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 4.6.1. 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 START a 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 Security Administrator a ATEAS Security Server na dedikovaný počítač (server) pro kamerový systém, na kterém bude probíhat záznam a řízení a vyhodnocování událostí. ATEAS Security Observer se poté instaluje na příslušný počet klientských stanic, které budou mít systému přistup.

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

1.2. Shodný postup instalace

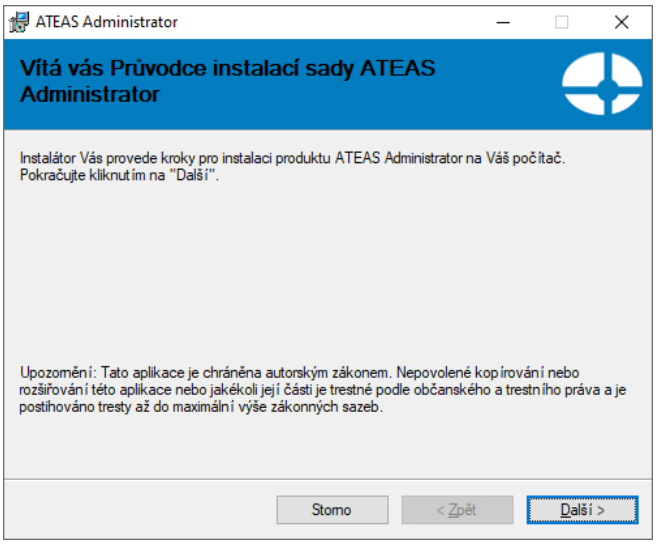
Všechny tři uvedené aplikace se instalují zcela analogicky se stejným instalačním průvodcem. Odkazy na instalaci všech těchto aplikací včetně dalších důležitých odkazů naleznete přímo na stránce, která se automaticky otevře po vložení či připojení instalačního média. K dispozici jsou tyto odkazy:

- úvodní kapitola dokumentace produktu o instalaci systému,
- instalace administračního serveru systému,
- instalace kamerového serveru systému (32-bitová a 64-bitová edice),
- instalace kamerového klienta systému (32-bitová a 64-bitová edice),
- 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.

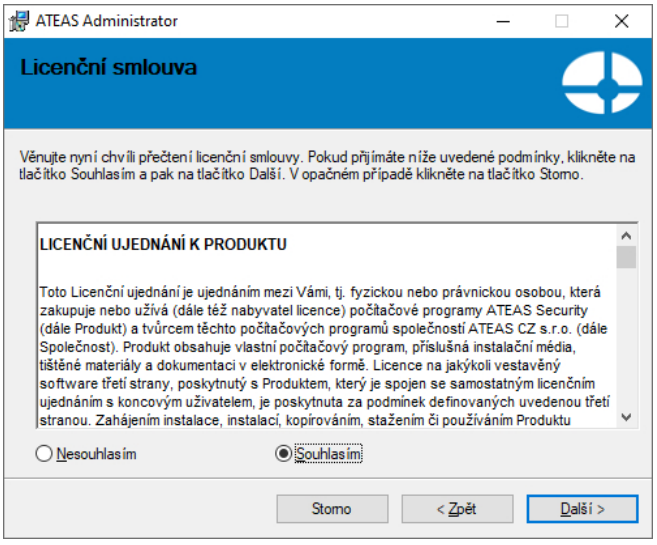
Pořadí, v jakém budete tyto tři produkty instalovat, je libovolné. Zde si ukážeme průběh instalačního průvodce pro ATEAS Security Administrator, u zbylých dvou aplikací je průběh zcela analogický s několika málo drobnými změnami, které jsou popsány dále v této kapitole.

Krok 1 – Uvítací obrazovka instalátoru.



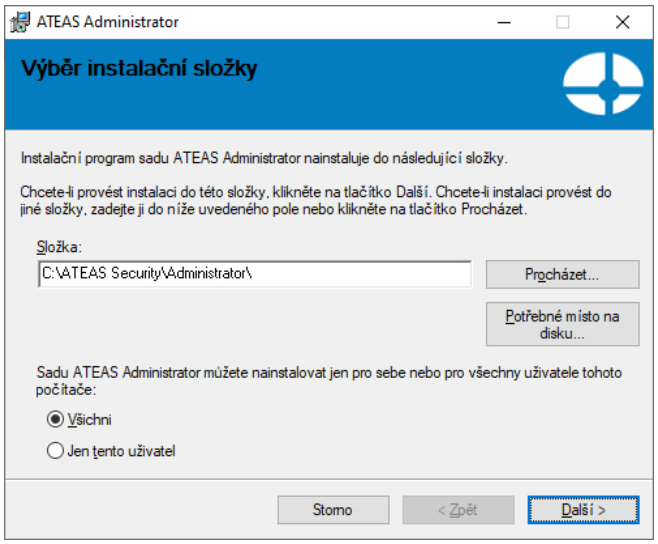
V instalaci pokračujte stisknutím tlačítka **DALŠÍ**.

Krok 2 – Licenční ujednání.



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

Krok 3 – Výběr instalační složky.



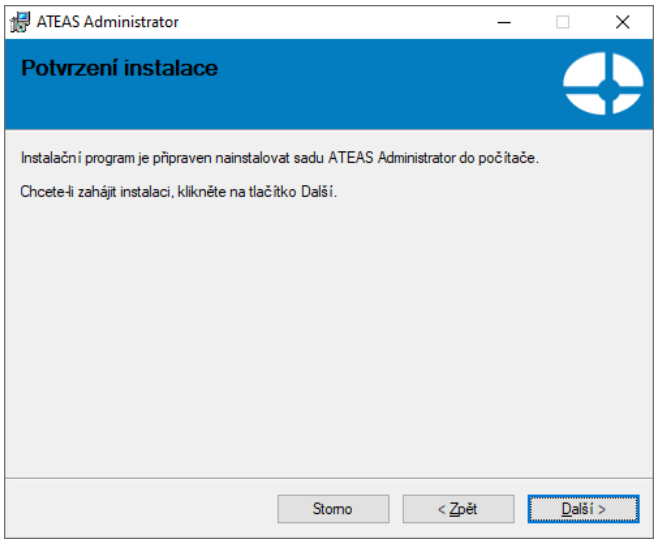
POZOR

Pokud chcete používání aplikací ATEAS Security (týká se zejména klientské aplikace) umožnit i jiným uživatelům systému Windows, je nutné označit přepínač Všichni.

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.

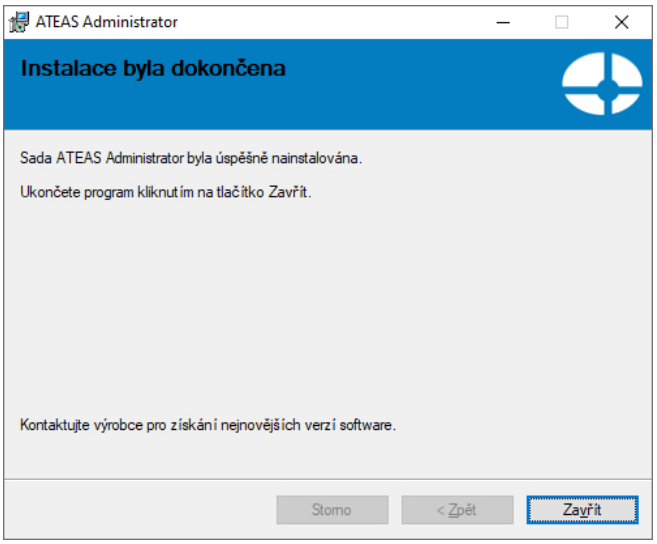
V instalaci pokračujte stisknutím tlačítka **DALŠÍ**.

Krok 4 – Potvrzení instalace.



V instalaci pokračujte stisknutím tlačítka **DALŠÍ**.

Krok 5 – Dokončení instalace.



Tlačítkem **ZAVŘÍT** je instalace dokončena.

1.3. Specifika administračního serveru

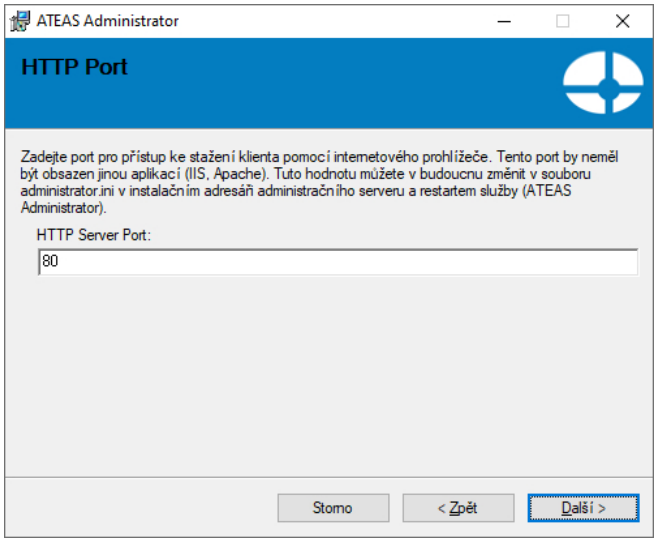
Při instalaci administračního serveru se ještě před zahájením samotné instalace zobrazuje doplňkový dialog, který upozorňuje na skutečnost, že při aktualizaci systému na novější verzi nebude možné systém aktivovat pokud není aktivní služba ATEAS PMA. Před zahájením aktualizace je tedy nutné se ujistit,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

> **POZNÁMKA**
>
> V edici START 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 řídící 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

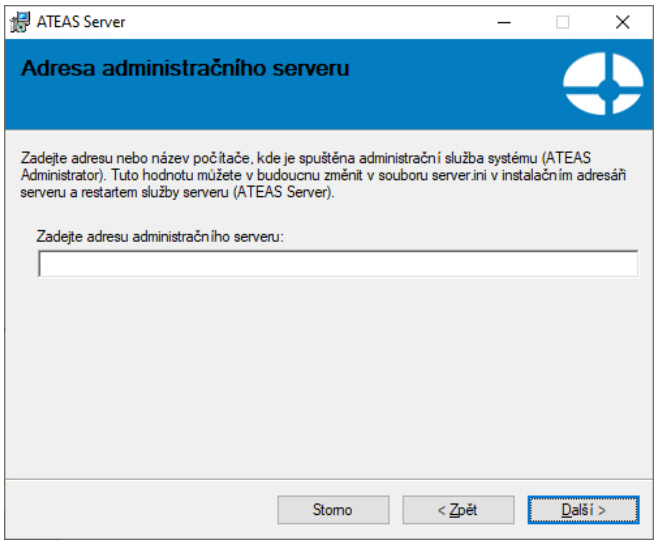
Pomocí webového prohlížeče lze stáhnout či nainstalovat i kamerový server, jeho připojení do systému však může provést pouze administrátor systému.



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 kdekoliv 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.

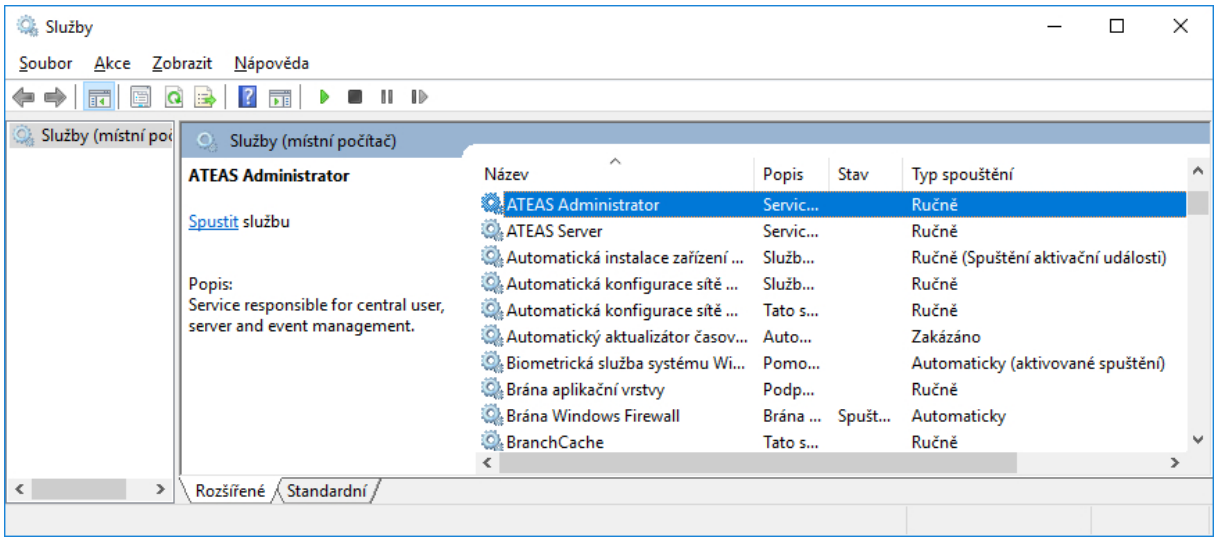
V budoucnu lze tuto hodnotu změnit v souboru server.ini v klíči ADMIN v instalačním adresáři a restartem služby ATEAS Server.

1.5. 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.

1.6. 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 WEBCLIENTFORCESSL (implicitně OFF): Povoluje nebo zakazuje nezabezpečený provoz webového klienta. Při nastavení na ON bude možné webového klienta provozovat pouze na zabezpečené verzi protokolu http a adresa tak bude vždy začínat na https://.

1.7. 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 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 použití 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 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.

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

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 autorizaci k http serveru.

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

1.8. 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.

1.9. 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.

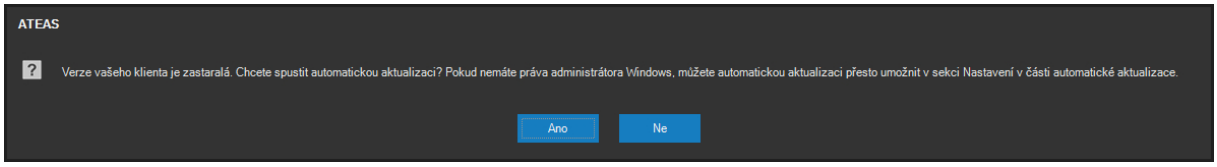
POZNÁMKA

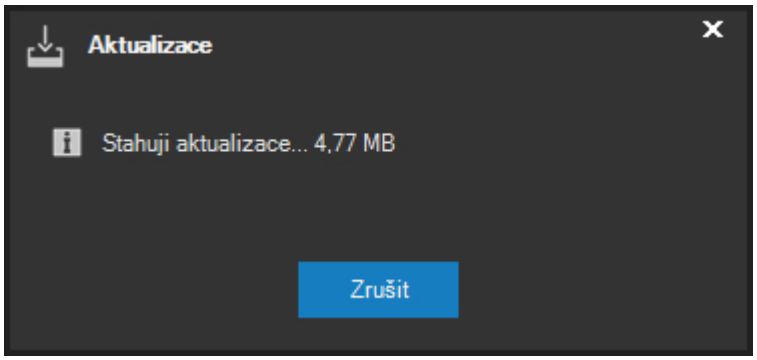
Při reinstalaci administračního serveru systému je automaticky nahrazena starší verze produktu, není nutné provádět ruční odinstalaci.

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.





ATEAS Server se automaticky aktualizuje naprosto nezávisle na přihlášeném uživateli a jeho oprávnění, pro provoz služeb ATEAS Security není nutné, aby byl nějaký uživatel vůbec přihlášen. Je tomu tak proto, že služby běží pod účtem Local System. Pro automatickou aktualizaci klienta jsou však vyžadována práva administrátora k lokálnímu počítači. Od verze 3.9.5 je však možné provést automatickou aktualizaci klienta i pokud klient běží pod účtem s omezeným přístupem k lokálnímu počítači pomocí nastavení administrátorského účtu, pod kterým bude aktualizace spuštěna. Pro více informací si prosím přečtěte subkapitolu Automatické aktualizace v kapitole Lokální nastavení.

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 zprávy tlačítkem **ANO**, neboť počítače video stěny často nemusí mít připojena periferní zařízení.

1.10. 32-bitové a 64-bitové verze aplikací

Na úvodní stránce instalačního média jsou pro kamerové servery (ATEAS Server) a klienty (ATEAS Observer) k dispozici 32-bitové a 64-bitové verze instalací. 32-bitové edice mohou být instalovány jak na 32-bitové, tak na 64-bitové operační systémy Windows. 64-bitové edice aplikací jsou kompatibilní pouze s 64-bitovým operačním systémem. Mezi provozem 32-bitové a 64-bitové verze aplikace na 64-bitovém operačním systému nejsou zásadní (tj. za všech okolností měřitelné) rozdíly ve spotřebě výkonu. 64-bitové edice tedy mohou znamenat přínos pouze spíše u extrémnějších konfigurací, kde by aplikaci nestačil 32-bitový adresní prostor (pod 4 GB RAM) pro její provoz.

POZNÁMKA

Administrační server systému je vždy 64-bitový.

Jednotlivé edice lze libovolně nahrazovat. Je tedy možné kdykoliv odinstalovat 32-bitovou edici aplikace a do stejné složky instalovat 64-bitovou edici a dojde k převzetí veškerých nastavení. Stejným způsobem je možný i přechod z 64-bitové na 32-bitovou edici aplikace.

POZNÁMKA

Při automatických aktualizacích kamerových serverů a klientů platí velmi důležitá zásada zachování edice. Při automatické aktualizaci se 32-bitová edice vždy aktualizuje na 32-bitovou edici, a 64-bitová edice na 64-bitovou. Pokud se tedy na daném počítači rozhodneme pro změnu edice, je nutné provést tuto změnu ručně.

1.11. Více síťových karet v počítači

Pokud je v libovolném počítači v systému použito více síťových karet, je fungování celého systému nadále automatické bez nutnosti dodatečného nastavování. Více síťových karet lze použít například v serveru pro fyzické (jiné aktivní síťové prvky) či virtuální (pomocí VLAN) oddělení sítě kamerových bodů a sítě klientů. Vzhledem k tomu, že administrační server provádí verifikaci kamerových serverů, které se připojují do systému, musí být dodržen princip, podle něhož se kamerové servery připojují k administračnímu serveru z adresy, pod kterou jsou v systému identifikovány. Pokud je tedy kamerový server součástí dvou sítí (např. 10.0.0.X a 10.0.1.Y s maskami podsítě 255.255.255.0) a administrační server je v síti 10.0.0.X, musí být kamerový server do systému přidán také s adresou v síti 10.0.0.X, kamerový server poté již sám automaticky zvolí příslušný síťový interface pro připojení k administračnímu serveru. Pokud je administrační server na stejném počítači jako popisovaný kamerový server, může být pro jejich propojení a identifikaci zvolen libovolný interface (musí si však odpovídat adresa v klíči ADMIN v server.ini a adresa, která je použita při registraci (přidání) kamerového serveru do systému.

Jedinou teoretickou výjimkou bez praktického významu by mohla být situace, kdy může kamerový server provést připojení k administračnímu serveru z více síťových interfaců. V takovém případě, aby vždy došlo ke správné identifikaci kamerového serveru, může být nutné tuto adresu doplnit do souboru server.ini ke klíči LOCALIP a restartovat službu kamerového serveru. V naprosté většině případů lze klíč LOCALIP ponechat bez vyplnění.

Při dodržení výše uvedených principů bude systém bez problémů fungovat i na serveru (počítači) s více než dvěma síťovými rozhraními. Pokud bude existovat více oddělených sítí na více síťových rozhraních, na kterých budou do systému přistupovat klienti, musí mít tyto klienti nastaven profil na REMOTE. Při tomto profilu totiž klient automaticky použije pro adresu kamerového serveru adresu administračního serveru použitou při přihlášení.

Pokud mají někteří uživatelé profil LOCAL a příslušný kamerový server má více síťových rozhraní, může být nutné určit síťové rozhraní, které bude použito pro multicastové vysílání. To je možné v klíči MULTICASTSOURCEIP v souboru server.ini. V naprosté většině případů lze tento klíč ponechat bez vyplnění.

POZOR

Více síťových karet (rozhraní) v počítači s kamerovým serverem nelze zaměňovat s možností definovat pro server adresu LAN a WAN pro vzdálený přístup z prostředí WAN či internetu.

1.12. 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 implementovánu 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.

1.13. Webový klient a zabezpečení

Pokud je po instalaci administračního serveru povolen provoz webového klienta pomocí položky WEBCLIENT v konfiguračním souboru administrator.ini, je možné na daných portech (http nebo https) přistoupit na domovskou stránku Vašeho kamerového systému a webového klienta spustit.

Architektura ATEAS Security je založena na optimalizaci přenosů tak, že do klienta vždy proudí data přímo z kamerového serveru a nikoliv přes server administrační. To znamená, že pokud se uživatel přihlásí z místa své pobočky do kamerového systému a bude dohlížet kamery na své pobočce, přihlášení proběhne k centrálnímu serveru, nicméně data budou proudit nejkratší cestou přímo ze serveru umístěného na jeho pobočce směrem ke klientovi.

Tento princip je plně respektován i při použití webového klienta.

POZOR

Proto je pro provoz webového klienta důležité, aby byly dostupné i porty kamerových serverů v systému pro webový přístup – 8507pro nezabezpečenou a 8508 pro zabezpečenou komunikaci.

Pokud se uživatel pokusí na webovou stránku systému přistoupit pomocí zabezpečené verze protokolu http (https://) anebo pokud je použití zabezpečené komunikace vynuceno položkou WEBCLIENTFORCESSL, je třeba, aby Váš kamerový systém disponoval příslušnými certifikáty.

POZNÁMKA

Může se jednat jak o testovací certifikáty vydávané zdarma nebo přímo Vámi, tak o jakékoliv Vaše komerční certifikáty vystavené certifikační autoritou, která ověří Vaší identitu.

Jelikož certifikát musí být vydán vždy pro příslušný server, jeho jméno, adresu či doménu, nelze správné certifikáty dodat na Váš systém již s instalací kamerového systému. V podsložkách ssl Vašeho administračního a kamerového serveru se nacházejí certifikáty ateas_root.pfx a ateas_127_0_0_1.pfx, které mohou posloužit pro otestování zabezpečené verze webového klienta. První certifikát je testovací kořenový certifikát ATEAS a druhý je certifikát založený na tomto kořenovém certifikátu vydaný pro server „127.0.0.1“.

POZNÁMKA

Pokud tyto testovací certifikáty nainstalujete, Váš prohlížeč bude akceptovat připojení k serveru jako důvěryhodné pouze při přístupu na adresu „127.0.0.1“, tj. pouze přímo z počítače, kde je server nainstalován.

Instalace certifikátů do kamerového systému

Instalaci certifikátu pro Váš server (administrační i kamerový), lze jednoduše provést tak, že certifikát umístíte ve formátu PFX (Personal Information Exchange) přímo do složky ssl v instalační složce příslušného serveru a restartujete server.

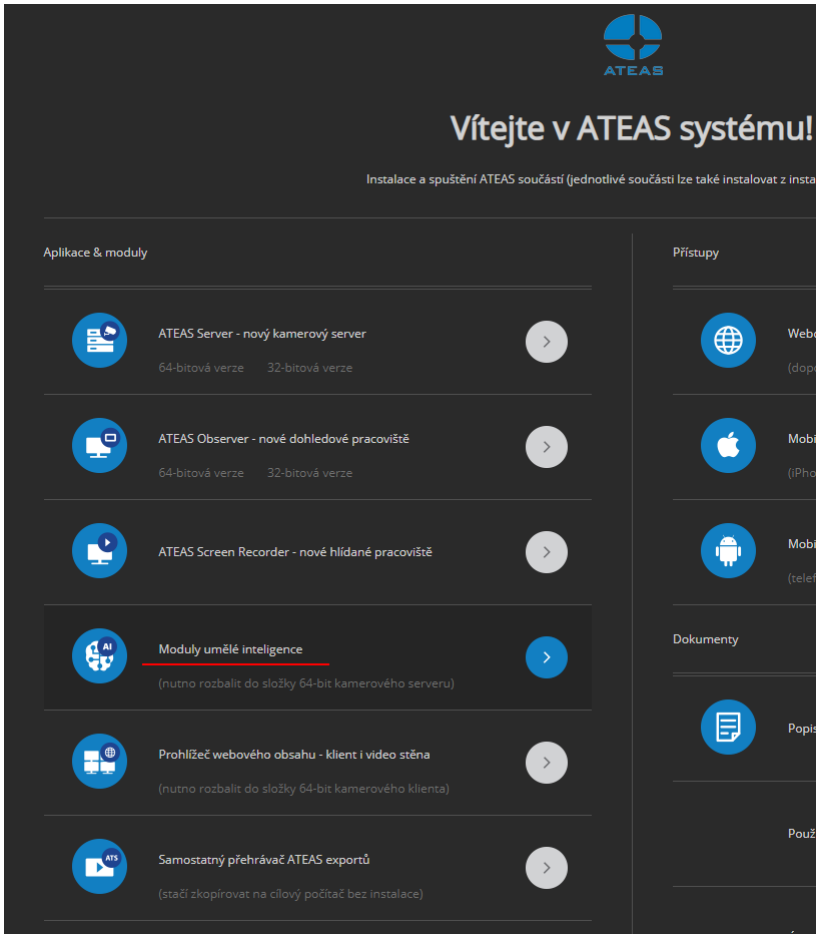
Pokud jsou data certifikátu chráněna heslem, je možné toto heslo službě administračního nebo kamerového serveru předat pomocí parametru –ssl při startování služby. Více viz také kapitola Parametrické spouštění aplikací.

POZNÁMKA

Heslo pro testovací certifikáty dodané spolu s instalací je „ateas“. Heslo není nutné zadávat pomocí přepínače ssl do doby, než bylo pomocí tohoto přepínače předáno jiné heslo.

1.14. 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**.

1.15. 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.

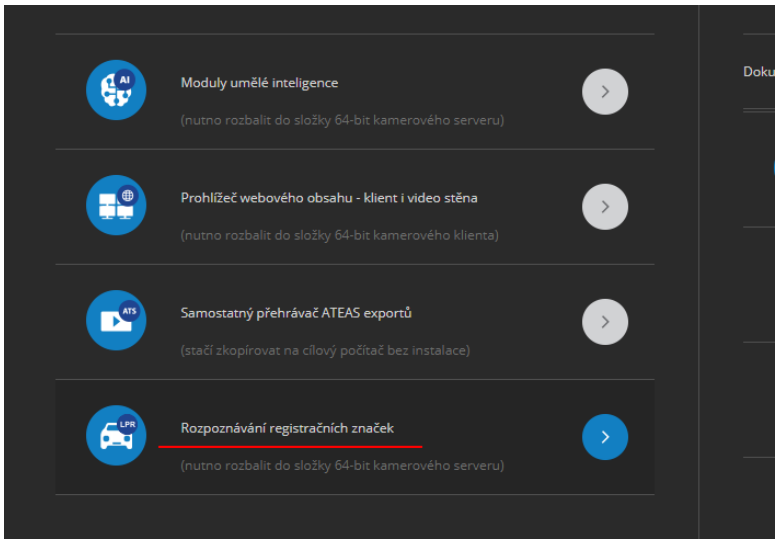
Archiv musí být rozbalen do instalační složky klienta ATEAS.

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.

1.16. Instalace rozpoznávání registračních značek

Instalaci rozpoznávání registračních značek vozidel 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 touto funkcí vybaven.



Po instalaci je pak možné pokračovat v administraci doplňků v části SPZ.

> **POZNÁMKA**
>
> Funkce rozpoznávání registračních značek vozidel vyžaduje dodatečnou licenci.

1.17. 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.

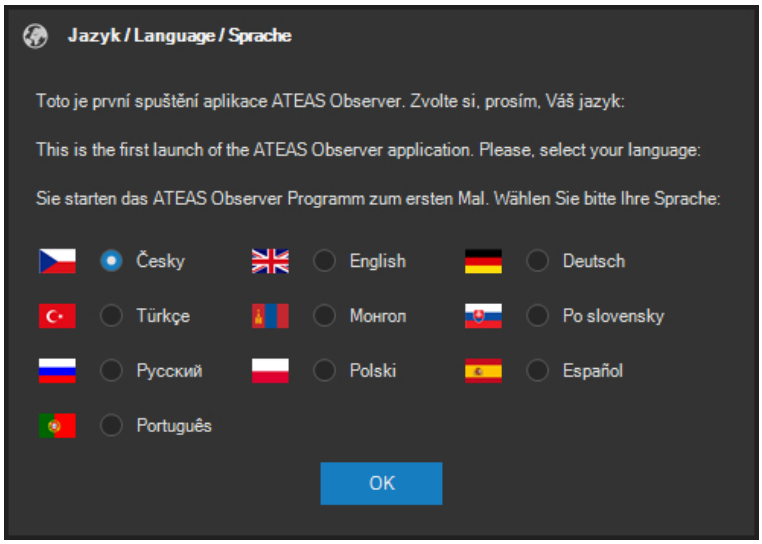
Kapitola 2 - První spouštění

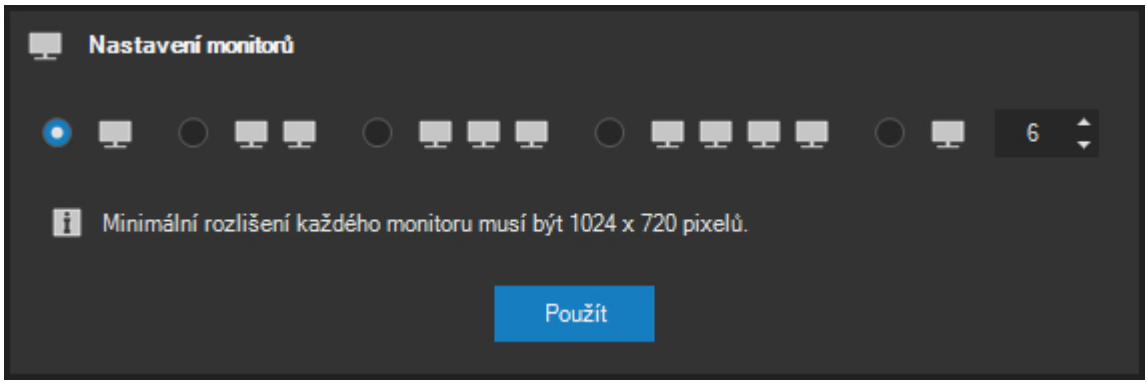
2.1. První přihlášení a zadání licenčního klíče

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.

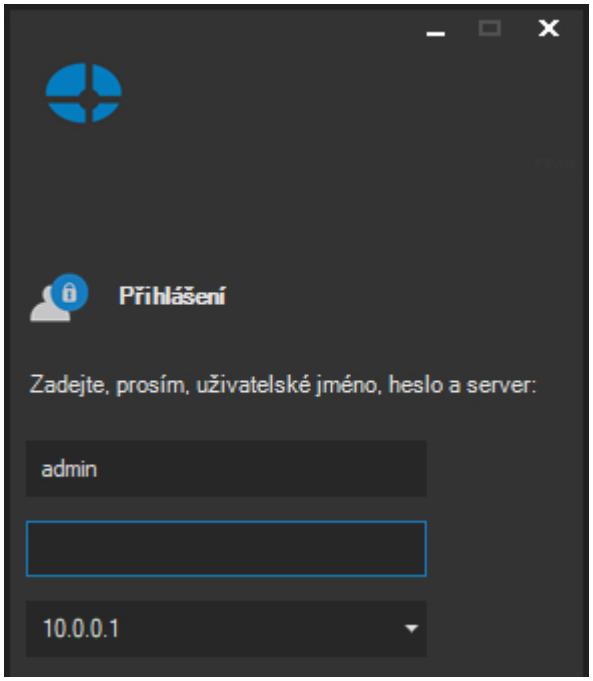
Při prvním spouštění aplikace na dané stanici jsou vyvolány dialogy pro základní nastavení aplikace ještě před jejím spuštěním, to se týká nastavení jazyka a počtu monitorů. V obou případech je zapotřebí vybrat některou z nabízených možností (jazyk může být předvybrán dle nastavení operačního systému)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



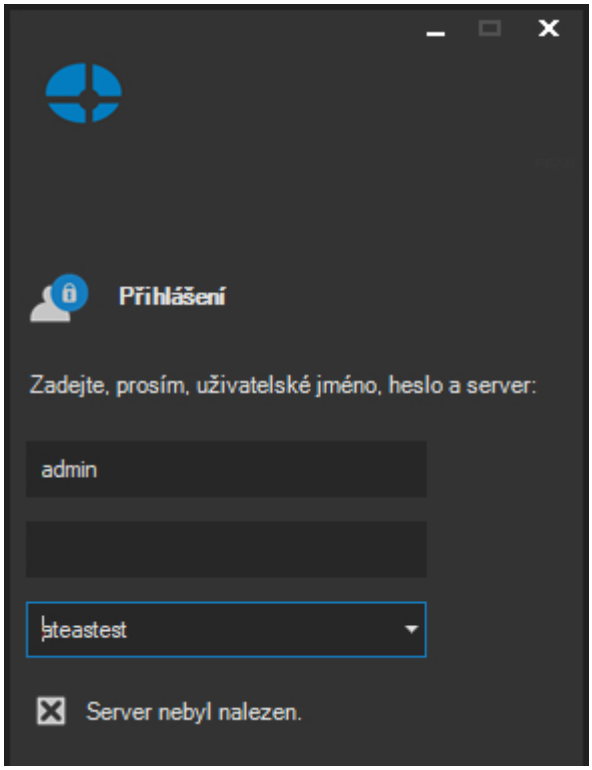


Po spuštění klientské aplikace ATEAS Security Observer bude systém vyžadovat zadání uživatelského jména, hesla a serveru pro přihlášení. V systému je předdefinován administrátorský účet **admin** s heslem **admin**. Systém neakceptuje shodu uživatelského jména a hesla a vynutí si při prvním přihlášení 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:

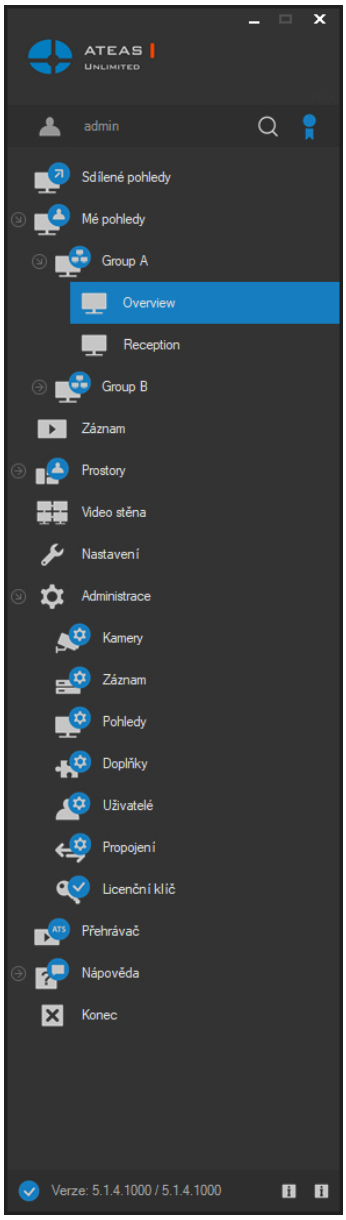
- chybně zadané uživatelské jméno anebo heslo, u hesel jsou vždy rozlišována velká a malá písmena (jsou case sensitive), administrátor systému má možnost provést reset Vašeho hesla,
- chybná adresa nebo název serveru,
- problémy s připojením do sítě,
- překročení limitu současných přístupů do systému dle aktuální licence,
- neplatná (stará) verze klientské aplikace,
- duplicitní přihlášení.

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),

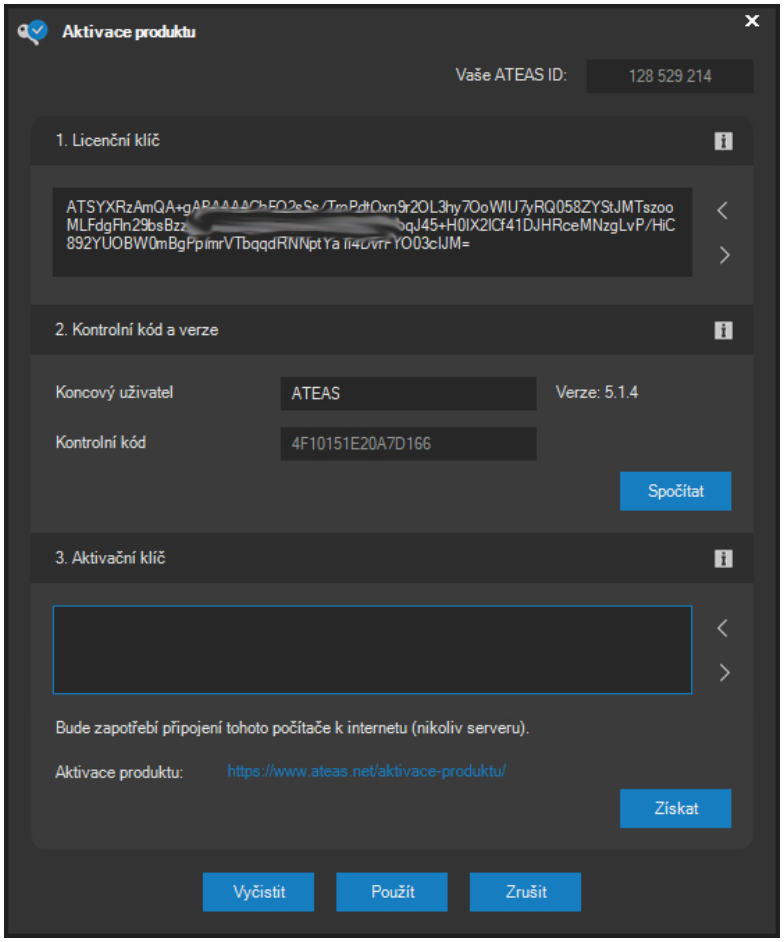
- u hesel se rozlišují velká a malá písmena,
- není možné zadat heslo shodné s uživatelským jménem (bez respektu na velká a malá písmena).

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 zelený 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. Licenční číslo je zadáváno centrálně pro celý systém a není nutné ho zadávat při instalaci žádné další klientské aplikace či kamerového serveru.



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 soboru lze provést pomocí tlačítka s bílou šipkou směřující vzhůru. Více informací naleznete v části dokumentace o aktivaci produktu v plné verzi tohoto dokumentu, který je též k dispozici na adrese Vašeho administračního serveru.

Pokud nemáte licenční číslo, je možné zadáním textu START software aktivovat pro čtyři kamery na neomezenou dobu zdarma a licenční číslo doplnit kdykoliv později bez nutnosti reinstalace.

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 **ZÍSKAT** 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).

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

POZOR

Pokud v systému není ještě zadáno žádné licenční číslo, povede tlačítko **ZRUŠIT** k ukončení klientské aplikace.

2.2. 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.

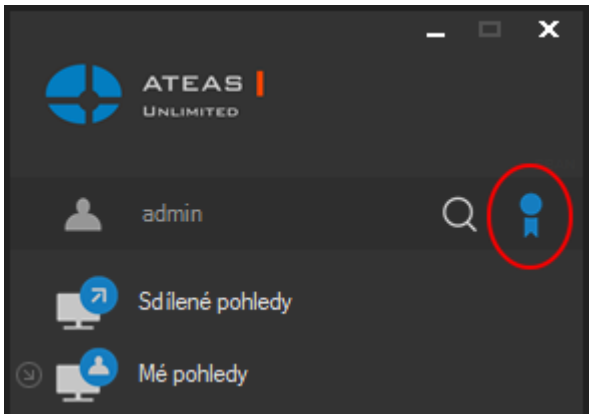
2.3. Certifikované instalace

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.

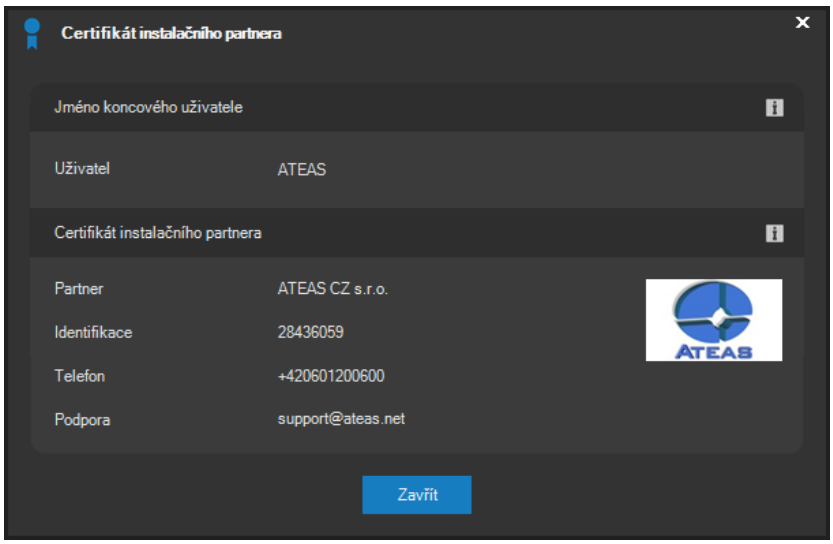
O tom, že Váš systém je certifikovanou instalací, informuje výrazná barva symbolu certifikátu v levém horním rohu okna s hlavní nabídkou aplikace.



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

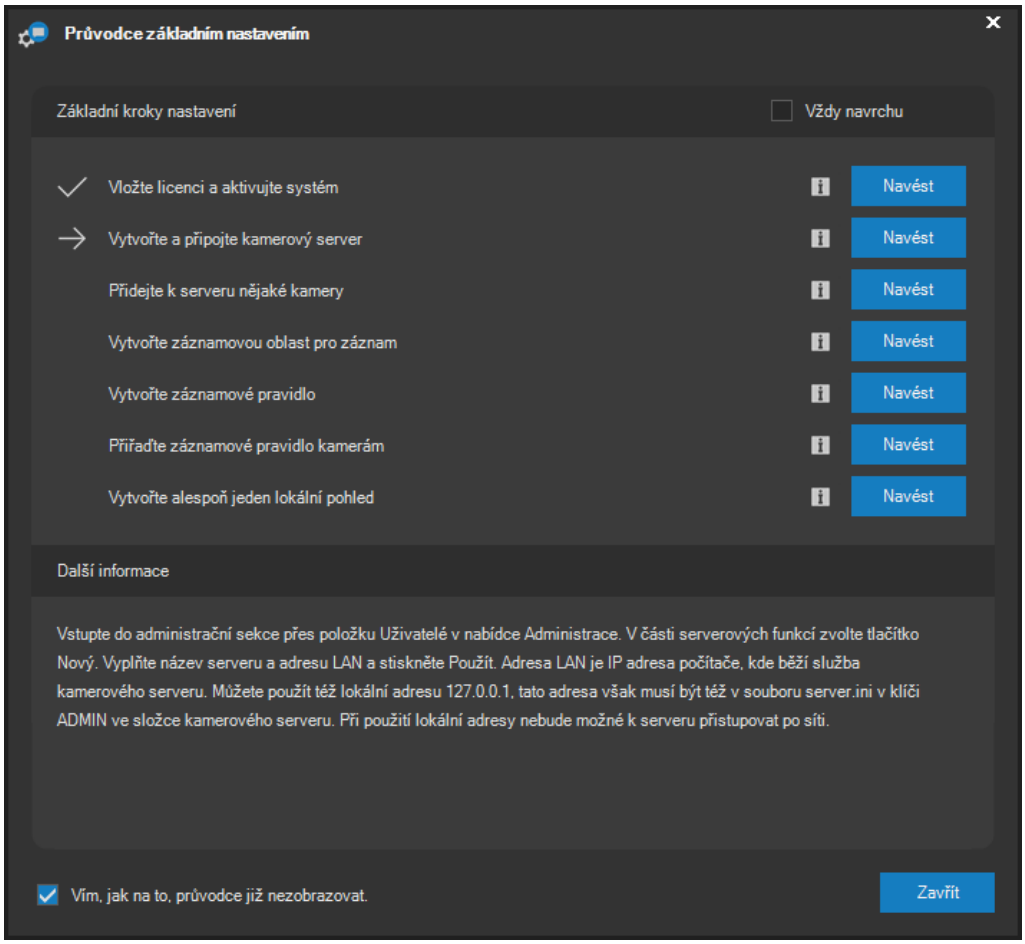
Pokud se Vám zobrazuje jiný název koncového uživatele systému, měl byl Váš instalační partner zjednat nápravu. Systém s chybným označením koncového uživatele je považován na nesprávně licencovaný.

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, pokud se jedná o licencovaný produkt a nikoliv edici START.

2.4. 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. Zobrazování průvodce přes ostatní okna lze však vypnout zrušením zaškrtnutí volby Vždy navrchu.

2.5. 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

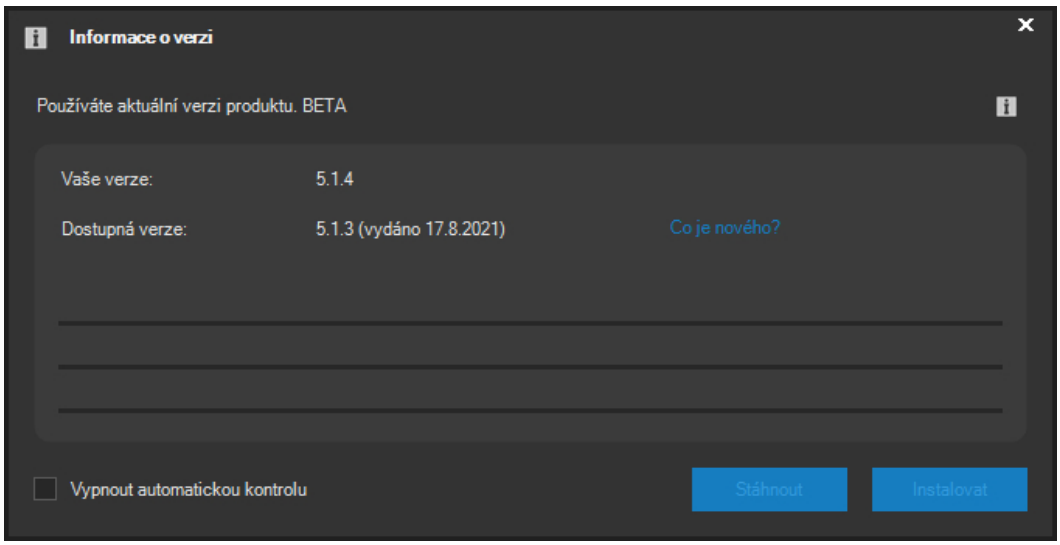
Zde máme na mysli přihlašování k více různým kamerovým systémům, kde každý má svůj vlastní licencovaný administrační server a nikoliv situaci, kdy existuje více serverů v rámci jednoho kamerového systému. Zde se samozřejmě uživatel přihlašuje centrálně pouze jednou a může v rámci edice UNLIMITED získat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

2.6. Informace o verzi

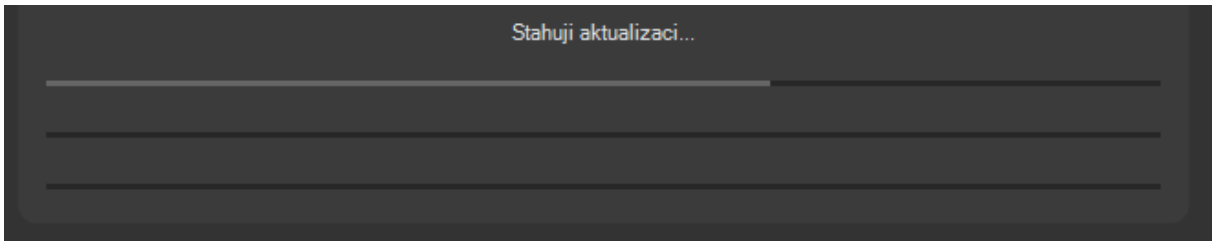
Ve spodní části okna s hlavní nabídkou se v pravém spodním rohu nachází informační symboly (vedle indikátoru spojení s administračním serverem a informace o aktuální verzi). Pokud je počítač, na kterém je spuštěna klientská aplikace, současně připojen k internetu, je možné kliknutím na symbol vpravo 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. V dialogu se také nachází odkaz na webové stránky ATEAS, ze kterých je možné po přihlášení pomocí údajů ATEAS Login provést stažení nejnovějšího obrazu instalačního média, a odkaz na stránku s popisem přidaných funkcí a možností v nových verzích ATEAS.

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 a kliknutím na tlačítko **ZAVŘÍT**.

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



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

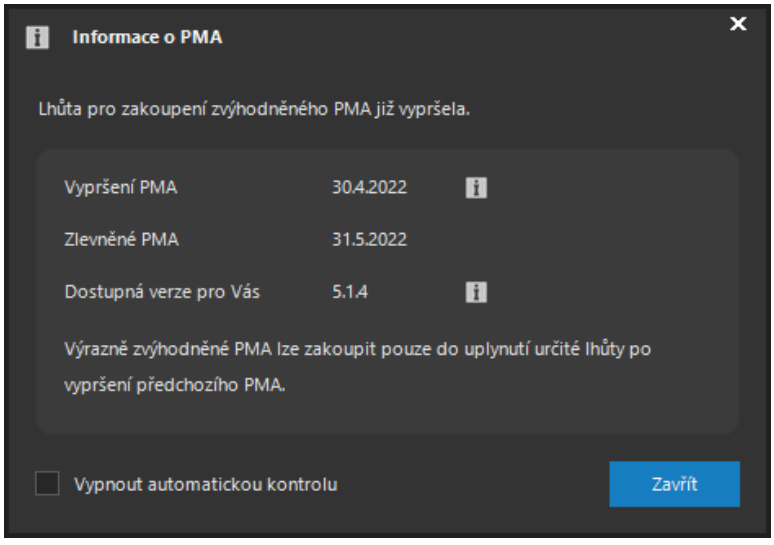
Novou verzi můžete po instalaci úspěšně aktivovat pouze tehdy, máte-li na ní nárok (volné aktualizace po nákupu licenčního čísla či samostatná smlouva o podpoře produktu PMA).

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. Od verze 4.0.2 výše je klientská aplikace zpětně kompatibilní a může přistupovat ke starším verzím systému, ne však starším než 4.0.1.

2.7. 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.



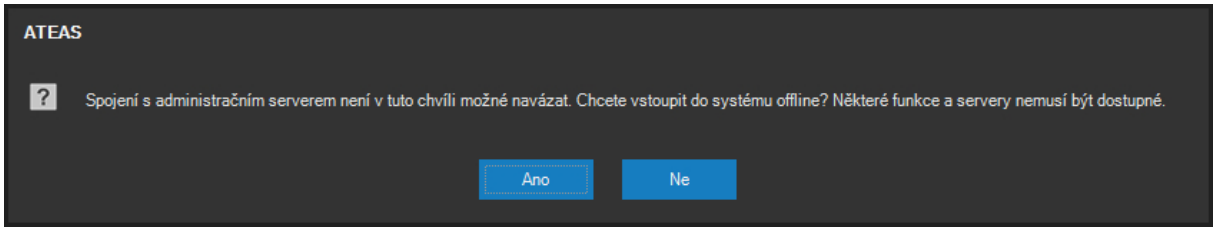
Služba ATEAS PMA garantuje možnost aktualizace Vašeho systému na nejnovější dostupnou verzi. Abyste mohli aktualizaci provést, je třeba mít aktivovánu službu ATEAS PMA. Pokud je služba PMA obnovována pravidelně, je možné ji získat za výrazně výhodnějších podmínek. Z tohoto důvodu, pokud je aplikace připojena 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.

2.8. Offline přihlášení

Pokud je administrační server systému nedostupný, je možné vstoupit do systému offline (tedy bez vytvoření spojení s administračním serverem systému). Aplikace tuto možnost nabídne poté, co není možné vytvořit spojení s administračním jádrem systému anebo pokud dojde k vyčerpání přednastaveného počtu pokusů o přihlášení v případě automatického přihlášení.



Pokud zvolíte tlačítko **ANO** a pokud jste zadali správné uživatelské jméno a heslo, budete moci vstoupit do systému offline. Při offline přihlášení je uživateli přidělena poslední dostupná sada oprávnění a omezení.

> **POZNÁMKA**
>
> Z tohoto důvodu nebude offline přihlášení možné, pokud na dané stanici nedošlo v minulosti ke korektnímu přihlášení online.

Po offline přihlášení do systému jsou k dispozici vždy alespoň funkce pro práci s lokální databází snímků a lokálně uloženými sekvencemi, které byly exportovány ze záznamových databází kamerových serverů. V edici UNLIMITED je navíc možné, že budete moci přistupovat online k některým kamerovým serverům v systému včetně živého přístupu ke kamerám a jejich záznamu. Tuto možnost však musí povolit administrátor systému. Více viz subkapitola Základní správa serverů.

POZOR

Z bezpečnostních důvodů se může do systému offline přihlásit vždy pouze poslední uživatel, který byl na daném počítači přihlášen online.

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.

Nastavení – lokální nastavení stanice.

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.

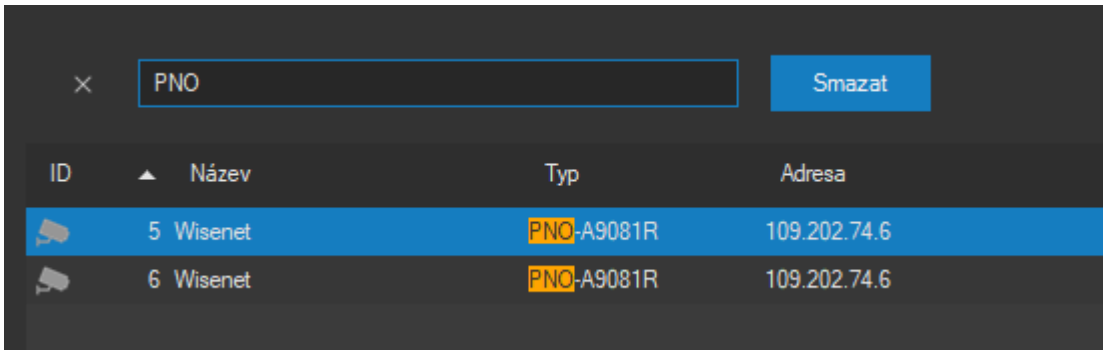
Klientskou aplikaci ATEAS Observer lze pomocí lokálního nastavení také spouštět automaticky po startu Windows a automaticky přihlásit konkrétního uživatele. Navíc lze pomocí automatického načtení pracovního prostoru zajistit otevření definovaných pohledů a jejich umístění na příslušné monitory. Více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

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 vyhledávácího panelu.



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 zadaných 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.

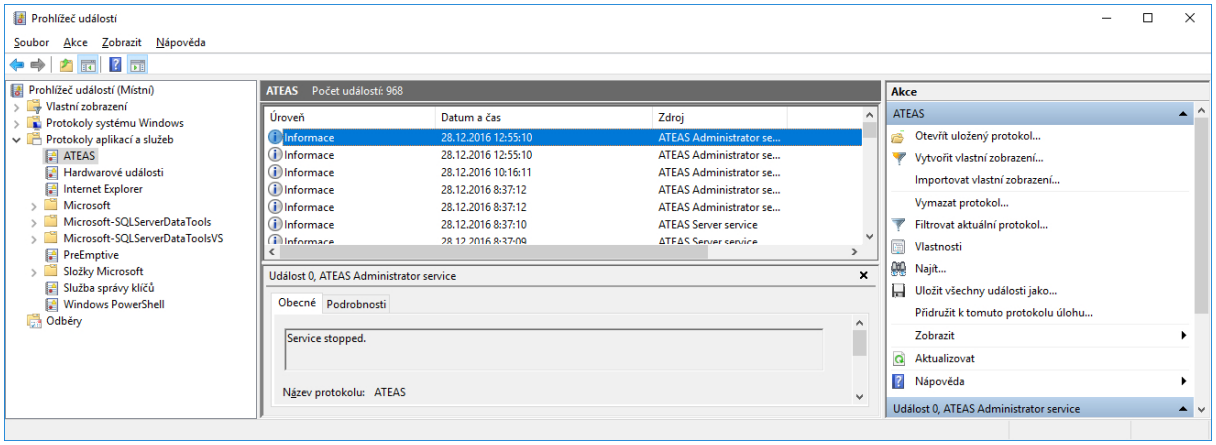
Řazení seznamů se provede jednoduše kliknutím na záhlaví příslušného sloupce. Opětovné kliknutí způsobí změnu řazení z vzestupného na sestupné a opačně. Chceme-li data setřídit podle více sloupců, použijeme při volbě dalšího sloupce v pořadí klávesu SHIFT.

2.12. 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 nárokující plynulé video ve vysokém rozlišení okamžitě přetížili procesory serveru. Bližší informace jsou uvedeny v kapitolách o GPU akceleraci.

2.13. Protokoly

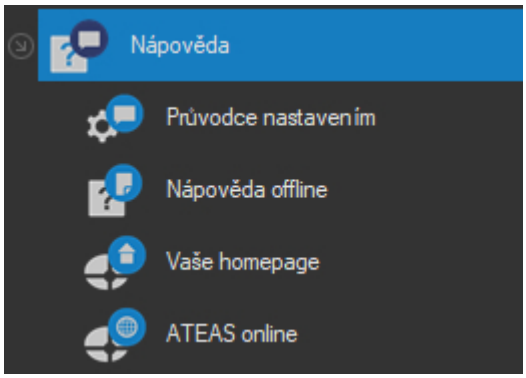
Po instalaci libovolné aplikace systému ATEAS Security je v systému vytvořen nový událostní protokol s názvem ATEAS, do kterého jsou zapisovány veškeré důležité okolnosti běhu aplikací. Tento protokol je dostupný v Ovládacích panelech, Nástrojích pro správu, Prohlížeč událostí. V případě havárie nebo 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.