Stručná příručka: Konzole AVG Business Management Console

Pomoc s řešením problémů najdete v naší online dokumentaci:

https://businesshelp.avast.com/

Obsah

Seznámení s konzolemi AVG Business Management Console

Konzole AVG Business Management Console umožňují spolehlivou a snadnou ochranu všech vašich počítačů s Windows i serverů. Flexibilní správa představuje nejsnazší způsob ochrany firem. Konzole Management Console poskytují:

- Úplnou kontrolu nad chováním antiviru na koncových zařízeních
- Centrální správu více zařízení – přes cloud nebo místně přes On-Premise Console
- Kompletní přehled o současném stavu všech vašich zařízení s možností nastavit okamžitá upozornění
- Automatické a bezproblémové aktualizace

Konzole AVG Business Management Console jsou hladce propojené s aplikací AVG Business Antivirus a umožňují vám:

- Pomocí virtualizace chránit důvěrné informace
- Chránit různé platformy – počítače i servery
- Automaticky nebo ručně instalovat aktualizace na nejnovější verzi
- Přidávat další úroveň ochrany – zdokonalený firewall pro koncová zařízení
- Kompletně chránit servery
- Zabezpečit vašeho e-mailového klienta

AVG Business Antivirus nainstalovaný na zařízení přes konzole AVG Business Management Console můžete ovládat na dálku. Na každém zařízení zvlášť můžete měnit nastavení, aniž byste u něj museli být fyzicky přítomní nebo by vám ho musel někdo přinést.

Nastavení konzole Management Console

Systémové požadavky konzole

AVG Business Cloud Console

Prohlížeče (jsou doporučovány nejnovější verze):

- Google Chrome
- Firefox
- Safari
- Microsoft Edge
- Internet Explorer

AVG Business On-Premise Console

Windows:

- 7 SP1 nebo vyšší, 8.x, 10
- Server 2008 R2 SP1, 2012 a 2012 R2, 2016, 2019 – libovolná edice
- Small Business Server 2008, 2011 (pouze 64bitová verze)
- Exchange Server 2003 x86 (až 18.8), 2007, 2010, 2013, 2016, 2019 (pouze 64bitová verze)
- SharePoint Server 2003, 2007, 2010, 2012, 2016, 2019 (pouze 64bitová verze)

Koncová zařízení s aplikací AVG 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

Správa oprav AVG Business

Pouze Windows:

- 7 SP1 nebo vyšší, 8.x, 10
- Server 2008 R2 s nejnovější aktualizací Service Pack kromě Server Core, 2012, 2016, 2019
- Exchange Server 2010 SP2, 2013, 2016

Požadavky na nastavení firewallu pro účely konzole

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

Porty

TCP a UDP:

- 80 – kontroly zranitelnosti na internetu a aktualizace funkcí
- 443 – vyjednávání se šifrovacím klíčem FFL
- 8080, 8090 – komunikace mezi konzolí a klienty v místní síti (pouze On-Premise Console)
- 4158 – zrcadlo pro aktualizace v rámci místní sítě
- 7074 – vzdálené nasazování v rámci místní sítě

Webové adresy

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

Nastavení konzole

Cloud Console

1. Přejděte na https://console.avg.com/.
2. Klikněte na možnost **Zaregistrovat** a zadejte všechny požadované údaje, abyste si mohli vytvořit účet.

On-Premise Console

1. Přejděte na https://www.avg.com/en-us/installation-files-business.
2. Na kartě Firma klikněte u položky AVG On-Premise Management Console na tlačítko **Stáhnout**.

V případě On-Premise Console se řiďte postupem instalace podle příslušného operačního systému, který je uvedený v tématu Správa konzole On-Premise Console.

Aktivace licencí na konzoli Management Console

Aktivační kód dostanete v potvrzení nákupu. Společně s ním dostanete i informace o zakoupené edici. Tento kód slouží k aktivaci licence na software.

1. Při prvním spuštění konzole se vám zobrazí žádost o zadání licenčního kódu.
2. Zadejte licenční kód.
3. Klikněte na možnost **Aktivovat licenční kód**.

Aktivace dalších licencí

1. Přejděte na stránku *Předplatná*.
2. Proveďte jeden z následujících úkonů:
   - Pokud máte licenční kód, klikněte na možnost **Máte aktivační kód?**, kód zadejte a klikněte na možnost **Aktivovat**.
   - U předplatného, které chcete koupit, klikněte na tlačítko **Koupit** a dokončete transakci.

Přiřazování licencí k zařízením

Tato akce je možná až po přidání zařízení do sítě.

Tento postup vyžaduje restart zařízení.

1. Na stránce *Zařízení* proveďte jeden z následujících úkonů:
   - Chcete-li zahrnout všechna zařízení ve skupině, u názvu skupiny klikněte na tlačítko **Více**. Pak klikněte na možnost **Upravit skupinu**.
   - Chcete-li zahrnout několik zařízení, zaškrtněte příslušná pole. Pak klikněte na možnosti **Akce** ▸ **Změnit předplatné**.
   - V případě jednoho zařízení klikněte na tlačítko **Více** umístěné u daného zařízení a pak klikněte na možnost **Změnit předplatné**.
2. Z rozevíracích nabídek vyberte licenci, kterou chcete použít.
3. U licence, kterou chcete použít, klikněte na tlačítko **Použít**, případně, pokud měníte předplatné pro celou skupinu zařízení, klikněte na tlačítko **Uložit skupinu**.

Přidání zařízení přes instalační soubor nebo sdílený odkaz

Cloud Console a On-Premise Console

Stažení instalačního programu

1. Zvolte potřebný typ instalačního programu:
   - Soubor .exe pro Windows (pracovní stanice a servery)
   - Soubor .msi pro Windows (nasazení pomocí GPO)
2. Vyberte předplacené produkty.
3. Kliknutím na položku **Pokročilá nastavení** zobrazte následující možnosti.
4. Vyberte skupinu a pravidlo, které bude zařízení používat.
   - **Pokud chcete, můžete zaškrtnutím příslušného pole aktivovat zařízení a vybrat požadovaná předplatná až po instalaci.**
5. Vyberte, zda chcete ze zařízení automaticky odebrat konkurenční antivirové produkty.
   - **Možnost odebrání konkurenčních antivirových produktů je ve výchozím stavu zaškrtnutá. Doporučujeme, abyste tuto možnost při instalaci antivirové služby nechali zaškrtnutou.**
6. Vyberte velikost instalačního programu (Malý, nebo Úplný).
   - **Když vyberete Malý, 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 AVG.**
7. V pravidle, které nastavujete pro zařízení, zkontrolujte, zda jste správně nastavili případný proxy server.
8. Klikněte na tlačítko **Stáhnout** a určete, kam chcete instalační balíček stáhnout – například na flash disk nebo síťovou jednotku.

Pod tlačítkem *Stáhnout* můžete na této stránce také kliknout na možnost **Nasdílet odkaz ke stažení** a odeslat odkaz ke stažení. Soukromý odkaz ke stažení následně můžete zkopírovat a poslat požadovaným příjemcům.

Pouze On-Premise Console

Odeslání odkazu ke stažení e-mailem

Než z konzole On-Premise Console odešlete odkazy ke stažení, je nutné nastavit SMTP server.

1. Do pole *Příjemci* zadejte e-mailové adresy cílových uživatelů oddělené čárkami.
2. V případě potřeby upravte *předmět* odesílaného e-mailu.
3. Chcete-li upravit odesílaný e-mail, zaškrtněte pole *Zadejte svou vlastní zprávu* a pak zadejte text zprávy.
4. Vyberte předplacené produkty.
5. Kliknutím na položku **Pokročilá nastavení** zobrazte následující možnosti.
6. Vyberte skupinu a pravidlo, které bude zařízení používat.
    - **Pokud chcete, můžete zaškrtnutím příslušného pole aktivovat zařízení a vybrat požadovaná předplatná až po instalaci.**
7. Vyberte, zda chcete ze zařízení automaticky odebrat konfliktní antivirové produkty.
    - **Možnost odebrání konkurenčních antivirových produktů je ve výchozím stavu zaškrtnutá. Doporučujeme, abyste tuto možnost při instalaci antivirové služby nechali zaškrtnutou.**
8. Vyberte velikost instalačního programu (Malý, nebo Úplný).
    - **Když vyberete Malý, 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 AVG.**
9. V šabloně nastavení, kterou nastavujete pro zařízení, zkontrolujte, zda jste správně nastavili případný proxy server.
10. Klikněte na tlačítko **Odeslat**.

Instalace na místního klienta

Až budete mít instalační soubor nebo odkaz ke stažení z konzole AVG Business Management Console, je třeba na koncová zařízení nainstalovat AVG Business Antivirus.

1. Instalační soubor zkopírujte do umístění, které je přístupné z koncového zařízení.

2. Dvojím kliknutím instalační soubor spusťte.
3. Když se zobrazí dotaz, zda smí aplikace provádět změny v zařízení, klikněte na možnost **Ano**.
4. Počkejte, než se AVG Business Antivirus nainstaluje na zařízení.
5. Na výzvu restartujte zařízení.
6. Zařízení by nyní mělo být k dispozici v konzoli.

Přidávání zařízení pomocí vzdáleného nasazení

Požadavky na vzdálené nasazení

- Přihlašovací údaje správce k počítači nebo doméně Windows. Pokud používáte přihlašovací údaje k doméně, uveďte i název domény: (např. VASE_DOMENA\uzivatel).
- Síťové údaje zařízení, na která provádíte nasazení. Podle těchto údajů dokážete zařízení najít v síti.
- Připravte počítače na instalaci klienta. Pokud instalujete Avast Business Antivirus, odinstalujte z nich veškerý ostatní antivirový software.

Na každém zařízení nakonfigurujte následující:

Windows Vista/7/8.x/10

Povolení datových přenosů WMI

- Spusťte příkaz NETSH: netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes

Povolení sdílených složek správců

- Otevřete Editor registru.
- Přejděte na: HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Vytvořte novou položku DWORD LocalAccountTokenFilterPolicy s hodnotou 1.

Povolení sdílení souborů a tiskáren

- V Ovládacích panelech klikněte na možnost Síť a internet ▸ Centrum síťových připojení a sdílení.

- Klikněte na možnost Změnit pokročilé nastavení sdílení a pak povolte Sdílení souborů a tiskáren.

Firewall

1. Přejděte do nastavení firewallu.
2. Přejděte do části Nastavení ▸ Profily ▸ Přímé připojení k internetu ▸ Aplikace ▸ Generic Host Process (a Generic Host Process(2)).
3. Povolte:
    - Data serverů DCOM
    - Server Microsoft DCOM
    - Data klientů DCOM (ve výchozím stavu by měla být povolená)
    - Klient Microsoft DCOM (ve výchozím stavu by měl být povolený)

Povolení služby DCOM

1. Spusťte příkaz dcomcnfg.
2. Přejděte do části Služba komponent ▸ Počítače.
3. Klikněte pravým tlačítkem na položku Tento počítač ▸ Vlastnosti.
4. Klikněte na kartu Výchozí vlastnosti.
5. Zaškrtněte pole *Povolit používání objektů DCOM v tomto počítači*.

Povolení služby RPC

1. Spusťte příkaz services.msc.
2. Najděte a povolte službu Vzdálené volání procedur (RPC).

Podrobnosti o vzdáleném nasazení

Vzdálené nasazení je k dispozici až poté, co jiným způsobem instalace přidáte do sítě nejméně jedno zařízení. Také je nutné určit Master Agenta. Proto je nejvhodnější, když první zařízení, které přidáte do sítě, budete používat jako Master Agenta. Níže najdete souhrn procesu vzdáleného nasazení:

Zjišťování zařízení

Proces zjišťování zařízení používá protokol ARP (Address Resolution Protocol) k pingování všech IP adres v podsíti s cílem zjistit jejich MAC adresu. V závislosti na síti to může zabrat až 15 minut i déle.

Když dostane odpověď s MAC adresou, proběhne reverzní vyhledání přes DNS, aby byl zjištěn název hostitele příslušné IP adresy. Když je obdržen název hostitele, vytvoří se záznam zařízení a uloží se do seznamu, který bude po dokončení zjišťování přenesen do webové služby.

Po dokončení úvodního ověřování bude proces automaticky pravidelně hledat hostitelská zařízení a porovnávat je s uloženým seznamem. Od této chvíle bude proces pouze přidávat nová hostitelská zařízení, ale nebude je odebírat.

Ověřování

Při vzdáleném nasazení jsou předávány přihlašovací údaje správců ze seznamu (VASE_DOMENA\uzivatelske_jmeno a heslo), dokud některý z nich neumožní přístup do cílového počítače. Pokud žádné z těchto přihlašovacích údajů nebudou fungovat, proces se ukončí a zobrazí chybovou zprávu.

Klient počká na provedené změny zařízení / přihlašovacích tabulek, aby zjistil, zda bylo něco označeno k nasazení (na základě MAC adresy hostitelského počítače).

Požadavky

Chcete-li automaticky nasadit antivirus na několik zařízení na dálku, musíte mít:

- Konzoli Cloud Console nebo On-Premise Console 6.0 a vyšší
- Antivirus 18.6 nebo vyšší
- Nejméně jedno nainstalované a aktivované zařízení
- Funkční Master Agent
- Zapnuté Sdílení souborů a tiskáren pro sítě Microsoft
- Operační systém Microsoft Windows podporovaný službou Active Directory
- Platné přihlašovací údaje k Active Directory s oprávněními správce
- Otevřené všechny potřebné porty (7074)

Nasazování instalačních programů na dálku

Testování sítě

1. Klikněte na možnost **Zahájit proces nasazení**.

- Pokud nemáte k dispozici Master Agenta, klikněte na možnost **Přidat nového Master Agenta** a podle pokynů nastavte Master Agenta.
- Pokud máte k dispozici nejméně jednoho Master Agenta, vyberte toho, kterého chcete použít.

2. V části Přihlašovací údaje k Active Directory zadejte následující údaje:
   - Doména
   - Uživatelské jméno
   - Heslo
3. Klikněte na možnost **Prohledat síť** a počkejte, než se dokončí zjišťování zařízení.

Nasazení v síti

1. V části *Skupiny Active Directory* přejděte na složku s nechráněnými zařízeními a zaškrtněte pole u zařízení, do nichž chcete provést nasazení.
2. Klikněte na položku **Určete nastavení instalačního programu**.
3. V části *Vyberte licenci* zvolte jedno z předplatných antiviru, která máte k dispozici.
4. V části *Nasadit ve skupině v konzoli AVG Business* proveďte jeden z následujících úkonů:
   - Vyberte skupinu.
   - Vyberte možnost **Zkopírovat strukturu skupiny Active Directory do vybrané skupiny**, abyste mohli použít existující strukturu skupiny Active Directory.
   - Vyberte pravidlo.
5. Vyberte, zda chcete ze zařízení automaticky odebrat konfliktní antivirové programy.
6. Klikněte na možnost **Zahájit nasazování v zařízeních**.
   - **Počkejte, než nasadíme antivirus do zařízení. Během toho můžete přejít na jiné stránky. Průběh vzdáleného nasazení můžete kdykoli zkontrolovat výběrem tlačítka Vzdálené nasazení, které najdete v navigační nabídce.**
7. Klikněte na tlačítko **Dokončit vzdálené nasazení**.

Konfigurace pravidel a komponenty

Hlavním nástrojem ke správě zařízení jsou pravidla, která představují skupiny bezpečnostních nastavení pro chování aplikace AVG Business Antivirus na koncových zařízeních s různými operačními systémy (pracovní stanice s Windows, servery s Windows a MacOS X). Veškeré změny pravidel jsou aplikovány v zařízeních a skupinách, které jsou k těmto pravidlům přiřazeny.

AVG Business Management Console obsahuje výchozí šablonu s doporučenou konfigurací. Tuto šablonu můžete použít, případně ji můžete duplikovat a přizpůsobit si ji. Také můžete vytvořit zcela novou šablonu. Výchozí šablonu nelze smazat, dokud nevytvoříte další pravidlo.

Jedno pravidlo obsahuje nastavení pro pracovní stanice i servery s Windows, takže není potřeba vytvářet samostatná pravidla pro každý operační systém. Můžete tak zároveň konfigurovat nastavení pro skupinu zařízení, která mají nainstalovaných několik typů operačních systémů. Pravidla můžete vytvářet kliknutím na možnost **Přidat pravidlo** na stránce *Pravidla*. Před výběrem nastavení jednotlivých komponent budete moci pravidlo pojmenovat.

Komponenty antiviru podle produktové licence

Komponenta	AVG File Server Business	AVG Email Server Business	AVG Business Antivirus	AVG Internet Security Business
Souborový štít	X	X	X	X
Webový štít			X	X
E-mailový štít			X	X
Behaviorální štít			X	X
Antispam			X	X
Zdokonalený firewall			X	X
Skartovač dat			X	X
Exchange		X		X
Sharepoint	X	X	X	X

Zapnutí a vypnutí komponent

Téměř všechny štíty a nástroje v aplikaci AVG Business Antivirus lze v pravidlech 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.

1. V pravidle, které nastavujete, vyberte kartu *Aktivní ochrana*.
2. Vyberte kartu příslušného operačního systému (Pracovní stanice s Windows, Server s Windows).
3. U komponent, které 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**.

Instalace a odinstalace komponent

Většina funkcí aktivní ochrany je instalována s aplikací AVG Business Antivirus. Přes pravidlo je ale můžete podle potřeby odinstalovat či znovu nainstalovat.

1. V pravidle, které nastavujete, vyberte kartu *Aktivní ochrana*.
2. Vyberte kartu příslušného operačního systému (Pracovní stanice s Windows, Server s Windows).
3. U komponent, které chcete změnit, proveďte jeden z následujících kroků:
    - Pokud komponenta ještě není nainstalovaná, klikněte na možnost **Nainstalovat komponentu**. Pak klikněte na možnost **Chápu, nainstalovat komponentu**.
    - Pokud už je komponenta nainstalovaná, klikněte u ní na tlačítko **Více** a pak klikněte na možnost **Odinstalovat komponentu**. Pak klikněte na možnost **Chápu, odinstalovat komponentu**.

Podrobnosti o konfiguraci jednotlivých komponent, které jsou k dispozici v pravidlech konzolí AVG Business Management Console, najdete v článku Konfigurace nastavení a pravidel v konzolích AVG Business Management Console.

Konfigurace výjimek

Zástupné znaky

Řada štítů a dalších komponent v aplikaci AVG 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:** `ab?.html` odpovídá souborům `abc.html`, `abd.html`, `abe.html` atd. a **neodpovídá** souboru `abc.htm`.
*	Nahrazuje nula nebo více znaků **Příklad:** `*mtl` odpovídá souborům `abc.html` a `d.html`. `*txt` odpovídá souborům `abc.txt`, `x.txt` a `xyztxt`.

Výjimky

Můžete nastavit výjimky, které budou uplatněny v jednotlivých štítech a komponentách AVG Business Antivirus. Stačí v pravidlech přejít na kartu *Nastavení antiviru*.

Veškeré změny výjimek v pravidlech jsou uplatňovány v síti každých 5 až 10 minut. Pravidla z konzole mají přednost před místními nastaveními.

1. Přejděte na kartu *Nastavení antiviru* pro požadovaný operační systém.
2. V části *Výjimky* proveďte jeden z následujících úkonů:
   - Klikněte na možnost **Cesty k souborům**, zadejte cestu k souboru, který chcete vyloučit, a pak klikněte na tlačítko **Přidat**.
   - Klikněte na možnost **Adresy URL**, zadejte webovou adresu, kterou chcete vyloučit, a pak klikněte na tlačítko **Přidat**.
3. Až budete hotoví, klikněte na možnost **Použít změny**.

Pokud máte několik typů operačních systémů, které používají stejné pravidlo, nezapomeňte přidat výjimky do této části na kartě Pracovní stanice s Windows a/nebo Server s Windows.

Konfigurace automatických aktualizací

Zařízení můžete nastavit, aby automaticky aktualizovala program AVG Business Antivirus a jeho virové definice.

Konfigurace aktualizací

Aktualizace jsou odesílány přímo přes servery AVG nebo přes libovolného nakonfigurovaného Master Agenta / místní aktualizační server v síti. Pokud jste vybrali ruční aktualizace, bude třeba instalovat aktualizace do všech zařízení v síti ručně přes stránku *Zařízení*.

Vytváření a konfigurace testů

Při nastavování testu můžete nakonfigurovat typy souborů a programů, které jsou testovány aplikací AVG Business Antivirus, a to za předpokladu, že jste vybrali typ Pokročilý test (Uživatelský, Po restartu). Proto v pravidlech nelze určovat hlavní nastavení toho, co má být testováno (výjimky ale určovat lze).

Typy testů

- **Rychlý test –** vyhledává běžné hrozby.
- **Úplný systémový test –** provádí podrobný test každého souboru na zařízení.
- **Test výměnných médií –** testuje jednotky USB a vyměnitelná média připojená k zařízení.
- **Uživatelský test –** umožňuje určit typy souborů, citlivost testu, fungování či akce a také zahrnout zkomprimované soubory.
- **Test po restartu (pouze MS Windows) –** testuje zařízení po spuštění.

Cloud Console

Vytváření naplánovaných testů

Plánovat lze jen rychlé a úplné systémové testy.

1. Přejděte na stránku *Pravidla*.
2. Klikněte na pravidlo, ke kterému chcete přidat plánované testy.
3. Klikněte na kartu **Nastavení služeb**.
4. Rozbalte část **Antivirové testy**.
5. Pro **Rychlý test** a **Úplný systémový test** nakonfigurujte následující:
    - **Četnost:** máte na výběr z možností Denně, Týdně a Měsíčně.
    - **Den v týdnu/měsíci:** zvolte, ve který den se má test spouštět.
    - **Čas zahájení:** vyberte, kdy se má test spouštět.
6. Po dokončení klikněte na možnost **Použít**.

Vytváření jednorázových testů

1. Na stránce *Zařízení* proveďte jeden z následujících úkonů:
    - V případě jednoho zařízení klikněte na tlačítko **Více**, které je umístěné napravo od názvu zařízení.
    - V případě několika zařízení zaškrtněte pole všech zařízení, která chcete do testu zahrnout, a pak klikněte na možnost **Akce**.
2. Najeďte myší nad **Antivirové testy**.
3. Klikněte na typ úlohy, kterou chcete vytvořit:
    - Rychlý antivirový test
    - Úplný systémový antivirový test
    - Pokročilé antivirové testy
4. Zadejte podrobnosti o testu a zvolte příslušná nastavení. Pak klikněte na tlačítko **Vytvořit**.

On-Premise Console

1. Klikněte na možnost **Otestovat zařízení**.
2. Vyberte typ testu:
    - **Rychlý test –** vyhledává běžné hrozby.
    - **Úplný systémový test –** provádí podrobný test každého souboru na zařízení.

- **Test výměnných médií –** testuje jednotky USB a vyměnitelná média připojená k zařízení.
- **Uživatelský test –** umožňuje určit typy souborů, citlivost testu, fungování či akce a také zahrnout zkomprimované soubory.
- **Test po restartu (pouze MS Windows) –** testuje zařízení po spuštění.

o Když vyberete Uživatelský test nebo Test po restartu, můžete nakonfigurovat další možnosti.

3. Pokud chcete nastavit úlohu jako opakovanou, vyberte možnost *Naplánovat test* a nastavte četnost (jednorázově, denně, týdně nebo měsíčně) a datum a čas zahájení.
4. Zadejte požadovaný název testu.
5. Klikněte na možnost **Spustit test**.

Veškeré hrozby odhalené při tomto testu jsou obvykle přesouvány do Virové truhly na zařízení. Tyto nálezy můžete prohlížet a spravovat v části Podrobnosti o zařízení.

Konfigurace testů

Konfigurace Testů po restartu

Testy po restartu jsou k dispozici pouze pro zařízení s Microsoft Windows a spouští se před spuštěním operačního systému.

Umístění k testování ve Windows: umožňuje z rozevírací nabídky vybrat přednastavená umístění a přidat je do seznamu k testování. V případě potřeby můžete také zadat cestu ke konkrétnímu umístění, které chcete testovat. Veškerá umístění, která nechcete testovat, můžete ze seznamu odebrat. Stačí kliknout na tlačítko Smazat.

Restartovat zařízení: umožňuje okamžitý restart zařízení, aby bylo možné spustit Test po restartu. Pokud toto pole nezaškrtnete, Test po restartu se spustí až při příštím spuštění zařízení.

Před restartem upozornit uživatele zprávou: zadejte text, který se zobrazí koncovému uživateli a který upozorní koncového uživatele, že se blíží restart zařízení.

Určete, kdy se zpráva výše zobrazí: vyberte, s jakým předstihem před restartem se má zpráva zobrazit: 1 minut, 10 minutu, 30 minut nebo 1 hodinu.

Heuristika: umožňuje antiviru zjišťovat neznámý malware. Analyzuje kód souborů a hledá v něm příkazy, které mohou naznačovat škodlivé úmysly. Výchozí nastavení je

Normální. Čím je citlivost vyšší, tím roste pravděpodobnost, že antivirus malware odhalí. Také tím však roste počet falešných pozitivních nálezů (souborů nesprávně identifikovaných jako malware).

PUP a podezřelé soubory: určete, zda chcete při testu vyhledávat potenciálně nežádoucí programy (PUP).

Rozbalovat archivy: určete, zda mají být při testu rozbalovány archivy (takové testy bývají pomalejší, ale podrobnější).

Při zjištění hrozby: určete, kterou akci má AVG provést, když zjistí hrozbu: Automaticky vyčistit, Přesunout do truhly, Opravit, Smazat nebo Žádná akce.

Zrušit test na pracovní stanici: určete, zda je možné zrušit probíhající test na pracovní stanici.

Konfigurace Uživatelských testů

Uživatelské testy vám nabízejí nejvíce možností nastavení toho, které soubory, složky, programy a procesy mají být aplikací AVG Business Antivirus testovány. V rámci jedné úlohy testování můžete vybrat různé možnosti testování pro pracovní stanice s Windows, servery s Windows a zařízení s MacOS X.

Konfigurace umístění

Z rozevírací nabídky můžete vybrat přednastavená umístění a přidat je do seznamu k testování. V případě potřeby můžete také zadat cestu ke konkrétnímu umístění, které chcete testovat. Veškerá umístění, která nechcete testovat, můžete ze seznamu odebrat. Stačí kliknout na tlačítko Smazat.

Karta Typy souborů

Můžete vybrat, zda mají být testovány všechny soubory (nejen běžné oblasti, kde se nacházejí hrozby). Dále můžete test nastavit, zda má poznávat typy souborů podle jejich obsahu (což vyžaduje testování celého souboru), nebo podle přípony (v takovém případě budou testovány jen soubory s příponami, které zadáte do pole zobrazeného po výběru této možnosti).

Karta Citlivost

Citlivost heuristiky: Heuristika umožňuje antiviru zjišťovat neznámý malware. Analyzuje kód souborů a hledá v něm příkazy, které mohou naznačovat škodlivé úmysly. Výchozí nastavení je Normální. Čím je citlivost vyšší, tím roste pravděpodobnost, že antivirus malware odhalí. Také tím však roste počet falešných pozitivních nálezů (souborů nesprávně identifikovaných jako malware). Emulace kódu rozbalují a testují soubory podezřelé na malwarový obsah v emulovaném prostředí, odkud nemohou zařízením nijak uškodit. Možnost *Používat emulaci kódu* je ve výchozím stavu zapnutá.

Citlivost: můžete vybrat, aby byly testovány celé soubory (v takovém případě budou testy pomalejší, ale podrobnější).

PUP a podezřelé soubory: určete, zda chcete při testu vyhledávat potenciálně nežádoucí programy (PUP).

Odkazy: určete, zda mají být při testech otevírány veškeré odkazy v souborech (v takovém případě budou testy pomalejší, ale podrobnější).

Karta Výkon

Priorita: určete prioritu testu na koncových zařízeních. Testy s vyšší prioritou jsou rychlejší, ale vyžadující více výpočetních prostředků.

Stálá mezipaměť: určete, zda chcete zrychlovat testy používáním stálé mezipaměti a/nebo zda chcete ukládat data o testovaných souborech do stálé mezipaměti (v takovém případě bude test pomalejší).

Přístup k souborům: určete, zda chcete test zrychlit čtením souborů v pořadí, ve kterém byly uloženy na disk (tato možnost je efektivní jen u svazků NTFS).

Karta Akce

Použít akci: určete akce, které mají být automaticky provedeny při zjištění viru, potenciálně nežádoucího programu (PUP) nebo podezřelého souboru. Máte na výběr z možností Automaticky vyčistit, Přesunout do truhly, Opravit, Smazat a Žádná akce.

Pokud AVG z nějakého důvodu nemůže provést hlavní akci, pokusí se provést akci zvolenou v části *Pokud se akce nezdaří, použít*

Možnosti: určete, zda má být zvolená akce provedena po restartu.

Zpracovávání infikovaných archivů: určete, zda chcete infikovaný soubor pouze odebrat z archivu (a když se to nepovede, nedělat nic dalšího), zda chcete infikovaný soubor odebrat z archivu (a když se to nepovede, odebrat celý archiv), nebo zda chcete odebrat celý archiv.

Karta Archivy

Určete, zda mají být při testování rozbalovány všechny soubory v archivech.

Konzole AVG Business Management Console nabízejí spoustu dalších funkcí a možností. Další informace najdete v naší znalostní databázi na https://businesshelp.avast.com/.