

## Nastavení bezpečnostního subsystému pro operační systém MS Windows

Bezpečnostní subsystém je založen na bázi endpoint management aplikací AppGuard a DriveLock. Aplikace DriveLock Device Control spravuje všechna vyměnitelná média a externí zařízení, přičemž umožňuje provádět následující řízení externích médií:

- Flexibilní kontrola všech externě připojených médií, umožňuje určit, kdo a kdy může používat konkrétní externí zařízení.
- Integrovaná kontrola toku dat umožňuje definovat, kdo smí číst nebo kopírovat soubory.
- Rozsáhlý audit operací se soubory, kdy lze sledovat, kdo zkopíroval který soubor, na jaké médium a kdy to bylo provedeno.

## Nastavení systému AppGuard

AppGuard zablokuje veškerý malware na úrovni jádra operačního systému, ještě než se dále rozšíří a způsobí škody a zaručuje tzv. Zero-day ochranu tj. zabrání v den 0 spuštění úplně nových, neznámých škodlivých kódů (malwarů).

### Technická specifikace

Umístění aplikace :        %systemdrive%\ProgramFiles(x86)\AppGuardLLC\AppGuard Enterprise

Typ spouštění služba Windows , AppGuardAgent.exe

Umístění auditních záznamů:

- %systemdrive%\Program Files (x86)\AppGuard LLC\AppGuard Enterprise\egalog.log a debuglog.log Logy aktuálního dne,

Následně se tyto záznamy přesouvají v šifrované podobě do následujících složky

- %systemdrive%\Program Files (x86)\AppGuard LLC\AppGuard Enterprise\{generovane ID}, tyto auditní záznamy je možné dešifrovat pouze přenosem na centrální AGMS konzoli

### Základní konfigurace AppGuardu

V případě systému AppGuard je nastavena nejprísnější politika Workstation – Locked, kdy jsou zablokovány některé funkce Windows, například Powershell a příkazový řádek., systém umožňuje spuštění běžných aplikací, které byly v okamžiku certifikace nainstalovány v notebooku. Tuto ochranu může pozastavit pouze administrátor po zadání bezpečnostní hesla (Pass Phrase).

## Zapnutí Administrátorského modu (deaktivace AppGuard)

Admin mode je určen k vypnutí všech ochranných mechanismů AppGuardu. Zapnutí admin mode se provádí přes poklepání na ikonu z oznamovací oblasti, kdy se otevře následující ovládací okno.

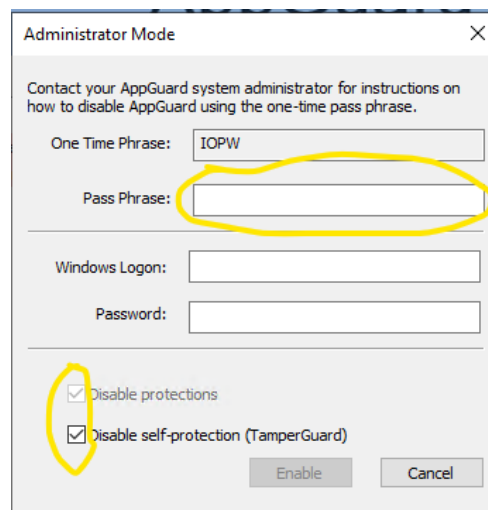
Stisknutím tlačítka **Advanced** otevřeme ovládací panel pro aktivaci admin mode

Je nutné označit volby:

- Disable
- protencions  
Disable self-  
protections

a vyplnit Pass Phrase<sup>1</sup>

Vše se potvrdí tlačítkem **Enable**



## Vypnutí Administrátorského modu (aktivace AppGuard)

Stejný postup jako u zapnutí je nutné odznačit volby:

- Disable protections
- Disable self-protections

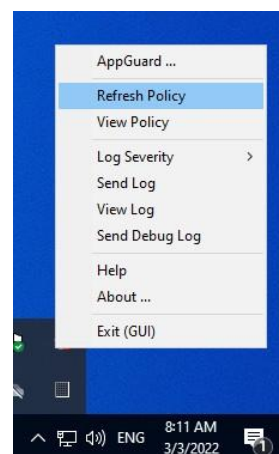
Vše se potvrdí tlačítkem **Disable**<sup>2</sup>.

## Nastavení nové politiky

V případě nutných změn nelze novou konfiguraci vytvářet v lokálním systému. Za tímto účelem je u dodavatele udržován aktuálně platný konfigurační soubor.

V případě nutné změny jsou tyto prováděny u dodavatele, přičemž po provedené změně je tento soubor konfigurace předán bezpečnostním nebo systémovému správci.

Vlastní aplikace nastavení se provádí tak, že dodaný konfigurační soubor se nahraje do složky %systemdrive%\ProgramData\Appguard\Policy. Nová politika se aplikuje po restartu Windows či vyvoláním volby **Refresh policy**.



<sup>1</sup> Pass Phrase je jedinečné heslo, které bylo předáno při úvodní instalaci

<sup>2</sup> Systém po startu (restartu) automaticky, bez ohledu na předchozí nastavení, startuje s vypnutým admin modem

## Nastavení systému DriveLock

DriveLock Device Control spravuje všechna vyměnitelná média a externí zařízení. Kontrola externích disků:

- Flexibilní kontrola všech externě připojených médií, správce určí, kdo a kdy může používat externí disky.
- Integrovaná kontrola toku dat prostřednictvím kontroly typu dat: Definujete, kdo smí číst nebo kopírovat které soubory.
- Rozsáhlý audit operací se soubory: Můžete sledovat, kdo zkopíroval který soubor, na jaké médium a kdy to bylo provedeno.

### Technická specifikace

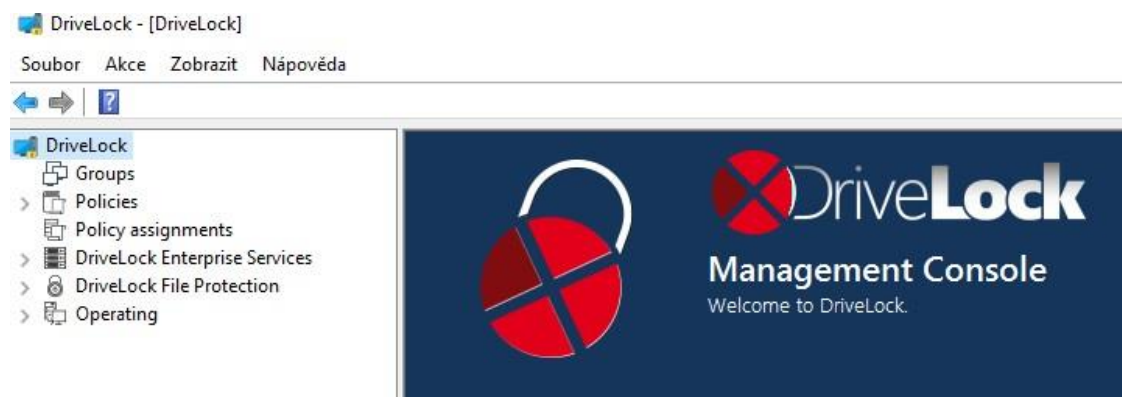
Umístění aplikace : %systemdrive%:\Program Files\CenterTools\DriveLock

Typ spouštění : služba Windows , proces DriveLock.exe

Umístění logů: využívá se integrovaný systém Windows dostupný přes Prohlížeč událostí

### Konfigurace politik

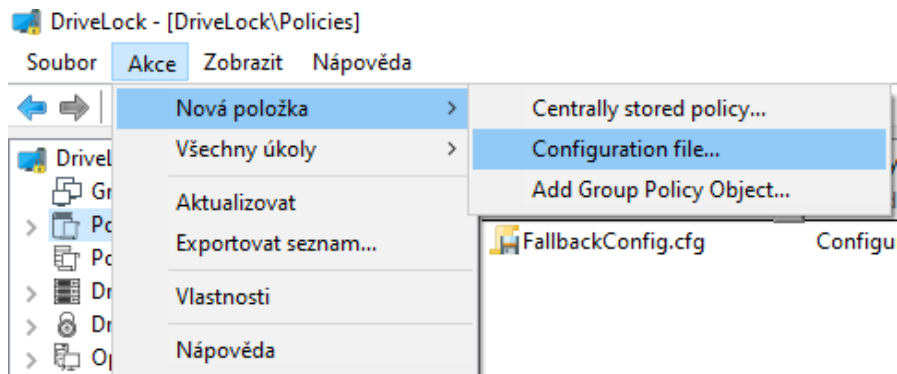
Jednotlivé politiky se konfigurují pomocí správcovské konzole DriveLock Management Console



správcovská konzole  
DriveLock

## Vytvoření politiky

Vybrat volbu Policies – horní menu Akce a dále postupovat dle obrázku Pro offline konfiguraci je nutné konfigurační soubor jako FallbackConfig.cfg



postup tvorby nové politiky

## Editace politiky

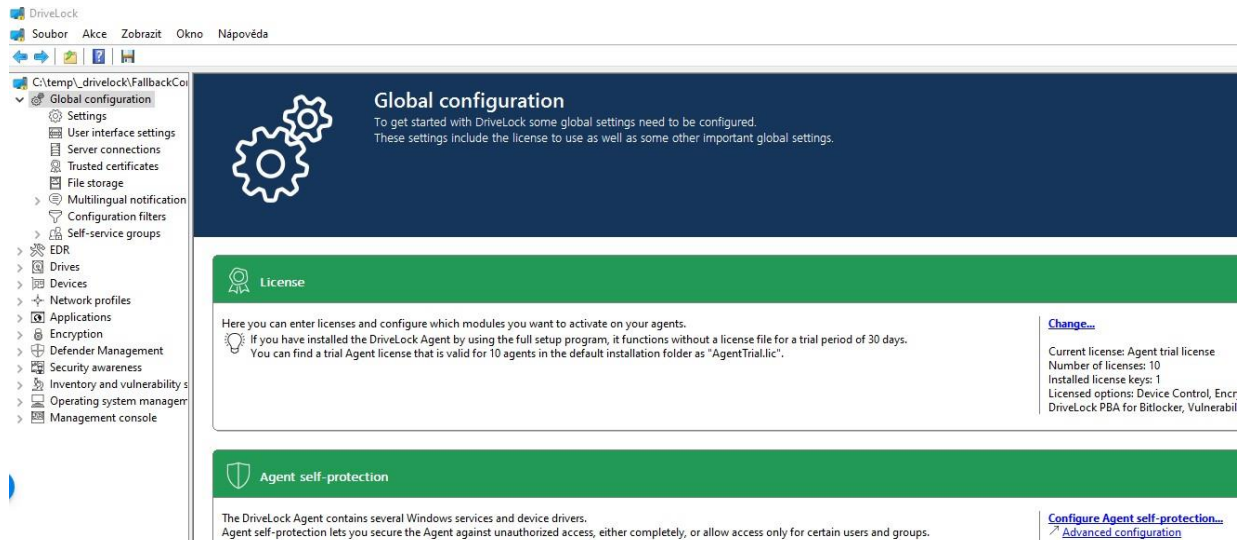
Příslušnou politiku lze v konzoli aplikace DriveLock editovat dvojklikem na vybraný soubor politiky, nebo přes pravé tlačítko a volbu **Edit**.

Policy name	Policy type	Size
Sem zadejte text	Sem zade...	Sem za...
FallbackConfig.cfg	Configuratio...	22,5 kB

## Globální nastavení agenta

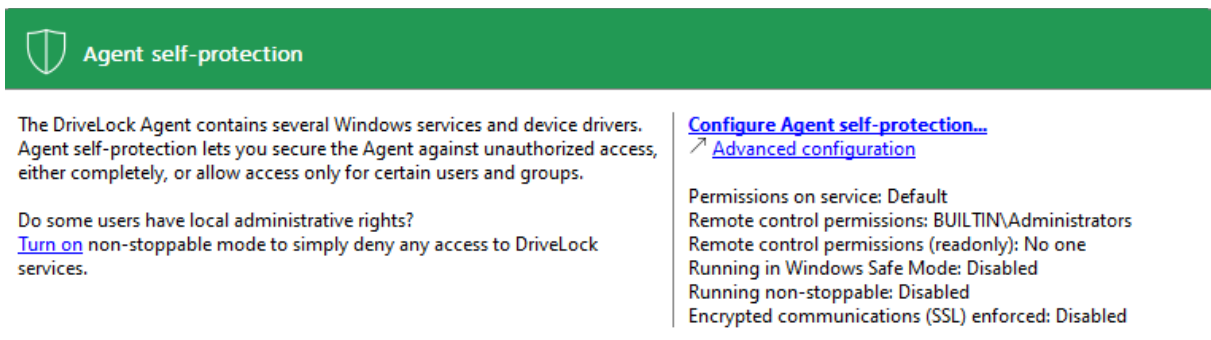
V sekci Global configuration lze nastavit zásadní parametry pro běh agenta, jako jsou:

- oprávnění na ukončení agenta,
- nastavení licence
- nastavení notifikací pro uživatele.
- nastavení notifikací pro uživatele.



The screenshot shows the DriveLock configuration interface. The left sidebar lists various settings categories like Settings, User interface settings, Server connections, etc. The main content area is titled 'Global configuration' and contains two sections: 'License' and 'Agent self-protection'. The 'License' section includes instructions on how to enter licenses and activate modules, with a 'Change...' link. The 'Agent self-protection' section provides information on securing the agent against unauthorized access, with a 'Configure Agent self-protection...' link.

### Globální nastavení agenta



**Agent self-protection**

The DriveLock Agent contains several Windows services and device drivers. Agent self-protection lets you secure the Agent against unauthorized access, either completely, or allow access only for certain users and groups.

Do some users have local administrative rights?  
[Turn on](#) non-stoppable mode to simply deny any access to DriveLock services.

[Configure Agent self-protection...](#)  
[Advanced configuration](#)

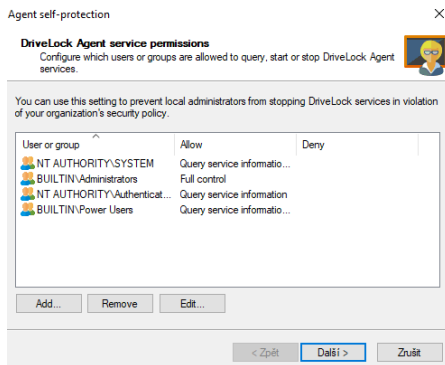
Permissions on service: Default  
 Remote control permissions: BUILTIN\Administrators  
 Remote control permissions (readonly): No one  
 Running in Windows Safe Mode: Disabled  
 Running non-stoppable: Disabled  
 Encrypted communications (SSL) enforced: Disabled

### zabezpečení agenta

## Zabezpečení agenta

Drivelock (vypnutí služby) je možné omezit pouze na určitou skupinu uživatelů. V případě nastavení aplikace příslušného notebooku je zvolena volba pouze pro uživatele ve skupině

„builtin\administrators“



### Agent self-protection and global security settings

These settings control how DriveLock protects itself against unauthorized access to Agent services, and global security settings for Agents.

#### Permissions on DriveLock Agent services (Not configured)

Configures which users or groups are allowed to query, start or stop DriveLock Agent services. You can use this setting to prevent local administrators from stopping DriveLock services in violation of your organization's security policy.

#### Run DriveLock Agent services in non-stoppable mode (Disabled)

Configures whether DriveLock Agent services can be stopped. You can use this setting to prevent all users from stopping DriveLock services.

#### Start DriveLock Agent in Safe Mode (Disabled)

Configures whether DriveLock is active when the computer is running in "Safe mode".

#### Password to uninstall DriveLock (Not configured)

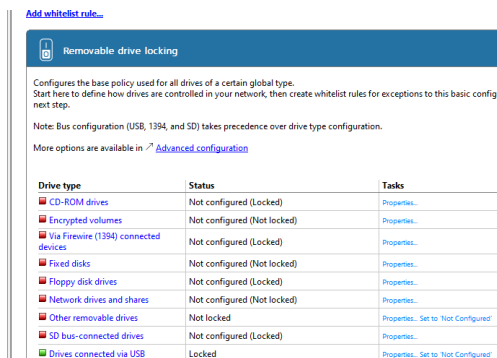
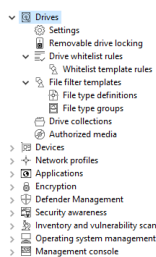
Configures a password that is required to uninstall the DriveLock Agent. Configure this option to prevent local administrators from uninstalling the DriveLock Agent.

## Zabezpečení agenta

## Nastavení správce disků

V této sekci lze povolit či zakázat připojení jednotlivých disků na základě rozhraní. V tabulce lze vidět, které rozhraní je zamčeno (Locked) či povoleno (Not locked).

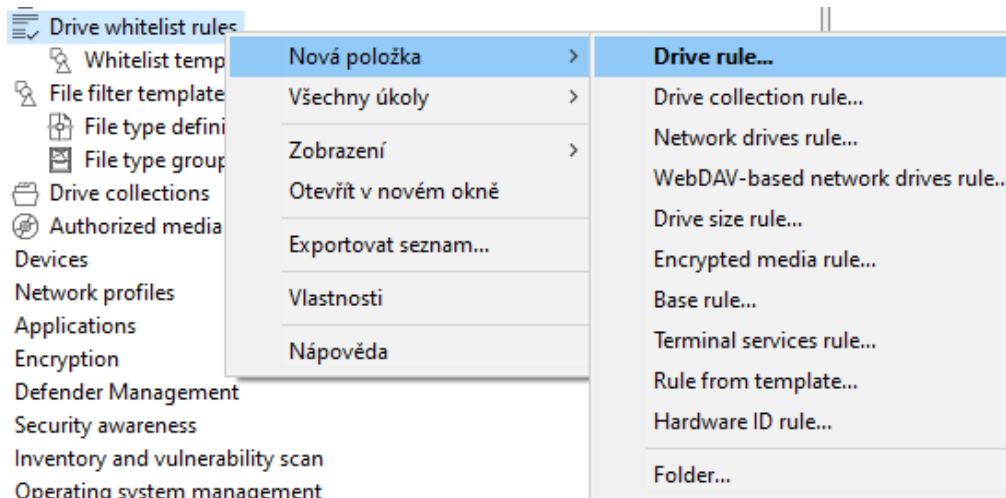
Nastavení správy externích disků je založeno na principu „Blacklist“ pro všechna zařízení a „WhiteList“ pro schválená zařízení (zakázat vše a povolovat výjimky).



## globální správa externích zařízení

Kliknutím na název rozhraní lze editovat stav. Lze povolit rozhraní na základě uživatelského účtu nebo v případě volby Deny (lock for all users) lze v sekci Drive whitelist rules povolit jednotlivá zařízení.

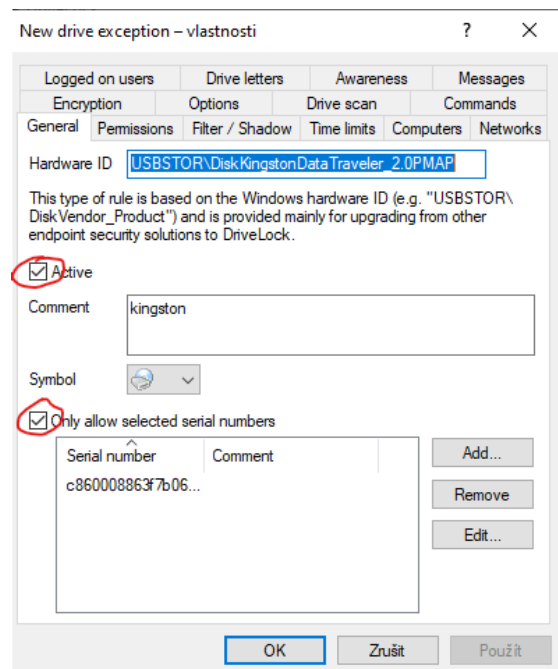
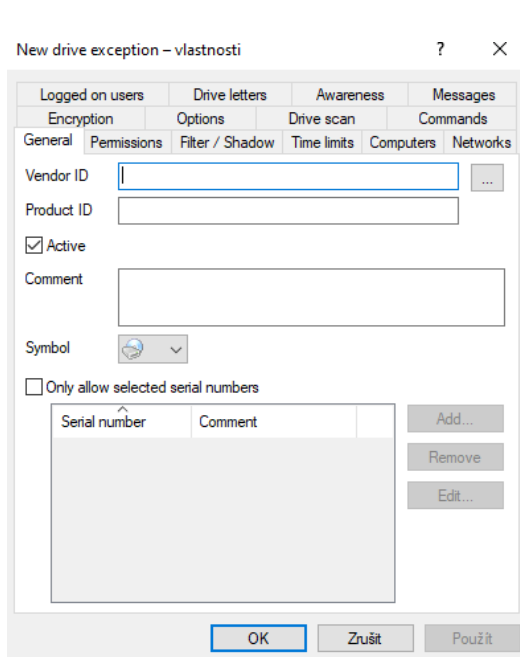
## Přidání nového zařízení



### Přidání nového zařízení

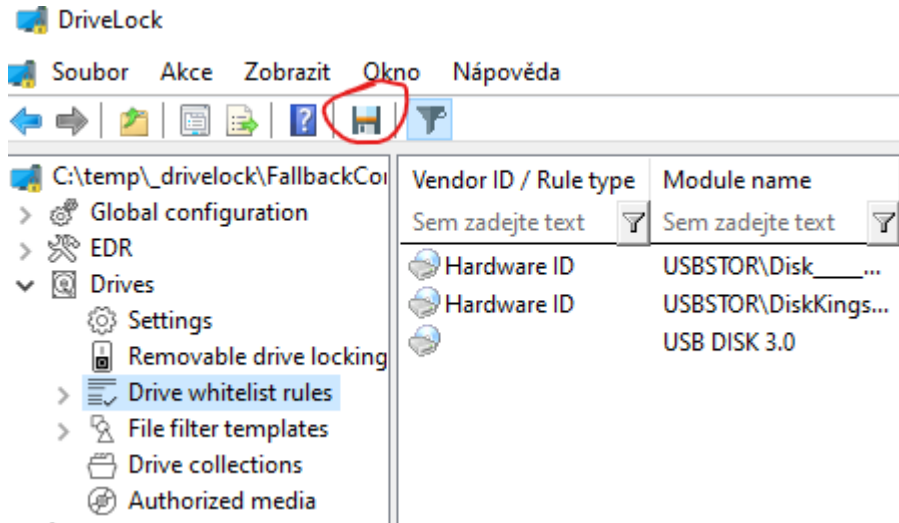
- 1) Právě tlačítko na položku menu
- 2) Výběr zařízení na základě připojených zařízení k danému počítači
- 3) Pro povolení zařízení musí být vybrána volba **Active**

Zároveň musí být nastavena volba omezení na základě sériového čísla (volba **Only allow selected serial numbers** )



## Aplikace politiky

- 1) Uložit v konzoli pomocí tlačítka **Uložit**



- 2) Zavřít okno politiky
- 3) Kopírovat uložený soubor **FallbackConfig.cfg** do systémové složky DriveLock - **C:\Program Files\CenterTools\DriveLock** ( přepsat stávající soubor )

Do umístění souboru s konfigurací se lze dostat například z okna hlavní konzole pomocí následující volby

- 4) Restartovat službu DriveLock



## Antivirová ochrana

K zajištění této funkcionality bude využíván program Windows Defender, který představuje klasický antivirový program v kombinaci se systémem AppGuard (viz předchozí bod)

---

U KPS bylo rozhodnuto, že offline aktualizace antivirových definic nebude prováděna. Bezpečnostní správce informačního systému má za to, že větší riziko, vzhledem ke konfiguraci notebooku představuje tato aktualizace než její neprovedení.

---

- Bezpečnostní správce / správce informačního systému zajistí, aby rezidentní část antivirového software byla aktivována při startu notebooku a pracovala při jeho běhu. Rezidentní ochrana notebooku bude zapnuta, a to včetně testování SSD a USB flash pamětí.
  - V případě, že je nalezen vir, je oprávněn jej odstranit správce informačního systému. Uživatel, který vir zjistil, neprodleně o této skutečnosti informuje Bezpečnostního správce informačního systému. Bezpečnostní správce informačního systému pak zajistí v součinnosti se správcem informačního systému provedení kompletních antivirových testů na všech nosičích utajovaných informací, které byly od poslední kompletní kontroly používány. V případě, že infikovaná data pocházejí od jiného subjektu, informuje Bezpečnostní správce informačního systému daný subjekt o zjištěném viru.
- 

Vzhledem k instalované technologii AppGuard lze konstatovat, že vir se z případně nakaženého souboru vzhledem k „sandboxování“ nebude v informačním systému šířit dále.

---