí hlavní a dodatečné ovládací lišty. Teprve poté provede případně další funkci jako je přepnutí do detailu apod.

14.7. Využití integrované kamery

POZNÁMKA

Možnost vysílání videa z mobilního zařízení je k dispozici až od edice ATEAS Security PROFESSIONAL.

Aplikace nabízí unikátní možnost vysílání živého videa, zvuku a GPS souřadnic přímo z Vašeho mobilního zařízení do systému ATEAS, kde je s Vaší kamerou zacházeno stejně jako s běžnými dohledovými kamerami. Aby mohla být kamera Vašeho zařízení použita, je třeba, aby administrátor systému přidal do systému kameru typu uživatel, který se bude přihlašovat na mobilním zařízení.

Pro využití zvuku je nutné v administraci takto přidané kamery aktivovat zvuk. Pro využití GPS souřadnic (a zobrazení v souřadnicově orientované mapě živě i ze záznamu) je nutné lokalizovat kameru na libovolné výchozí místo do mapy.

Vysílání lze zahájit tlačítkem se symbolem kamery na úvodní obrazovce u seznamu serverů, stejným tlačítkem lze pak vysílání vypnout.

POZNÁMKA

Na akci zahájení vysílání může být v systému navázána událost, a operátor tak může být na tuto skutečnost upozorněn.

Pokud je pro dané zařízení aktivována funkce rozpoznávání RZ vozidel anebo rozpoznávání obličejů, je možné získat výsledek okamžitě na displej Vašeho telefonu. To platí i pro zobrazení rozpoznávaných obličejů z databáze a pro všechny systémové a uživatelské seznamy RZ vozidel.



Kapitola 15 - Přístup ze zařízení Android

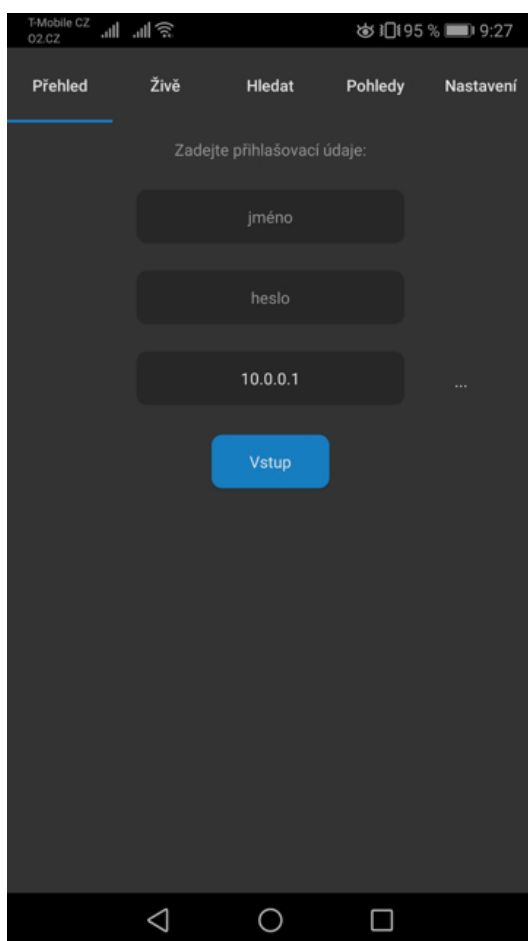
15.1. Podporované funkce

Aplikace pro platformu Android je určena pro zařízení typu telefon, TV či displej a je vybavena mimo jiné těmito funkcemi:

- výkonné zobrazování plynulého videa (podporovaný formát MJPEG, H264, H265 a AV1),
- hardwarová akcelerace videa,
- zobrazení mobilních pohledů až do 16 kamer současně,
- podpora sekundárního streamu ve sdílených pohledech,
- současné přehrávání všech kamer v pohledu s náhledem časové osy,
- přehrávání zvuku (podporovaný formát G711),
- vysílání zvuku do kamery,
- digitální zoom a digitální PTZ pro všechny kamery včetně záznamu,
- vysoce citlivé ovládání otočných kamer dle nastavených PTZ priorit v systému a oprávnění,
- přechod na preset body otočných kamer,
- možnost aktivace výstupů kamer dle oprávnění,
- intuitivní prohlížení záznamu a jeho přehrávání včetně zvuku,
- náhled a přehrávání událostí,
- možnost lokálního nastavení zobrazení videa,
- možnost exportu snímků,
- vysílání videa (a zvuku) z kamery mobilního zařízení do systému včetně GPS souřadnic,
- zobrazování metadat z neuronových sítí živě i ze záznamu,
- push-video notifikace při událostech v systému,
- možnost detekce RZ přímo na displeji zařízení,
- možnost rozpoznání obličeje přímo na displeji zařízení,
- zobrazení a odbavení požadavku vícefaktorové autentizace.

15.2. Spuštění a přihlášení

Do kamerového systému je možné vstoupit pouze se znalostí přihlašovacích údajů.



POZNÁMKA

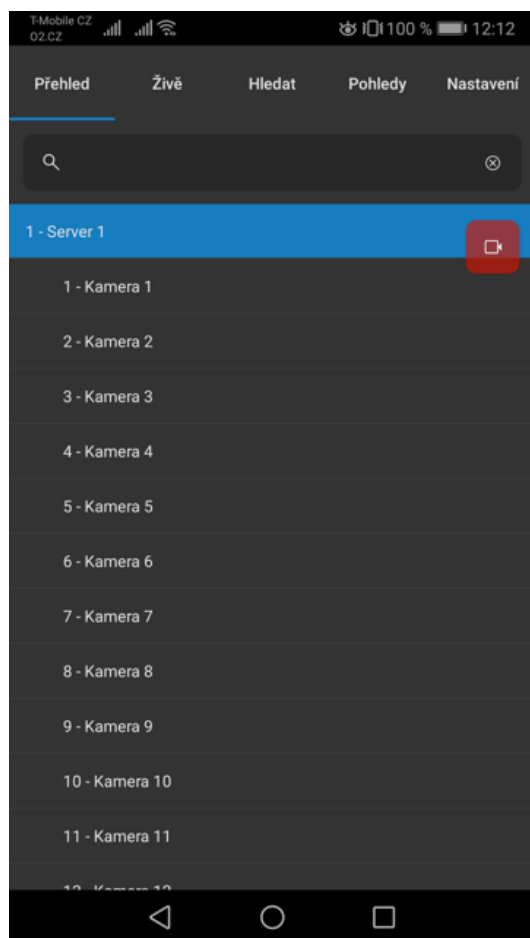
Aplikace si zapamatuje poslední přihlášení a pokud tuto funkci nedeaktivujete v nastavení aplikace, budou opakovaná přihlášení již zcela automatická.

Při přihlašování k více kamerovým systémům se jejich adresy ukládají do historie, kterou je možné zobrazit a provést výběr kamerového systému přímo z ní.

TIP

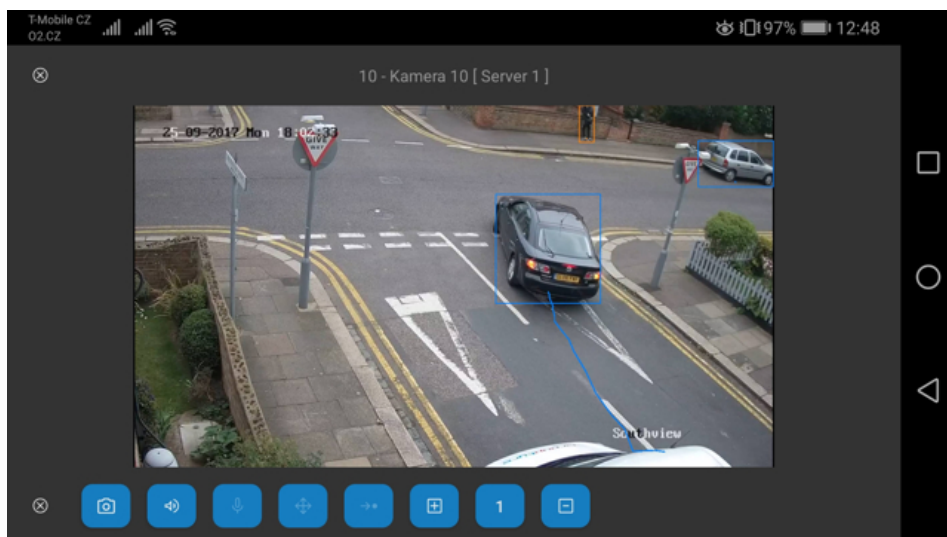
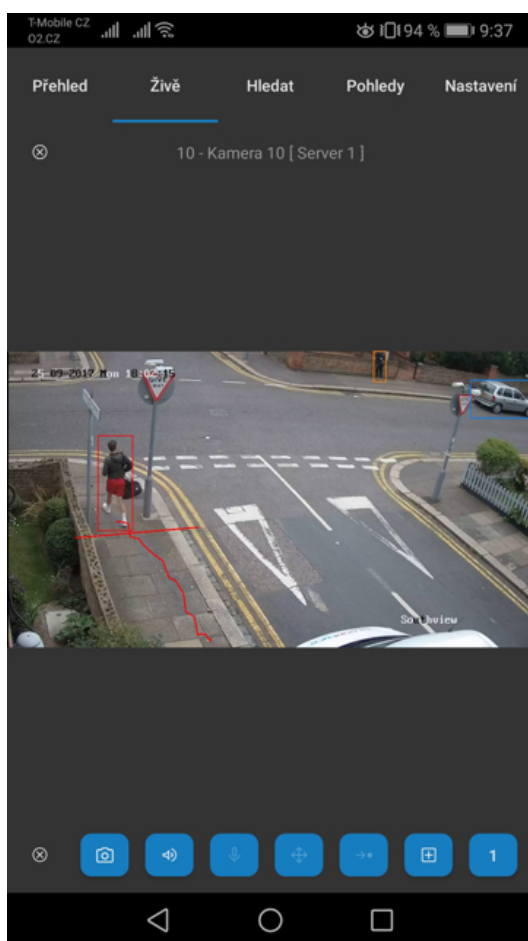
Jednotlivé položky historie lze pojmenovat a lépe se tak v historii orientovat.

15.3. Seznam kamer a živé video



Po přihlášení se aplikace automaticky připojí ke všem dostupným kamerovým serverům. Výběrem serveru lze zobrazit seznam dostupných kamer. Mezi kamerami lze vyhledávat za pomoci pole pro vyhledávání nad seznamem serverů. Vyhledávání je vždy prováděno nad všemi kamerovými servery.

Výběrem kamery je možné se přepnout do režimu živého videa.



V režimu živého videa jsou k dispozici následující tlačítka:

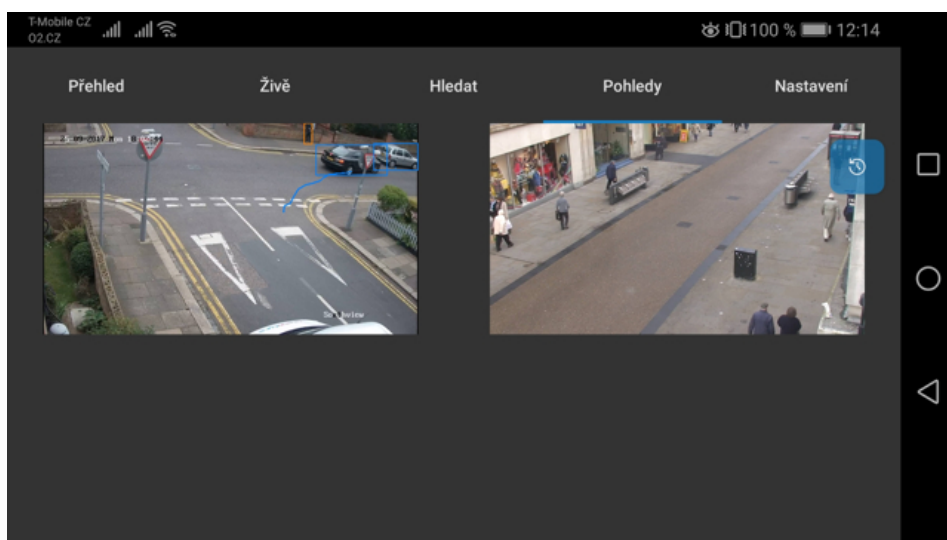
- tlačítko pro uložení snímku,
- tlačítko pro připojení či odpojení zvuku,

- tlačítko pro aktivaci či deaktivaci vysílání zvuku do kamery,
- tlačítko pro aktivaci PTZ ovládání kamery,
- tlačítko pro zobrazení seznamu presetů,
- tlačítko pro aktivaci výstupu,
- tlačítko pro změnu čísla výstupu,
- tlačítko pro deaktivaci výstupu.

V režimu živého videa lze kamery jednoduše přepínat pomocí gesta swipe (přejetí po displeji). Pokud byla kamera vybrána ze seznamu kamer, bude přepínání prováděno mezi kamerami serveru. Pokud byla zvolena v pohledu, bude přepínání prováděno mezi kamerami daného pohledu.

15.4. Pohledy více kamer

V části Pohledy lze zobrazit seznam pohledů, které administrátor umístil do skupiny pohledů s názvem Mobile. Může se jednat o pohledy sestávající z matice 4, 9 nebo 16 kamer. Výběrem pohledu je pohled přepnut do režimu živého náhledu. Pohledy zohledňují sekundární streamy, pokud jsou v pohledu použity.

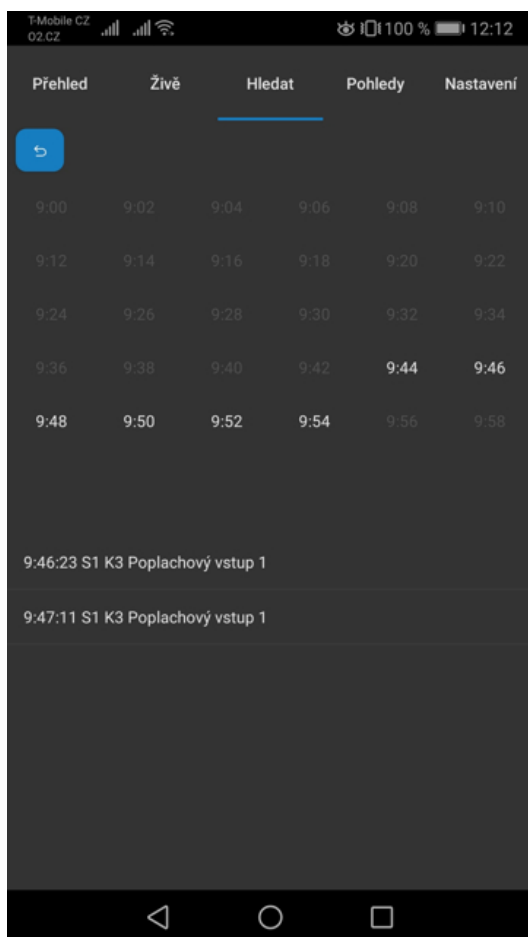


15.5. Přehrávání záznamu

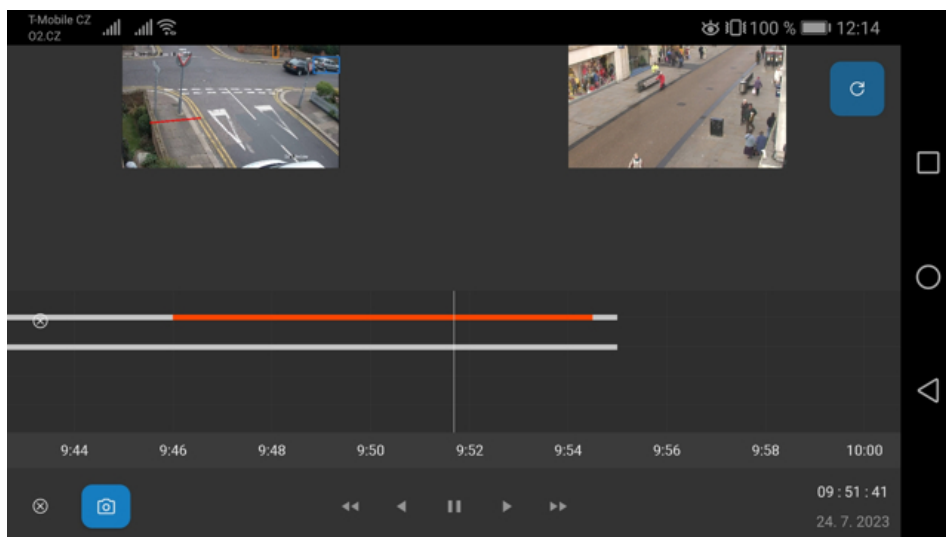
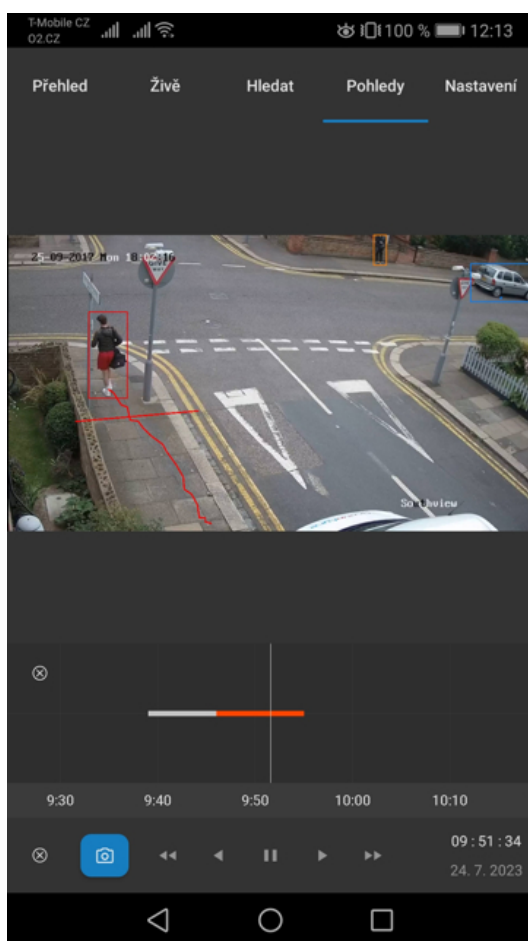
Do přehrávání záznamu vybrané kamery je možné vstoupit přímo z hlavního menu aplikace anebo přepnutím pohledu do režimu přehrávání. Pokud platí první možnost, bude pro vybranou kameru zobrazen nejprve časový přehled, kde je možné postupným výběrem dospět až k podrobnému hodinovému přehledu s výpisem událostí.

POZNÁMKA

V přehledu jsou vizuálně odlišeny údaje o dnech či hodinách, ve kterých se vyskytují nějaké události.

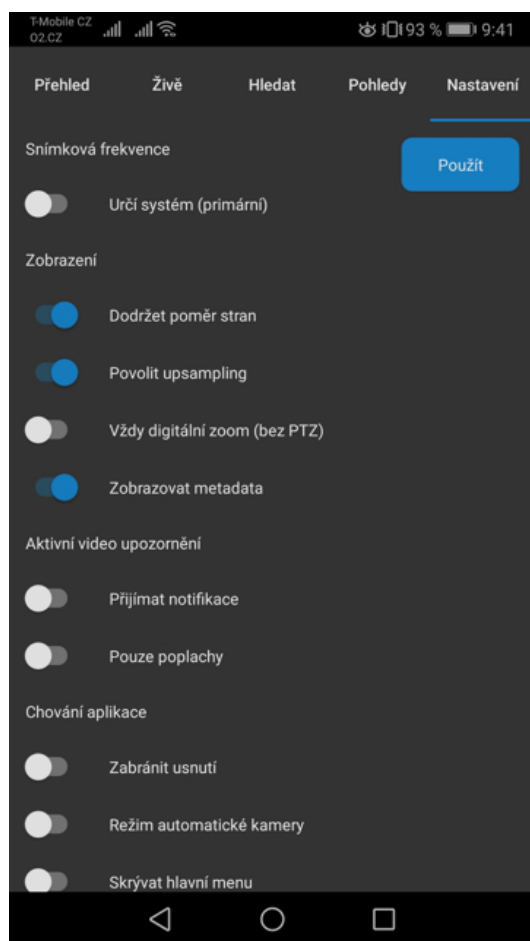


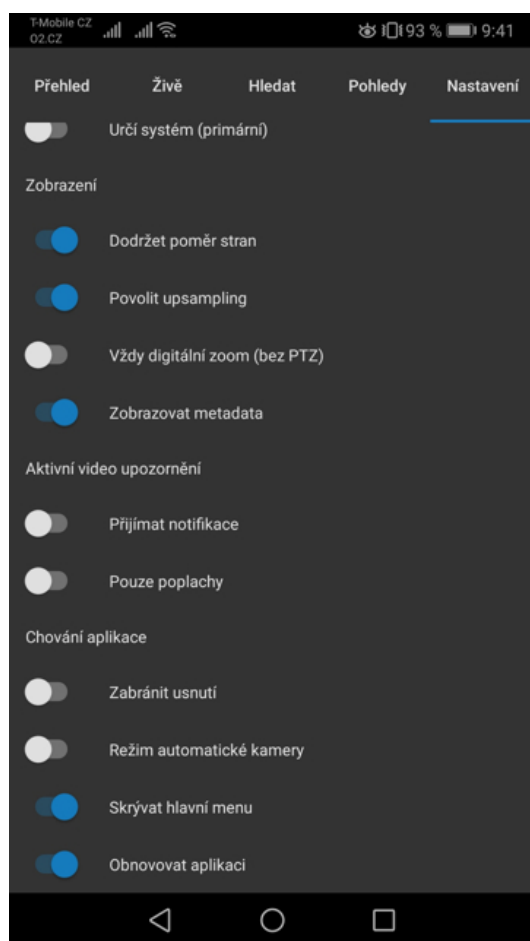
V samotném přehrávání jsou pak dispozici dvě ovládací lišty s náhledem časové osy a s ovládáním přehrávání, ve kterém je možné měnit směr a rychlost přehrávání.



15.6. Nastavení

Část Nastavení obsahuje možnosti uzpůsobení zobrazení či chování aplikace, jak ukazuje následující obrázek.

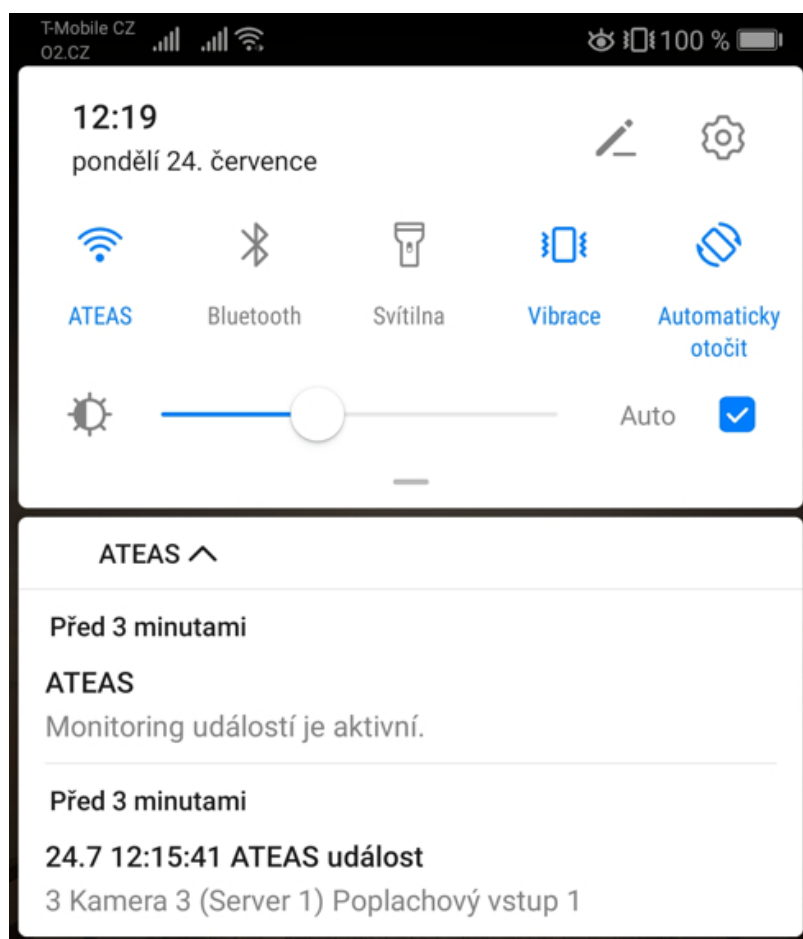




Volba Skrývat hlavní menu inteligentně zvětšuje obraz zobrazovaného videa, pokud není zaznamenán po určitou dobu žádný dotyk na obrazovce. Tuto lištu je možné opět zobrazit dvojitým dotykem. Podobný princip je použit i u ostatních ovládacích lišt (funkce živého náhledu, přehrávání, časová osa). Dvojitý dotyk vždy postupně zobrazí hlavní a dodatečné ovládací lišty. Teprve poté provede případně další funkci jako je přepnutí do detailu apod.

15.7. Notifikace

V části Nastavení lze aktivovat funkci push-video. Po aktivaci bude zařízení přijímat notifikace o událostech v systému, které lze jedním dotykem přehrát. Tato funkce využívá datové spojení přímo s administračním serverem systému, nikoliv služby výrobce operačního systému, a je vysoce optimalizována pro minimální nároky na spotřebu energie.



Pokud Vaše zařízení nemá v určité chvíli datové spojení, notifikace budou doručeny, jakmile to bude možné.

TIP

Pro omezení počtu notifikací lze aktivovat volbu Pouze poplachy nebo omezit uživatelský účet, aby měl oprávnění přijímat události pouze z určitých kamer.

15.8. Využití integrované kamery

POZNÁMKA

Možnost vysílání videa z mobilního zařízení je k dispozici až od edice ATEAS Security PROFESSIONAL.

Aplikace nabízí unikátní možnost vysílání živého videa, zvuku a GPS souřadnic přímo z Vašeho mobilního zařízení do systému ATEAS, kde je s Vaší kamerou zacházeno stejně jako s běžnými dohledovými kamerami. Aby mohla být kamera Vašeho zařízení použita, je třeba, aby administrátor systému přidal do systému kameru typu uživatel, který se bude přihlašovat na mobilním zařízení.

Pro využití zvuku je nutné v administraci takto přidané kamery aktivovat zvuk. Pro využití GPS souřadnic (a zobrazení v souřadnicově orientované mapě živě i ze záznamu) je nutné lokalizovat kameru na libovolné výchozí místo do mapy.

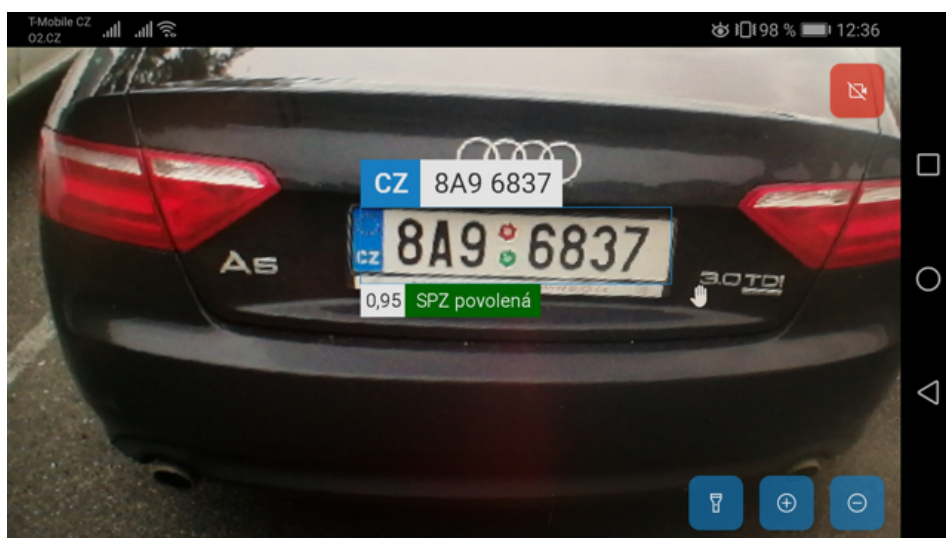
Vysílání lze zahájit tlačítkem se symbolem kamery na úvodní obrazovce u seznamu serverů, stejným tlačítkem lze pak vysílání vypnout.

POZNÁMKA

Na akci zahájení vysílání může být v systému navázána událost, a operátor tak může být na tuto skutečnost upozorněn.

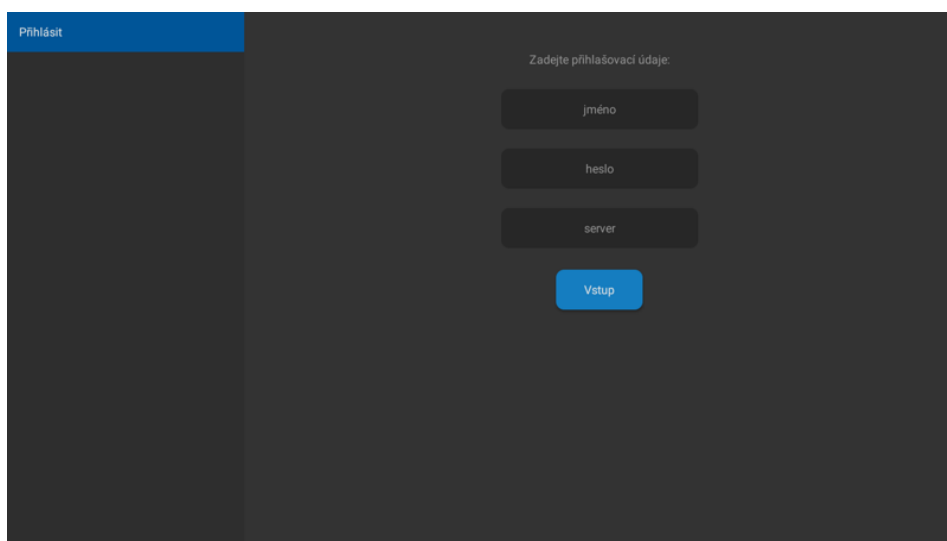
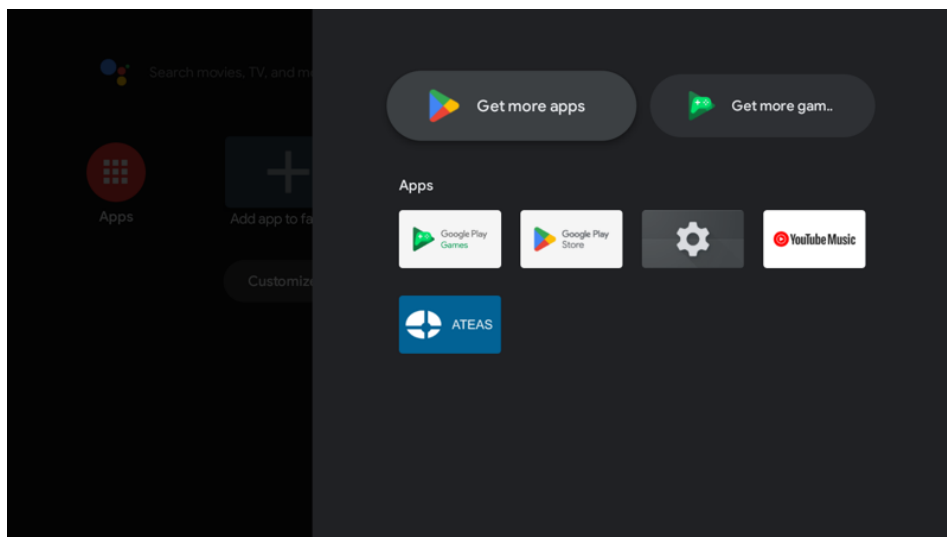
Pokud to dané zařízení podporuje, je možné provádět lineární zoom pomocí tlačítek nebo použít funkci pinch-to-zoom přímo v obraze. Během vysílání videa je také možné aktivovat světlo.

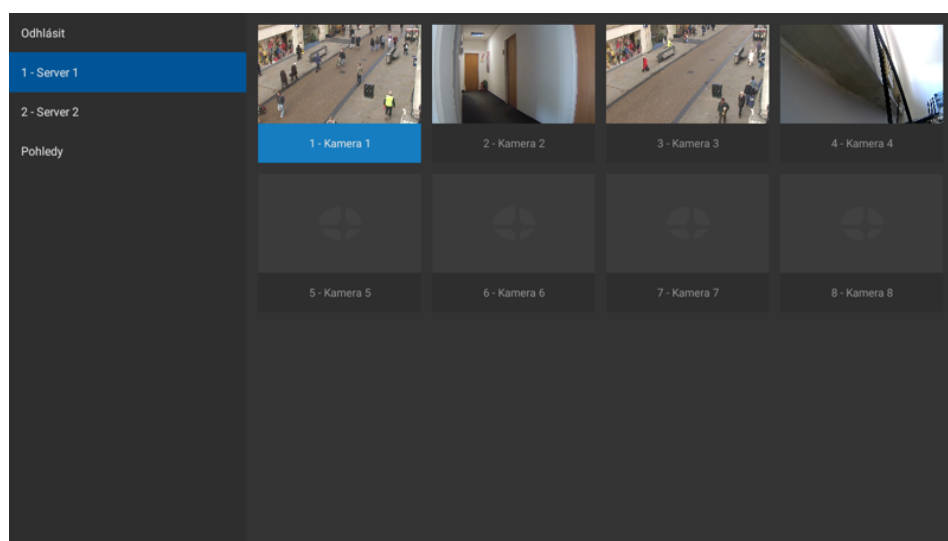
Pokud je pro dané zařízení aktivována funkce rozpoznávání RZ vozidel anebo rozpoznávání obličejů, je možné získat výsledek okamžitě na displej Vašeho telefonu. To platí i pro zobrazení rozpoznaných obličejů z databáze a pro všechny systémové a uživatelské seznamy RZ vozidel.



15.9. Android TV

Pro zařízení typu TV či displej má aplikace upravené uživatelské rozhraní, aby ji bylo možné pohodlně ovládat i pomocí dálkového ovladače.





V TV rozhraní lze jednoduše zobrazovat jednotlivé kamery nebo pohledy. Pohledy zohledňují sekundární streamy, pokud jsou v pohledu použity.

TIP

Náhled kamery je možné na server nahrát z dialogu po uložení snímku kamery.

15.9.1. Video stěna

Zařízení typu TV a displej mohou být součástí ATEAS video stěny a je možné je vzdáleně ovládat a zacházet s nimi stejným způsobem jako s běžnými stanicemi osazenými klientem v podřízeném režimu (pro ovládání z jiných počítačů).

Kapitola 16 - Aplikace pro monitoring obrazovky

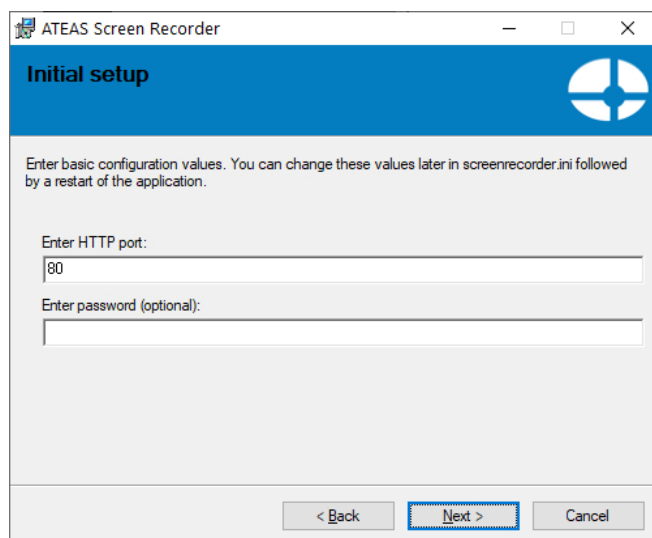
16.1. Instalace a zprovoznění

Součástí bezpečnostních systémů bývá i požadavek na monitoring obrazovek počítačů (nebo vybraného okna) některých uživatelů v podobě živého náhledu a záznamu činnosti. Součástí ATEAS Security je aplikace ATEAS Screen Recorder, která umožňuje s počítačem, na který je nainstalována, zacházet jako s kamerou. Oprávnění uživatelé tedy mohou sledovat živé video, kamera může provádět záznam včetně např. detekce pohybu apod. S daty uloženými z obrazovky počítače je možné poté dále zacházet stejně jako s daty z libovolné kamery včetně možností synchronního přehrávání s ostatními kamerami, vyhledávání a přehrávání, exportu snímků či videa atd.

POZOR

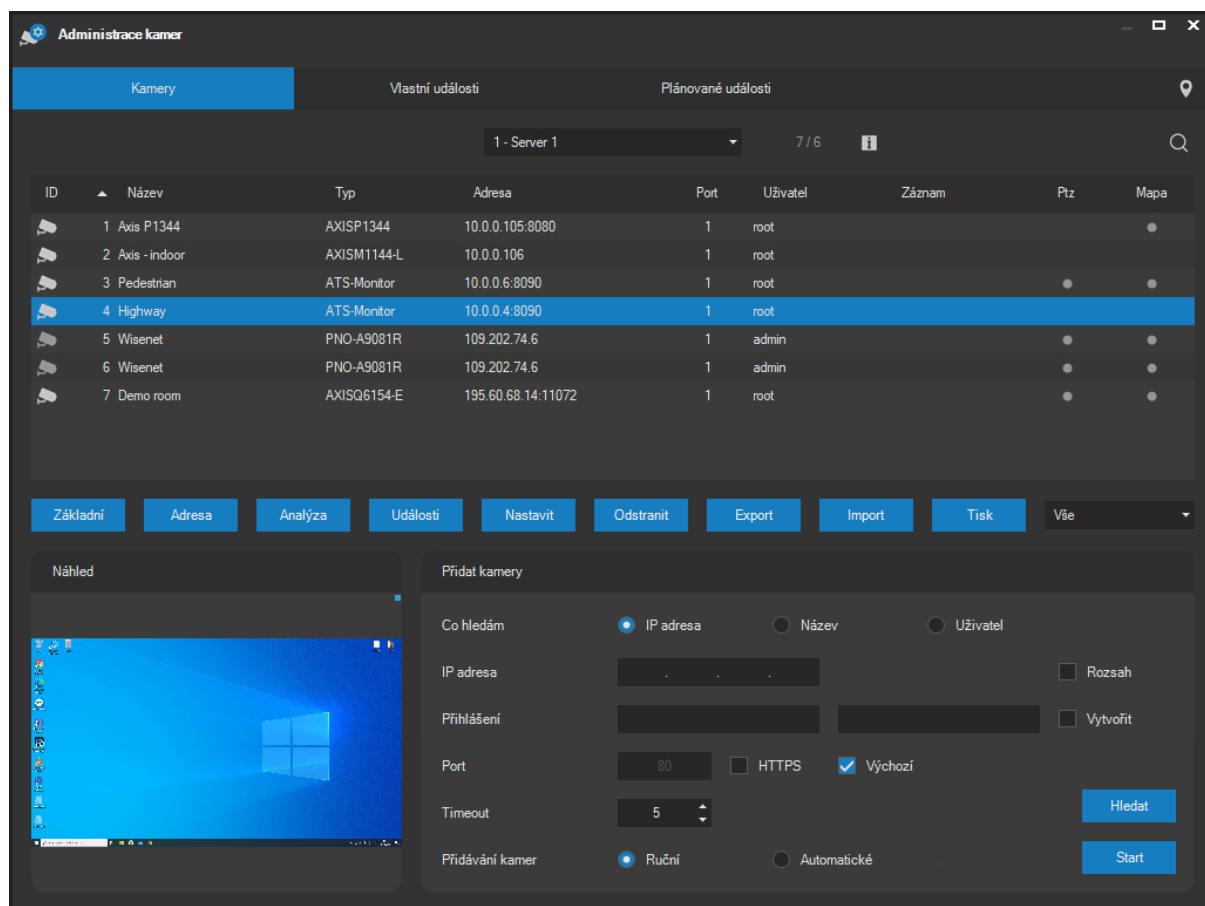
Možnost přidat k serveru obrazovku počítače jako kameru typu ATEAS Monitor je k dispozici až od verze ATEAS Security PROFESSIONAL.

Odkaz na instalaci aplikace pro monitoring obrazovky počítače je k dispozici na úvodní stránce instalačního média a pomocí webového rozhraní administračního serveru systému. Instalace probíhá pomocí stejného průvodce jako instalace jiných aplikací. Jediným specifickým dialogem je možnost zadání základních parametrů nastavení - HTTP port a heslo.



The screenshot shows the 'Initial setup' window of the ATEAS Screen Recorder application. The window has a blue header with the title 'Initial setup' and the ATEAS logo. Below the header, there is a text box with the instruction: 'Enter basic configuration values. You can change these values later in screenrecorder.ini followed by a restart of the application.' There are two input fields: 'Enter HTTP port:' with the value '80' entered, and 'Enter password (optional):' which is empty. At the bottom, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

V textovém poli Zadejte port můžete ponechat implicitní hodnotu 80 anebo provést změnu na jiné číslo síťového portu. Volitelně je možné zadat heslo, které bude vyžadováno při přidávání kamery do systému (uživatelské jméno může být libovolné). Tyto hodnoty lze později měnit v souboru screenrecorder.ini, který je umístěn v instalační složce aplikace.



POZNÁMKA

Aplikace ATEAS Screen Recorder je z důvodu možností přístupu k obrazovce počítače a z důvodu bezpečnosti spuštěna vždy až s přihlášením uživatele do systému.

POZOR

Aplikace ATEAS Screen Recorder nepodporuje více přihlášených uživatelů současně, a tudíž současné přidání více kamer na různých portech jednoho počítače (např. dva současně přihlášení uživatelé k jedné pracovní stanici Windows).

Po instalaci aplikace dojde k jejímu automatickému spuštění a je také zajištěno automatické spuštění po restartech počítače a přihlášení uživatelů. Spuštění aplikace je implicitně indikováno ikonou ATEAS v oznamovací oblasti hlavního panelu Windows (system tray). Kliknutím pravým tlačítkem na tuto ikonu se rozevře kontextová nabídka s jedinou položkou Exit, pomocí které je možné aplikaci ukončit.

POZNÁMKA

Pro utajení běhu aplikace ATEAS Screen Recorder na počítači je možné potlačit zobrazení ATEAS ikony v oznamovací oblasti pomocí nastavení v INI souboru. Viz další subkapitola.

16.2. Nastavení

Nastavení videa se provádí přímo nastavením kamery v klientské aplikaci. Podporováno je nastavení snímkové frekvence (v rozsahu 1 - 25 FPS) a nastavení stupně komprese videa (podporovaný formát je MJPEG).

Nastavení aplikace se provádí v souboru screenrecorder.ini, který je umístěn v instalační složce aplikace. Po změně libovolného z klíčů v tomto souboru je nutné provést restart aplikace ATEAS Screen Recorder, aby se změny projevy. K dispozici jsou tyto klíče:

HTTPPORT - udává číslo portu, na kterém bude kamera dostupná,

SHOWICON - udává, zdali bude zobrazena ikona v oznamovací oblasti (hodnota 1) anebo bude skryta (hodnota 0),

PASSWORDHASH - udává otisk hesla použitého pro přístup ke kameře. Pokud je hodnota smazána, heslo nebude vyžadováno. Vzhledem k tomu, že v tomto klíči se při instalaci zapisuje otisk (hash) hesla, není možné sem vložit nové heslo přímo.

POZNÁMKA

Pokud tedy chcete nastavit nové heslo pro kameru - obrazovku - na tomto počítači, je nutné provést reinstalaci aplikace ATEAS Screen Recorder.

PROCID – implicitně není vyplněno. Tato položka může obsahovat ID procesu. Pokud je ID procesu vyplněno, aplikace ATEAS Screen Recorder nepoužije pro vytvoření video streamu celou plochu, ale pouze hlavní okno zadaného procesu.

POZNÁMKA

V praxi lze monitoring vybraného okna použít např. pro offline otestování fotek či videa z místa budoucí instalace modulu pro detekci a rozpoznávání RZ vozidel.

MUTEXLEVEL – pokud je hodnota nastavena na 1, nebude možné aplikaci spustit vícekrát. Při nastavení na 0 a instalaci aplikace do oddělených složek je možné docílit vícenásobného spuštění aplikace, což je možné využít např. u tenkých klientů (terminálové služby).

CAPTUREMOUSE – hodnota je implicitně nastavena na 0, pokud je změněna na 1, bude automaticky součástí videa také kurzor myši.

ACTIVESCREEEN - hodnota je implicitně nastavena na 0, pokud je změněna na 1, bude možné vzdálený počítač ovládat přímo z klienta ATEAS. Aby bylo možné ovládat všechna okna na daném počítači včetně oken s nastavením apod., je nutné aplikaci spustit jako administrátor. Počítač bude možné ovládat včetně všech událostí myši a klávesnice.

POZNÁMKA

Pro ideální vyhlazení obrazu při ovládání je vhodné aktivovat na klientu ATEAS akceleraci GPU pro zobrazení videa.

Kapitola 17 - Příloha 1 – Konfigurace sítě

Při provozu aplikací ATEAS Security je v případě potřeby nutné provést konfiguraci síťových prvků (to se může týkat například nastavení routerů, pokud je kamerový systém umístěn uvnitř lokální sítě), tak aby mohly být serverové aplikace kontaktovány na uvedených portech. Následující tabulka shrnuje základní síťové porty. Klient systému je vždy stranou, která spojení vytváří, na klientské straně není třeba provádět žádná speciální nastavení.

POZNÁMKA

Pro základní fungování systému postačí otevření portu 8501 pro administrační a portu 8502 pro kamerový server. Ostatní porty slouží pro pokročilejší či doplňkové funkce a integrace.

17.1. Administrační server

Port	Transportní protokol	Aplikační protokol	Komunikace
8501	TCP	ATEAS	Základní komunikační port
8503	TCP	ATEAS	Podpora cloudového připojení
8504	TCP	ATEAS	Příjem externích událostí z jiných systémů
9001 - N	TCP	WebSocket / TLS	Podpora cloudového připojení pro web klienta
80	TCP	HTTP	Domovská stránka systému, webový klient, automatické aktualizace
443	TCP	HTTPS / TLS	Domovská stránka systému, webový klient, automatické aktualizace
162	UDP	SNMP	Příjem trapů pro aktivaci událostí

17.2. Kamerový server

Port	Transportní protokol	Aplikační protokol	Komunikace
8502	TCP	ATEAS	Základní komunikační port
8505	TCP	ATEAS	Vlastní události kamer

8506	TCP	HTTP	Přístup k webovému rozhraní všech kamer
8507	TCP	WebSocket	Nezabezpečené vysílání pro web
8508	TCP	WebSocket / TLS	Zabezpečené vysílání pro web
8509	TCP	HTTP	Vysílání videa pomocí DLNA
3702 - 3	UDP	SOAP	Vyhledávání Onvif kamer (WS Discovery)
8080	TCP	HTTP	Body Worn System

POZOR

Pokud je použito schéma přenosu dat z kamer RTP/UDP, UDP porty jsou alokovány dynamicky a musí být nastavena výjimka pro celý kamerový server, nikoliv pro konkrétní porty. To platí i pro klienta, pokud má profil LOCAL a připojuje se tak na multicastové adresy a přijímá data pomocí protokolu UDP.

Kapitola 18 - Příloha 2 – ATEAS API

18.1. Princip komunikace

Je možné využít komunikační kanál založený na protokolu TCP anebo HTTP. Použití TCP protokolu je jednodušší a může být podporováno širším spektrem nejrůznějších zařízení. Přenos však není možné nijak zabezpečit anebo vyžadovat autentizaci. U protokolu HTTP je možné vynutit použití TLS protokolu pro maximální zabezpečení a také volitelně vyžadovat přihlašovací údaje.

Při použití tohoto API je administrační či kamerový server stranou naslouchající na příslušných síťových portech, externí zařízení je stranou vytvářející a udržující spojení.

Administrační server naslouchá na API portu 8504 (TCP) a na portu 80 (HTTP), který je výchozím HTTP portem administračního serveru a lze ho změnit v konfiguračním souboru. Kamerový server naslouchá na API portu 8505 (TCP) a na portu 8080 (HTTP), který výchozím HTTP portem kamerového serveru a lze ho změnit v konfiguračním souboru.

Protokol HTTP používá standardní HTTP návratové kódy. Zasílání dat se provádí metodou HTTP POST. Protokol HTTP také může vracet data ve formátu JSON.

Pomocí protokolu TCP mohou být zasílány nevyžádané informace, např. o událostech v systému. Pro tento účel je na úrovni protokolu HTTP použit protokol WebSocket. Informace mohou být ve formátu JSON nebo XML.

Kódování textu u protokolu TCP je nastavitelné při otevírání portu, u protokolu HTTP se využívá kódování UTF8.

TIP

Odkaz na příklad implementace pro protokol TCP a HTTP naleznete na domovské stránce Vašeho administračního serveru.

18.2. ATEAS API pro administrační server

18.2.1. Externí události

Příjem externí události

Protokol	API
TCP	[ATEAS EVENT (status) (objectid) (elementid)]
HTTP	POST /api-base/event DATA: status=(status)&objectid=(objectid)&elementid=(elementid)

Parametry:

Parametr	Hodnota	Výchozí	Význam
status	START, STOP		Zahájení či ukončení
objectid	1 – 10 000		Číslo objektu
elementid	1 – 99 999		Číslo prvku

Příklad:

Protokol	API
TCP	[ATEAS EVENT START 1 1]
HTTP	DATA: status=START&objectid=1&elementid=1

18.2.2. Video stěna

Přepnutí obsahu na video stěnu

Protokol	API
TCP	[ATEAS VIDEOWALL (monitor) (submonitor) (serverid) (deviceid) (wallid) (meta)]
HTTP	POST /api-base/videowall DATA: monitor=(monitor)&submonitor=(submonitor)& serverid=(serverid)&deviceid=(deviceid)&wallid=(wallid)&meta=(meta)

Parametry:

Parametr	Hodnota	Výchozí	Význam
monitor	1 – 192		Číslo monitoru
submonitor	0 – 16	0	Číslo submonitoru
serverid	1 – 9 999		Číslo serveru
deviceid	1 – 999		Číslo zařízení
wallid	1 – 1000	1	Číslo video stěny
meta	0 – 1	0	Připojení metadat

Příklad:

Protokol	API
TCP	[ATEAS VIDEOWALL 1 1 1 10 1 0]
HTTP	DATA: monitor=1&submonitor=1&serverid=1&deviceid=10&wallid=1&meta=0

POZNÁMKA

Hodnotu submonitor je nutné použít pro monitory typu 4, 9 nebo 16.

POZNÁMKA

Jsou-li obě hodnoty serverid a deviceid rovny nule, dojde k vypnutí příslušného monitoru (vypnutí videa a přechod do výchozí podoby s logem ATEAS).

POZNÁMKA

Pokud je serverid nastaveno na hodnotu nula, je pozitivní deviceid interpretováno jako číslo URL webového obsahu vložené do systému administrátorem.

POZNÁMKA

U protokolu TCP je při použití nepovinného parametru wallid nutné použít i parametr submonitor, aby bylo možné zprávu správně zpracovat.

18.2.3. Registrační značky

Změna zařazení RZ

Protokol	API
TCP	
HTTP	POST /api-base/plate DATA: plate=(plate)&list=(list)

Parametry:

Parametr	Hodnota	Výchozí	Význam
plate	(značka)		Registrační značka
list	none, white, black, user1, user2, vlastní		Zařazení do seznamu

Příklad:

Protokol	API
TCP	
HTTP	DATA: plate=2A56217&plate=white

JSON odpověď:

```
{
  "Plate": "2A56217",
  "List": "white"
}
```

POZNÁMKA

Registrační značky lze zadat v dekorativním či normalizovaném tvaru.

POZNÁMKA

Parametr list je nepovinný a pokud je vynechán, bude pouze zjištěno aktuální zařazení RZ do seznamu.

18.2.4. Databáze obličejů

Přidání skupiny osob

Protokol	API
TCP	
HTTP	POST /api-base/face/group/add DATA: name=(name)

Parametry:

Parametr	Hodnota	Výchozí	Význam
name	(name)		Název skupiny

Příklad:

Protokol	API
----------	-----

TCP	
HTTP	DATA: name=group

JSON odpověď:

```
{
  "result": "ok",
  "id": 2,
  "name": "group"
}
```

POZNÁMKA

Nelze vytvářet skupiny s duplicitním názvem bez ohledu na velká a malá písmena.

Odebrání skupiny osob

Protokol	API
TCP	
HTTP	POST /api-base/face/group/remove DATA: id=(id)

Parametry:

Parametr	Hodnota	Výchozí	Význam
id	(id)		Číslo skupiny

Příklad:

Protokol	API
TCP	

HTTP	DATA: id=2
-------------	------------

JSON odpověď:

```
{  
  "result": "ok"  
}
```

Přejmenování skupiny osob

Protokol	API
TCP	
HTTP	POST /api-base/face/group/name DATA: id=(id)&name=(name)

Parametry:

Parametr	Hodnota	Výchozí	Význam
id	(id)		Číslo skupiny
name	(name)		Nový název skupiny

Příklad:

Protokol	API
TCP	
HTTP	DATA: id=2&name=group

JSON odpověď:

```
{  
  "result": "ok"  
}
```

```
}
```

Přidání osoby

Protokol	API
TCP	
HTTP	POST /api-base/face/person/add DATA: name=(name)&group=(group)&uuid=(uuid)

Parametry:

Parametr	Hodnota	Výchozí	Význam
name	(name)		Jméno osoby
group	(id)	1	Číslo skupiny
uuid	(uuid)		Vlastní identifikátor

Příklad:

Protokol	API
TCP	
HTTP	DATA: name=person&group=&uuid=

JSON odpověď:

```
{
  "result": "ok",
  "id": 1,
  "name": "person",
  "uuid": ""
}
```

POZNÁMKA

Parametr uuid může sloužit jako externí identifikátor např. v přístupovém systému. Jeho hodnota je poté součástí události rozpoznání obličeje.

Odebrání osoby

Protokol	API
TCP	
HTTP	POST /api-base/face/person/remove DATA: id=(id)

Parametry:

Parametr	Hodnota	Výchozí	Význam
id	(id)		Číslo osoby

Příklad:

Protokol	API
TCP	
HTTP	DATA: id=1

JSON odpověď:

```
{
  "result": "ok"
}
```

Změna osoby

Protokol	API
TCP	
HTTP	POST /api-base/face/person/update DATA: id=(id)&name=(name)&group=(group)&uuid=(uuid)

Parametry:

Parametr	Hodnota	Výchozí	Význam
id	(id)		Číslo osoby
name	(name)		Nové jméno osoby
group	(id)		Číslo skupiny
uuid	(uuid)		Vlastní identifikátor

Příklad:

Protokol	API
TCP	
HTTP	DATA: id=1&name=person&group=2&uuid=

JSON odpověď:

```
{
  "result": "ok",
  "name": "person",
  "uuid": ""
}
```

Přidání obličeje

Protokol	API
----------	-----

TCP	
HTTP	POST /api-base/face/person/image DATA: person=(person)&serverid=(serverid)&index=(index)&data=(data)

Parametry:

Parametr	Hodnota	Výchozí	Význam
person	(id)		Číslo osoby
serverid	(id)		Číslo serveru pro analýzu
index	0 – 9	0	Index obrázku
data	(uuid)		Data obrázku

Příklad:

Protokol	API
TCP	
HTTP	DATA: person=1&serverid=1&index=0&data=

JSON odpověď:

```
{
  "result": "ok",
  "image": "/9j/4AA..."
}
```

POZNÁMKA

V parametru data je očekáván obrázek ve formátu jpeg či bmp v kódování base64 s barevnou hloubkou 24 nebo 32 bitů. Pokud je parametr data prázdný, dojde k odstranění obrázku.

POZNÁMKA

Po vložení obličeje do databáze je vrácen obrázek v kanonickém tvaru ve formátu jpeg a kódování base64.

18.2.5. Správa uživatelů a skupinPřidání uživatele

Protokol	API
TCP	
HTTP	POST /api-base/user/add DATA: name=(name)&group=(name)&slave=(slave)

Parametry:

Parametr	Hodnota	Výchozí	Význam
name	(name)		Jméno uživatele
group	(name)	USER	Název skupiny
slave	(slave)	0	Podřízený účet video stěny

Příklad:

Protokol	API
TCP	
HTTP	DATA: name=operator

JSON odpověď:

```
{
  "result": "ok",
  "userid": 2,
```

```
"group": "USER"  
}
```

POZNÁMKA

Kromě systémových skupin USER a ADMINISTRATOR mohou být použity také libovolné existující názvy skupin.

Odstranění uživatele

Protokol	API
TCP	
HTTP	POST /api-base/user/delete DATA: userid=(id)

Parametry:

Parametr	Hodnota	Výchozí	Význam
userid	(id)		Identifikace uživatele

Příklad:

Protokol	API
TCP	
HTTP	DATA: userid=2

JSON odpověď:

```
{  
  "result": "ok",  
  "userid": 2  
}
```

Profil uživatele

Protokol	API
TCP	
HTTP	POST /api-base/user/profile DATA: userid=(id)&serverid=(id)&profile=(profile)

Parametry:

Parametr	Hodnota	Výchozí	Význam
userid	(id)		Identifikace uživatele
serverid	(id)		Identifikace serveru
profile	(profile)		Profil serveru (no, default, local, remote)

Příklad:

Protokol	API
TCP	
HTTP	DATA: userid=1&serverid=1&profile=default

JSON odpověď:

```
{
  "result": "ok",
  "userid": 1,
  "profile": "default"
}
```

Přidání skupiny

Protokol	API
TCP	
HTTP	POST /api-base/group/add DATA: name=(name)

Parametry:

Parametr	Hodnota	Výchozí	Význam
name	(name)		Název skupiny
group	(name)	USER	Základní skupina

Příklad:

Protokol	API
TCP	
HTTP	DATA: name=operators

JSON odpověď:

```
{
  "result": "ok",
  "groupid": 1,
  "group": "USER",
}
```

POZNÁMKA

Základní skupina musí být jedna z předdefinovaných systémových skupin USER nebo ADMINISTRATOR.

Odstranění skupiny

Protokol	API
TCP	
HTTP	POST /api-base/group/delete DATA: groupid=(id)

Parametry:

Parametr	Hodnota	Výchozí	Význam
groupid	(id)		Identifikace skupiny

Příklad:

Protokol	API
TCP	
HTTP	DATA: groupid=1

JSON odpověď:

```
{
  "result": "ok",
  "groupid": 1
}
```

Profil skupiny

Protokol	API
TCP	
HTTP	POST /api-base/group/profile DATA: groupid=(id)&serverid=(id)&profile=(profile)

Parametry:

Parametr	Hodnota	Výchozí	Význam
groupid	(id)		Identifikace skupiny
serverid	(id)		Identifikace serveru
profile	(profile)		Profil serveru (no, default, local, remote)

Příklad:

Protokol	API
TCP	
HTTP	DATA: groupid=1&serverid=1&profile=default

JSON odpověď:

```
{
  "result": "ok",
  "groupid": 1,
  "profile": "default"
}
```

18.2.6. Správa zařízení

Přidání zařízení

Protokol	API
TCP	
HTTP	POST /api-base/device/add DATA: serverid=(serverid)&host=(host) &user=(user)&password=(password) &deviceid=(deviceid)

Parametry:

Parametr	Hodnota	Výchozí	Význam
----------	---------	---------	--------

serverid	(id)		Identifikace serveru
host	(host)		Název či IP bod
user	(user)		Uživatelské jméno
password	(password)		Heslo
deviceid	(id)	0	Identifikace zařízení
index	(index)	1	Index zařízení

Příklad:

Protokol	API
TCP	
HTTP	DATA: name=10.0.0.100&serverid=1&user=root&password=pass&deviceid=&index=

JSON odpověď:

```
{
  "result": "ok",
  "serverid": 1,
  "deviceid": 1,
  "model": "Axis P1346",
  "format": "mjpg",
  "profile": "",
  "ptz": "no",
  "audio": "full"
}
```

POZNÁMKA

Při vynechání parametru deviceid nebo hodnotě nula bude číslo zařízení přiřazeno automaticky.

POZNÁMKA

Parametr index může být nastaven na vyšší hodnotu pro přístup k zařízením s více zdroji na jedné IP adrese.

Odstranění zařízení

Protokol	API
TCP	
HTTP	POST /api-base/device/delete DATA: serverid=(serverid)&deviceid=(deviceid)

Parametry:

Parametr	Hodnota	Výchozí	Význam
serverid	(id)		Identifikace serveru
deviceid	(id)		Identifikace zařízení

Příklad:

Protokol	API
TCP	
HTTP	DATA: serverid=1&deviceid=1

JSON odpověď:

```
{
  "result": "ok",
  "serverid": 1,
  "deviceid": 1
}
```

Nastavení zařízení

Protokol	API
TCP	
HTTP	POST /api-base/device/setup DATA: serverid=(serverid)&deviceid=(deviceid)&format=(format)&profile=(profile) &ptz=(ptz)&audio=(audio)&rule=(rule)

Parametry:

Parametr	Hodnota	Výchozí	Význam
serverid	(id)		Identifikace serveru
deviceid	(id)		Identifikace zařízení
name	(name)	""	Název zařízení
format	(format)	""	Formát (mjpg, mpg4, h264, h265, av1)
profile	(profile)	""	Video profil
ptz	(ptz)	""	PTZ podpora (yes, no)
audio	(audio)	""	Audio podpora (yes, no)
rule	(rule)	""	Název záznamového pravidla nebo none

Příklad:

Protokol	API
TCP	
HTTP	DATA: serverid=1&deviceid=1&format=h264&rule="base"

JSON odpověď:

```
{  
  "result": "ok",
```

```

"serverid": 1,
"deviceid": 1
}

```

POZNÁMKA

Nativně přidaná zařízení mohou pro změnu video formátu použít parametr format. Onvif kompatibilní zařízení mohou využít parametr profile pro výběr existujícího media profilu.

POZNÁMKA

Rule může být nastaveno na none, čímž bude aktuální pravidlo odebráno od zařízení.

18.2.7. Notifikace událostí

Přihlášení k odběru

Protokol	API
TCP	automaticky
HTTP	GET /api-base/events/subscribe&filter=all

HTTP verze tohoto API používá protokol SSE (Server Sent Events), tím je zajištěna maximální a jednoduchá interoperabilita s desktop i webovými aplikacemi.

TCP XML zahájení události

```

<?xml version="1.0" encoding="utf-8"?>
<ateas>
  <event>
    <id>1-464646</id>
    <level>1</level>
    <server>
      <id>1</id>
      <name>Server 1</name>
    </server>
  </event>
</ateas>

```

```
<camera>
  <id>1</id>
  <name>Camera 1</name>
</camera>
<source>
  <id>1</id>
</source>
<datetime>
  <utcstamp>128989433710312500</utcstamp>
  <localvalue>1.7.2023 9:05:51</localvalue>
</datetime>
<data></data>
<dataex></dataex>
<uuid></uuid>
</event>
</ateas>
```

TCP XML ukončení události

```
<?xml version="1.0" encoding="utf-8"?>
<ateas>
  <eventstop>
    <id>1-464646</id>
    <datetime>
      <utcstamp>128989433710312500</utcstamp>
      <localvalue>1.7.2023 9:05:51</localvalue>
    </datetime>
    <data></data>
  </eventstop>
</ateas>
```

HTTP JSON zahájení události

```
{
  "Action": "START",
  "ID": "1-464646",
  "Time": {
    "Timestamp": 133758779641144365,
    "LocalValue": "12.11.2024 10:39:24"
```

```
{
  "Type": "EVENT",
  "Server": {
    "ID": 1,
    "Name": "Server 1"
  },
  "Device": {
    "ID": 1,
    "Name": "Device 1"
  },
  "Source": 1,
  "Input": {
    "Number": 1
  },
  "LicensePlate": {
    "RawText": "001ATEAS",
    "NiceText": "001 ATEAS",
    "Country": "CZ",
    "Direction": ""
  },
  "WagonNumber": {
    "RawText": "218124712173",
    "NiceText": "2181 2471 217-3",
    "Direction": "LEFT",
    "Checksum": 1
  },
  "Face": {
    "UUID": "1",
    "Name": "Test face",
    "Group": "Main"
  },
  "Image": {
    "Detail": "base64",
    "Image": "base64"
  }
}
```

Pokud existuje objekt image, obsahuje JPEG data kódovaná pomocí Base64 schématu.

HTTP JSON ukončení události

```
{  
  "Action": "STOP",  
  "ID": "1-464646",  
  "Time": {  
    "Timestamp": 133758780524709309,  
    "LocalValue": "12.11.2024 10:40:52"  
  }  
}
```

POZNÁMKA

Události jsou centralizovány ze všech kamerových serverů systému.

POZNÁMKA

Číslo zdroje jednoznačně určuje daný typ události, které lze zobrazit pomocí testovacího programu.

Příklady ID zdroje:

- 1 – detekce pohybu na kameře
- 2 – výpadek kamery
- 3 – poplachový vstup kamery, data obsahují číslo vstupu
- 10 – 14 - rozpoznání RZ vozidla, data obsahují RZ vozidla v dekorativním tvaru
- 32 – kontrola kvality videa, data obsahují požadovanou úroveň snímkové frekvence
- 40 – detekce pohybu na serveru
- 51 – 100 – vlastní události
- 110 – událost ručního nahrávání kamery
- 111 – 130 – Onvif události, data mohou obsahovat dodatečné informace
- 131 – 150 – komplexní události
- 151 – 200 – vlastní události
- 201 – 250 – analytické události

POZNÁMKA

UTC časové razítko udává absolutní čas výskytu události nezávislý na časové zóně a změnách letního času jako počet 100 nanovteřinových intervalů od 1. ledna 1601 UTC.

18.2.8. Notifikace přihlášení

Přihlášení k odběru

Protokol	API
TCP	automaticky
HTTP	

XML přihlášení uživatele

```
<?xml version="1.0" encoding="utf-8"?>
<ateas>
  <user>
    <id>10</id>
    <name>tester</name>
    <action>login</action>
    <datetime>
      <utcstamp>128989433710312500</utcstamp>
      <localvalue>22.7.2023 15:05:23</localvalue>
    </datetime>
  </user>
</ateas>
```

POZNÁMKA

Při odhlášení má parametr akce hodnotu logout.

POZNÁMKA

UTC časové razítko udává absolutní čas výskytu události nezávislý na časové zóně a změnách letního času jako počet 100 nanovteřinových intervalů od 1. ledna 1601 UTC.

18.3. ATEAS API pro kamerový server

18.3.1. Externí události

Příjem externí události

Protokol	API
TCP	[ATEAS EVENT (status) (deviceid) (code) (data)]
HTTP	

Parametry:

Parametr	Hodnota	Výchozí	Význam
status	START, STOP		Zahájení či ukončení
deviceid	1 – 999		Číslo zařízení
code	(dle nastavení)		Název vlastní události
data	(max. 1000 znaků)		Dodatečná data

Příklad:

Protokol	API
TCP	[ATEAS EVENT START 1 TEMPERATURE 76]
HTTP	

POZNÁMKA

Kód událostí musí odpovídat vytvořenému názvu v části administrace kamer.

POZNÁMKA

Událost může být ukončena explicitně anebo automaticky nastavením maximální doby trvání.

18.3.2. Metadata

Vkládání metadat

Protokol	API
TCP	[ATEAS META (deviceid) (timestamp) (code) (data)]
HTTP	

Parametry:

Parametr	Hodnota	Výchozí	Význam
deviceid	1 – 999		Číslo zařízení
timestamp	0 – N		UTC časové razítko
code	(dle nastavení)		Název vlastní události
data	(max. 1000 znaků)		Metadata

Příklad:

Protokol	API
TCP	[ATEAS META 1 0 SCAN AB512459]
HTTP	

POZNÁMKA

UTC časové razítko udává absolutní čas výskytu události nezávislý na časové zóně a změnách letního času jako počet 100 nanovteřinových intervalů od 1. ledna 1601 UTC.

POZNÁMKA

Časové razítko může mít hodnotu 0. V takovém případě bude čas určen serverem. Vlastní zadání času je vhodné při offline nahrávání dat do systému, při kterém není akceptován čas menší než 30 dní v minulosti a větší než 1 minutu v budoucnosti dle času serveru.

POZNÁMKA

Kód událostí musí odpovídat vytvořenému názvu v části administrace kamer.

18.4. Parametrické spouštění aplikací

Aplikace ATEAS Security je možné spouštět také s dodatečnými parametry, které jsou předány spustitelnému souboru při startu aplikace či služby. Přidání těchto parametrů je možné v nastavení služby v systému Windows. V současné době existují parametry popsané níže.

18.4.1. Administrační server

Parametr	Hodnoty	Význam	Poznámka
-ssl	heslo	Heslo certifikátu	Je nutné zadat, pokud je použitý certifikát ve formátu PFX chráněn heslem.

18.4.2. Kamerový server

Parametr	Hodnoty	Význam	Poznámka
-ssl	heslo	Heslo certifikátu	Je nutné zadat, pokud je použitý certifikát ve formátu PFX chráněn heslem.
-loglevel	0 - 1	Nastavení úrovně logování	Pozitivní hodnota zapíná výpis zaplnění vyrovnávací paměti serveru do podsložky log.

18.4.3. Kamerový klient

Parametr	Hodnoty	Význam	Poznámka
-l, -login	složená	Přihlašovací údaje	Automatické přihlášení klienta.
-v, -view	složená	Definice pohledu	Automatické otevření pohledu.

Volba **login**:

Parametr	Hodnoty	Význam	Poznámka
u:, user:	řetězec	Uživatelské jméno	Součást přihlašovacích údajů.
p:, password:	řetězec	Heslo	Součást přihlašovacích údajů.
a:, administrator:	řetězec	Administrační server	Adresa či název serveru.

Volba **view**:

Parametr	Hodnoty	Význam	Poznámka
c:, camera:	složená	Seznam kamer	Identifikace kamer pro zobrazení.
s:, screen:	1 - 16	Obrazovka	Identifikace obrazovky pro pohled.
p:, position:	složená	Pozice okna	Lze zvolit umístění okna s pohledem.
t:, timestamp:	číslo	Časové razítko	Počet vteřin od 1.1.2010 0:00:00 UTC.
f:, full:	prázdná	Maximalizovaný pohled	Pohled bez zobrazených ovládacích panelů.
a:, autoplay:	prázdná	Automatické spuštění	Spuštění při přístupu k záznamu.

Volba **camera** (server-camera-extra):

Parametr	Hodnoty	Význam	Poznámka
server	1-9999	Číslo serveru	Identifikace serveru.
camera	1-999	Číslo kamery	Identifikace kamery.

extra	řetězec	Dodatečné parametry	m – připojení metadat.
--------------	---------	---------------------	------------------------

POZNÁMKA

Je-li část server vynechána, předpokládá se server s číslem 1. Část extra je nepovinná.

Volba **position** (x,y,w,h):

Parametr	Hodnoty	Význam	Poznámka
x	0-100	X souřadnice	Relativní umístění okna.
y	0-100	Y souřadnice	Relativní umístění okna.
w	10-100	Šířka	Relativní umístění okna.
h	10-100	Výška	Relativní umístění okna.

Příklady:

Přihlášení k systému a otevření pohledu s dvěma kamerami v režimu živého obrazu v pohledu na druhé obrazovce bez ovládacích prvků v implicitní velikosti:

```
observer -l u:admin p:12345 a:10.0.0.1 -v c:1-1 c:1-2-m s:2 f:
```

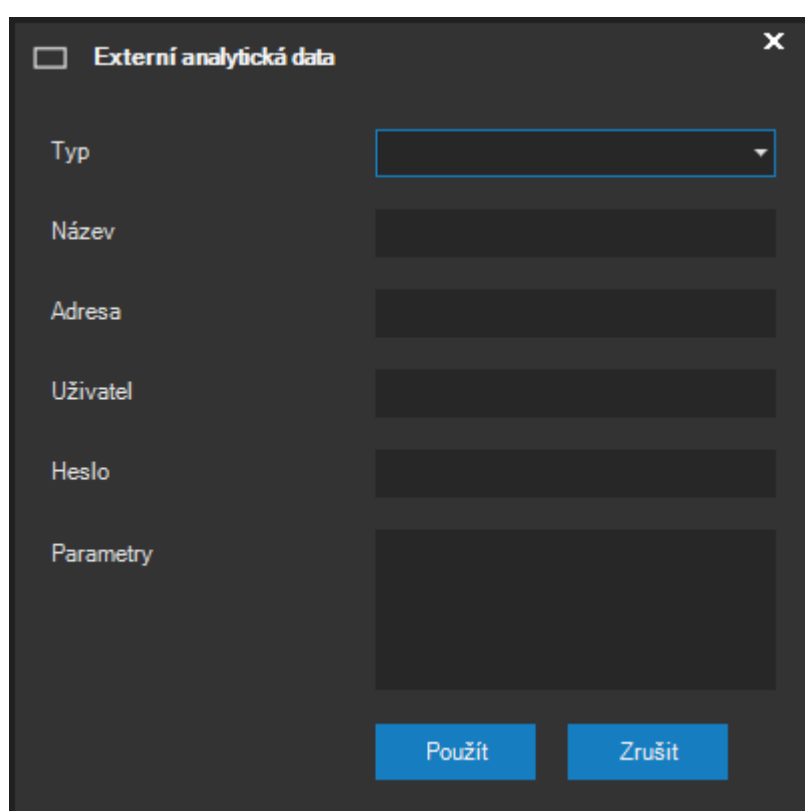
POZNÁMKA

Je možné definovat až 16 pohledů.

Kapitola 19 - Příloha 3 – Externí analytická data

19.1. Předpoklady

Pro realizaci propojení na externí zdroj analytických dat je nutné přidat k příslušným kamerám jeden či více externích zdrojů analytických dat podle popisu v kapitole Základní nastavení kamery, část Externí analytická data. Vyplnit je třeba následující dialog.



19.2. Integrace se systémem VTrack

19.2.1. Připojení metadat ze serveru

Pro připojení analýzy VTrack jako externího zdroje dat spuštěné přímo na serveru VTrack je třeba použít tyto hodnoty:

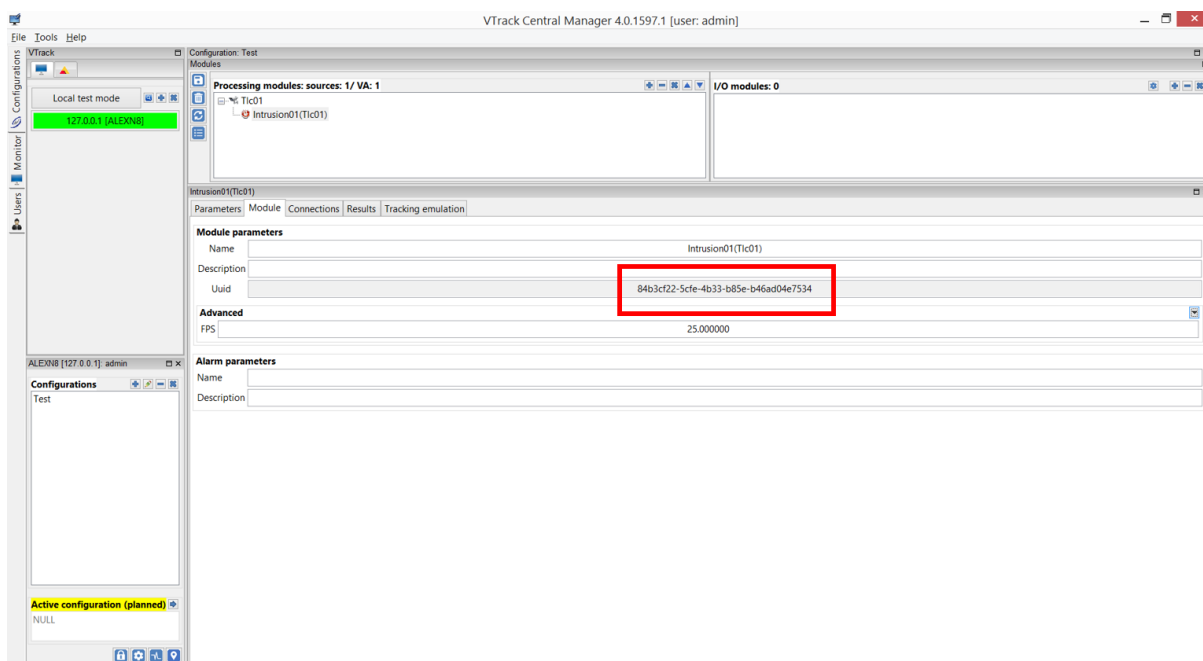
Typ: VTRACK (výběr ze seznamu).

Název: Libovolný název pro externí zdroj analytických dat.

Adresa: Adresa a port serveru VTrack (IP adresa nebo název). Např. 10.0.0.1:30002.

Uživatel a heslo: Je-li nutné pro připojení ke zdroji použít přihlášení, uvedeme uživatelské jméno a heslo.

Parametry: Je třeba vyplnit jednoznačný identifikátor konkrétní spuštěné analýzy, viz následující obrázek.



19.2.2. Připojení metadat z kamery

Pro připojení analýzy VTrack jako externího zdroje dat spuštěné přímo v kameře je třeba použít tyto hodnoty:

Typ: VTRACK (výběr ze seznamu).

Název: Libovolný název pro externí zdroj analytických dat.

Adresa: Adresa zdroje metadat, jejíž součástí je adresa kamery, název aplikace a další parametry.

Jako příklad uvádíme adresu pro kameru Axis na adrese 10.0.0.1 a aplikaci Intrusion:

10.0.0.1/local/vtIntrusion/results.cgi?tags=metadata

Uživatel a heslo: Je-li nutné pro připojení ke zdroji použít přihlášení, uvedeme uživatelské jméno a heslo.

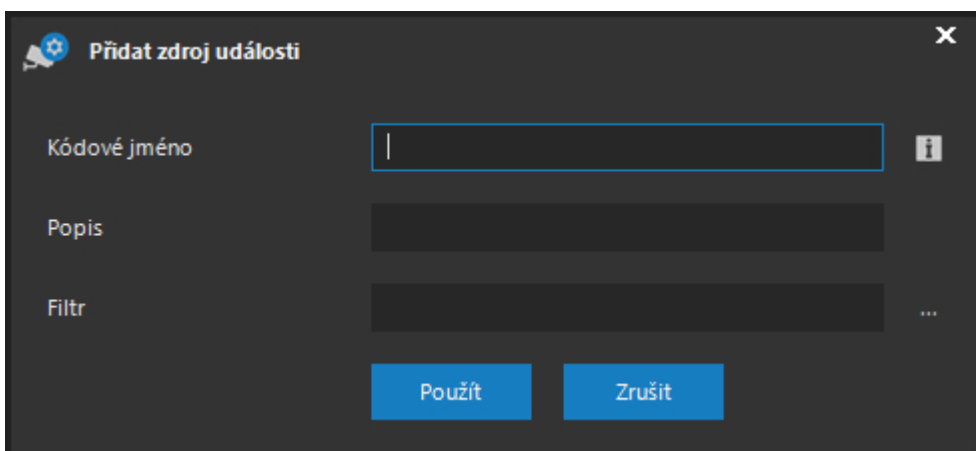
Parametry: Není třeba zadávat žádnou hodnotu.

POZNÁMKA

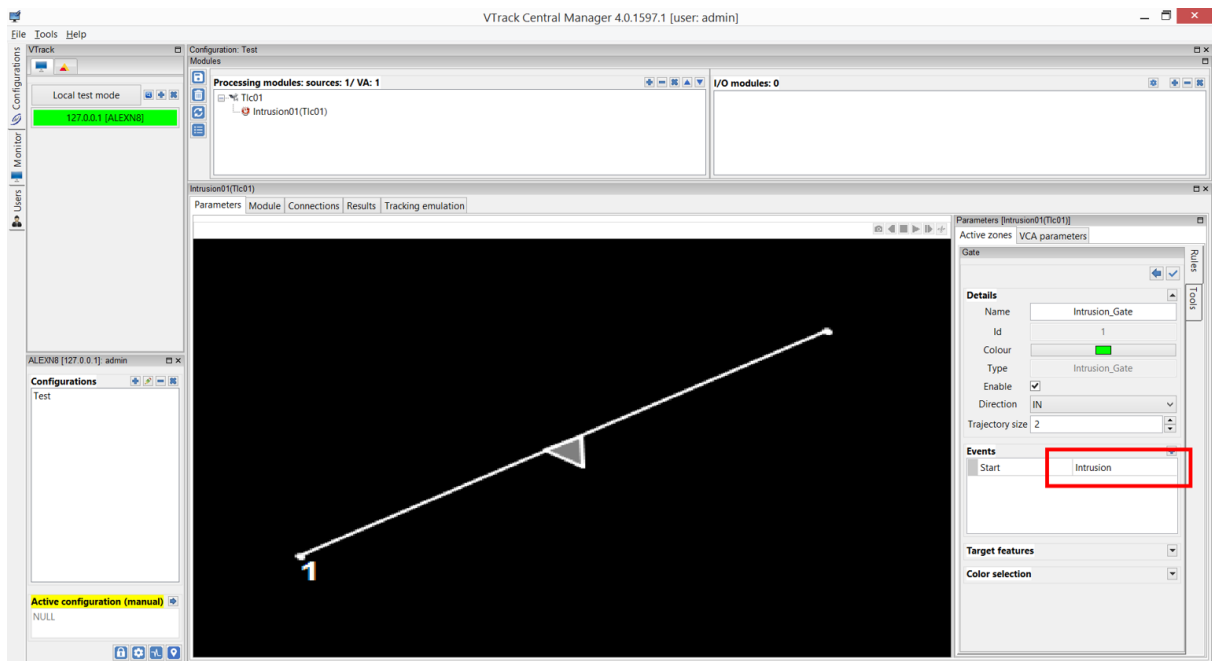
Aktuálně lze využít pouze pro vybraná kamerová zařízení. Pro správné nastavení adresy pro jiné aplikace či výrobce kamer je třeba využít nástroje a dokumentaci systému VTrack.

19.2.3. Propojení událostí

Aby bylo možné v externím zdroji analytických dat automaticky detekovat také poplachové situace, musí být v ATEASu vytvořeny vlastní kamerové události s názvy, které budou odpovídat událostem v systému VTrack. Více informací o vytvoření vlastních událostí naleznete v příslušné kapitole dokumentace. Při tvorbě vlastní události v ATEASu je nutné zadat název události (kódové jméno) a její popis.



Kódové jméno pak musí odpovídat hodnotě vyplněné v systému VTrack, jak ukazuje následující obrázek.



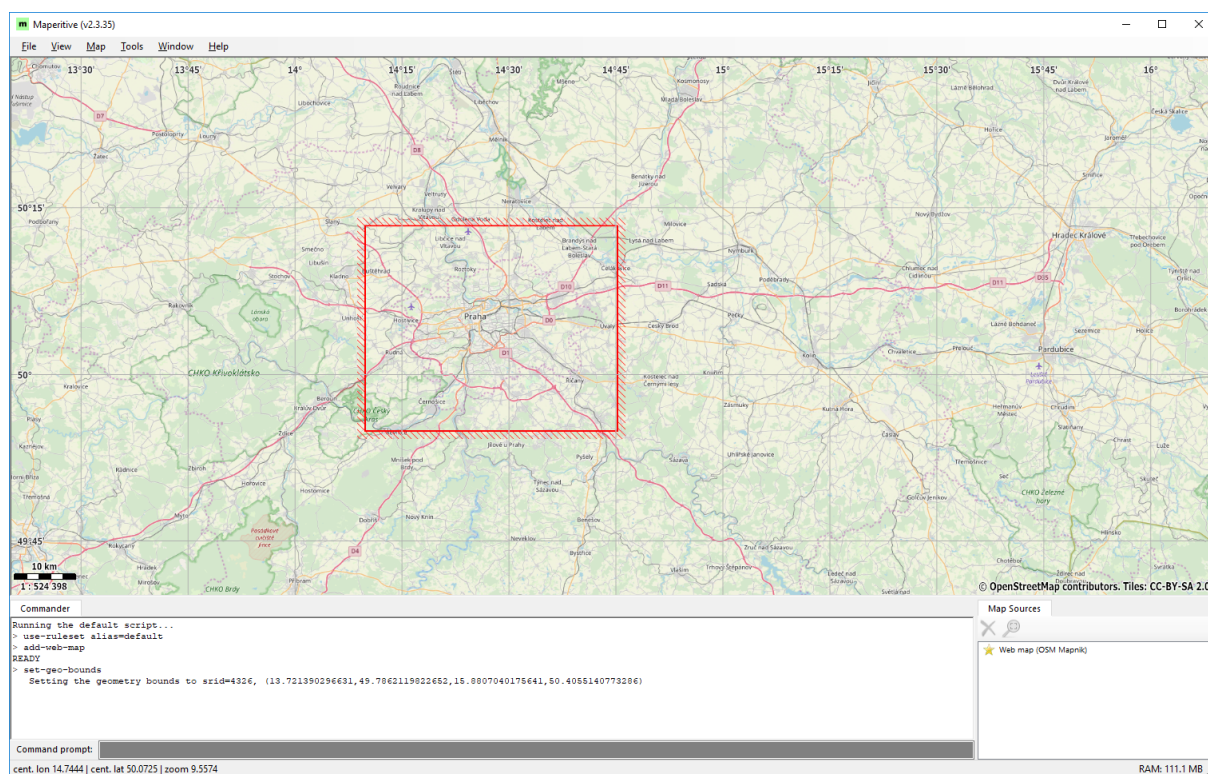
Kapitola 20 - Příloha 4 – Zdroje OpenStreetMap

20.1. Tvorba map z volných mapových zdrojů

Mapový model OpenStreetMap (OSM) je volně použitelný vektorový mapový model. Data pro libovolné území na světě mohou být jednoduše převedena a použita v mapovém rozhraní systému ATEAS. Převod do tzv. hybridního modelu je nutný, protože práce s vektorovým formátem pro velká území je pomalá. Pro převod do hybridního formátu (OSM tiles) je možné použít libovolné nástroje, zde uvádíme postup pro program Maperitive.

20.1.1. Výběr území a stažení dat

Po spuštění aplikace Maperitive najdete zájmové území a pomocí příkazu Map – Set Geometry Bounds určete cílový obdélník.



Pomocí příkazu Map – Download OSM Data (Overpass API) stáhněte data na lokální počítač.

V pravém spodním rohu okna vypněte zobrazení Web map a ponechte zobrazenou právě staženou mapu. Mapu není třeba dále ukládat, nicméně je to možné příkazem

```
save-source index=n file="cesta"
```

kde index musí být nastaven na hodnotu stažené mapy (lze zjistit jejím skrytím a zobrazením – index bude vypsán do konzole aplikace) a file musí být nastaveno na platnou cestu k novému souboru, např. d:\savedmap.osm. Příkazy se zapisují do příkazového řádku aplikace.

Takto uloženou mapu můžete příště kdykoliv znovu načíst.

POZNÁMKA

Pokud server odmítne všechna data poslat (rozsah stahovaných dat je příliš velký), je buď možné provést stažení a převod po částech anebo provést převod přímo z webové mapy, což ale bude velmi pomalé.

20.1.2. Převod dat

Po stažení dat je možné provést jejich převod pomocí příkazu

```
generate-tiles minzoom=m maxzoom=n
```

kde m je minimální zoom (obvykle např. 12) a n je maximální zoom (nejvíce 19).

Po provedení převodu jsou data umístěna ve složce Tiles v aplikační složce Maperitive. Soubor s koncovkou json, který je také vytvořen, není potřeba a lze ho smazat. Pro snazší manipulaci s daty je vhodné z nich vytvořit např. zip archiv, neboť data budou obsahovat značný počet souborů. Data ze složky Tiles je pak možné smazat.

20.1.3. Použití dat

Vytvořená data můžeme umístit do složky s libovolným názvem (např. OSM-Praha) a složku umístíme buď např. přímo do složky maps nebo kamkoliv do struktury map na administračním serveru systému určené pro automatickou distribuci.

Pokud bude po otevření v mapovém okně mapa příliš malá, znamená to, že byl minimální zoom v příkazu generate-tiles příliš malý. To lze jednoduše dodatečně vyřešit tak, že z mapových podkladů smažete složku s názvem odpovídajícím číslu minimálního zoomu. Tento proces lze provést i opakovaně. Po nové synchronizaci map lze pak vždy ověřit výsledek této operace a zhodnotit úvodní velikost mapové vrstvy.

20.1.4. Podpora různých úrovní detailů

Výhodou OSM mapového modelu, který má ATEAS implementován, je jednoznačnost přepočtu zemského povrchu na plošný mapový model v podobě převedených mapových souborů. Tato vlastnosti lze využít, když potřebujeme kombinovat více území. Např. pokud nám postačí přehledová mapa celé ČR a k tomu podrobná mapa několika měst v jedné mapové scéně, pro celou ČR použijeme např.

```
generate-tiles minzoom=10 maxzoom=13
```

a pro města pak

```
generate-tiles minzoom=13 maxzoom=19
```

Vytvořené převedené podklady pak jednoduše zkopírujeme do jedné složky, kolize souborů se vyskytnou pouze v případě, že jsou stejná data součástí více převodů, a není nutné se jich všimnout.

20.2. Tvorba map z rastrových podkladů

Velmi podobný postup lze použít i v případě, kdy potřebujeme převést do OSM modelu rastrové podklady.

POZNÁMKA

Rastrové podklady sice můžete použít přímo jako jednoduchou mapu, nicméně pro velikost obrázku v mnoha tisících bodů šířky či výšky (při exportu CAD výkresů) je z důvodu výkonu mapy nezbytné provést převod.

Pro otevření rastrového podkladu v Maperitive potřebujeme jeho georeferenci ve formátu georef (world file), např. pro soubor cadexport.jpg budeme potřebovat cadexport.jpg.georef. Poté je postup převodu zcela shodný jako v předchozí subkapitole.

Pokud není převáděný rastr georeferencovaný a jeho georeferenci nepotřebujeme, tak můžeme v Maperitive označit přibližně stejné velké území kdekoliv a příkazem export-bitmap si georef soubor vytvořit.

Pokud rastr nebude georeferencovaný, nebudou fungovat minimálně tyto dvě funkce:

- při zobrazení mapy nebude možné správně zobrazit pozici mobilního zařízení vysílajícího video,
- nebude možné se „prozoomovat“ z úrovně mapy města až např. přímo do areálu či budovy, bude tedy nutné pro vstup do areálu použít funkci umístění mapy (symbol dveří) a vstoupit do jiné mapy kliknutím na tento symbol.

Pokud chceme převést georeferencovaný tiff soubor, lze použít nějaký z volně dostupných nástrojů pro vytvoření georef souboru z takového souboru.

Kapitola 21 - Příloha 5 – JSON integrace dat

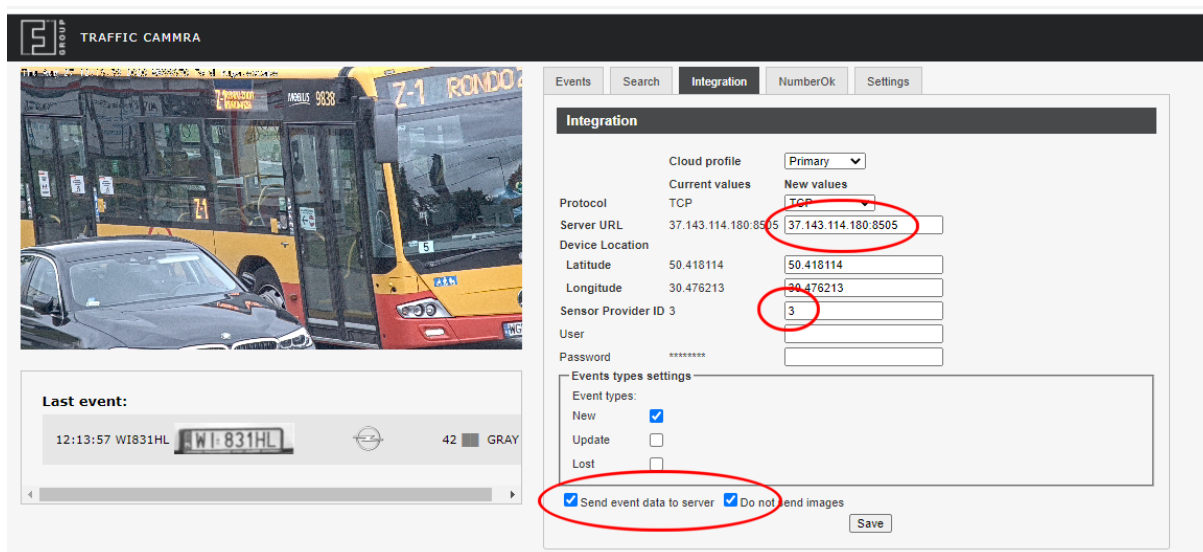
21.1. Předpoklady

Kromě rozhraní ATEAS API podporuje ATEAS na svých integračních událostních portech také data přenášená ve formátu JSON (JavaScript Object Notation).

21.2. Integrace aplikace Cammra

21.2.1. Příjem metadat přes TCP

Aplikace Cammra může být jednoduše nastavena tak, aby vysílala metadata o detekovaných RZ vozidel, státní příslušnosti, typu, modelu a barvě vozidla přímo do kamerového serveru ATEAS. V integračním rozhraní je potřeba zvolit JSON formát a nasměrovat data na událostní port kamerového serveru. Dále je také nutné nastavit ostatní volby dle obrázku.



Důležitým údajem je Sensor Provider ID, pomocí kterého se provede vazba na číslo kamery na příslušném kamerovém serveru ATEAS. Dále je také vhodné vypnout zasílání obrazových dat pomocí volby Do not send images.

21.2.2. Příjem metadat přes HTTP

Alternativně lze použít též protokol HTTP. V tomto případě bude využit HTTP integrační komunikační kanál administračního serveru, kam musí být data zasílána. Aby bylo možné odvodit nejen číslo

kamery, ale i serveru, je pro položku Sensor Provider ID možné použít tvar S-K, kde S je číslo serveru a K číslo kamery, tedy např. 1-5.

POZNÁMKA

Identifikace serveru může být vynechána, v takovém případě se předpokládá server s číslem 1.

Aby bylo možné data přijímat, je nutné při otevírání HTTP komunikačního kanálu povolit skupinu Road, která se váže k této aplikaci. Adresa bude vypadat následovně:

`http(s)://administrator/api-base/road`

21.2.3. Metadata a události

Externí aplikace poté poskytuje svá metadata pro danou kameru, která jsou automaticky přiřazena událostnímu zdroji - RZ značkám vozidel. Dále jsou také přijímána a ukládána další doplňková data, podle kterých je možné provádět vyhledávání v okně Záznam. Princip vyhledávání je popsán v části o vyhledávání metadat, vyhledávací výrazy mohou obsahovat libovolně řazená slova přirozeně interpretována vyhledávacím algoritmem, na jejichž pořadí nezáleží. Např.

2A CZ skoda – vyhledá všechna vozidla typu Škoda s českou RZ obsahující 2A.

rapid green – vyhledá všechny zelené Škody Rapid.

POZNÁMKA

Aby mohla v systému vzniknout událost, musí být událostním zdrojům vytvořen časový plán obvyklým způsobem.

21.2.4. Grafické výstupy

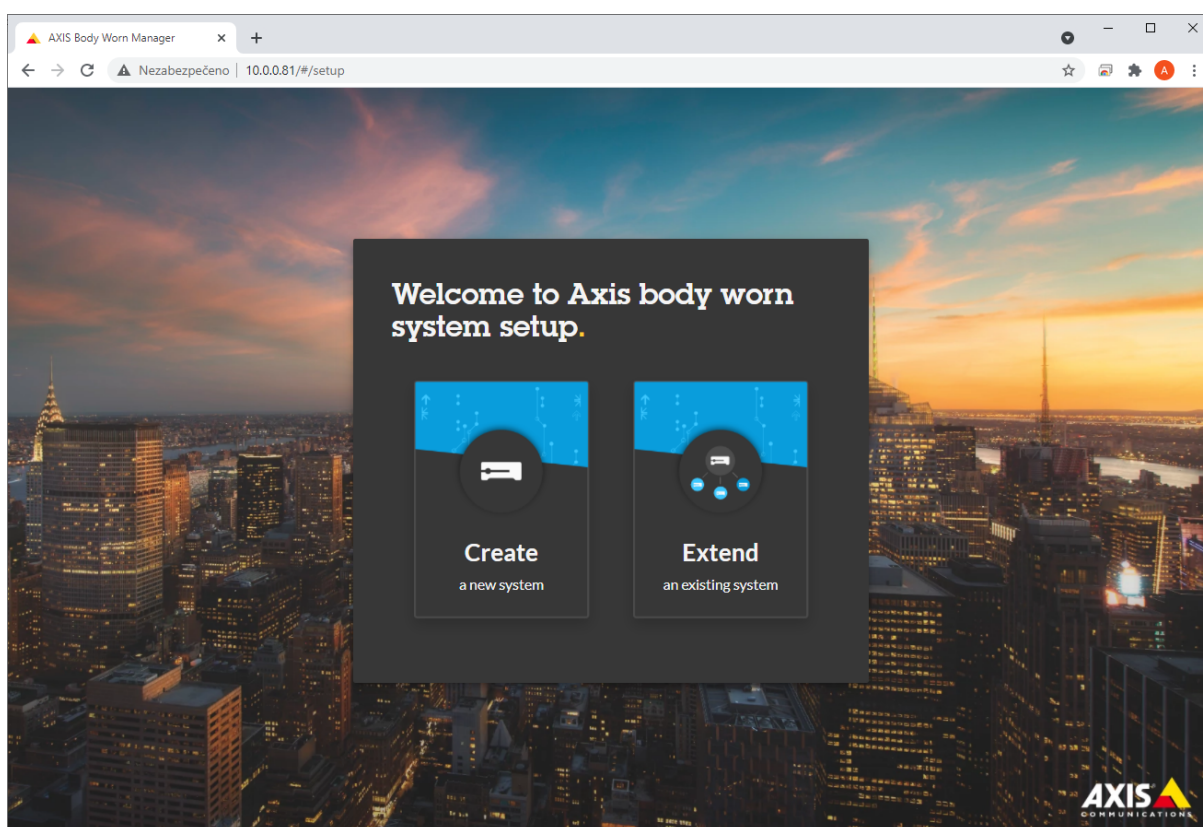
Grafický modul ATEAS umožňuje pokročilou tvorbu grafů i z externě zasílaných metadat. Základní grafické výstupy zahrnují četnosti průjezdů vozidel podle dnů či hodin. Pokročilé výstupy pak mohou obsahovat další rozdělení grafu podle přijatých metadat na určité pozici – grafy podle státu RZ, podle typu či modelu vozidla apod.

Pokud chceme generovat statistiky pro určitou podmnožinu dat (např. rozdělení dle modelu všech českých aut), je vhodné kombinovat nástroj vyhledávání metadat s vlastní tvorbou grafu.

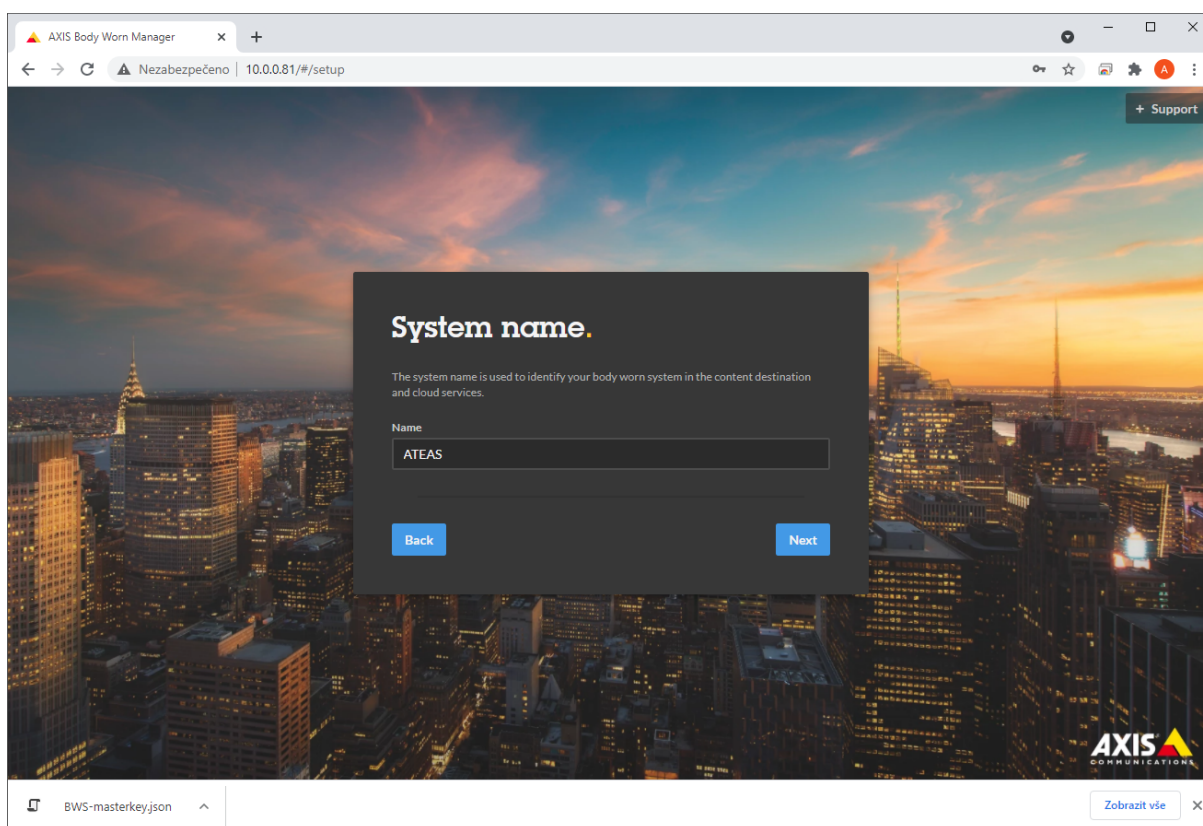
Kapitola 22 - Příloha 6 – Integrace Axis Body Worn

22.1. Propojení se serverem ATEAS

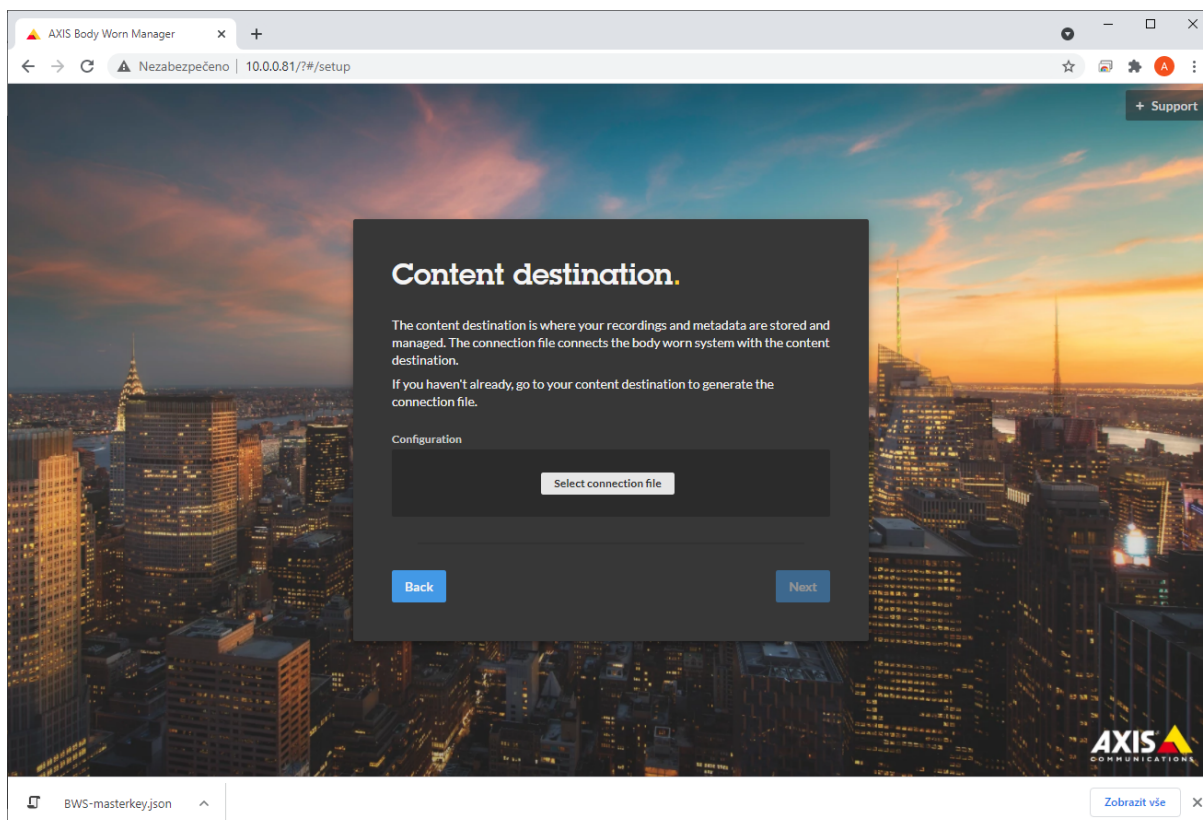
Systém Axis nositelných kamer (BWS – Body Worn System) se skládá z několik komponent, z nichž je pro integraci podstatný řídicí prvek BWS systému (controller), který při úvodním nastavení vyžaduje spojení s úložištěm dat, kam budou za provozu automaticky nahrávána všechna video, audio data a metadata z kamer. Postup propojení je následující.



Po úvodní obrazovce je nutné vyplnit název systému.



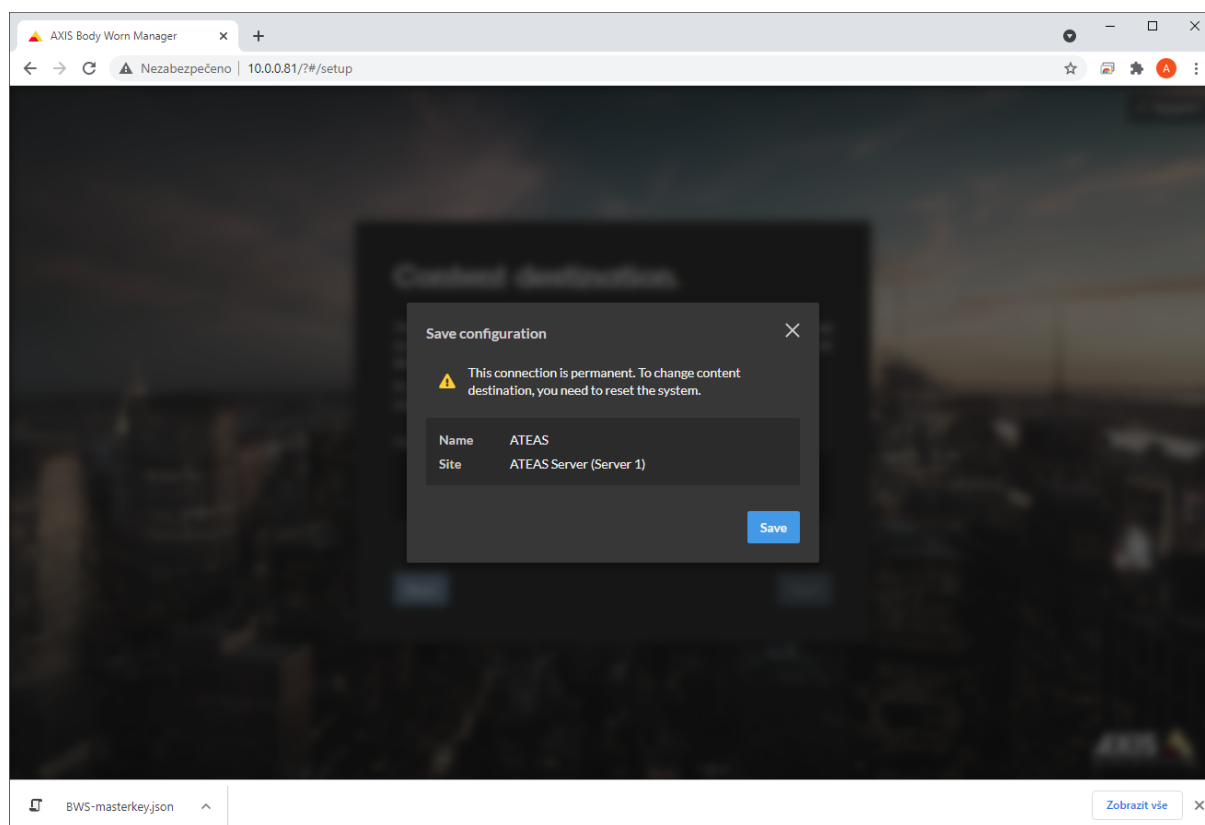
Dále následuje klíčová fáze vytvoření propojení na cílový kamerový server.



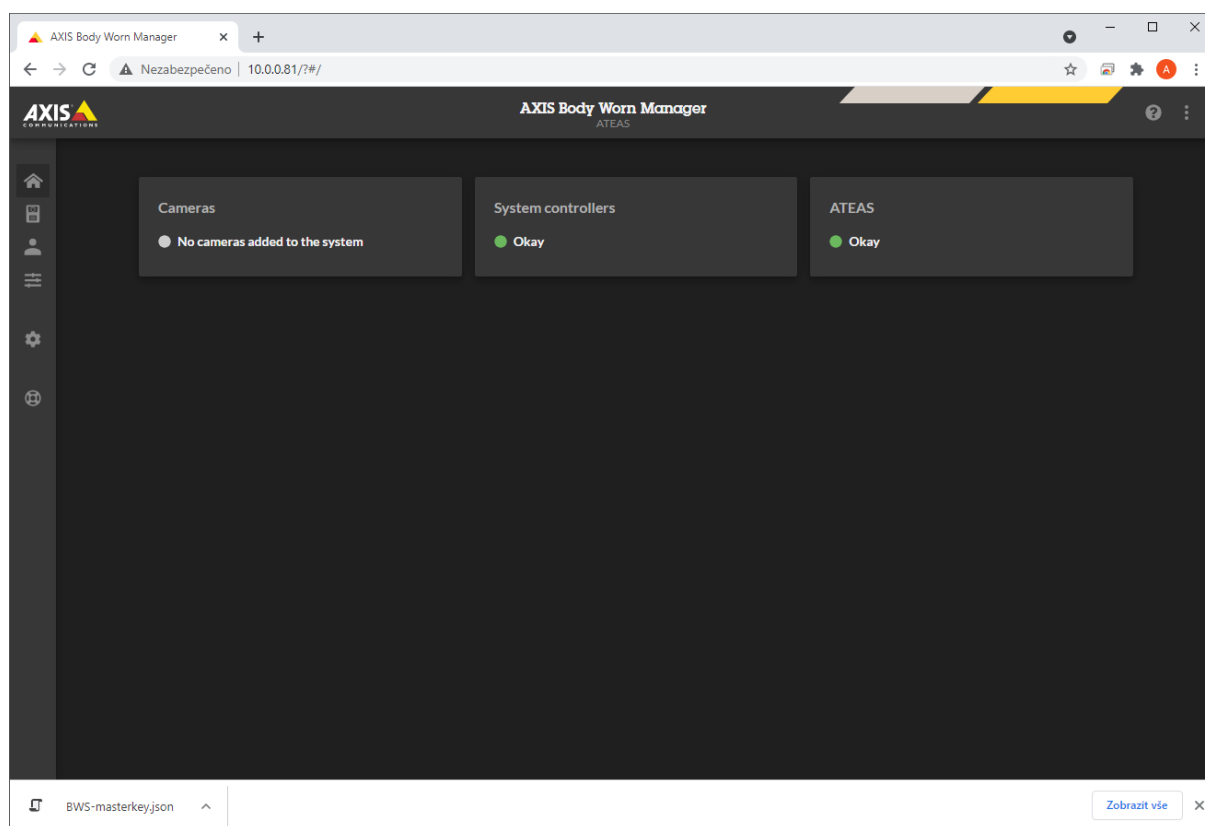
Soubor ve formátu JSON, který slouží pro předání parametrů propojení se systémem BWS, je automaticky vytvořen v instalační složce každého kamerového serveru v podsložce connect. Tato složka poté také slouží jako pracovní složka pro datovou výměnu se systémem BWS.

Jedním ze základních parametrů připojení je URL adresa a přihlášení. Tyto parametry jsou kamerovým serverem automaticky určeny z IP adresy serveru použité pro identifikaci k administračnímu jádru systému a z hodnot umístěných v souboru server.ini (HTTPPORT, HTTPUSER a HTTPPASS - lokální port a přihlašovací údaje k http serveru, který je součástí kamerového serveru ATEAS).

Po nahrání souboru s JSON konfigurací systém BWS informuje o tom, že se jedná o permanentní nastavení, které nelze změnit jinak než resetem BWS.



Úspěšné připojení řídicího prvku BWS k serveru ATEAS je poté indikováno světelnou signalizací controlleru a také na webu zařízení.



22.2. Přidání kamer a uživatelů

Přidávání kamer a uživatelů se provádí přímo na webu BWS controlleru. Jelikož BWS může být konfigurován tak, že uživatelé mohou využívat různé kamery, je z hlediska ATEASu za kameru považován uživatel BWS, nikoliv kamera.

Při přidání uživatele se automaticky provede také přidání kamery k serveru ATEAS s daným názvem, pokud tomu nebrání např. tyto skutečnosti:

- žádná volná licence na serveru,
- duplicitní číslo kamery.

Přidání uživatelé BWS mají pro přehlednější zobrazení v seznamu kamer stejně jako mobilní uživatelé, kteří streamují do ATEASu ze svých mobilních zařízení či kamer s operačním systémem Android či iOS, přiřazen indikátor uživatele.

POZOR

Vzhledem k tomu, že BWS nahrává na ATEAS server data se starším časem než je aktuální čas, je pro přidání BWS kamery pod daným číslem nutné, aby pro dané ID kamery na serveru neexistoval žádný záznam. Pro uvolnění ID pro BWS tedy nemusí stačit pouhé odstranění kamery.

POZNÁMKA

Jelikož u BWS je možné sdílet kameru mezi více uživateli, jsou licence BWS kamer (tj. uživatelů) započítávány v poměru 4 : 1. Jedna kamerová licence ATEAS vystačí pro čtyři BWS uživatele.

22.3. Provoz systému

Za běžného provozu jsou data z BWS systému do ATEAS serveru přenášena zcela automaticky a bez jakýchkoliv dalších akcí. Po jejich přenesení je možné je přehrávat všemi běžnými způsoby od chvíle, kdy se daný časový interval pro příslušnou kameru objeví na časové ose či v náhledu časového úseku.

Kapitola 23 - Příloha 7 – Certifikáty

23.1. Úvod

V této části si ukážeme, jak nasadit certifikát pro provoz zabezpečené komunikace mezi webovým prohlížečem a servery ATEAS. To je důležité zejména pro provoz webového klienta. Postup není specificky vlastní systému ATEAS, ale předpokládá obecnou znalost fungování komunikace pomocí protokolů HTTP a HTTPS (tedy TLS).

Celý proces nasazení certifikátů je otázkou několika minut a v tomto popisu si ukážeme jak využít již existujícího certifikátu včetně zajištění důvěryhodnosti v prostředí internetu, tak vytvoření vlastního certifikátu např. pro provoz pouze v rámci intranetu.

Narozdíl od webových aplikací běžně dodávaných včetně implementace do zákaznické infrastruktury nemá pochopitelně ATEAS možnost dopředu vědět, ve které doméně ho bude zákazník provozovat, proto není možné přibalit nějaký „univerzální“ certifikát, který by umožnil okamžitý důvěryhodný provoz HTTPS v síti zákazníka.

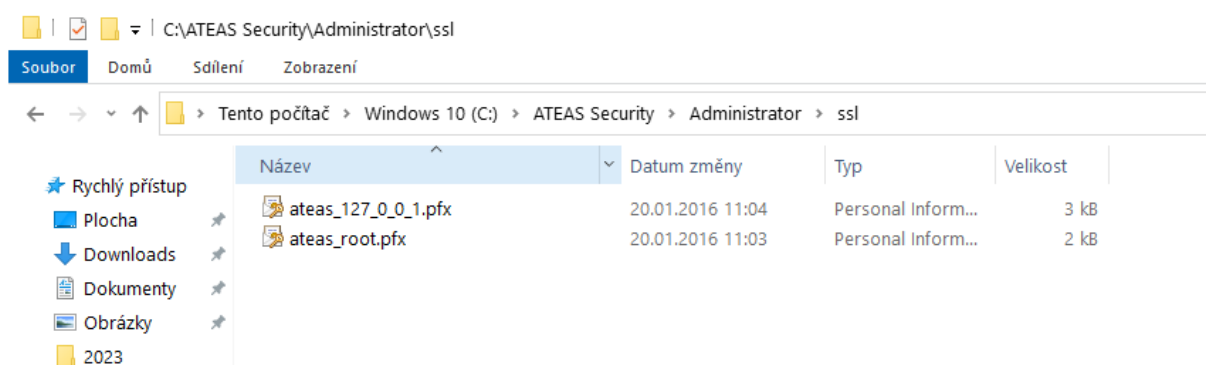
23.2. Předpoklady

Přestože je proces nasazení certifikátu velmi jednoduchý, předpokládají se základní znalosti na úrovni správy ATEAS systému a fungování certifikátů v komunikaci mezi klienty a servery pomocí protokolu HTTP. Pro přehlednost zde tyto základní předpoklady shrnujeme.

POZNÁMKA

Pro další podrobnosti je Vám k dispozici uživatelská dokumentace ATEAS.

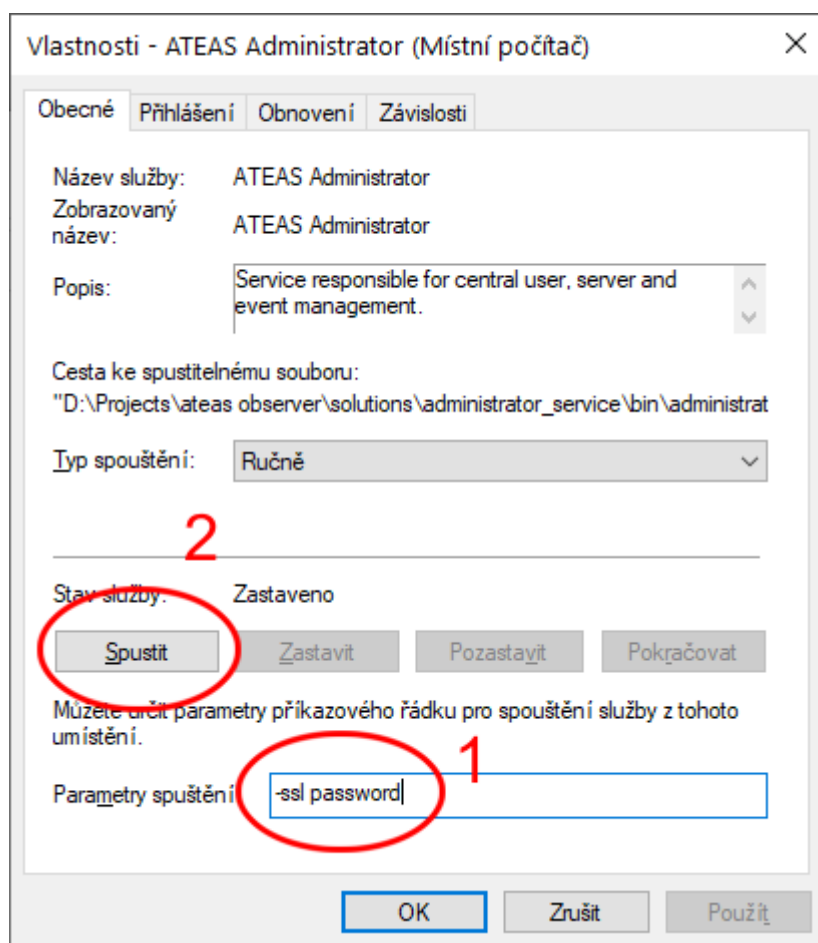
- Certifikát pro administrační server i kamerový server ATEAS je očekáván ve formátu PFX, musí obsahovat soukromý klíč (jinak by nebylo možné realizovat část kryptografie, kdy server prokazuje svůj původ) a je obvykle zabezpečen heslem pro otevření.
- Certifikát se umístí do složky ssl v instalační složce administračního či kamerového serveru.



POZNÁMKA

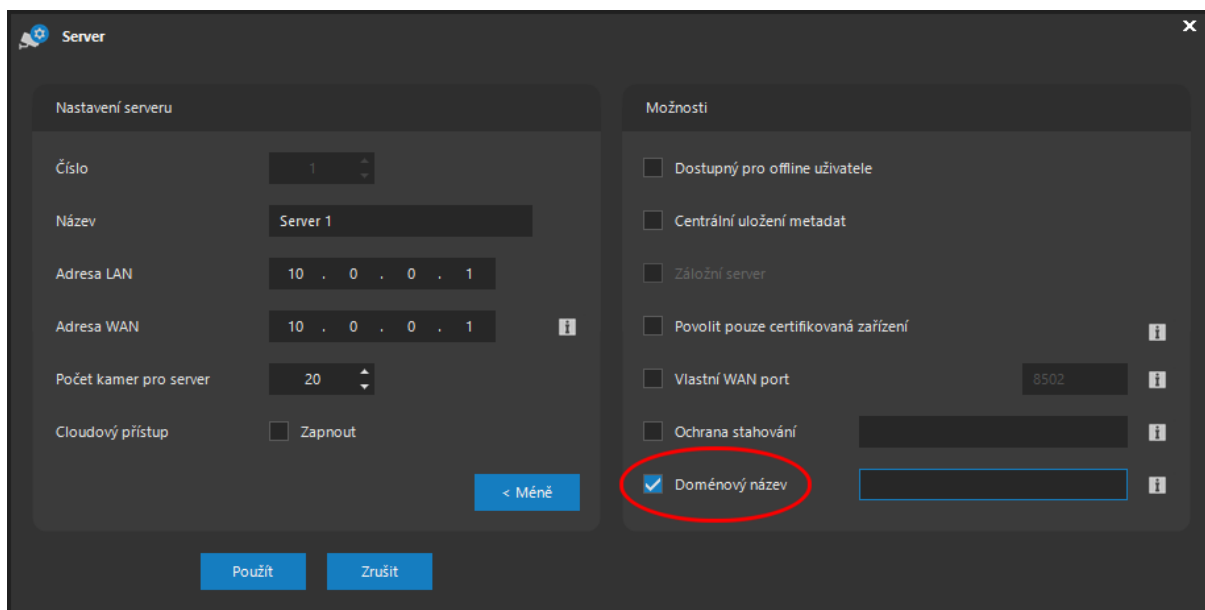
Certifikáty již umístěné v této složce jsou určeny pro testovací účely pro přístup přímo z počítače, kde je nainstalován server. Není třeba je mazat, nově přidaný certifikát bude mít přednost.

- Heslo pro otevření souboru certifikátu se službě administračního či kamerového serveru předá v parametru `-ssl` při startu služby.



Heslo pro certifikát zde nezůstane viditelné, neboť parametry spuštění služby nejsou trvalé. ATEAS proto heslo k souboru v šifrované podobě uloží, aby při restartu služby či serveru mohl soubor s certifikátem opět použít.

- Certifikáty mohou být vystaveny na IP adresu anebo na doménový název. Certifikáty na IP adresy nejsou běžné a v praxi se dají maximálně použít v rámci intranetu. Certifikáty vydávané certifikačními autoritami včetně těch zdarma (např. Let's Encrypt) budou vždy vystaveny na doménový název. V takovém případě je potřeba přiřadit domény kamerovým serverům ATEAS.



POZNÁMKA

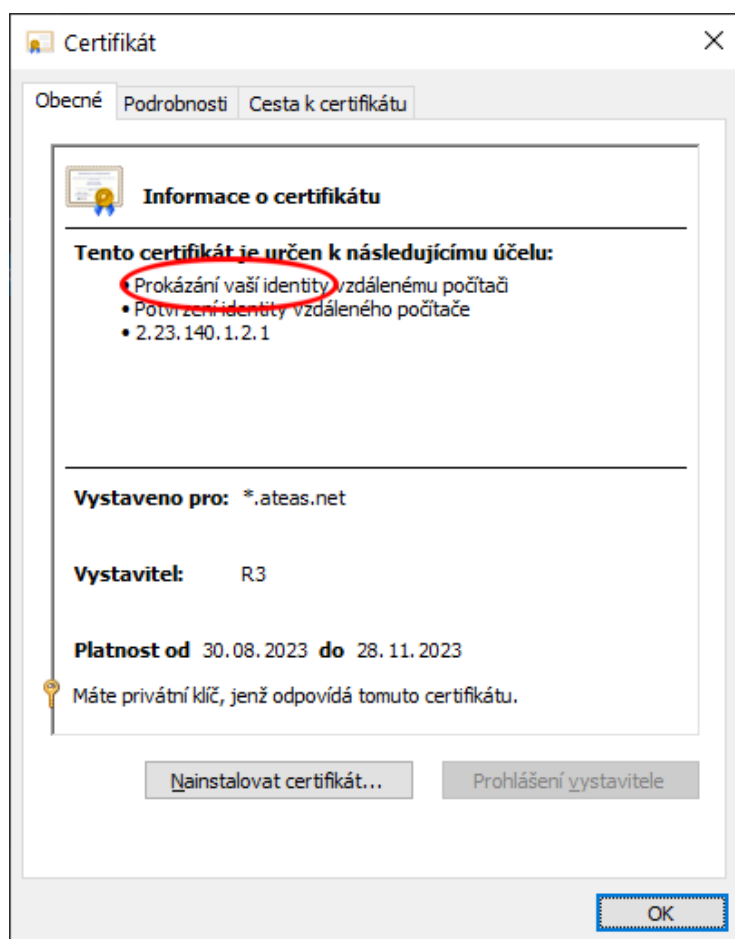
Administračnímu serveru systému není potřeba doménu přiřazovat, neboť je dána zadáním ve webovém prohlížeči.

23.3. Certifikáty

Bližší informace k certifikátům jsou nad rámec tohoto textu, nicméně zde uvádíme pár relevantních informací pro jejich nasazení v rámci ATEAS systému.

ATEAS bude akceptovat všechny certifikáty ve formátu PFX. Důvěryhodnost HTTPS spojení je dána samotným certifikátem a nastaveními v prostředí klienta (důvěryhodné kořenové certifikační autority apod.). ATEAS a webový prohlížeč provedou negociaci verze protokolu TLS a (uvažujeme-li nové verze ATEAS a .NET) a domluví se na použití nejvyšší možné a akceptovatelné verze pro obě strany (nejčastěji TLS 1.3).

Aby mohl být certifikát použit pro prokazování původu serveru, musí mít tuto skutečnost uvedenu v seznamu způsobů použití (účelů, pro který byl vydán). Při použití již existujících certifikátů organizace je toto automatické, při generování vlastního certifikátu je na to třeba pamatovat.



23.3.1. ACME protokol

Vzhledem k popularitě služeb jako je Let's Encrypt, ale také vzhledem k extrémnímu nárůstu počtu vydávaných certifikátů pro provoz zejména webových aplikací, byl v rámci RFC 8555 standardizován protokol ACME (Automatic Certificate Management Environment), který slouží k automatizaci procesu vydávání a obnovy certifikátů. Tento protokol je běžně používán společnostmi nabízejícími webhostingové služby nebo přímo koncovými zákazníky, kteří provozují vlastní infrastrukturu pro webové služby.

Na první pohled by se mohlo zdát vhodné, aby byl ACME protokol implementován přímo v ATEAS systému, čímž by bylo možné získání a nasazení certifikátu plně automatizovat. Minimálně ze dvou důvodů se však toto řešení nejeví jako praktické:

- Primárně je klientský přístup v rámci ATEAS realizován proprietárním protokolem, nikoliv protokolem HTTPS, který je použit pouze pro omezenou část funkcí ATEAS – zejména webový rozcestník pro stažení instalátorů či dokumentace, automatické aktualizace systému, nové na HTTP založené komunikační API a webový klient systému. Zapojení automatizace pro získání certifikátů pro HTTPS se tedy nejeví jako plně odůvodněné.

- Druhým a hlavním důvodem je samotné fungování ACME. Správa certifikátů pro určité domény je podřazena ACME uživatelským účtům vedeným přímo u poskytovatele této služby. Aby tedy kamerový systém ATEAS mohl spravovat certifikát např. pro doménu `cctv.mycompany.com` na již existující doméně `mycompany.com`, musel by získat přístup k ACME přihlašovacím údajům. To může být v praxi větší problém než samotný export certifikátu a jeho jednoduché nasazení v rámci ATEAS systému.

23.3.2. Wildcard certifikáty

Certifikáty vydávané na doménové jméno mohou být úspěšně použity pouze při komunikaci se vzdáleným serverem na adrese (URL) přesně odpovídající doménovému jménu a to včetně dodržení řádu domény (domény druhého či třetího řádu). Není však příliš praktické spravovat různé certifikáty pro většinu domén třetího řádu (např. `www.mycompany.com`, `helpdesk.mycompany.com`, `webmail.mycompany.com` atd.). Tento problém řeší právě wildcard certifikáty, které umožňují verifikaci všech domén vyššího řádu.

POZNÁMKA

Také wildcard certifikáty je možné získat zdarma např. v rámci služby Let's Encrypt. Jeho získání je však v rámci ACME složitější o to, že nestačí pouze prokázat schopnost ovládat obsah na dané doméně, ale také DNS záznamy pro danou doménu.

Následuje příklad wildcard certifikátu `ateas.net`:

Obecné		Podrobnosti
Vydán pro		
Běžný název (CN)	*.ateas.net	
Organizace (O)	<Není součástí certifikátu>	
Organizační jednotka (OU)	<Není součástí certifikátu>	
Vydal:		
Běžný název (CN)	R3	
Organizace (O)	Let's Encrypt	
Organizační jednotka (OU)	<Není součástí certifikátu>	

Jedním wildcard certifikátem tak lze zabezpečit všechny kamerové servery v rámci edice ATEAS UNLIMITED, jelikož ATEAS tyto wildcard certifikáty podporuje.

TIP

Pokud použijete wildcard certifikáty, bude možné použít tentýž certifikát pro administrační server a všechny kamerové servery v systému.

23.4. Použití existujícího certifikátu organizace

V tomto postupu si ukážeme, jak jednoduché je nasadit již existující certifikát pro `ateas.net` pro provoz webového obsahu a webového klienta ATEAS např. na adrese `cctv.ateas.net`.

23.4.1. Získání certifikátu

V prvním kroku je třeba získat již existující certifikát ideálně hned ve formátu PFX, nicméně je možný jakýkoliv jiný formát.

POZNÁMKA

Postup se bude lišit v závislosti na Vašem dodavateli webhostingových služeb, ve většině kvalitních služeb je přístup k certifikátu okamžitě možný z administračního rozhraní. Pokud jsou webové služby nasazeny na Vaší vlastní infrastruktuře, požádejte správce této služby o export certifikátu.

Z administračního rozhraní dodavatele služeb pro provoz `ateas.net` lze veřejnou část wildcard certifikátu Let's Encrypt získat ve formátu CRT a samostatně uložit též soukromý klíč.

+ Nový SSL certifikát

Doména/Subdoména	Typ	Stav	Datum platnosti
ateas.net	bezplatný certifikát Let's Encrypt Wildcard	Aktivní	28.11.2023

[Detail](#)

.CRT

```
-----BEGIN CERTIFICATE-----
MIIE7jCCA9agAwIBAgISA5/0l0CXEiCcYRA9fMqsuAjj4MA0GCSqGSIb3DQEBCwUA
MDIxCzAJBgNVBAYTA1VTMRWwFAYDVQQKEw1MZXR0cyBfYmNyeXB0MQswCQYDVQQD
EwJSMzAeFw0yMzA4MzAxMTE3NDdaFw0yMzExMjg0MTE3NDZaMBYxZDASBgNVBAMM
CyouYXRlYXN0bWV0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqwvJ
6u2S2S0Uoh/14N+xi4Ff/ou40UEmarEaze7yY0x3Ig8RJKAyDUk0SvaSX0QUZjR
BNi8h10LcaIx0trcbF04/fjwYVMhsI2p00hSM/oh1FoAskCp3pavZY+zfqSuyrYG
TeqazN1Xh+2Lo21TGCzejs5dChRZMVnu0+d6EAFt5s2P5XdB4btKjM8uDMedKaH
+aRspXopGLICQqA8wIm+HlzMdAT8ic3eCe5891Boohw7sb0oiZgBpCOKHdAwNfVf
oxRu97YIrnCRqoAzjZvXHEMAJhwPF1QUX521PNw4Mh5vNDZEMKKe4MvUm6UddNGm
/LVBsnPtyRkFujB7ewIDAQABo4ICGDCCAhQwDgYDVVR0PAQH/BAQDAgWgMB0GA1Ud
JQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAMBGNVHRMBAf8EAJAAMB0GA1UdDgQW
BBRhSncMrcwz59gi0Mr09AFGqsb1uzAfBgNVHSMEGDAWgBQULrMXt1hwy65QCUDm
H6+diXCxjBVBggrBgEFBQcBAQRJMEcwIQYIKwYBBQUHMAAGGFWH0dHA6Ly9yMy5v
LmxlbmNyLm9yZzAibGgrBgEFBQcwoAoYWAHR0cDovL3IzLmkubGVuY3Iub3JnLzAh
BgNVHREEGjAYGgsqLmF0ZWZzLm5ldIIJYXRlYXN0bWV0MBMGA1UdIAQMMAowCAYG
Z4EMAQIBMIIBBAYKKwYBBAHwQIEAgSB9QSB8gDwAHUAejKMVN13LbYg6jjgUh7p
hBZwHhOFTTVSK8E6V6NS61IAAAGKRmDbeAAABAMARjBEAiBEJLyqXopHcwsCiAP1
YZmAzS2AG/Gp32tSLD2tSt9F1AIGbPKEmw8LC3aDWB+erS4+3Q16MSZsU4qQdRSf
ymZ41vsAdwC3Pvsk35xNunXyOcw6WPRsXfxcZ3qfNcSeHQBjE20mQAAAYpGYntf
AAAEAwBIMEYCIQC1G1Zf6sskYBUEb4IriN17DiKLrrRwRUD8TLd8PCrYiwIhAOpC
euA/UTmeGPW74WmPYOgx45/SEVEAIk+L4DHGQq09MA0GCSqGSIb3DQEBCwUAA4IB
AQBekXTX5OIUOHbZ1kd3J9yMaCyLSq90rFuSqEFR3ic8EBY4wDDsX2FORS0Uu5o
vwT8//wqGaPb/ucJRfMP2Pbc5+7M/Irbo+eFyatctAk+CN311ym5w+PoU+xSR4V9
JfFP5dxjtEfts2spAoA2ihIW1tT4f32sRd8h81hi20y1KYRMF6hTJKPbckXEBNW1
eic9Zk9uuFaAm1J/1kpPn97YwYv8spuHAG5ONT98myU2trxI70QtavV120Ew9rA6
ZSMfta9NyIQ+Mw9Pt1JpuOLpRbPeDyTpFqfBpQTJaMMqyEiMMGdd2GJTj3DBskVh
+iCUDCzrxCS05wQ6P3g/+gOQ
-----END CERTIFICATE-----
```

.KEY

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAKgggSkAgEAAoIBAQCrc8nq7ZJ1JXRS
```



Textové soubory uložíme jako `ateas.crt` a `ateas.key`.

23.4.2. Export certifikátu

Pro vytvoření souboru ve formátu PFX můžeme použít např. `openssl`.

POZNÁMKA

Pokud Vám Váš dodavatel nebo správce systému umožní export certifikátu již ve formátu PFX, lze tento krok vynechat.

```
openssl pkcs12 -export -out ateas.pfx -inkey ateas.key -in ateas.crt
```

Tímto příkazem získáme certifikát včetně soukromého klíče ve formátu PFX. Program openssl bude při uložení souboru vyžadovat heslo pro pozdější otevření souboru.

Příkazový řádek

```
C:\openssl\bin>openssl pkcs12 -export -out ateas.pfx -inkey ateas.key -in ateas.crt
Enter Export Password:
Verifying - Enter Export Password:

C:\openssl\bin>
```

23.4.3. Nasazení certifikátu

Nasazení výsledného souboru ve formátu PFX se již provede zcela standardním způsobem, který je popsán výše v části Předpoklady. Soubor se jen umístí do příslušné složky a služba serveru se restartuje s použitím hesla pro otevření souboru.

23.4.4. Úprava DNS záznamu

Abychom mohli otestovat fungování exportovaného certifikátu při použití v ATEAS systému, upravíme ještě DNS záznam pro cctv.ateas.net tak, aby odpovídal IP adrese, na které je spuštěn administrační server ATEAS.

POZNÁMKA

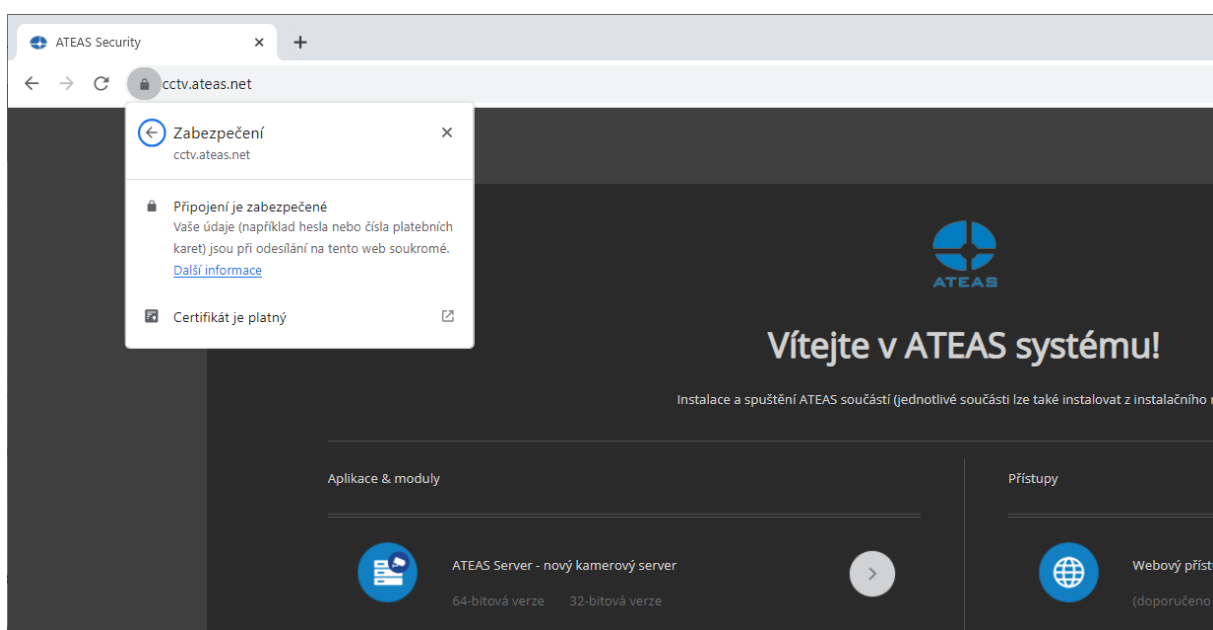
Stejně tak bude nutné přesměrovat domény jednotlivých kamerových serverů.

Používáme-li IPv4 adresu, přidáme k DNS záznamům nový záznam typu A, např. následovně.

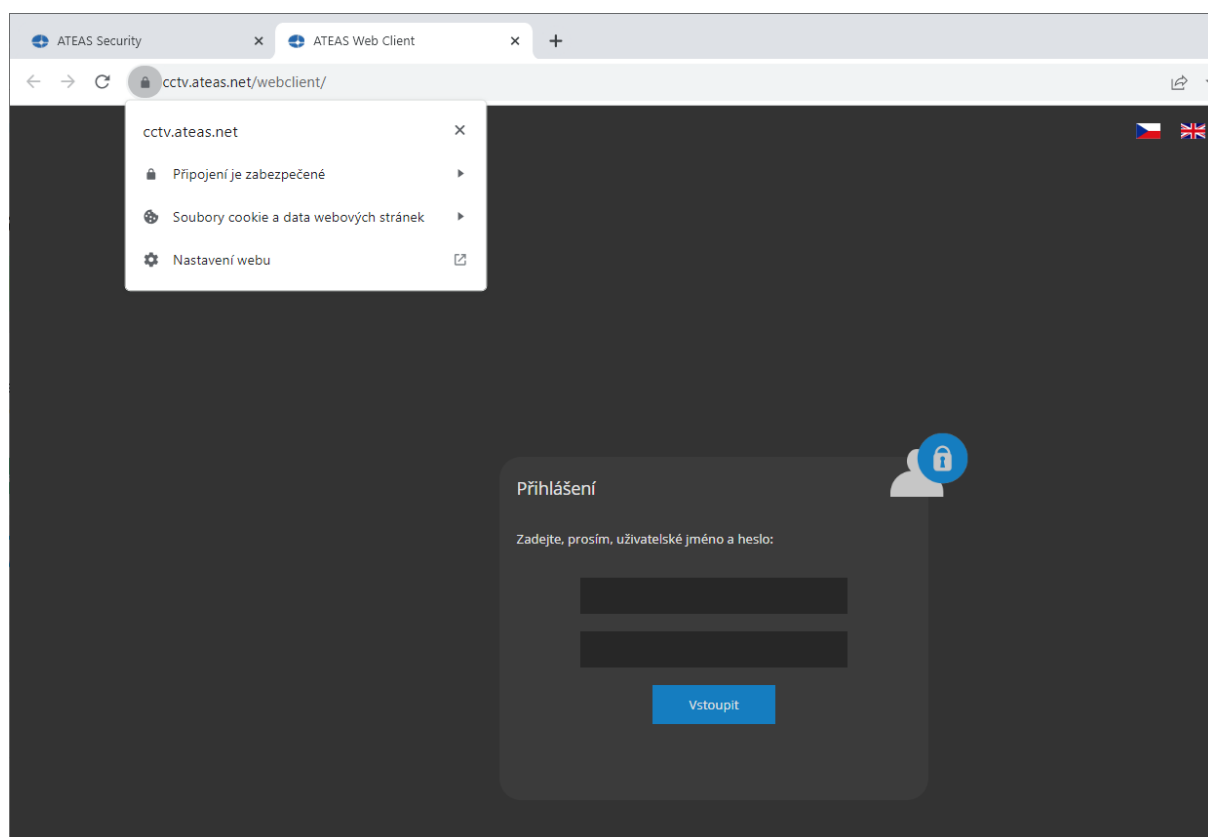
cctv	360	A	37.143.114.180	Upravit
------	-----	---	----------------	-------------------------

23.4.5. Test certifikátu

Nyní, pokud přistoupíme na adresu `cctv.ateas.net`, Let's Encrypt wildcard certifikát by měl zajistit správnou verifikaci této domény včetně indikace, že se jedná o důvěryhodné spojení, neboť prostředí klienta považuje Let's Encrypt za důvěryhodnou certifikační autoritu.



Stejně tak bude zabezpečen i přístup k serveru, pokud spustíme webového klienta.



Architektura v rámci ATEAS systému (pokud není pro některé kamerové servery aktivován režim cloud) spojuje klienta s kamerovými servery, ke kterým má přístup, vždy přímo, tedy nikoliv prostřednictvím administračního serveru, čímž jsou významně optimalizovány datové toky v síti např. v systému s centrální správou a lokálními kamerovými servery.

POZNÁMKA

Na pozadí tedy budou vytvořena dodatečná spojení pomocí WebSocket protokolu (v rámci HTTPS) s kamerovými servery, kdy budou postupně verifikovány také certifikáty kamerových serverů při přenosu videa z kamer.

23.5. Použití nového certifikátu

Pro HTTPS komunikaci s administračním a kamerovými servery ATEAS je také možné vytvořit vlastní certifikát ať už odvozený od existujícího certifikátu nějaké kořenové certifikační autority nebo tzv. self-signed certifikát, kdy si sami vytvoříme jak nový kořenový certifikát, tak certifikát pro kamerový systém.

POZNÁMKA

Je logické, že takový typ certifikátu sice zajistí nejvyšší úroveň šifrování komunikace, ale nezajistí apriori jeho důvěryhodnost.

To znamená, že webový prohlížeč bude na nedůvěryhodnost (nikoliv nezašifrování) spojení upozorňovat. V rámci intranetu se tomu samozřejmě dá předjít importem příslušných certifikátů mezi důvěryhodné certifikační autority a tím tento problém eliminovat. V rámci otevřeného internetu to však nebude možné. Záleží tedy, v jakém prostředí má být webové rozhraní kamerového systému ATEAS provozováno.

K vytvoření vlastního certifikátu, který bude ATEAS akceptovat, je možné použít libovolný nástroj kompatibilní se standardem x509 pro formát certifikátu. Těchto nástrojů je nepřeberné množství, mnohé z nich jsou vybaveny i grafickým uživatelským rozhraním. Zde se přidržíme referenčního nástroje openssl.

23.5.1. Vytvoření kořenového certifikátu

K vytvoření certifikátů nové certifikační autority můžeme použít např. následující příkaz:

```
openssl req -x509 -newkey rsa:4096 -sha256 -days 3650  
-keyout testroot.key  
-out testroot.crt  
-nodes  
-subj "/CN=TestRoot"
```

Tento příkaz vytvoří v souboru testroot.crt certifikát nové certifikační autority TestRoot. Ostatní parametry mají následující význam:

- -newkey určuje, že má být vytvořen nový soukromý klíč RSA s délkou klíče 4 kB,
- -days určuje desetiletou platnost certifikátu,
- -out a -keyout udávají názvy výstupních souborů,
- -nodes vypíná použití hesla pro uložení privátního klíče (zde pro jednoduchost),
- -subj udává v klíči CN název autority, jiné parametry nejsou potřeba.


```
Příkazový řádek
C:\openssl\bin>openssl req -x509 -newkey rsa:4096 -sha256 -days 3650 -keyout testroot.key -out testroot.crt -nodes -subj
"/CN=TestRoot"
Generating a RSA private key
.....++++
.....++++
writing new private key to 'testroot.key'
-----
C:\openssl\bin>
```

POZNÁMKA

Pokud ne zadáte parametr subj, bude openssl příkaz fungovat interaktivně a bude možné postupně zadat i jiné vlastnosti pro certifikát.

23.5.2. Vytvoření certifikátu serveru

Nyní vytvoříme certifikát pro server, který bude podepsaný naší nově vytvořenou certifikační autoritou. Opět využijeme openssl a v prvním kroku vytvoříme požadavek pro certifikační autoritu ve formátu CSR. Tento požadavek běžně vytváříte v operačních systémech Windows či macOS pomocí vestavěných nástrojů (certmgr.msc či Keychain na macOS).

```
openssl req -new -newkey rsa:2048
-keyout 10.0.0.1.key
-out 10.0.0.1.csr
-nodes
-subj "/CN=10.0.0.1"
```

Příkaz je velmi podobný jako v předchozím případě s těmito hlavními rozdíly:

- -new se postará o vytvoření požadavku na certifikační autoritu,

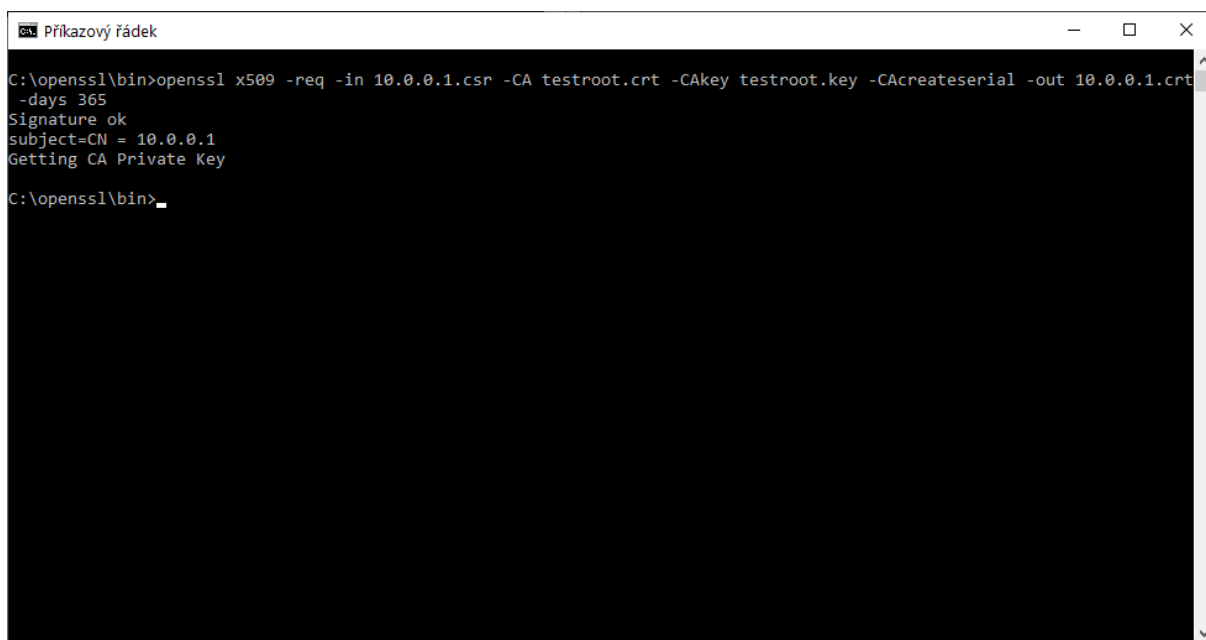
- -subj již musí obsahovat přesný název serveru, kde bude certifikát nasazen, tj. doménové jméno nebo jako v tomto případě IP adresu.

Nyní musí naše certifikační autorita požadavek uložený v souboru CSR zpracovat (schválit) a vytvořit certifikát pro náš server.

```
openssl x509 -req -in 10.0.0.1.csr  
-CA testroot.crt  
-CAkey testroot.key  
-CAcreateserial  
-out 10.0.0.1.crt  
-days 365
```

V příkazu vidíme, že certifikační autorita zpracovává náš požadavek na certifikát pro server 10.0.0.1 a nakonec ho podepíše svým kořenovým certifikátem (proto musíme příkazu poskytnout i soukromý klíč autority). Další parametry znamenají:

- -CA a -CAkey udávají veřejnou a soukromou část certifikátu autority,
- -CAcreateserial zakládá číselnou řadu pro sériová čísla certifikátů autority,
- -days určuje roční platnost certifikátu pro náš server.



```
Příkazový řádek  
C:\openssl\bin>openssl x509 -req -in 10.0.0.1.csr -CA testroot.crt -CAkey testroot.key -CAcreateserial -out 10.0.0.1.crt -days 365  
Signature ok  
subject=CN = 10.0.0.1  
Getting CA Private Key  
C:\openssl\bin>
```

Opakováním postupu v této subkapitole je možné certifikovat libovolné množství dalších serverů.

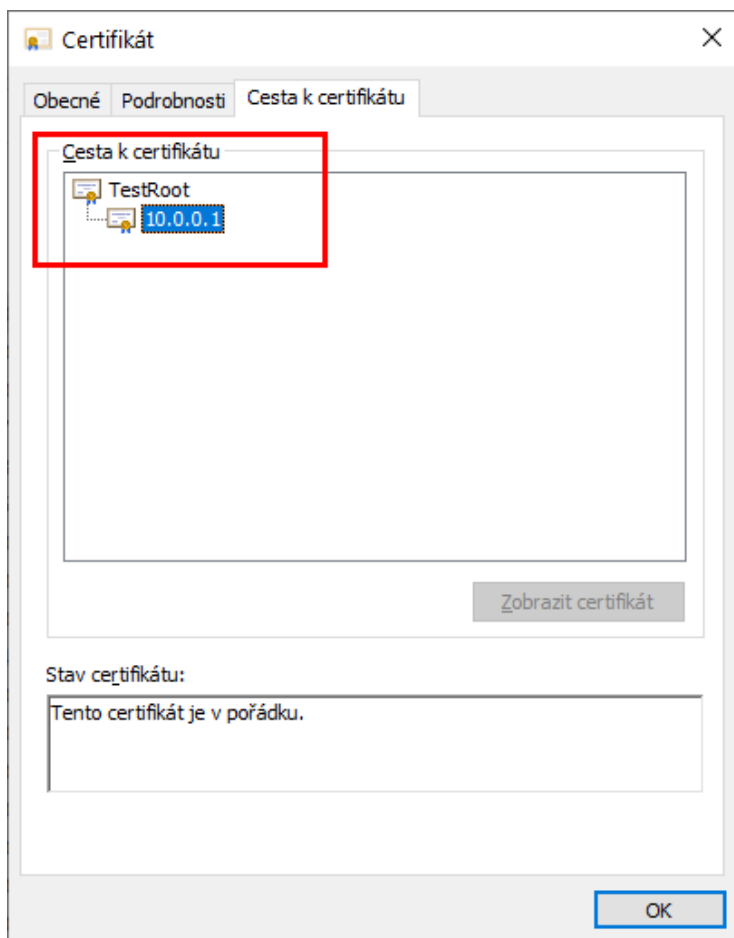
POZNÁMKA

Při druhém serveru v pořadí by se však měl parametr CCreateserial nahradit parametrem CAserial a poskytnout cestu k souboru, ve kterém autorita ukládá sériová čísla vydaných certifikátů.

Výsledný certifikát vidíme na následujícím obrázku.

POZOR

Aby se mohla načíst celá cesta k certifikátu, je nutné předem importovat certifikát naší certifikační autority mezi důvěryhodné kořenové certifikační autority.



Nyní máme vytvořen vlastní certifikát pro provoz ATEAS serveru na adrese 10.0.0.1. Zbývá dodat, že teoreticky (a kryptograficky validně) by bylo možné vytvořit certifikát serveru hned v prvním kroku při

použití názvu serveru (namísto našeho názvu TestRoot). Čtenáři se základní gramotností v oblasti certifikátů bude však ihned jasný do očí bijící defekt takového přístupu. Každý server by byl v takovém případě sám svým vydavatelem certifikátu a bylo by nutné zavést každý server jako důvěryhodnou kořenovou certifikační autoritu. To se jednak míjí s principem vydávání certifikátů a zároveň to též znesnadňuje jejich správu.

POZNÁMKA

Při vytváření vlastních certifikátů tedy respektujte zavedené a zde ukázané principy a vyhněte se tvorbě self-signed certifikátů přímo na úrovni jednotlivých serverů ATEAS.

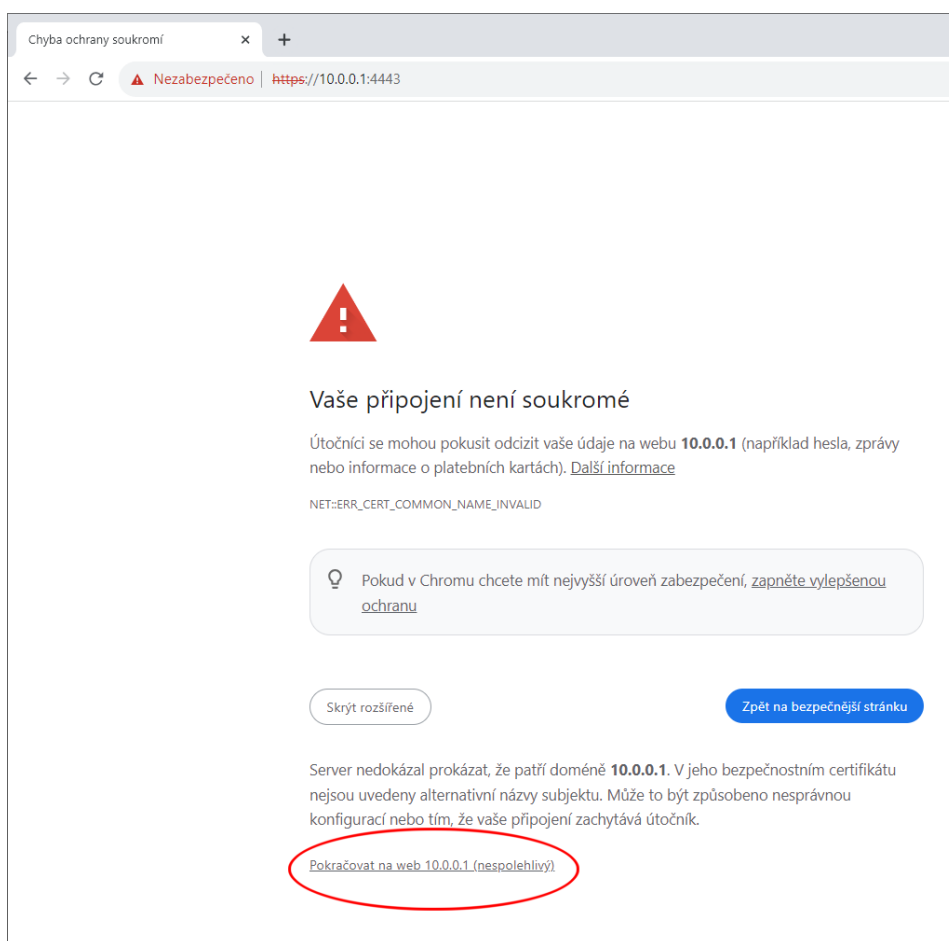
23.5.3. Nasazení certifikátu

Nyní již zbývá pouze převést vydaný certifikát pro adresu 10.0.0.1 (podepsaný a schválený naší certifikační autoritou) do formátu PFX. V průběhu exportu si openssl opět vyžádá heslo. Výsledný certifikát v souboru PFX již nasadíte obvyklým způsobem popsáním v části Předpoklady.

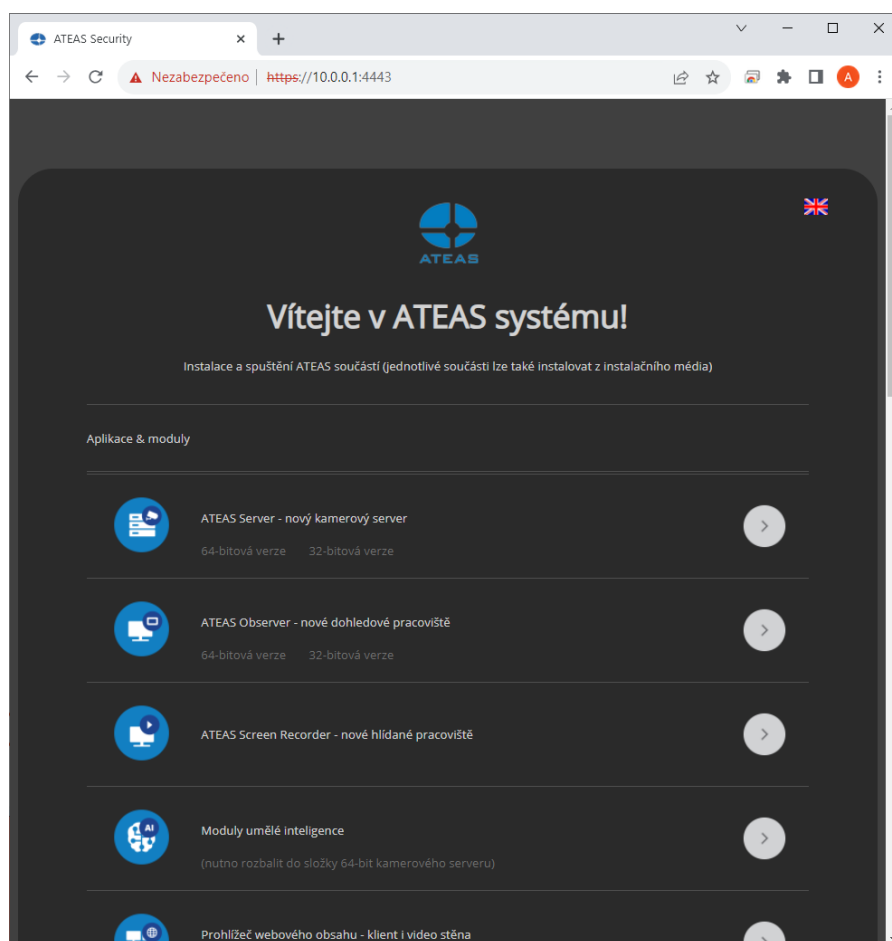
```
openssl pkcs12 -export -out 10.0.0.1.pfx -inkey 10.0.0.1.key -in 10.0.0.1.crt
```

23.5.4. Předběžný test certifikátu

Při přístupu k systému přes HTTPS prohlížeč (zde Chrome) nejprve zobrazí varování (eliminujeme ho v další subkapitole), ve kterém tvrdí, že server nebyl schopen prokázat svůj původ. Jelikož jsme již ovšem importovali naši certifikační autoritu mezi důvěryhodné certifikační autority, nebude to otázka důvěryhodnosti.



Pokud přes varování přejdeme pomocí odkazu výše, certifikát bude funkční, zůstane však aktivní varování v podobě červeného zvýraznění a textu nezabezpečeno.



23.5.5. Prokázání původu serveru

Abychom eliminovali tento pro uživatele poněkud nepřívětivý krok, musíme ještě provést poslední úpravu našeho certifikátu. Náš systém již důvěřuje certifikační autoritě TestRoot, nicméně prohlížeč nyní stále tvrdí, že server nebyl schopen prokázat svůj původ na adrese 10.0.0.1. Je tomu tak proto, že moderní verze prohlížečů vyžadují uvedení tzv. alternativního jména v certifikátu. K tomu si vytvoříme jednoduchý rozšiřující soubor 10.0.0.1.ext s tímto minimálním obsahem:

```
[v3_ca]
extendedKeyUsage = serverAuth
subjectAltName = IP:10.0.0.1
```

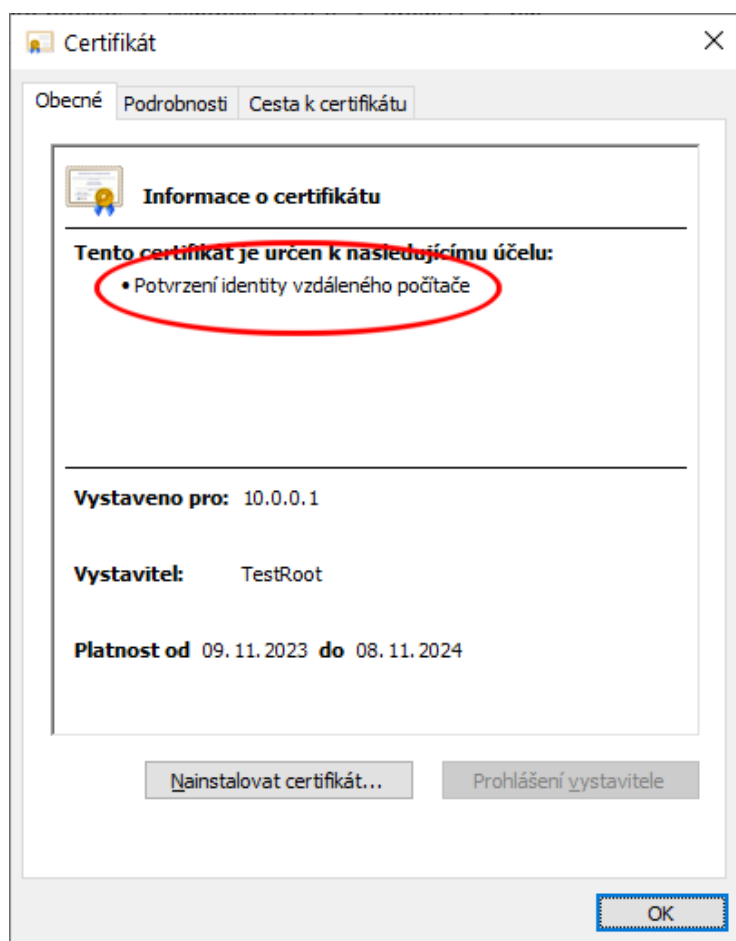
POZNÁMKA

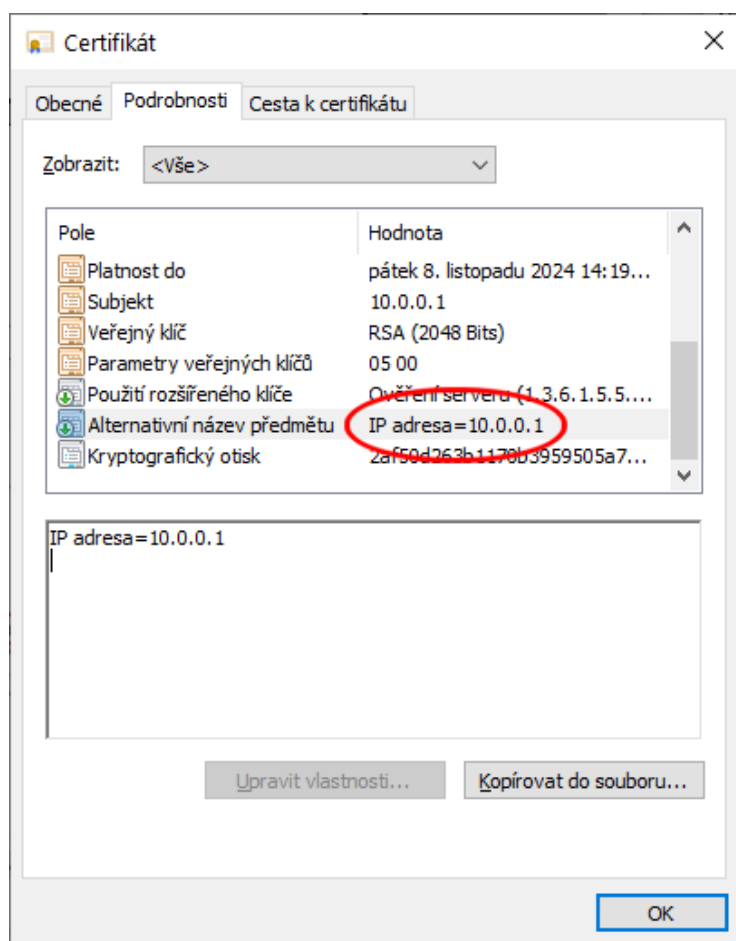
Pokud bychom vystavovali certifikát pro doménu, text IP bychom změnili na DNS. Použití IP adresy je navíc možné až ve verzi 3 standardu X509.

Autorita tedy rozšíří příkaz pro vytvoření certifikátu serveru na tuto podobu:

```
openssl x509 -req -in 10.0.0.1.csr  
-CA testroot.crt  
-CAkey testroot.key  
-CAcreateserial  
-out 10.0.0.1.crt  
-days 365  
-extfile 10.0.0.1.ext  
-extensions v3_ca
```

Nyní jsme pro certifikát definovali rozšířenou vlastnost použití pro prokázání původu serveru a vyhověli jsme požadavku prohlížečů na uvedení alternativního jména. Tyto dvě změny vidíme na následujících obrázcích.





23.5.6. Závěrečný test certifikátu

Po převodu certifikátu do PFX a jeho nasazení způsobem ukázaným výše a zajištěním jeho důvěryhodnosti importem naší certifikační autority mezi důvěryhodné kořenové certifikační autority pak budeme moci k systému přistoupit již bez jakýchkoliv varování ze strany prohlížeče.

