

Stručná příručka: Avast Business Antivirus

Pomoc s řešením problémů najdete v naší online dokumentaci:

<https://businesshelp.avast.com/>

Obsah

Stručná příručka: Avast Business Antivirus	1
Obsah	2
Nastavení zařízení	4
Systémové požadavky.....	4
Koncová zařízení s aplikací Avast Business Antivirus.....	4
Požadavky na nastavení firewallu	4
Porty.....	4
Webové adresy.....	5
Instalace aplikace Avast Business Antivirus na zařízeních	5
Přízpůsobení instalace.....	5
Doporučené komponenty pro servery a pracovní stanice.....	6
Doporučeno pro firmy	6
Doporučeno pro servery	6
Aktivace licencí na zařízení.....	6
Konfigurace nastavení a komponenty	7
Komponenty antiviru podle produktové licence.....	7
Zapnutí a vypnutí komponent.....	7
Instalace a odinstalace komponent	8
Konfigurace výjimek	9
Zástupné znaky	9
Výjimky	9
Přidávání výjimek	9
Konfigurace automatických aktualizací.....	10
Konfigurace automatických aktualizací	10
Vytváření a konfigurace testů.....	10

Typy testů	10
Přizpůsobení úplných virových testů.....	11
Citlivost	11
Testované oblasti.....	11
Archivy.....	12
Typy souborů	12
Výjimky	13
Přizpůsobení cílených testů.....	13
Citlivost	13
Archivy.....	13
Typy souborů	14
Přizpůsobení testů z Průzkumníku	15
Citlivost	15
Archivy.....	15
Typy souborů	15
Přizpůsobení testů po restartu	16
Citlivost	16
Testované oblasti.....	16

Nastavení zařízení

Systémové požadavky

Koncová zařízení s aplikací Avast Business Antivirus

Windows:

- 7 SP1 nebo vyšší, 8.x kromě edic RT a Starter, 10 kromě edic Mobile a IoT Core Edition
- Server 2008 R2, 2012 R2, 2016, 2019, všechny edice s nejnovější aktualizací Service Pack, kromě Server Core
- Microsoft Exchange Server 2010 SP2, 2013, 2016, 2019
- Microsoft SharePoint Services 3.0 a SharePoint Server 2010 nebo vyšší

Mac:

- MacOS 10.10 (Mavericks nebo novější a alespoň 500 MB volného místa na disku)

Linux:

- CentOS 7 a novější
- Debian 8 a novější
- Red Hat Enterprise Linux 7.4 a novější
- Ubuntu LTS 16.04 a novější

Požadavky na nastavení firewallu

Na firewallu nebo proxy serveru je nutné povolit určité porty a webové adresy, aby konzole mohla fungovat, aby klienty Avast Business Antivirus mohly komunikovat a aby fungovalo ověřování.

Porty

TCP a UDP:

- 53 – služby bezpečné DNS (pouze pokud používáte komponentu Ověřené weby)
- 80 – kontroly zranitelnosti na internetu a aktualizace funkcí
- 443 – vyjednávání se šifrovacím klíčem FFL (pouze pokud používáte komponentu Ověřené weby)

Webové adresy

- *.avast.com
- *.avcdn.net
- *.mailshell.net (pouze pokud používáte Antispam)

Instalace aplikace Avast Business Antivirus na zařízeních

Instalační program nespravované aplikace Avast Business Antivirus si můžete stáhnout z <https://www.avast.com/installation-files>. Klikněte na kartu Firma a poté vyberte online či offline instalační program verze antiviru, kterou máte. Stažený instalační program můžete spustit na zařízení, na kterém chcete antivirus nainstalovat.

Když vyberete online instalační program, ostatní služby budou staženy po instalaci antivirového agenta. Tato možnost není doporučována, když instalujete antivirus na několik zařízení zároveň, protože každé z nich následně začne stahovat ostatní služby ze serverů Avastu.

Přizpůsobení instalace

1. Instalační soubor zkopírujte do umístění, které je přístupné z koncového zařízení.
2. Dvojitým kliknutím instalační soubor spustíte.
3. Když se zobrazí dotaz, zda smí aplikace provádět změny v zařízení, klikněte na možnost **Ano**.
4. Klikněte na možnost **Přizpůsobit** a proveďte jeden z následujících úkonů:
 - Výběrem možnosti **Doporučená ochrana** nainstalujte všechny komponenty.
 - Výběrem možnosti **Minimální ochrana** nainstalujte jen Souborový štít, Webový štít a E-mailový štít.
 - Po výběru možnosti **Vlastní ochrana** můžete zvolit komponenty, které chcete nainstalovat.
5. Klikněte na tlačítko **Nainstalovat** a počkejte, než se Avast Business Antivirus nainstaluje na zařízení.
6. Na výzvu restartujte zařízení.

Doporučené komponenty pro servery a pracovní stanice

Firmy mají jiné potřeby než běžní uživatelé, a proto některé komponenty aplikace Avast Business Antivirus nedoporučujeme ve firemních sítích používat.

Doporučeno pro firmy

Následující komponenty je třeba zcela odinstalovat nebo pomocí příslušného posuvníku **vypnout**:

- Ověřené weby
- Inspektor Wi-Fi

Pokud je neodeberete, můžete se potýkat s nestabilitou připojení k síti, pomalejším fungováním počítače nebo chybami.

Doporučeno pro servery

Následující komponenty je třeba zcela odinstalovat nebo pomocí příslušného posuvníku **vypnout**, případně vůbec do zařízení neinstalovat:

- Webový štít
- E-mailový štít

Aktivace licencí na zařízení

Předplatné aplikace Avast Business Antivirus můžete aktivovat po nainstalování aplikace na zařízení.

1. Na zařízení otevřete Avast Business Antivirus.
2. Klikněte na ikonu **Menu**.
3. Klikněte na možnost **Zadat aktivační kód**.
4. Zadejte aktivační kód a poté klikněte na tlačítko **Zadat**.
5. V případě potřeby potvrďte předplatné a jeho komponenty.

Konfigurace nastavení a komponenty

Avast Business Antivirus nabízí spoustu komponent, a to jak v základní variantě, tak ve variantách Pro a Plus.

Komponenty antiviru podle produktové licence

Komponenta	Avast Business Antivirus	Avast Business Antivirus Pro	Avast Business Antivirus Pro Plus
Souborový štít	X	X	X
Webový štít	X	X	X
E-mailový štít	X	X	X
Behaviorální štít	X	X	X
Štít vzdáleného přístupu			X
Inspektor Wi-Fi	X	X	X
Ověřené weby	X	X	X
Firewall	X	X	X
Sandbox	X	X	X
Antispam	X	X	X
Exchange		X	X
Sharepoint		X	X
Štít webové kamery			X
SecureLine VPN			X
Skartovač dat		X	X
Passwords			X
Ochrana hesel			X
Aktualizace aplikací	X	X	X
Čištění prohlížečů			X
Záchranný disk	X	X	X

Zapnutí a vypnutí komponent

Spoustu štítů a nástrojů v aplikaci Avast Business Antivirus lze v zařízení zapnout či vypnout. To se hodí zejména v případě, kdy instalujete na server jen několik komponent nebo kdy chcete nainstalovat jen minimum nástrojů. Některé nástroje ale lze pouze nainstalovat nebo zcela odinstalovat – například Sandbox nebo Záchranný disk.

1. Otevřete klienta Avast Business Antivirus.
2. Klikněte na kartu komponenty, kterou chcete zapnout nebo vypnout:
 - **Ochrana:** Souborový štít, Webový štít, E-mailový štít, Behaviorální štít, Sandbox, Inspektor Wi-Fi, Ověřené weby, Firewall
 - **Soukromí:** Passwords, Antispam, Skartovač dat, Štít webové kamery
 - **Výkon:** Aktualizace aplikací
3. Klikněte na tlačítko komponenty
4. U komponenty, kterou chcete změnit, proveďte jeden z následujících kroků:
 - Chcete-li komponentu zapnout, přepněte příslušný posuvník do polohy **Zapnuto**.
 - Chcete-li komponentu vypnout, přepněte příslušný posuvník do polohy **Vypnuto**.
5. V případě potřeby potvrďte volbu.

Instalace a odinstalace komponent

Většina funkcí aktivní ochrany je instalována s aplikací Avast Business Antivirus. Přes nabídku Řešení problémů je ale můžete podle potřeby odinstalovat či znovu nainstalovat. Komponenty pro ochranu systému MacOS X nelze nainstalovat ani odinstalovat, ale můžete je vypnout.

1. Otevřete klienta Avast Business Antivirus.
2. Přejděte do části **Menu > Nastavení > Obecné > Řešení problémů**.
3. Klikněte na možnost **Přidat/změnit komponenty**.
4. U komponent, které chcete změnit, proveďte jeden z následujících kroků:
 - Pokud komponenta ještě není nainstalovaná, zaškrtněte její pole.
 - Pokud komponenta už je nainstalovaná, zrušte zaškrtnutí jejího pole.
5. Až změny dokončíte, potvrďte je kliknutím na tlačítko **Změnit**.

Podrobnosti o konfiguraci jednotlivých komponent, které jsou k dispozici v nastaveních aplikace Avast Business Antivirus, najdete v článku [Konfigurace nastavení v aplikaci Avast Business Antivirus](#).

Konfigurace výjimek

Zástupné znaky

Řada štítů a dalších komponent v aplikaci Avast Business Antivirus (včetně hlavní antivirové komponenty) vám umožňuje nastavovat výjimky či blokovat konkrétní cesty. Zástupné znaky vám pomohou, když neznáte přesnou cestu či název souboru, který chcete zahrnout nebo vyloučit. Také vám pomohou označit více souborů v jedné cestě. Některé cesty k souborům ale používání zástupných znaků neumožňují.

Znak	Význam
?	Nahrazuje jeden znak Příklad: <code>ab?.html</code> odpovídá souborům <code>abc.html</code> , <code>abd.html</code> , <code>abe.html</code> atd. a neodpovídá souboru <code>abc.htm</code> .
*	Nahrazuje nula nebo více znaků Příklad: <code>*mtl</code> odpovídá souborům <code>abc.html</code> a <code>d.html</code> . <code>*txt</code> odpovídá souborům <code>abc.txt</code> , <code>x.txt</code> a <code>xyztxt</code> .

Výjimky

Můžete nastavit výjimky, které budou uplatněny v jednotlivých štítech a komponentách aplikace Avast Business Antivirus. Stačí na stránce **Nastavení** ► **Obecné** přejít na kartu *Výjimky*.

Přidávání výjimek

1. Otevřete klienta Avast Business Antivirus.
2. Vpravo nahoře klikněte na **Menu** a poté na možnost **Nastavení**.
3. V části **Obecné** ► **Výjimky** klikněte na možnost **Přidat výjimku** a proveďte jeden z následujících úkonů:
 - Zadejte nebo najděte cestu k souboru, který chcete vyloučit.
 - Zadejte nebo najděte cestu ke složce, kterou chcete vyloučit.
 - Zadejte webovou adresu, kterou chcete vyloučit.
4. Až budete hotoví, klikněte na možnost **Přidat výjimku**.

Konfigurace automatických aktualizací

Na svých zařízeních můžete automaticky aktualizovat virové definice i verzi aplikace Avast Business Antivirus, když jsou k dispozici nové aktualizace. Také můžete nastavit, aby byla zařízení aktualizována ručně. Další informace najdete v tématu [Aktualizace aplikace Avast Business Antivirus](#).

Konfigurace automatických aktualizací

1. Vpravo nahoře klikněte na **Menu**.
2. Klikněte na možnost **Nastavení**.
3. V části *Obecné* vyberte kartu **Aktualizace**.
4. U dvou tlačítek **Vyhledat aktualizace** klikněte na položku **Více možností**.
5. Vyberte možnost **Automatická aktualizace**.

Vytváření a konfigurace testů

V nastaveních virových testů můžete nastavit typy souborů a programy, které má aplikace Avast Business Antivirus testovat. Proto jsou hlavní nastavení testování konfigurována v nastaveních testů, zatímco výjimky jsou nastavovány v části *Obecné*.

Typy testů

- **Úplný virový test** – Provádí podrobný test systému, který kontroluje všechny pevné disky, rootkity a automaticky spouštěné programy.
- **Cílený test** – Otestuje pouze složky vybrané při zahájení testu.
- **Test z Průzkumníku** – Otestuje vybrané složky nebo jednotky, ale je k dispozici jen z kontextové nabídky Windows, když kliknete pravým tlačítkem na soubor, složku nebo jednotku.
- **Test po restartu (pouze MS Windows)** – Otestuje zařízení po spuštění.

Nastavení jednotlivých typů testů můžete otevřít tím, že kliknete na možnosti Menu > Nastavení a pak přejdete na možnosti Ochrana > Testy na viry.

Přizpůsobení úplných virových testů

Citlivost

V nastavení citlivosti testů můžete určit, jak mají být testy citlivé. Čím je citlivost vyšší, tím je ochrana lepší, ale také tím vyšší je možnost výskytu falešných poplachů na malware. Když citlivost snížíte, falešných poplachů bude méně, avšak účinnost testů bude nižší. Posuvník Citlivost testu lze nastavit do polohy střední, vysoké nebo nízké citlivosti.

Hledat potenciálně nežádoucí programy (PUP): umožňuje Avastu hledat programy, které jsou tajně stahovány s jinými programy a provádějí nežádoucí činnost.

Během testu následovat odkazy: umožňuje Avastu testovat také ostatní soubory používané testovanými soubory, jestli neobsahují potenciálně škodlivý obsah.

Testovat celé soubory (u velkých souborů velmi pomalé): umožňuje Avastu testovat celé soubory, nikoli pouze jejich části, jež jsou obvykle postiženy škodlivým kódem.

Priorita testu: určuje množství systémových prostředků, které smí Avast při testování používat. Vyšší priorita znamená rychlejší testování a zároveň může zpomalovat ostatní procesy na zařízení.

Testované oblasti

Výběrem příslušných polí můžete oblasti uvedené v seznamu zahrnout do testování. Hlavní možnosti oblastí jsou následující:

- **Všechny pevné disky:** umožňuje Avastu otestovat všechny pevné disky v počítači.
- **Systémová jednotka:** možnosti v této části se týkají dat uložených na fyzických zařízeních, jako jsou pevné disky nebo jednotky USB.

Při testování oblasti určené výše budou použity následující možnosti.

Všechna vyměnitelná média: umožňuje Avastu testovat aplikace, které se spouštějí automaticky, když k počítači připojíte jednotku USB nebo když do něj vložíte jiné výměnné médium.

Rootkity: umožňuje Avastu hledat hrozby ukryté v systému.

UEFI BIOS: umožňuje Avastu při spouštění počítače testovat hlavní firmwarová rozhraní.

Disky CD a DVD: umožňuje Avastu hledat škodlivý obsah na discích CD a DVD.

Moduly načtené v paměti: umožňuje Avastu testovat aplikace a procesy spouštěné po startu systému nebo běžící na pozadí.

Archivy

V části Archivy můžete určit typy komprimovaných souborů, které má Avast při testování rozbalovat.

- **Testovat jen běžné instalační programy:** testuje pouze obsah spustitelných souborů, které slouží k instalaci aplikací.
- **Testovat všechny archivy:** testuje veškerý obsah souborů archivů (testy kvůli tomu potrvají výrazně déle).
- **Netestovat archivy:** vypne testování archivů Avastem.

Typy souborů

Určete typy souborů, které při testování počítače na přítomnost malwaru mají být testovány přednostně:

- **Typy založené na obsahu (pomalé):** testuje soubory, které jsou obvykle nejzranitelnější vůči útokům malwaru.
- **Typy podle přípony (rychlé):** testuje pouze soubory s rizikovými příponami, jako jsou .exe, .com, .bat.
- **Testovat všechny soubory (velmi pomalé):** testuje všechny soubory v počítači na přítomnost malwaru.

Během testu provádět automatické akce: když povolíte tuto možnost, můžete určit automatickou akci při nálezů infikovaného souboru:

- **Automaticky vyčistit:** Avast se pokusí o opravu infikovaného souboru. Pokud se mu to nepovede, přesune soubor do Virové truhly. A pokud se mu ani to nepovede, soubor smaže.
- **Přesunout soubor do Virové truhly:** infikovaný soubor nebude automaticky opraven a místo toho bude přesunut do Virové truhly.
- **Smazat soubor:** Avast se infikovaný soubor nepokusí opravit ani přesunout do Virové truhly, ale automaticky jej smaže.

Po dokončení testu vypnout počítač: umožňuje Avastu po dokončení testu vypnout počítač.

Generovat report: umožňuje Avastu automaticky vytvářet a ukládat report. Umístění souboru reportu je uvedené pod touto možností.

Výjimky

Ačkoli se vylučování souborů či složek z testů nedoporučuje, můžete pro účely řešení problémů pro určité soubory či složky dočasně nastavit výjimky z testování. Ve spodní části stránky s nastaveními testů klikněte na možnost **Zobrazit výjimky**. Pak se řiďte pokyny v části [Konfigurace výjimek](#).

Přizpůsobení cílených testů

Citlivost

V nastavení citlivosti testů můžete určit, jak mají být testy citlivé. Čím je citlivost vyšší, tím je ochrana lepší, ale také tím vyšší je možnost výskytu falešných poplachů na malware. Když citlivost snížíte, falešných poplachů bude méně, avšak účinnost testů bude nižší. Posuvník Citlivost testu lze nastavit do polohy střední, vysoké nebo nízké citlivosti.

Hledat potenciálně nežádoucí programy (PUP): umožňuje Avastu hledat programy, které jsou tajně stahovány s jinými programy a provádějí nežádoucí činnost.

Během testu následovat odkazy: umožňuje Avastu testovat také ostatní soubory používané testovanými soubory, jestli neobsahují potenciálně škodlivý obsah.

Testovat celé soubory (u velkých souborů velmi pomalé): umožňuje Avastu testovat celé soubory, nikoli pouze jejich části, jež jsou obvykle postiženy škodlivým kódem.

Priorita testu: určuje množství systémových prostředků, které smí Avast při testování používat. Vyšší priorita znamená rychlejší testování a zároveň může zpomalovat ostatní procesy na zařízení.

Archivy

V části Archivy můžete určit typy komprimovaných souborů, které má Avast při testování rozbalovat.

- **Testovat jen běžné instalační programy:** testuje pouze obsah spustitelných souborů, které slouží k instalaci aplikací.
- **Testovat všechny archivy:** testuje veškerý obsah souborů archivů (testy kvůli tomu potrvají výrazně déle).
- **Netestovat archivy:** vypne testování archivů Avastem.

Typy souborů

Určete typy souborů, které při testování počítače na přítomnost malwaru mají být testovány přednostně:

- **Typy založené na obsahu (pomalé):** testuje soubory, které jsou obvykle nejzranitelnější vůči útokům malwaru.
- **Typy podle přípony (rychlé):** testuje pouze soubory s rizikovými příponami, jako jsou .exe, .com, .bat.
- **Testovat všechny soubory (velmi pomalé):** testuje všechny soubory v počítači na přítomnost malwaru.

Během testu provádět automatické akce: když povolíte tuto možnost, můžete určit automatickou akci při nálezů infikovaného souboru:

- **Automaticky vyčistit:** Avast se pokusí o opravu infikovaného souboru. Pokud se mu to nepovede, přesune soubor do Virové truhly. A pokud se mu ani to nepovede, soubor smaže.
- **Přesunout soubor do Virové truhly:** infikovaný soubor nebude automaticky opraven a místo toho bude přesunut do Virové truhly.
- **Smazat soubor:** Avast se infikovaný soubor nepokusí opravit ani přesunout do Virové truhly, ale automaticky jej smaže.

Po dokončení testu vypnout počítač: umožňuje Avastu po dokončení testu vypnout počítač.

Generovat report: umožňuje Avastu automaticky vytvářet a ukládat report. Umístění souboru reportu je uvedené pod touto možností.

Přizpůsobení testů z Průzkumníku

Citlivost

V nastavení citlivosti testů můžete určit, jak mají být testy citlivé. Čím je citlivost vyšší, tím je ochrana lepší, ale také tím vyšší je možnost výskytu falešných poplachů na malware. Když citlivost snížíte, falešných poplachů bude méně, avšak účinnost testů bude nižší. Posuvník Citlivost testu lze nastavit do polohy střední, vysoké nebo nízké citlivosti.

Hledat potenciálně nežádoucí programy (PUP): umožňuje Avastu hledat programy, které jsou tajně stahovány s jinými programy a provádějí nežádoucí činnost.

Během testu následovat odkazy: umožňuje Avastu testovat také ostatní soubory používané testovanými soubory, jestli neobsahují potenciálně škodlivý obsah.

Testovat celé soubory (u velkých souborů velmi pomalé): umožňuje Avastu testovat celé soubory, nikoli pouze jejich části, jež jsou obvykle postiženy škodlivým kódem.

Priorita testu: určuje množství systémových prostředků, které smí Avast při testování používat. Vyšší priorita znamená rychlejší testování a zároveň může zpomalovat ostatní procesy na zařízení.

Archivy

V části Archivy můžete určit typy komprimovaných souborů, které má Avast při testování rozbalovat.

- **Testovat jen běžné instalační programy:** testuje pouze obsah spustitelných souborů, které slouží k instalaci aplikací.
- **Testovat všechny archivy:** testuje veškerý obsah souborů archivů (testy kvůli tomu potrvají výrazně déle).
- **Netestovat archivy:** vypne testování archivů Avastem.

Typy souborů

Určete typy souborů, které při testování počítače na přítomnost malwaru mají být testovány přednostně:

- **Typy založené na obsahu (pomalé):** testuje soubory, které jsou obvykle nejzranitelnější vůči útokům malwaru.

- **Typy podle přípony (rychlé):** testuje pouze soubory s rizikovými příponami, jako jsou .exe, .com, .bat.
- **Testovat všechny soubory (velmi pomalé):** testuje všechny soubory v počítači na přítomnost malwaru.

Během testu provádět automatické akce: když povolíte tuto možnost, můžete určit automatickou akci při nálezů infikovaného souboru:

- **Automaticky vyčistit:** Avast se pokusí o opravu infikovaného souboru. Pokud se mu to nepovede, přesune soubor do Virové truhly. A pokud se mu ani to nepovede, soubor smaže.
- **Přesunout soubor do Virové truhly:** infikovaný soubor nebude automaticky opraven a místo toho bude přesunut do Virové truhly.
- **Smazat soubor:** Avast se infikovaný soubor nepokusí opravit ani přesunout do Virové truhly, ale automaticky jej smaže.

Po dokončení testu vypnout počítač: umožňuje Avastu po dokončení testu vypnout počítač.

Generovat report: umožňuje Avastu automaticky vytvářet a ukládat report. Umístění souboru reportu je uvedené pod touto možností.

Přízpusobení testů po restartu

Citlivost

V nastavení citlivosti testů můžete určit, jak mají být testy citlivé. Čím je citlivost vyšší, tím je ochrana lepší, ale také tím vyšší je možnost výskytu falešných poplachů na malware. Když citlivost snížíte, falešných poplachů bude méně, avšak účinnost testů bude nižší. Posuvník Citlivost testu lze nastavit do polohy střední, vysoké nebo nízké citlivosti.

Hledat potenciálně nežádoucí programy (PUP): umožňuje Avastu hledat programy, které jsou tajně stahovány s jinými programy a provádějí nežádoucí činnost.

Rozbalovat archivy: umožňuje Avastu rozbalovat soubory a složky v archivech, aby je bylo možné otestovat.

Testované oblasti

Výběrem příslušných polí můžete oblasti uvedené v seznamu zahrnout do testování. Hlavní možnosti oblastí jsou následující:

- **Všechny pevné disky:** umožňuje Avastu otestovat všechny pevné disky v počítači.
- **Systémová jednotka:** možnosti v této části se týkají dat uložených na fyzických zařízeních, jako jsou pevné disky nebo jednotky USB.

Při testování oblasti určené výše budou použity následující možnosti.

Automaticky spouštěné programy: umožňuje Avastu kontrolovat všechny automaticky spouštěné programy.

Během testu provádět automatické akce: když povolíte tuto možnost, můžete určit automatickou akci při nálezů infikovaného souboru:

- **Automaticky vyčistit:** Avast se pokusí o opravu infikovaného souboru. Pokud se mu to nepovede, přesune soubor do Virové truhly. A pokud se mu ani to nepovede, soubor smaže.
- **Přesunout soubor do Virové truhly:** infikovaný soubor nebude automaticky opraven a místo toho bude přesunut do Virové truhly.
- **Smazat soubor:** Avast se infikovaný soubor nepokusí opravit ani přesunout do Virové truhly, ale automaticky jej smaže.

Avast Business Antivirus nabízí spoustu dalších funkcí a možností. Další informace najdete v naší znalostní databázi na <https://businesshelp.avast.com/>.