



AVG E-mail Server Edice 2013

Uživatelský manuál

Verze dokumentace 2013.06 (12/3/2012)

Copyright AVG Technologies CZ, s.r.o. Všechna práva vyhrazena.
Všechny ostatní obchodní značky jsou majetkem jejich registrovaných vlastníků.

Tento produkt používá RSA Data Security, Inc. MD5 Message-Digest Algorithm, Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991.

Tento produkt obsahuje kód knihovny C-SaCzech, Copyright (c) 1996-2001 Jaromír Doleček (dolecek@ics.muni.cz).

Tento produkt používá kompresní knihovnu zlib Copyright (C) 1995-2002 Jean-loup Gailly and Mark Adler.



Obsah

1. Úvod	3
2. Podmínky instalace	4
2.1 Podporované operační systémy	4
2.2 Podporované e-mail servery	4
2.3 Hardwarové požadavky	4
2.4 Odinstalujte předchozí verze	4
2.5 Servisní balíčky pro MS Exchange	5
3. Instalační proces AVG	6
3.1 Spuštění instalace	6
3.2 Licenční ujednání	7
3.3 Aktivujte vaši licenci	7
3.4 Zvolte typ instalace	8
3.5 Uživatelská instalace - uživatelské volby	9
3.6 Dokončení instalace	10
4. Po instalaci	12
5. Komponenty Kontroly pošty pro MS Exchange	14
5.1 Přehled	14
5.2 Kontrola pošty pro MS Exchange (směrovací TA)	15
5.3 Kontrola pošty pro MS Exchange (SMTP TA)	17
5.4 Kontrola pošty pro MS Exchange (VSAPI)	17
5.5 Akce nad nálezy	20
5.6 Filtrování e-mailů	21
6. Komponenta Anti-Spam server pro MS Exchange	23
6.1 Princip komponenty Anti-Spam	23
6.2 Rozhraní komponenty Anti-Spam	23
6.3 Anti-Spam nastavení	24
7. AVG pro Kerio MailServer	29
7.1 Konfigurace	29
8. FAQ a technická podpora	33



1. Úvod

Tento uživatelský manuál je kompletní dokumentací programu **AVG E-mail Server 2013**.

AVG E-mail Server 2013 je jedním z produktů nové řady oceňovaného bezpečnostního software AVG, jež byl navržen pro klid vaší duše a stoprocentní bezpečnost vašeho serveru. Stejně jako všechny produkty nové řady AVG byl i **AVG E-mail Server 2013** kompletně od základů postaven tak, aby nadále dostal své pověsti uznávaného bezpečnostního programu a současně nabídl svým uživatelům zcela nové, efektivnější a uživatelsky přívětivé rozhraní.

Nový **AVG E-mail Server 2013** přináší moderní grafické rozhraní v kombinaci s agresivnějším a rychlejším testováním. Pro větší pohodlí přináší více procesů v plně automatickém režimu a nabízí nové 'inteligentní' uživatelské možnosti, které se přizpůsobí vašim potřebám.

Poznámka: Tato dokumentace obsahuje pouze popis specifických vlastností edice AVG E-mail Server 2013. Ostatní nastavení a vlastnosti aplikace AVG naleznete popsány v dokumentaci k Internet Security Edici, která je dostupná skrze <http://www.avg.cz>.



2. Podmínky instalace

2.1. Podporované operační systémy

AVG E-mail Server 2013 je určen k ochraně e-mail serverů s těmito operačními systémy:

- Windows 2008 Server (x64 a x86)
- Windows 2003 Server (x86, x64) SP1

2.2. Podporované e-mail servery

Podporovány jsou následující e-mail servery:

- MS Exchange Server 2003
- MS Exchange Server 2007
- MS Exchange Server 2010
- Kerio MailServer – verze 6.7.2 a vyšší

2.3. Hardwarové požadavky

Minimální hardwarové požadavky pro **AVG E-mail Server 2013** jsou tyto:

- Intel Pentium CPU 1,5 GHz
- 500 MB volného místa na pevném disku (z instalací dříve)
- 512 MB RAM paměti

Doporučené hardwarové požadavky pro **AVG E-mail Server 2013** jsou tyto:

- Intel Pentium CPU 1,8 GHz
- 600 MB volného místa na pevném disku (z instalací dříve)
- 512 MB RAM paměti

2.4. Odinstalujte předchozí verze

Máte-li nainstalovanou starší verzi **AVG E-mail Serveru**, je nutné ji před zahájením instalace **AVG E-mail Server 2013** odinstalovat. Odinstalaci je třeba provést ručně pomocí standardních funkcí Windows:

- V nabídce **Start/Nastavení/Ovládací panel/Přidat nebo odebrat programy** zvolte příslušný program (totéž lze také snadno provést z nabídky **Start/Programy/AVG/Odinstalovat AVG**).
- Pokud jste dříve používali verzi AVG 8.x či starší, nezapomeňte odinstalovat také jednotlivé serverové



doplňky.

Poznámka: Při procesu odinstalace bude restartován proces store.

Doplňky pro Exchange - spusíte setupes.exe s parametrem /uninstall ze složky, kde je doplněk nainstalován:

např. C:\AVG4ES2K\setupes.exe /uninstall

Doplňky pro Lotus Domino/Notes - spusíte setupln.exe s parametrem /uninstall ze složky, kde je doplněk nainstalován:

např. C:\AVG4LN\setupln.exe /uninstall

2.5. Servisní balíčky pro MS Exchange

Pro instalaci **MS Exchange 2003 Serveru** není nutná instalace žádných dodatečných balíčků, ale v každém případě doporučujeme, abyste se snažili udržovat svůj systém v co možná nejaktuálnějším stavu a pravidelně instalovali nové servisní balíčky a záplaty, aby bylo dosaženo nejvyšší možné úrovně bezpečnosti.

Servisní balíček pro MS Exchange 2003 Server (instalace je volitelná) najdete na adrese:

<http://www.microsoft.com/en-us/download/details.aspx?id=9664>

Při zahájení instalace budou prověřeny všechny verze systémových knihoven. Bude-li nutné doinstalovat novější knihovny, instalátor označí zastaralé knihovny koncovkou *.delete*. Takto označené knihovny pak budou odstraněny při restartu systému.

Servisní balíček pro MS Exchange 2007 Server (instalace je volitelná):

<http://www.microsoft.com/downloads/details.aspx?FamilyID=44c66ad6-f185-4a1d-a9ab-473c1188954c&displaylang=en>

Servisní balíček pro MS Exchange 2010 Server (instalace je volitelná):

<http://www.microsoft.com/en-us/download/details.aspx?id=28190>



3. Instalační proces AVG

Pro instalaci AVG na váš počítač potřebujete aktuální instalační soubor. Instalační soubor najdete na CD, které bylo součástí zakoupeného balení AVG, ale tento soubor může již být zastaralý.

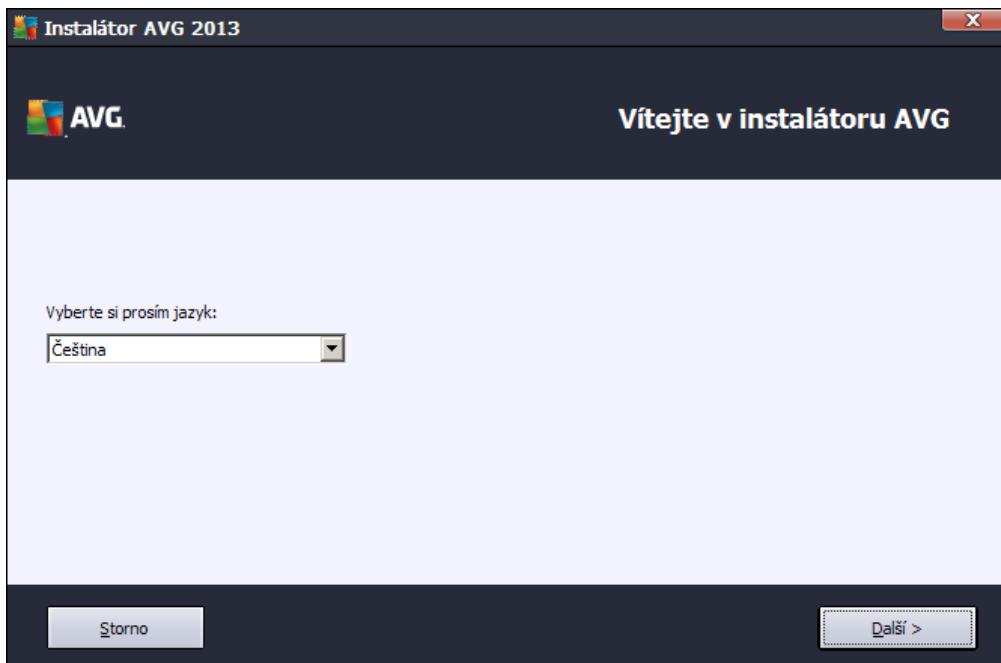
Doporučujeme vám proto navštívit [web AVG: http://www.avg.cz/stahnout?prd=msw](http://www.avg.cz/stahnout?prd=msw) a nejnovější instalační soubor si odtud stáhnout.

K dispozici jsou dva instalační balíčky - jeden pro 32bitové operační systémy (s označením x86) a jeden pro 64bitové operační systémy (s označením x64). Při instalaci je tedy třeba použít instalační balíček odpovídající vašemu operačnímu systému.

Během instalace budete požádáni o své licenční číslo. Ujistěte se proto prosím, že jej máte k dispozici. Pokud jste AVG zakoupili on-line, vaše licenční číslo vám bylo doručeno e-mailem.

Instalace probíhá ve sledu dialogových oken, z nichž každé vysvětluje, co je třeba v konkrétním kroku provést. Popis jednotlivých oken nyní nabízíme:

3.1. Spuštění instalace

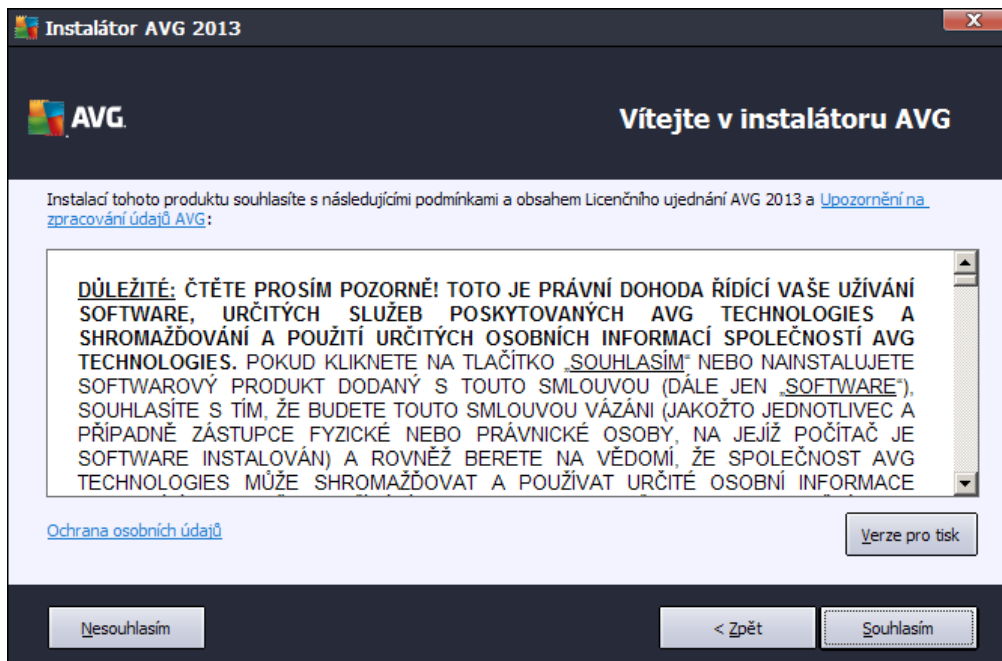


Instalační proces je zahájen otevřením úvodního dialogu. V něm máte možnost zvolit jazyk, v němž bude instalační proces probíhat. Do následující části procesu přejdete stiskem tlačítka **Další**.

Později v průběhu instalace si budete také moci zvolit další jazyky pro rozhraní aplikace.



3.2. Licenční ujednání

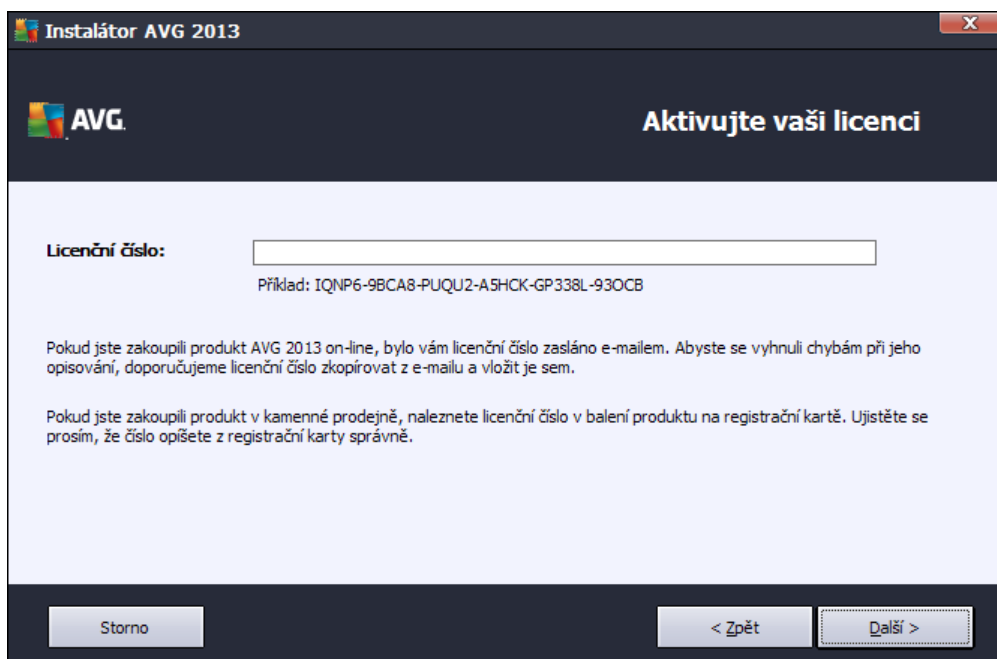


V tomto dialogu se nachází Licenční ujednání - tedy plné znění závazné licenční smlouvy AVG. Text si přečtete a svůj souhlas s licenčním ujednáním potvrdíte stiskem tlačítka **Souhlasím**.

Tlačítkem **Verze pro tisk** můžete v novém okně zobrazit verzi určenou pro tisk.

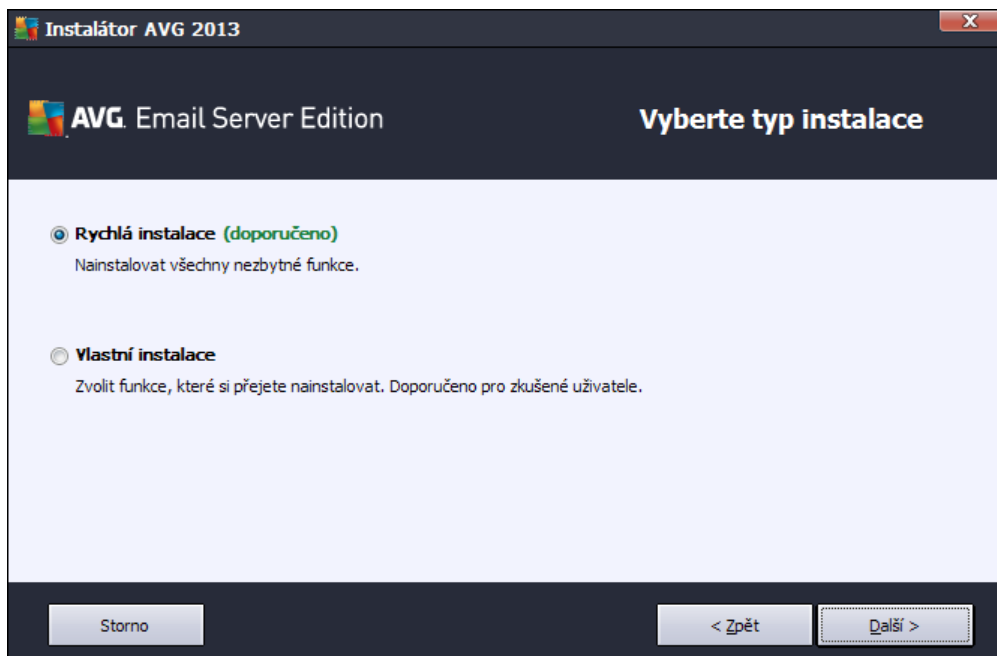
3.3. Aktivujte vaši licenci

V dialogu **Aktivujte vaši licenci** je třeba vyplnit vaše licenční číslo. Toto číslo najdete buďto na registrační kartě v krabicovém balení AVG, anebo v potvrzovacím e-mailu, který jste obdrželi při zakoupení AVG on-line. Licenční číslo musí být zadáno naprosto přesně ve tvaru, jak je uvedeno, proto prosím věnujte velkou pozornost jeho pípsu. Pokud máte číslo k dispozici v digitální formě, doporučujeme jej do příslušného pole zkopírovat (metodou kopírovat a vložit).



V instalaci pokračujte stiskem tlačítka **Další**.

3.4. Zvolte typ instalace



Dialog **Vyberte typ instalace** vám dává na výběr mezi **Expresní** a **Uživatelskou** instalací.

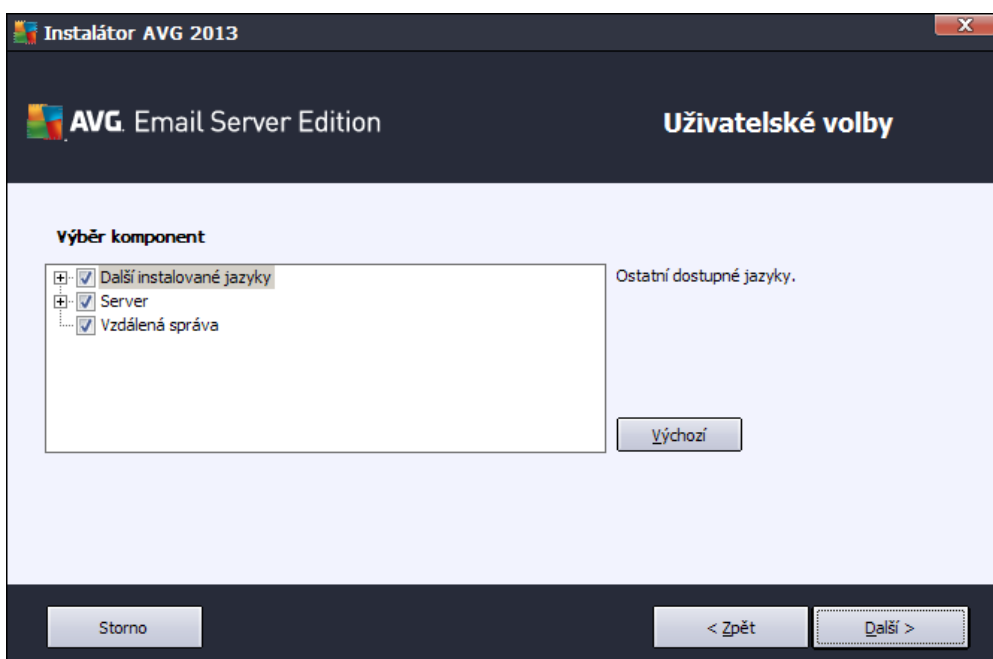
V těchto případech doporučujeme použít **expresní instalaci**, kdy bude AVG nainstalován zcela automaticky s nastavením definovaným výrobcem. Tohoto nastavení zaručuje maximální úroveň bezpečnosti a optimální využití zdrojů. Pokud se v budoucnu vyskytne potřeba některých konkrétních nastavení změnit, budete mít vždy možnost editovat konfiguraci AVG přímo v aplikaci.



Uživatelská instalace je vhodná pouze pro pokročilé a znalé uživatele. Doporučit ji lze v případě, že máte skutečný důvod instalovat AVG s nestandardním nastavením tak, aby vyhovovalo specifickým požadavkům vašeho systému.

Po zvolení Uživatelské instalace se ve spodní části dialogu zobrazí sekce **Cílové umístění**. Ta vám umožní zvolit, kam má být program AVG nainstalován. Ve výchozím nastavení bude program instalován do adresáře programových souborů umístěném typicky na disku C:. Pokud si přejete toto umístění změnit, pomocí tlačítka **Procházet** zobrazíte strukturu vašeho disku a zvolíte adresář, kam má být AVG instalován.

3.5. Uživatelská instalace - uživatelské volby



V sekci **Výběr komponenty** je zobrazen přehled komponent AVG, které můžete nainstalovat. Pokud vám výchozí nastavení nevyhovuje, máte možnost jednotlivé komponenty odebrat/přidat.

Volit můžete pouze z těch komponent, které jsou zahrnuty ve vámi zakoupené licenci AVG. Pouze tyto komponenty vám také budou v dialogu nabídnuty!

- **Vzdálená správa** - pokud budete chtít tuto instalaci spravovat vzdáleně, zaškrtněte tuto volbu.
- **Další instalované jazyky** - zvolte si jazyky uživatelského rozhraní, které chcete nainstalovat.

Základní přehled jednotlivých serverových komponent (doplěk):

- **Anti-Spam server pro MS Exchange**

Kontroluje všechny výchozí e-mailové zprávy a označuje nevyžádanou poštu jako SPAM. K analýze každé zprávy využívá několik metod, což zajišťuje maximální možnou ochranu proti nežádoucím zprávám.

- **Kontrola pošty pro MS Exchange (směrovací TA)**



Kontroluje všechny přicházející, odcházející a interní e-mailové zprávy procházející skrze HUB roli MS Exchange.

- **Kontrola pošty pro MS Exchange (SMTP TA)**

Kontroluje e-mailové zprávy procházející skrze SMTP rozhraní MS Exchange (lze nainstalovat na EDGE i HUB roli).

- **Kontrola pošty pro MS Exchange (VSAPI)**

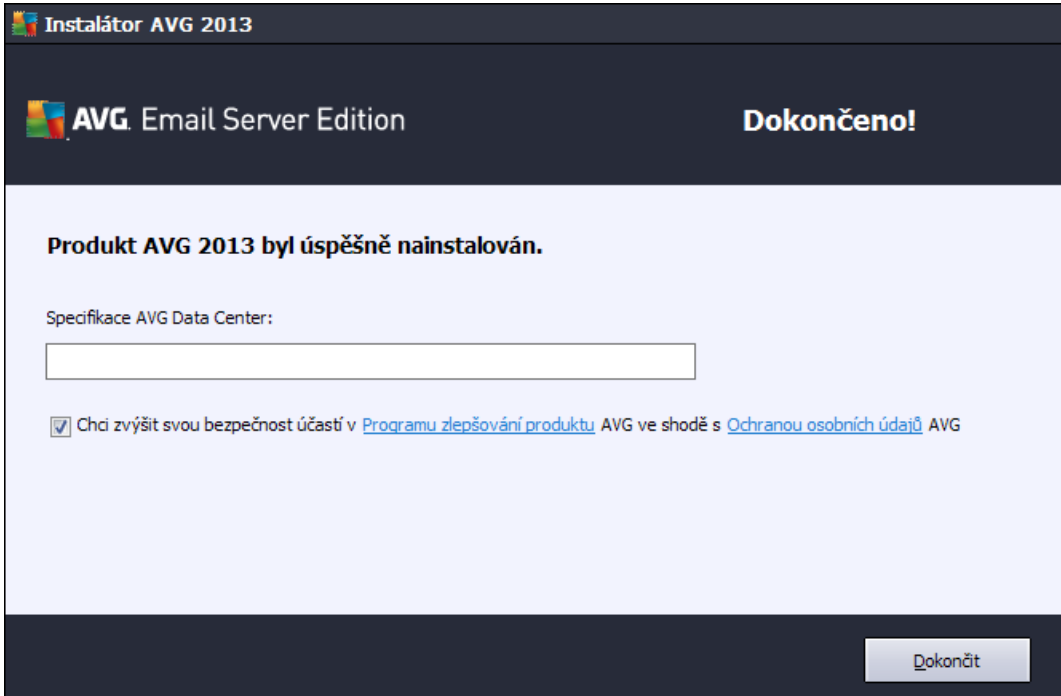
Kontroluje e-mailové zprávy uložené v uživatelských schránkách. Při nalezení viru dojde k přesunu do virového trezoru nebo kompletnímu odstranění.

Pro MS Exchange 2003 jsou k dispozici pouze komponenty Anti-Spam a Kontrola pošty (VSAPI).

Pokračujte stiskem tlačítka **Další**.

3.6. Dokončení instalace

Pokud jste v průběhu volby komponent vybrali **Vzdálenou správu**, můžete v tomto dialogu zadat připojovací adresy pro spojení s vaším AVG DataCenter.



Ve výchozím nastavení je zaškrtnuta také volba **Chci zvýšit svou bezpečnost účasti v AVG Product Improvement Program ve shodě s AVG Privacy Policy**. Označením této volby dáváte najevo svůj souhlas s účasti v Programu zlepšování produktu (a umožníte tak reportování informací o detekovaných hrozbách týmu expertů společnosti AVG). V rámci tohoto programu probíhá sběr anonymních informací o detekovaných hrozbách s cílem zvýšit celkovou úroveň bezpečnosti na Internetu.

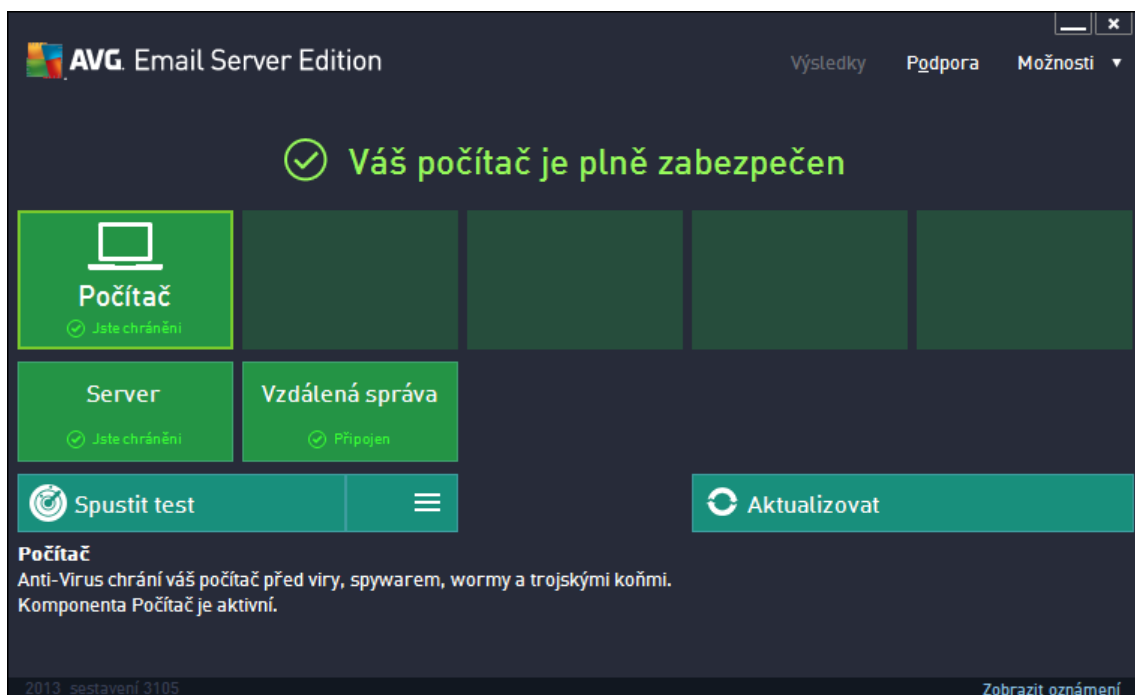


Své volby potvrďte stiskem tlačítka ***Dokončit***.

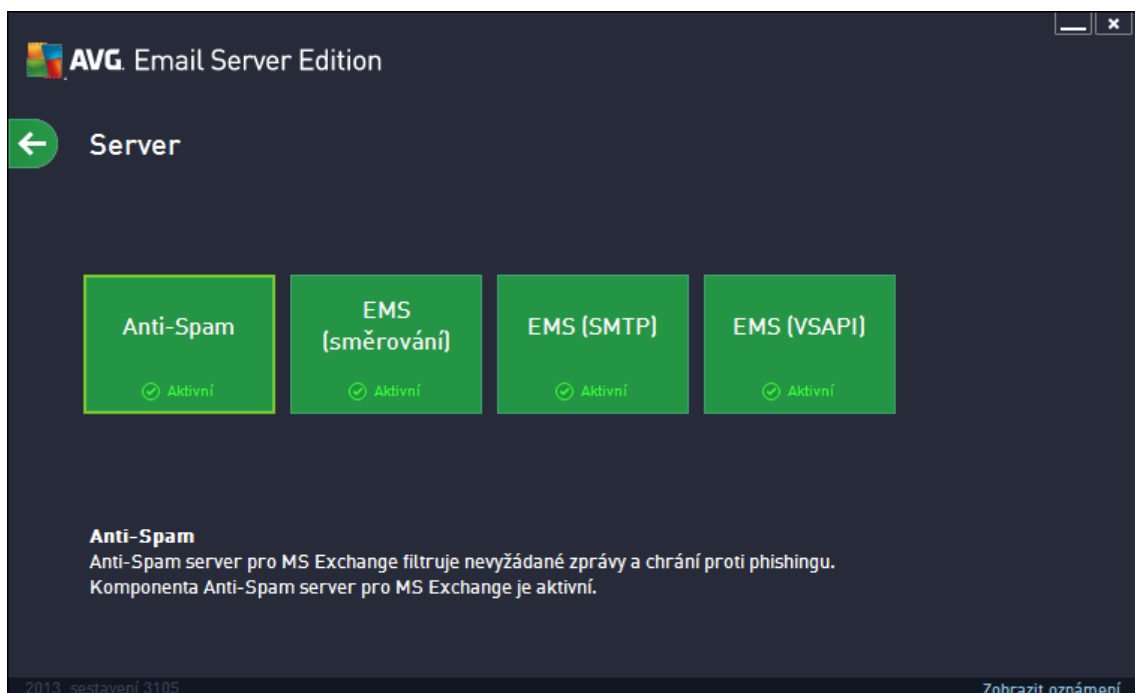
Program AVG je nyní nainstalován na vašem počítači/serveru a plně funkční. Program běží ve výchozím nastavení na pozadí a nevyžaduje vaši pozornost.

4. Po instalaci

Okamžitě po skončení instalace se objeví hlavní obrazovka **AVG E-mail Server 2013**:



Tento manuál se vztahuje pouze na bezpečnostní prvky, které jsou unikátní v rámci **AVG E-mail Server 2013**; všechny ostatní komponenty a možnosti nastavení jsou podrobně popsány v manuálu pro AVG Desktop. Pro zobrazení hlavního dialogu serverových komponent (jakéhosi rozcestníku) klikněte na tlačítko **Server**. Objeví se před vámi následující obrazovka:





Upozor ujeme, že všechny serverové komponenty (samoz ejm jen pokud jste p edtím n kterou z nich sami [neodebrali z instalace](#)) budou dostupné pouze v tom p ípad , že používáte MS Exchange verze 2007 i nov jší. MS Exchange 2003 podporuje výhradn komponenty Anti-Spam a Kontrola pošty (VSAPI).

Pro nastavení ochrany pro váš e-mail server zvolte odpovídající kapitolu:

- [*Komponenty Kontroly pošty pro MS Exchange*](#)
- [*Anti-Spam Server pro MS Exchange*](#)
- [*AVG pro Kerio MailServer*](#)

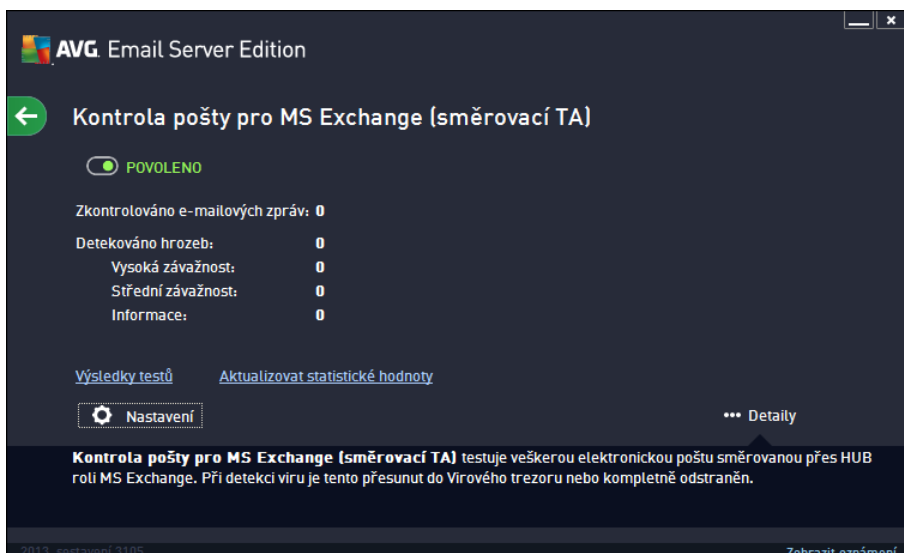
5. Komponenty Kontroly pošty pro MS Exchange

5.1. Přehled

Základní pohled jednotlivých komponent Kontroly pošty:

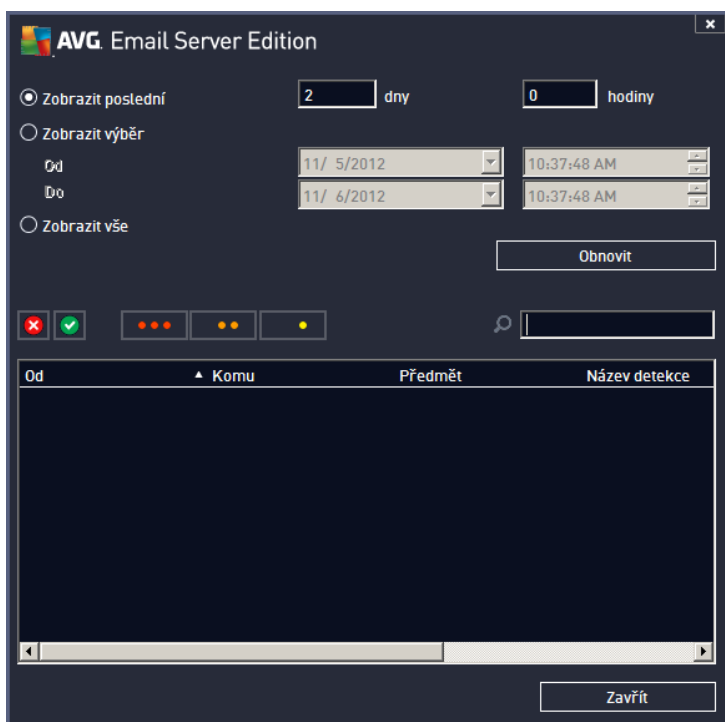
- [EMS \(směrování\) - Kontrola pošty pro MS Exchange \(směrovací transportní Agent\)](#)
Kontroluje všechny přicházející, odcházející a interní e-mailové zprávy procházející skrze HUB roli MS Exchange.
Dostupné pouze pro MS Exchange 2007/2010 a lze nainstalovat pouze na HUB roli.
- [EMS \(SMTP\) - Kontrola pošty pro MS Exchange \(SMTP transportní agent\)](#)
Kontroluje e-mailové zprávy procházející skrze SMTP rozhraní MS Exchange.
Dostupné pouze pro MS Exchange 2007/2010 a lze nainstalovat na EDGE i HUB roli.
- [EMS \(VSAPI\) - Kontrola pošty pro MS Exchange \(VSAPI\)](#)
Kontroluje e-mailové zprávy uložené v uživatelských schránkách. Při nalezení viru dojde k přesunu do virového trezoru nebo kompletnímu odstranění.

Kliknutím myši na ikonu požadované komponenty zobrazíte její rozhraní. Všechny komponenty Kontroly pošty sdílejí společné ovládací prvky:



- **POVOLENO/ZAKÁZÁNO** - kliknutí na toto tlačítko vypíná a zapíná danou komponentu (je-li komponenta zapnutá, jsou tlačítko i text zelené, je-li vypnutá, zobrazují se červeně).
- **Výsledky test**

Otevře nový dialog s pohledem výsledků testů:



Zde můžete zkontrolovat zprávy rozdelené do několika záložek podle jejich závažnosti. Více informací o konkrétní závažnosti a jejím nastavení naleznete v popisu nastavení jednotlivých serverových komponent.

Ve výchozím nastavení jsou zobrazeny pouze výsledky za poslední dva dny. Interval pro zobrazení můžete změnit tímto volbami:

- **Zobrazit poslední** - vložte preferovaný počet dní a hodin.
- **Zobrazit výběr** - zvolte libovolný časový a datumový rozsah.
- **Zobrazit vše** - zobrazí výsledky za celé období.

Tlačítkem **Obnovit** znovu načítáte výsledky testů.

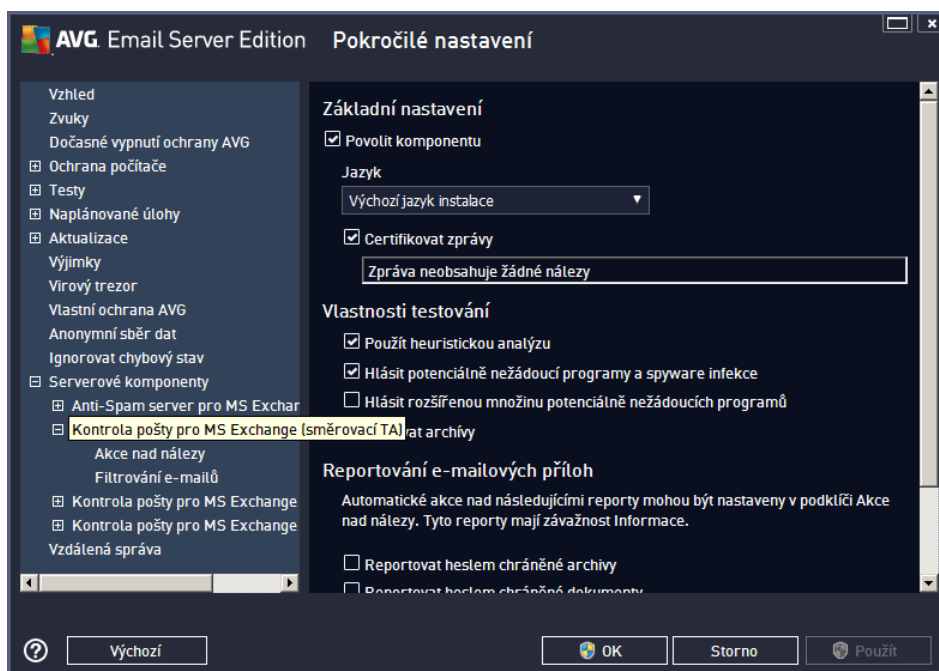
- **Aktualizovat statistické hodnoty** - aktualizuje statistiky uvedené v dialogu.

Stiskem funkčního tlačítka **Nastavení** otevřete nastavení dané komponenty (bližší nastavení jednotlivých komponent naleznete v kapitolách níže).

5.2. Kontrola pošty pro MS Exchange (směrovací TA)

Pro otevření možností nastavení komponenty **Kontrola pošty pro MS Exchange (směrovací transportní agent)**, klikněte v jejím rozhraní na tlačítko **Nastavení**.

V seznamu **Serverových komponent** pak zvolte položku **Kontrola pošty pro MS Exchange (směrovací TA)**.



V sekci **Základní nastavení** naleznete následující možnosti:

- **Povolit komponentu** - odškrtn te pro vypnutí celé komponenty.
- **Jazyk** - zvolte preferovaný jazyk komponenty.
- **Certifikovat zprávy** - zaškrtn te, pokud si p ežete p idat certifika ní poznámku ke všem testovaným zprávám. Zprávu m žete upravit v následujícím polí ku.

Sekce **Vlastnosti testování** obsahuje tato nastavení:

- **Použít heuristickou analýzu** - zaškrtn te pro povolení použití heuristické analýzy v pr b hu testování.
- **Hlásit potenciáln nežádoucí programy a spyware infekce** - zaškrtn te pro hlášení potenciáln nežádoucích program a spyware.
- **Hlásit rozší enou množinu potenciáln nežádoucích program** - zaškrtnutím tohoto polí ka aktivujete detekci rozší ené sady spyware: program , které jsou v p vodní podob od výrobce neškodné a v po ádku, ale mohou být snadno zneužity ke škodlivým ú el m, p ípadn jde o zásadn neškodné, avšak pon kud obt žující programy (r zné dopl ky do prohlíže e atd.). Jde o dodate né opat ení, které zlepšuje zabezpe ení vašeho po íta e na další úrovni, nicmén m že blokovat také n které legální programy, proto je ve výchozím nastavení tato možnost vypnuta. Tato detekce je dopl kem p edchozí možnosti, samostatn tedy není dosta ující: pokud chcete ochranu p ed základními typy spyware, pak ponechte vždy ozna ené p edchozí polí ko, a toto pak ozna te voliteln k n mu.
- **Testovat archívy** - zaškrtn te pro zahrnutí také testování archivních soubor (zip, rar, atp.)

Sekce **Reportování e-mailových p íloh** umož ũje vybrat položky, které si p ežete hlásit v pr b hu testování. Pokud je položka zaškrtnutá, bude každá zpráva s takovou p ílohou obsahovat v p edm tu text [INFORMACE] (ve výchozím nastavení). Toto výchozí nastavení lze zm nit ve v tv **Akce nad nálezy**, ást **Informace** (viz níže).



K dispozici jsou následující možnosti:

- **Reportovat heslem chráněné archivy**
- **Reportovat heslem chráněné dokumenty**
- **Reportovat dokumenty obsahující makro**
- **Reportovat skryté pípony**

Součástí nastavení jsou tyto podpoložky ve stromové struktuře:

- [Akce nad nálezy](#)
- [Filtrování e-mail](#)

5.3. Kontrola pošty pro MS Exchange (SMTP TA)

Konfigurace kontroly pošty pro MS Exchange (SMTP Transportní Agent) je stejná jako pro smrovač transportní agent. Více informací naleznete v kapitole [Kontrola pošty pro MS Exchange \(smrovač TA\)](#) výše.

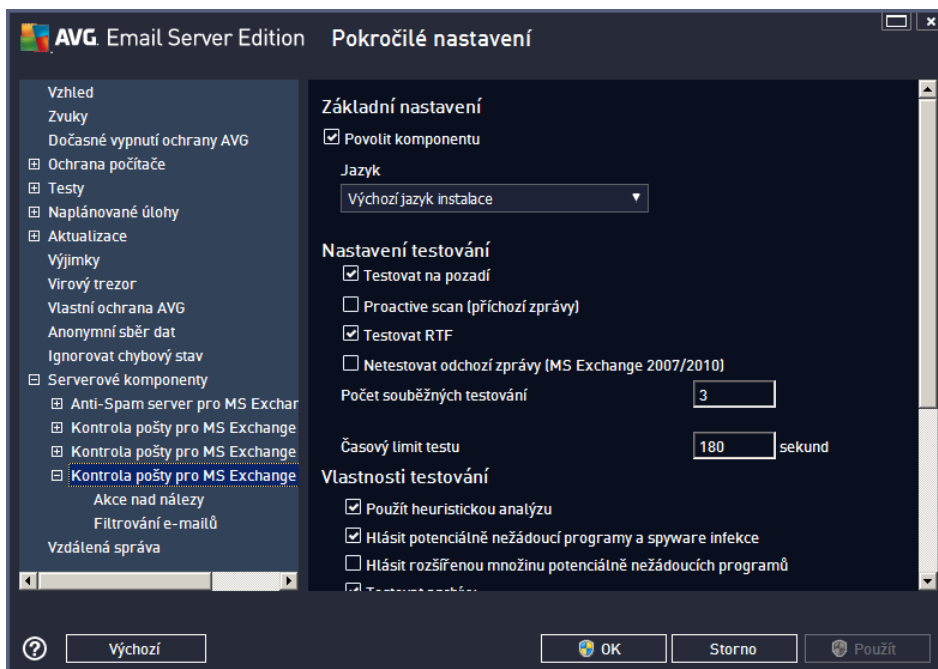
Součástí nastavení jsou také tyto podpoložky ve stromové struktuře:

- [Akce nad nálezy](#)
- [Filtrování e-mail](#)

5.4. Kontrola pošty pro MS Exchange (VSAPI)

Pro otevření možností nastavení komponenty **Kontrola pošty pro MS Exchange (VSAPI)**, klikněte v jejím rozhraní na tlačítko **Nastavení**.

V seznamu **Serverových komponent** pak zvolte položku **Kontrola pošty pro MS Exchange (VSAPI)**.



V sekci **Základní nastavení** naleznete následující možnosti:

- **Povolit komponentu** - odškrtnete pro vypnutí celé komponenty.
- **Jazyk** - zvolte preferovaný jazyk komponenty.

Sekce **Nastavení testování** obsahuje tato nastavení:

- **Testovat na pozadí** - zde můžete povolit nebo zakázat proces kontroly existujícího obsahu databáze na pozadí. Kontrola uložené pošty na pozadí je jedním z prvků rozhraní VSAPI 2.0/2.5. Antivirová kontrola probíhá pro každou databázi na serveru zvlášť; vždy jsou testovány zprávy i přílohy.

Pro každou databázi je zároveň použito jedno vlákno (*thread*) s nízkou prioritou, což znamená, že ostatní úlohy, jako například ukládání e-mail zpráv do Microsoft Exchange databáze, dostanou vždy přednost. Kontrola pošty na pozadí je aplikována pro tabulku se složkami v rámci Exchange úložiště. Složka, která již byla na pozadí jednou zkontrolována, bude znovu zkontrolována až po příjmu nových zpráv. Zprávy jednotlivých zpráv ve složkách jsou zpracovávány proaktivní kontrolou (*proactive scan*).

- **Proactive scan (příchozí zprávy)** - zde můžete povolit nebo zakázat funkci proaktivní kontroly z VSAPI 2.0/2.5. Tato funkce spojuje v dynamické správě priorit položek v testovací frontě. Jakmile jsou zprávy umístěny do úložiště na serveru Exchange, jsou zařazeny také do obecné fronty k testování s nízkou prioritou (maximum 30 položek). Následně jsou testovány podle metody FIFO (First in, first out). Pokud je k němu přidána nová položka, její priorita se změní na vysokou.

Nadbytečné zprávy jsou přesunuty do úložiště bez otestování.

I v případě vypnutí obou voleb (**Testování na pozadí** a **Proactive Scan**), zůstává i nadále aktivní rezidentní



test, který se spustí v momentě stahování zprávy klientem MS Outlook.

- **Testovat RTF** - zvolte, zdali si přejete testovat také RTF soubory.
- **Netestovat odchozí zprávy (MS Exchange 2007/2010)** - používáte-li zároveň serverové komponenty VSAPI a [smrovací TA](#) (tj. Routing Transport Agent), přičemž nezáleží na tom, zda jsou nainstalovány na jednom serveru, anebo na dvou různých, můžete se stát, že bude odchozí pošta provázána dvakrát: nejprve kontrolou v reálném čase (VSAPI On-access scanner), podruhé prostřednictvím smrovacího TA. To může způsobit určitá zpomalení na vašem serveru a mírné prodlevy při odesílání e-mailů. Pokud si jste jistí, že jsou obě serverové komponenty správně nainstalovány a aktivní, můžete se tomuto dvojímu testování odchozí pošty vyhnout zablokováním kontroly v reálném čase (VSAPI). Stačí pouze zaškrtnout toto políčko.
- **Počet a souběžných testování** - ve výchozím nastavení běží testovací proces paralelně ve více vláknech, zejména pro zvýšení obecného výkonu. Počet a souběžných vláken lze změnit v tomto nastavení.
Výchozí počet vláken je vypočítán jako dvojnásobek „počet procesorů“ + 1.
Minimální počet vláken je vypočítán jako („počet procesorů“ + 1) vyděleno dvěma.
Maximální počet vláken je vypočítán jako „počet procesorů“ krát 5 + 1.
Pokud je nastavena hodnota nižší nebo minimální, případně maximální či vyšší, je použita hodnota výchozí.
- **časový limit testu** - maximální souvislý interval (v sekundách), po který můžete jedno vlákno pokračovat k právě testovanému objektu (výchozí hodnota je 180 sekund).

Sekce **Vlastnosti testování** obsahuje tato nastavení:

- **Použít heuristickou analýzu** - zaškrtnete pro povolení použití heuristické analýzy v průběhu testování.
- **Hlásit potenciálně nežádoucí programy a spyware infekce** - zaškrtnete pro hlášení potenciálně nežádoucích programů a spyware.
- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** - zaškrtnutím tohoto políčka aktivujete detekci rozšířené sady spyware: programů, které jsou v podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům, případně jde o zásadně neškodné, avšak poněkud obtěžující programy (různé doplňky do prohlížeče atd.). Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta. Tato detekce je doplněna předchozí možností, samostatně tedy není dostatečná: pokud chcete ochranu před základními typy spyware, pak ponechte vždy označené předchozí políčko, a toto pak označíte volitelně k ním.
- **Testovat archívy** - zaškrtnete pro zahrnutí také testování archivních souborů (zip, rar, atp.)

Sekce **Reportování e-mailových příloh** umožní vybrat položky, které si přejete hlásit v průběhu testování. Toto výchozí nastavení lze změnit ve tvé **Akce nad nálezy**, část **Informace** (viz níže).

K dispozici jsou následující možnosti:

- **Reportovat heslem chráněné archívy**

- **Reportovat heslem chráněné dokumenty**
- **Reportovat dokumenty obsahující makro**
- **Reportovat skryté pípony**

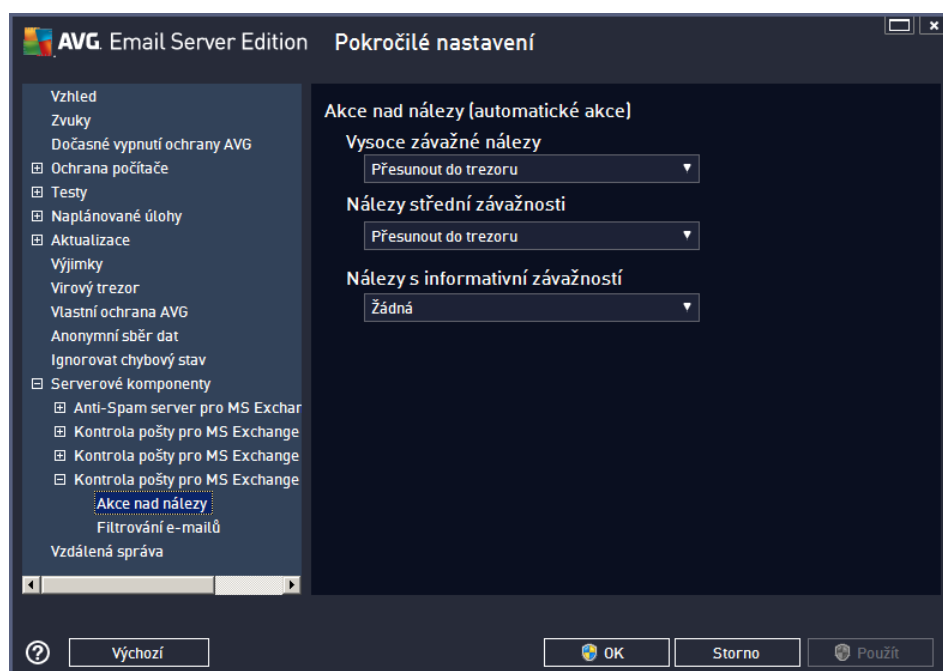
Některé prvky v tomto nastavení tvoří uživatelské rozšíření aplikace svého rozhraní Microsoft VSAPI 2.0/2.5. Pokud se chcete blíže informovat o tomto rozhraní, následujte tyto odkazy:

- <http://support.microsoft.com/default.aspx?scid=kb:en-us:328841&Product=exch2k> – popis princip spolupráce Exchange s antivirovými programy
- <http://support.microsoft.com/default.aspx?scid=kb:en-us:823166> – informace o doplňcích ve VSAPI 2.5 v aplikaci Exchange 2003 Server

Součástí nastavení jsou také tyto podpoložky ve stromové struktuře:

- [Akce nad nálezy](#)
- [Filtrování e-mailů](#)

5.5. Akce nad nálezy



V části **Akce nad nálezy** lze zaškrtnout a vybrat automatické akce, které mají být provedeny v průběhu testování. Akce jsou k dispozici pro následující položky:

- **Vysoce závažné nálezy** – nebezpečné kódy, které se kopírují a šíří se, často nepozorovaně, aby napáchaly škody v systému uživatele.
- **Nálezy střední závažnosti** – různé druhy programů, které mohou, ale také nemusí představovat hrozbu.

- **Nález s informativní závažností** – zahrnuje všechny nalezené potenciální hrozby, které nelze zařadit ani do jedné z výše uvedených kategorií.

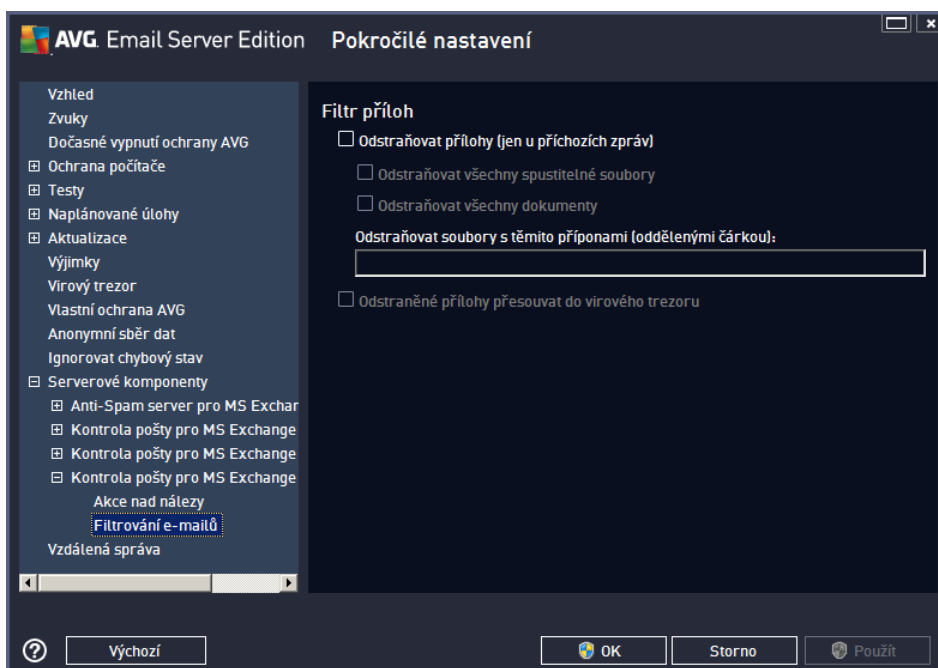
Z rolovací nabídky zvolte pro každou položku vždy jednu akci:

- **Žádná** – nebude provedena žádná akce.
- **Přesunout do trezoru** – dané nebezpečí bude přesunuto do Virového trezoru.
- **Odstranit** – dané nebezpečí bude odstraněno.

Pokud si přejete přidat do předem tu zprávy zpracované určitou akci textovou informaci pro lepší identifikaci a přehled, zaškrtněte příslušné políčko **Označit zprávy jako** a vložte požadovanou hodnotu.

Poslední zmíněnou vlastnost nelze aplikovat v případě nastavení Kontroly pošty pro MS Exchange (VSAPI).

5.6. Filtrování e-mailů



V části **Filtr příloh** můžete zvolit přílohy, které mají být automaticky odstraněny. K dispozici jsou následující možnosti:

- **Odstraňovat přílohy** - zaškrtněte pro povolení této funkce.
- **Odstraňovat všechny spustitelné soubory** - odstraní všechny spustitelné přílohy.
- **Odstraňovat všechny dokumenty** - odstraní všechny dokumenty v příloze.
- **Odstraňovat soubory s těmito příponami (oddělenými čárkou)** - Můžete připojit přípony, které si přejete automaticky odstranit. Hodnoty oddělte čárkou.



- **Odstranění položky přesouvání do virového trezoru** - zaškrtněte, pokud nechcete, aby byly filtrované položky odstraněny rovnou. Je-li toto políčko zaškrtnuté, budou všechny položky zvolené prostřednictvím tohoto dialogu automaticky přesouvány do karanténního prostředí Virového trezoru. Jedná se o bezpečné místo pro ukládání potenciálně škodlivých souborů - můžete k nim přistupovat a zkoumat je, aniž by mohly ohrozit váš systém. Do Virového trezoru se dostanete z hlavní obrazovky aplikace **AVG E-mail Server 2013**. V horní nabídce klikněte levým tlačítkem myši na položku **Možnosti** a následně z kontextového menu zvolte **Virový trezor**.

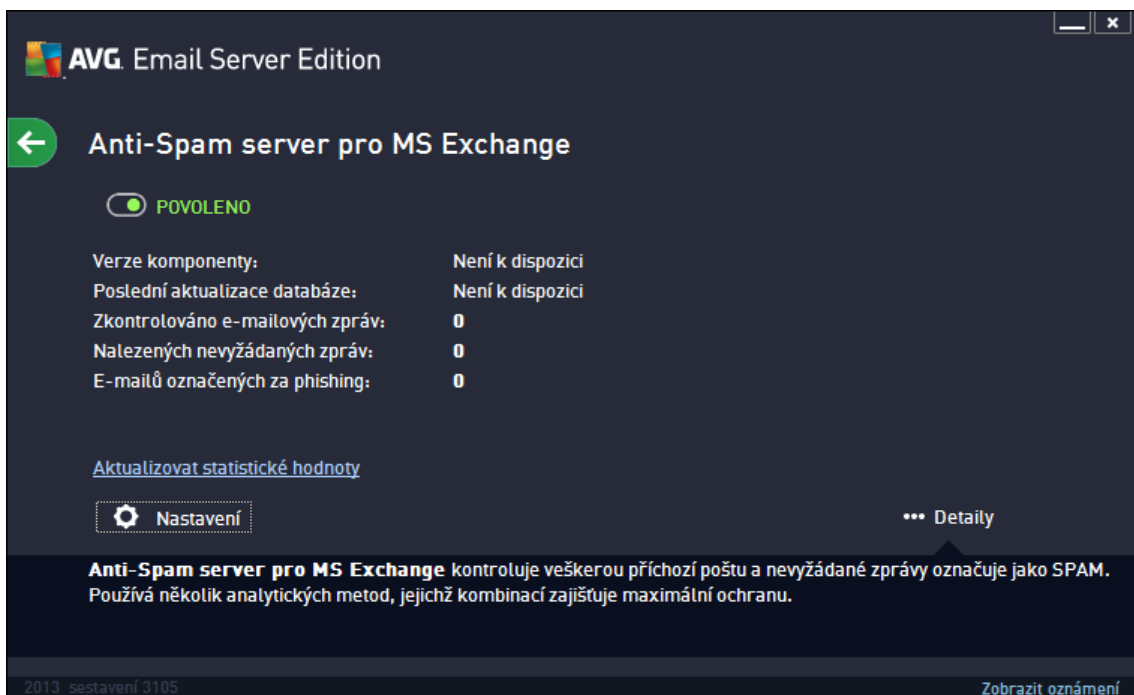
6. Komponenta Anti-Spam server pro MS Exchange

6.1. Princip komponenty Anti-Spam

Termínem *spam* označujeme nevyžádanou elektronickou poštu, převážně reklamního charakteru, jež je jednorázově hromadně rozesílána obrovskému počtu adresátů, čímž zahlcuje jejich poštovní schránky. Termín *spam* se nevztahuje na oprávněný e-mail komerčního charakteru, k jehož přijetí dal zákazník svůj souhlas. Spam je nejen nepříjemný a obtížný, ale je také častým zdrojem virů nebo distributorem textu urážlivého charakteru.

Komponenta **Anti-Spam** kontroluje veškerou příchozí poštu a nežádoucí zprávy označuje jako *spam*. K detekci spamu v jednotlivých zprávách používá několik analytických metod a zaručuje tedy maximální úroveň ochrany proti nevyžádané poště.

6.2. Rozhraní komponenty Anti-Spam



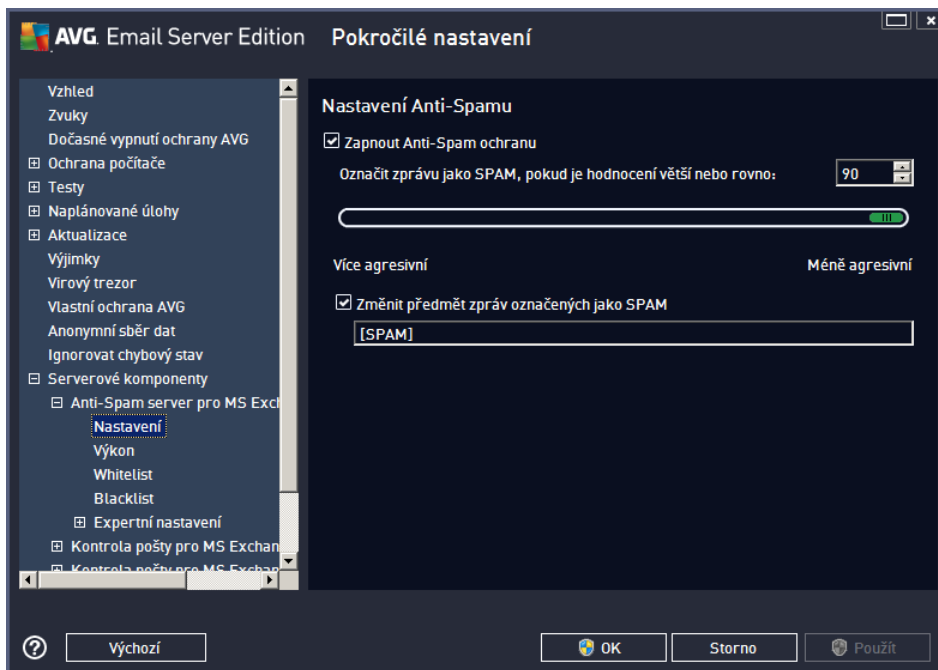
Tento dialog obsahuje základní informace o fungování komponenty, dále pak oznámení o jejím aktuálním stavu (*Povoleno/Zakázáno*) a stručný statistický přehled.

Dostupná tlačítka a odkazy:

- **POVOLENO/ZAKÁZÁNO** - kliknutí na toto tlačítko vypíná a zapíná danou komponentu (je-li komponenta zapnutá, jsou tlačítko i text zelené, je-li vypnutá, zobrazují se červeně).
- **Aktualizovat statistické hodnoty** - aktualizuje statistiky uvedené v dialogu.
- **Nastavení** - otevře [pokročilé nastavení komponenty Anti-Spam](#).

6.3. Anti-Spam nastavení

6.3.1. Nastavení



V tomto dialogu můžete označením položky **Zapnout Anti-Spam ochranu** celkově povolit i zakázat funkci komponenty **Anti-Spam**.

V tomto dialogu také můžete definovat, jak chcete nastavit úroveň ochrany proti spamu - více i méně agresivní. Na základě několika dynamických testovacích technik pak filtr komponenty **Anti-Spam** při adí každé zprávy určí skóre (například podle toho, nakolik se obsah zprávy blíží textu, který lze považovat za spam). Hodnotu úrovně citlivosti pro označení spamu lze nastavit buď přímo vepsáním číselné hodnoty (50 až 90) do příslušného pole nebo pomocí posuvníku.

Přehled úrovní ochrany, jež odpovídají jednotlivým hodnotám:

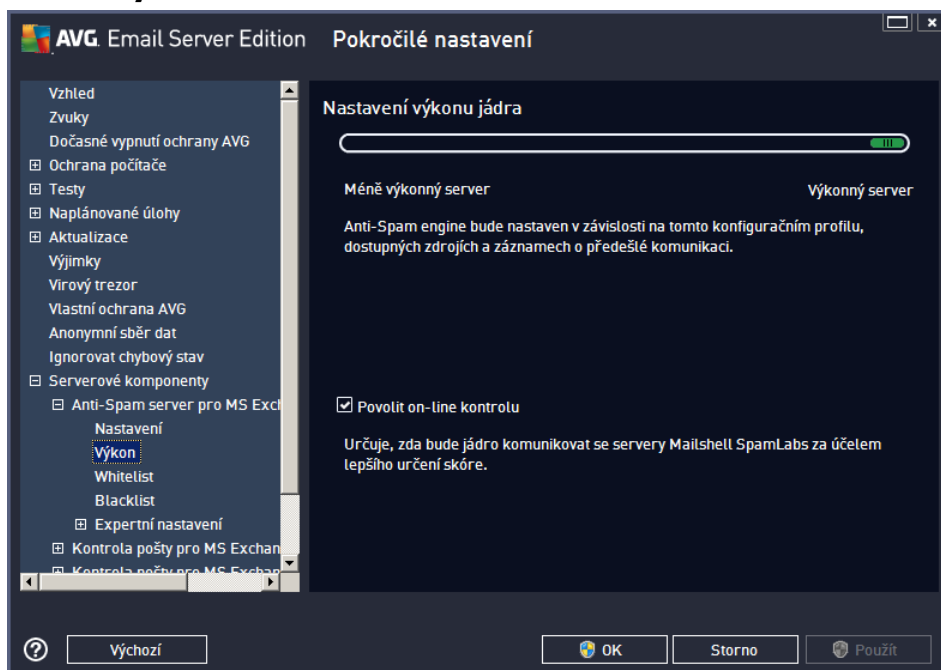
- **Hodnota 90** - Většina příchozí pošty bude normálně doručena, aniž by byla označena jako [spam](#). Snadno identifikovatelný [spam](#) bude odfiltrován, ale poměrně velká část spamových zpráv se přesto do vaší schránky dostane.
- **Hodnota 80-89** - E-mailové zprávy, u nichž se dá předpokládat charakter [spamu](#), budou odfiltrovány. Je možné, že omylem dojde i k odfiltrování některých zpráv, jež nejsou spamového charakteru.
- **Hodnota 60-79** - Toto nastavení je již považováno za poměrně agresivní konfiguraci. E-mailové zprávy, které mohou být považovány za [spam](#), budou odfiltrovány. Současně však dojde k poměrně velkému odchytu zpráv, které nejsou spamového charakteru, ale na základě určitých znaků mohou být takto vyhodnoceny.
- **Hodnota 50-59** - Velmi agresivní konfigurace. Nespamové e-mailové zprávy budou ve většině případů odfiltrovány spolu se zprávami pozitivně detekovanými jako [spam](#). **Tato konfigurace už není**

doporu eným nastavením pro b žné uživatele.

V dialogu můžete dále nastavit, jak se má zacházet s e-mailovými zprávami pozitivně detekovanými jako [spam](#) :

- **Zm nit p edm t zprávy u zpráv ozna ených jako spam** - ozna ením této položky zvolíte aktivujete textové pole, v němž máte možnost editovat text, kterým si p ežete ozna ovat zprávy detekované jako [spam](#) - tento text pak bude automaticky vepsán do p edm tu každé detekované e-mailové zprávy.
- **Zeptat se p ed ohlášením nesprávného nálezu** - pokud jste během instalace potvrdili svou ú ast v Programu zlepšování produktu (program slouží ke shromáždění nej erstv jších informací o virech, spywaru i škodlivých webových stránkách a vylepšování ochrany pro všechny naše uživatele), povolili jste odesílání reportů o detekovaných hrozbách do AVG. Tato hlášení jsou odesílána automaticky. Pokud si však p ežete mít možnost zkontrolovat, že detekovaná zpráva má být skute n klasifikována jako spam, ozna te položku Zeptat se p ed ohlášením nesprávného dotazu a p ed odesláním reportu vám bude zobrazen dotazovací dialog vyžadující vaše potvrzení.

6.3.2. Výkon



Dialog **Nastavení výkonu jádra** (odkazovaný položkou **Výkon**) nabízí možnost konfigurace parametrů výkonu komponenty **Anti-Spam**. Polohou posuvníku určete úroveň testovacího výkonu na ose **Nenáro ný / Výkonný** režim.

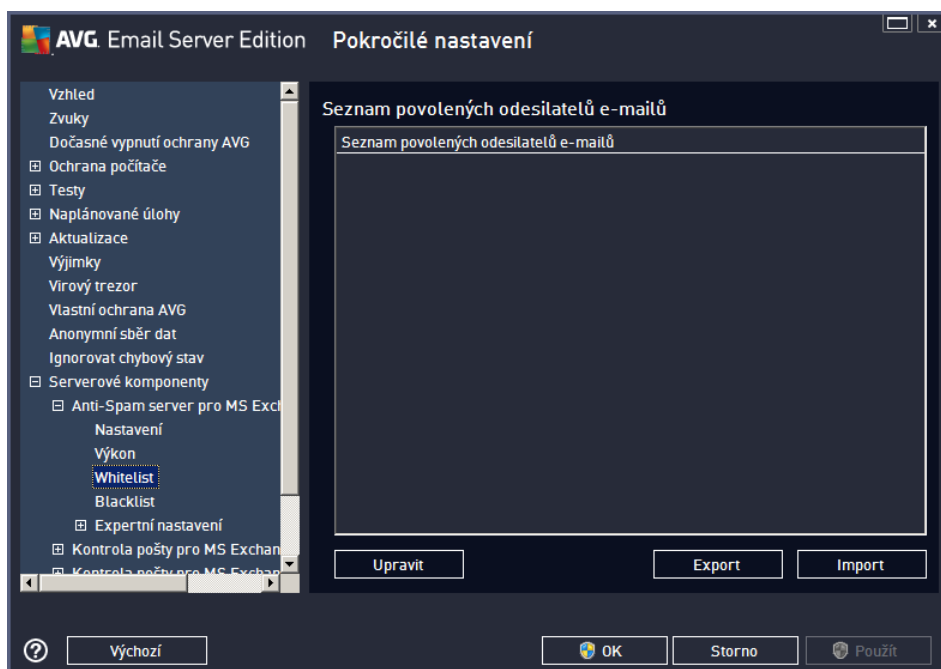
- **Výkonný režim** spot ebuje velký objem pam ti. B ěhem testovacího procesu budou k identifikaci [spamu](#) použity následující parametry: pravidla a spamové databáze, základní a pokro ilé nastavení, IP adresy spammerů a spamové databáze.
- **Nenáro ný režim** znamená, že b ěhem testovacího procesu nebudou k identifikaci [spamu](#) použita žádná pravidla. Identifikace [spamu](#) bude založena výhradn ě na porovnání s testovacími daty. Tento režim pro b žné používání nedoporu ujeme, nastavení lze doporu it výhradn ě u po íta s velmi nízkou úrovní hardwarového vybavení.

Položka **Povolit on-line kontrolu** je ve výchozím nastavení označena a určuje, že pro přesnější detekci [spamu](#) bude k testování použita i komunikace se servery společnosti [Mailshell](#), a během testování budou testovaná data porovnáována s databází této společnosti v online režimu.

Obecně doporučujeme podržet výchozí nastavení, pokud nemáte skutečný důvod tuto konfiguraci měnit. Změnu parametrů nastavení výkonu jádra lze doporučit výhradně znalým a zkušeným uživatelům!

6.3.3. Whitelist

Položka **Whitelist** otevírá dialog se seznamem e-mailových adres a doménových jmen, u nichž víte, že pošta z těchto adres/domén doručena nikdy nebude mít charakter [spamu](#):



V editačním rozhraní máte možnost sestavit seznam odesílatelů, u nichž předpokládáte, že vám nikdy nepošlou poštu, kterou lze považovat za [spam](#) (nevyžádanou poštu). Můžete také sestavit seznam kompletních doménových jmen (například [avg.com](#)), o nichž víte, že negenerují nevyžádanou poštu.

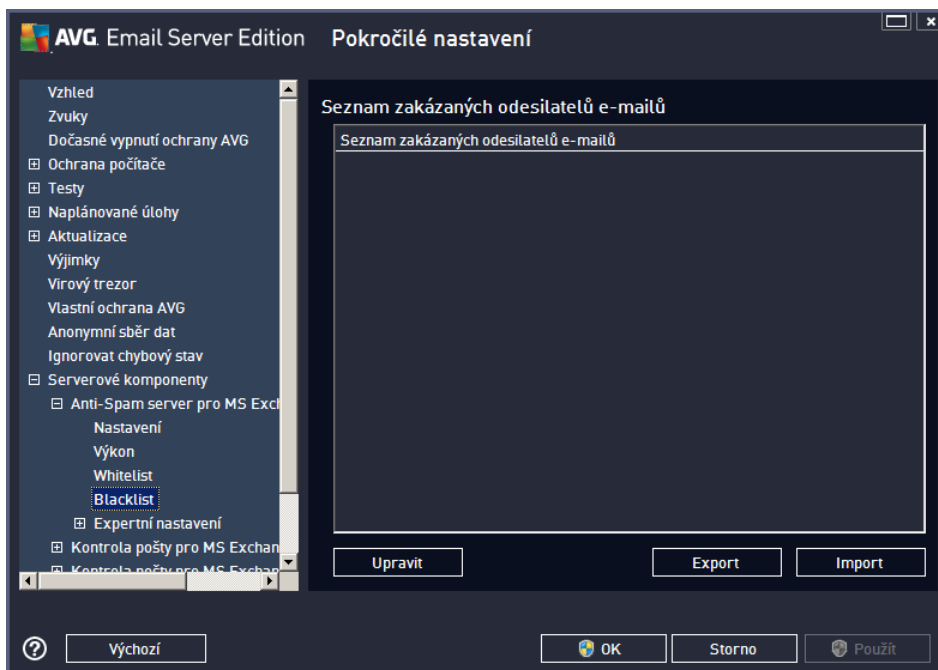
Jakmile budete mít připraven tento seznam adres a domén, můžete je zadat do **Whitelistu** dvěma způsoby: pomocí vložením jednotlivých adres nebo jednorázovým importem celého seznamu. K dispozici jsou vám tyto ovládací tlačítka:

- **Upravit** - stiskem tohoto tlačítka otevřete dialog, v němž můžete manuálně přidávat adresy ze seznamu (můžete také použít jednorázovou metodu „kopírovat a vložit“). Adresy/doménová jména vkládejte po jednom na každý řádek.
- **Import** - pokud již máte seznam adres/doménových jmen uložený v textovém souboru, můžete jej snadno importovat za použití tohoto tlačítka. Import lze provést buď z textového souboru (musí být ve formátu prostého textu a obsah musí být rozdělen tak, že každý řádek obsahuje pouze jednu položku - adresu nebo doménové jméno), z WAB souboru i přímo z adresáře Windows nebo Microsoft Office Outlooku.

- **Export** - pokud budete z libovolného dialogu chtít seznam adres/doménových jmen exportovat, můžete export provést pomocí tohoto tlačítka. Veškeré záznamy budou uloženy ve formátu prostého textu.

6.3.4. Blacklist

Položka **Blacklist** otevírá dialog se seznamem e-mailových adres a doménových jmen, která mají být zablokována pro příjem jakékoliv pošty. To znamená, že pošta odeslaná z kterékoliv uvedené adresy nebo domény bude vždy označena jako [spam](#):



V editačním rozhraní máte možnost sestavit seznam odesílatelů, u nichž předpokládáte, že poštu, kterou vám posílají, lze považovat za [spam](#) (nevyžádaná pošta). Můžete také sestavit seznam kompletních doménových jmen (například *spammingcompany.com*), u nichž je předpoklad, že budou generovat nevyžádanou poštu. Pošta odeslaná z kterékoliv uvedené adresy bude pak detekována jako [spam](#).

Jakmile budete mít připraven tento seznam adres a domén, můžete je zadat do **Blacklistu** dvěma způsoby: pomocí vložením jednotlivých adres nebo jednorázovým importem celého seznamu. K dispozici jsou vám tyto ovládací tlačítka:

- **Upravit** - stiskem tohoto tlačítka otevřete dialog, v němž můžete manuálně přidávat adresy ze seznamu (můžete také použít jednorázovou metodu „kopírovat a vložit“). Adresy/doménová jména vkládejte po jednom na každý řádek.
- **Import** - existující e-mail adresy můžete snadno importovat za použití tohoto tlačítka. Import lze provést buď z textového souboru (musí být ve formátu prostého textu a obsah musí být rozdělen tak, že každý řádek obsahuje pouze jedinou položku - adresu nebo doménové jméno), z WAB souboru či přímo z adresáře Windows nebo Microsoft Office Outlooku.
- **Export** - pokud budete z libovolného dialogu chtít seznam adres/doménových jmen exportovat, můžete export provést pomocí tohoto tlačítka. Veškeré záznamy budou uloženy ve formátu prostého textu.



6.3.5. Expertní nastavení

Tato větev obsahuje rozsáhlé možnosti nastavení komponenty Anti-Spam. Tato nastavení jsou určena výhradně pokročilým uživateli, jako jsou správci sítí, kteří potřebují antispamovou ochranu nastavit do detailů pro co nejlepší ochranu e-mailových serverů. Z tohoto důvodu není v dialogích pokročilého nastavení dostupná běžná nápověda, pouze stručný popis příslušné funkce přímo v dialogu.

Doporučujeme nenastavovat žádná pokročilá nastavení, pokud nejste dobře obeznámeni se všemi funkcemi nástroje Spamcatcher (MailShell Inc.). Nevhodné změny nastavení by mohly vyústit v nespolehlivost až nefunkčnost celé komponenty.

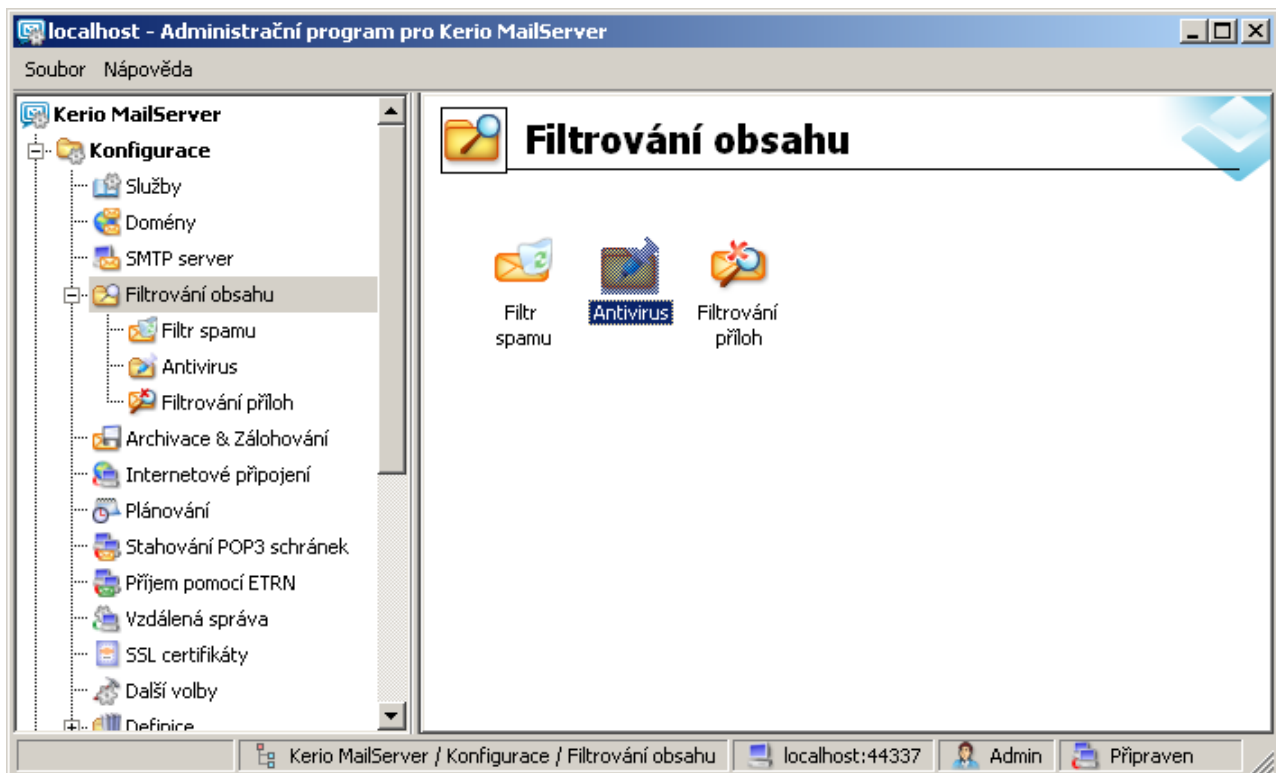
Pokud se přesto domníváte, že je nutné změnit konfiguraci služby Anti-Spam na úrovni vysoce pokročilého nastavení, pokračujte prosím podle instrukcí uvedených přímo v dialogu. Obecně platí, že v každém dialogu máte možnost zapnout jednu konkrétní funkci služby Anti-Spam a její popis je uveden přímo v dialogu:

- **Filtrování** - seznam jazyků, seznam zemí, povolené IP adresy, blokové IP adresy, blokové země, blokové znakové sady, falešní odesílatelé
- **RBL** - RBL servery, práh, časový limit, maximum IP adres, ignorované IP adresy
- **Internetové připojení** - časový limit, proxy server, autentifikace proxy

7. AVG pro Kerio MailServer

7.1. Konfigurace

Mechanismus antivirové ochrany je integrován přímo v aplikaci **Kerio MailServer**. Abyste aktivovali antivirovou ochranu **Kerio MailServeru** pomocí testovacího jádra AVG, spus te administrací konzoli programu Kerio. V navigační struktuře na levé straně okna této aplikace zvolte položku **Filtrování obsahu** ve tví **Konfigurace**.



Na hlavním panelu aplikace se zobrazí dialogové okno **Filtrování obsahu**. V rámci tohoto okna je možné volit ze tří nabídek:

- **Filtr spamu**
- **Antivirus** (viz kapitola **Antivirus**)
- **Filtrování příloh** (viz kapitola **Filtrování příloh**)

7.1.1. Antivirus

Na této záložce můžete zapnout nebo vypnout antivirovou kontrolu pomocí **AVG pro Kerio MailServer**. Pro aktivaci aplikace zvolte položku **Použít externí antivirový program** a vyberte možnost **AVG E-mail Server** z menu externího softwaru:



Antiviry

Použít integrovaný antivirový modul McAfee®

Použít externí antivirový program AVG Email Server Edition Volby

V následující části můžete specifikovat pravidla pro akce provedené v rámci detekce infikované zprávy nebo filtrování příloh:

Je-li ve zprávě nalezen virus

Zahodit zprávu

Doručit zprávu bez viru (resp. bez přílohy obsahující virus)

Přeposlat originální zprávu (včetně virů) správci na adresu:

Přeposlat filtrovanou zprávu správci na adresu:

Umožňuje definovat akce provedené při detekci viru nebo v rámci procesu filtrování příloh:

- **Zahodit zprávu** – pokud je tato možnost zvolena, infikovaná/filtrovaná zpráva je zamítnuta.
- **Doručit zprávu bez viru** – pokud je tato možnost vybrána, infikovaná/filtrovaná zpráva bude zbavena přílohy a doručena adresáti.
- **Přeposlat originální zprávu (včetně virů) správci na adresu** – zapnutí/vypnutí možnosti pro odesílání infikovaných zpráv na adresu zadanou v příslušném textovém poli.
- **Přeposlat filtrovanou zprávu správci na adresu** – zapnutí/vypnutí možnosti pro odesílání filtrovaných (bez těchto příloh) zpráv na adresu zadanou v příslušném textovém poli.

Nemůže-li být některá příloha zkontrolována (např. šifrovaný nebo poškozený soubor)

Doručit zprávu s varováním


Odmítnout zprávu - považovat tuto přílohu za virus (použijte se nastavení výše)

Umožňuje specifikovat akce pro soubory příloh, které nemohou být z jakéhokoli důvodu prošetřeny a otestovány:

- **Doručit zprávu s varováním** – zpráva (včetně přílohy) bude doručena nezkontrolovaná. Ke zprávě bude připojeno varování a uživatel bude upozorněn na to, že zpráva nebylo možno zkontrolovat, a že může obsahovat viry.
- **Odmítnout zprávu** – se zprávou bude naloženo, jako by příloha byla infikována. (tj. zpráva bude doručena bez přílohy, nebo zahozena). Tato možnost je nejbezpečnější, ovšem je potřeba vzít na v úvahu, že v podstatě znemožňuje zaslání zaheslovaných archivů.

7.1.2. Filtrování příloh

V nabídce *Filtrování příloh* je seznam s definicemi příloh pro jejich filtrování:



Filtrování příloh

Povolit filtrování příloh

Obsahuje-li zpráva přílohu blokovanou tímto filtrem:

Příloha bude ze zprávy odstraněna a zpráva bude doručena příjemci

Poslat odesílateli varování, že příloha nebyla doručena

Přeposlat původní zprávu správci na adresu:

Přeposlat filtrovanou zprávu správci na adresu:

Typ	Obsah	Akce	Popis
<input type="checkbox"/>	Jméno souboru *.exe	Blokovat	EXE files
<input checked="" type="checkbox"/>	Jméno souboru *.com	Blokovat	COM files
<input checked="" type="checkbox"/>	Jméno souboru *.scr	Blokovat	Screenshot files
<input checked="" type="checkbox"/>	Jméno souboru *.bat	Blokovat	BAT files
<input checked="" type="checkbox"/>	Jméno souboru *.vbs	Blokovat	Visual Basic scripts

Filtr příloh lze zapnout nebo vypnout pomocí položky **Povolit filtrování příloh**. Volitelně lze upravit také následující nastavení:

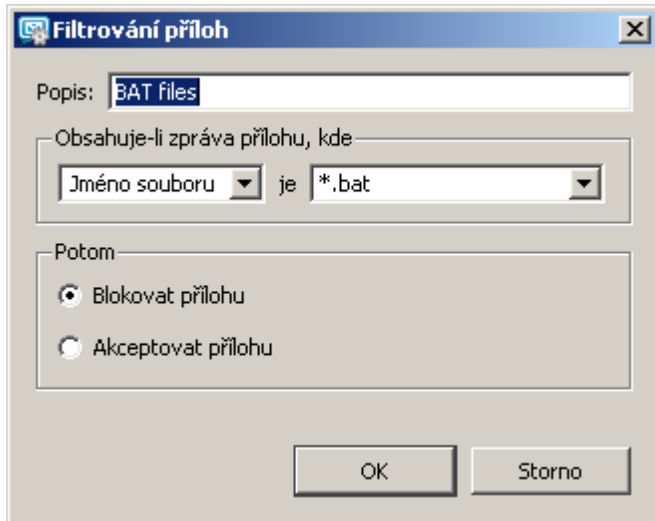
- **Poslat odesílateli varování, že příloha nebyla doručena** - odesílateli bude **Kerio Mailserverem** zasláno varování, že odeslal zprávu s infikovanou nebo nepovolenou přílohou.
- **Přeposlat původní zprávu správci na adresu** - zpráva bude přeposlána v původním tvaru, tedy i s infikovanou nebo zakázanou přílohou, na zadanou e-mailovou adresu. Nezáleží na tom, zda bude uvedena lokální nebo externí adresa.
- **Přeposlat filtrovanou zprávu správci na adresu** - zpráva bez infikované nebo zakázané přílohy bude, kromě níže vybraných akcí, také přeposlána na zadanou e-mailovou adresu. Toho lze využít například pro ověření správné funkce antivirové kontroly a filtru příloh.

V seznamu příloh jsou u každého prvku obsažena tři pole:

- **Typ** – specifikace druhu přílohy dané příponou zadanou v poli **Obsah**. Možné typy jsou *Jméno souboru* nebo *MIME typ*. V příslušném poli můžete také zahrnout/vyloučit daný typ přílohy do/z filtru.
- **Obsah** – zde můžete definovat příponu filtrovaných příloh. Pro zápis lze využít zástupné znaky operačního systému (například *et zec "*.doc.*" pro jakýkoli soubor s příponou .doc a libovolnou další za ní*).
- **Akce** – definice akce, která má být provedena s danou přílohou. Možné akce jsou **Akceptovat** (přijmout přílohu) a **Blokovat** (bude provedena akce definovaná nad seznamem zakázaných příloh).

- **Popis** – krátký popis dané přílohy.

Položka seznamu může být odstraněna pomocí tlačítka **Odebrat**. Při přidání položky je možné po stisknutí tlačítka **Přidat...** Stejně tak lze editovat existující záznam po stisknutí tlačítka **Změnit...** Objeví se toto okno:



- V poli **Popis** zadejte krátký popis druhu dané přílohy.
- V poli **Obsahuje-li zpráva o přílohu, kde** můžete vybrat typ přílohy (*Jméno souboru* nebo *MIME typ*). V dalším poli také můžete zvolit příponu z nabídky, nebo zadat příjmení vlastní.

V poli **Potom** můžete rozhodnout, zda danou přílohu blokovat nebo přijmout.



8. FAQ a technická podpora

V případě problémů s AVG se pokuste vyhledat řešení na webu [AVG \(http://www.avg.cz\)](http://www.avg.cz) v sekci **FAQ**.

Pokud na svůj dotaz nenajdete uspokojivou odpověď, obraťte se prosím na oddělení technické podpory AVG prostřednictvím kontaktního formuláře dostupného ze systémového menu volbou položky **Nápověda / Odborná pomoc online**.