

VIRUS BUSTER

for NetWare Servers

TARTALOMJEGYZÉK

VIRUSBUSTER FOR NETWARE SERVERS	1
Minimális rendszerkövetelmények	1
Telepítés	2
Automatikus telepítés	2
Kézi telepítés	2
A program felépítése	4
Ellenőrzési lehetőségek	4
Védelmi egységek	4
A program felhasználói felülete	5
A program ismertetése	5
Vírusirtó opciók	6
Keresés/irtás módja	6
Párhuzamos keresőszám	8
Keresőmotor leállítása	8
Keresőmotor indítása	8
Védelmi egység (domain) kezelés	9
Üzenetek irányítása	11
Üzenetek keletkezési helyei	11
Üzeneteket kiváltó események	12
Az üzenetek címzettjei	13
Az üzenetek jellemzői	14
Globális opciók	15
Karantén	16
Információk	16
Futás közbeni opciók	16
Regisztráció	17
PROGRAMFRISSÍTÉS (UPDATE MANAGER)	18
Beállítások	18
Modulok verziói	19
Azonnali frissítés	19
Információk	20
VÉGFELHASZNÁLÓI SZERZŐDÉS	21
KAPCSOLAT	22

VIRUSBUSTER FOR NETWARE SERVERS

Hálózati környezetben a kiszolgálók biztonsága kiemelkedően fontos szerepet játszik vírusvédelmi szempontból, ugyanis mindennapi munkavégzésünkhöz használt anyagaink túlnyomó részének tárolása és továbbítása szervereink segítségével történik. Ezért a kiszolgálók védelme nem csak a tárolt adatok biztonságát, hanem a hozzájuk kapcsolódó kliens gépek másodlagos védelmét is biztosítja.

A VirusBuster for NetWare Servers az adatok, rendszerek és ezáltal munka folyamatos védelmét biztosítja a szerverek nagyobb adatforgalmára optimalizálva. A könnyen kezelhető, hagyományos NetWare alapú felhasználói felület, az egyszerűen áttekinthető és módosítható beállítások, valamint a gyakori frissítések biztosítják, hogy a lehető legnagyobb hatékonysággal, könnyen és átláthatóan működjön a Novell NetWare szerver védelme.

A termék főbb tulajdonságai

- Hatékony, állandó védelem a hálózatban lévő Novell szerverek számára a vírusokkal szemben
- Különálló védelmi területek a háttértárak vagy azok egységeinek egyedi kezelésére
- Intelligens fájlvédelem, kiterjesztett írásvédelem a fertőzések megelőzésére
- Manuális és időzített víruskeresés
- Automatikus frissítés
- Intelligens karantén a fertőzött fájlok elkülönítésére
- Inkrementális vírusadatbázis frissítés

Minimális rendszerkövetelmények

A program elindításához minimálisan a következő rendszerösszetevők jelenléte szükséges:

- Novell NetWare Server 5.1+SP8, 6+SP5, 6.5+SP8
- Intel alapú (vagy kompatibilis) processzor
- 1024 MB memória (Novell NetWare Server 6.x esetén 2048 MB)
- 150 MB szabad merevlemez-kapacitás

Telepítés

A termék telepítő fájlban (.exe), illetve **.zip** csomagban áll rendelkezésre. Előbbi segítségével automatikusan telepítheti a terméket, utóbbi csomagból manuális módon üzemelheti be a védelmet.

VirusBuster Novell Kisvállalati Csomag licenc (3 felhasználóig) igénybe vétele esetén, a licenc nyújtotta kedvezmények kihasználásához az **autoexec.ncf** fájlba el kell helyezni a **load nlsapi.nlm** sort – a VirusBuster termékekre való hivatkozások előtt –, majd a termék indítása előtt újraindítani a számítógépet.

Automatikus telepítés

A termék a következő csomagban áll rendelkezésre:

nwshield-<termékverzió>-<engine verzió>-<nyelv>.exe

Például:

nwshield-2.2.08-4.2.13-hu.exe

- Az üdvözlő képernyő és a licenc szerződés elfogadása után a telepítés célmappáját kell meghatározni, ebbe a mappába fog települni a termék.
- A célmappa meghatározása után a telepítendő modulok verziószáma olvasható, itt ellenőrizheti, milyen verziószámú modulok kerülnek telepítésre.
- A következő ablakban a telepítendő komponenseket határozhatja meg, a főprogram telepítése kötelező, a Frissítő választható.
- A **[Tovább]** gombra kattintás után beállíthatja a telepítés után végrehajtandó műveleteket, melyeket a telepítő megkísérel automatikusan elvégezni.

Figyelem!

Amennyiben valamely művelet nem kerül végrehajtásra, akkor azt a telepítés után manuálisan kell elvégeznie a kézi telepítési útmutató segítségével!

Az itt beállítható műveletek megfelelnek a *Kézi telepítés* fejezetben leírt műveleteknek.

VirusBuster for NetWare Servers

- *Védelem indítása:* Kiválasztásakor a telepítés után automatikusan elindításra kerül a védelem a szerveren.

- *autoexec.ncf fájl kiegészítése:* Kiválasztása esetén a telepítő kiegészíti az **autoexec.ncf** fájlt, a *Kézi telepítés* fejezetben leírt módon.

- *Regisztráció:* Kiválasztása esetén a telepítő bekéri a regisztrációs adatokat.

VirusBuster Frissítő modul

- *Modul indítása:* Kiválasztásakor a telepítés után a telepítő elindítja a Frissítő modult.

- Ha kiválasztotta a *Regisztráció* műveletet, akkor a következő ablakban megadhatja a termék regisztrációs adatait.
- Ezek után elkezdődik a telepítés, és a befejezést követően a kijelölt műveletek is végrehajtásra kerülnek.

Kézi telepítés

A termék a következő csomagban áll rendelkezésre:

nwshield-<termékverzió>-<engine verzió>-<nyelv>.zip

Például:

nwshield-2.2.08-4.2.13-hu.zip

A terméket a szerver **sys:** volume-án, egy - a felhasználó által létrehozott - alkönyvtárban kell elhelyezni, így az a konzolról indítható. A telepítést manuálisan végezze, célszerűen adminisztrátori jogokkal felruházott felhasználó nevében.

A program első telepítése során az alábbiak szerint kell eljárni:

- Valamely munkaállomásról adminisztrátorként bejelentkezve a szerveren a **sys:system** alkönyvtárban belül készítsen egy **vbuster** nevű alkönyvtárt a program számára. Ebben az alkönyvtárban jön létre a konfigurációs fájl, valamint itt keletkezik a napló fájl is, illetve a program itt hozza létre a **quar** (karantén) és a **temp** (átmeneti fájlok helye) könyvtárakat. A létrehozott alkönyvtárt vegye fel a **search path** listába: **search add sys:system/vbuster**
- Másolja a program fájljait a létrehozott alkönyvtárba (**VBShLD4.NLM**, **VBENGINE.NLM**, **VBUSTER.INI** és a vírusadatbázist (a **DATABASE** könyvtárat és tartalmát)). Automatikus termékfrissítés használatához szükséges még a **VBUPDATE.NLM** és **VBUPDASC.NLM** felmásolása is.
- A **sys:system/AUTOEXEC.NCF** fájl végére írja be a következő sort:
search add sys:system/vbuster és ha azt szeretné, hogy a szerver indításakor automatikusan induljon a védelem is, akkor a következő sor beszúrása is szükséges:
load vbshld4.nlm. A **sys:system/AUTOEXEC.NCF** fájl módosítása munkaállomásról tetszőleges szerkesztőprogrammal megtehető, a szerverről pedig az **NWCONFIG.NLM** fájl segítségével (NCF files options/ Edit AUTOEXEC.NCF file).
- A Novell NetWare rendszeradminisztrációs programjában hozzon létre egy új, kizárólag a vírusvédelem szolgálatára szánt felhasználói azonosítót (user) adminisztrátori jogokkal. Javasolt felhasználói név: *vbuster*. Ezt a felhasználót kell majd a program különleges/speciális felhasználóinak csoportjába felvenni.
- Indítsa el a szerveren a programot a **load vbshld4** paranccsal, majd végezze el a program konfigurálását.

Ha minden rendben lezajlott, a modulok betöltődnek és a konzol képernyő listájában két új bejegyzés lesz látható (VBSshield Screen és VBSshield Console).

A program felépítése

A program az általánosan használt Novell NetWare betölthető modul (NLM, NetWare Loadable Module) formájában áll rendelkezésre, melyet a kiszolgáló gépen kell futtatni. Betöltés után a modul ellenőrzése alá vonja a kiszolgáló összes fájlműveletét, s a fájlokat - melyekre a műveletek vonatkoznak - a művelet végrehajtása előtt megvizsgálja. Amennyiben a vizsgált fájlban vírust talál, a beállításoknak megfelelő intézkedés-sorozatot indít el: a műveletkérést megtagadhatja, a vírusos fájlt karanténba helyezheti, az ismert vírust eltávolíthatja, üzenetet vagy elektronikus levelet küldhet az érintett felhasználónak, a rendszergazdának vagy bármely más kijelölt személynek. A működés közben összegyűlt információkat naplófájlba menti.

A program lehetővé teszi egy, a Novell NetWare lehetőségeit kihasználó fájlhozzáférési jogosultsági rendszer definiálását is. Ennek segítségével egyszerűen megakadályozható a megjelölt hálózati könyvtárak vagy fájlok írása, s ezáltal vírusfertőzése.

Ellenőrzési lehetőségek

A program a fájlok ellenőrzését kétféle módon valósítja meg. Egyrészt megfigyelés alatt tartja a kiszolgálóra vonatkozó összes fájlműveletet, azaz minden esetben megvizsgálja a beérkező kéréseket és csak a vírusmentes fájlok hozzáférését engedi meg. Másrészt pedig megadott időben az egyes védelmi egységekre teljes körű ellenőrzés kérhető, mely indítható időzítve vagy azonnal a konzol menüjéből is.

- **Hozzáféréskori ellenőrzés**
A hozzáféréskori ellenőrzés esetén egy fájlhoz való hozzáféréskor (például a fájl olvasásakor) automatikusan ellenőrzi azt. Védelmi egységenként (domain) beállítható, hogy mely fájlok elérésekor történjen ellenőrzés. Erre a célra két lista szolgál, melyek egyike az ellenőrizendő fájlmaszkokat tartalmazza, míg a másik a kivételek maszkjait írja le.
- **Periodikus ellenőrzés**
A periodikus ellenőrzés esetén egy védelmi egység (domain) valamennyi ellenőrizendő fájljának vizsgálatára sor kerül. A periodikus ellenőrzés indítása történhet manuálisan és automatikusan is védelmi egységenként (domain) meghatározott időpontokban.
- **A fájlok írásvédelme**
A program a Novell NetWare hálózati operációs rendszer hozzáférés-védelmét kiegészítve képes megoldani a fájlok írásvédelmét. Az írásvédelem független a felhasználóktól, azaz minden felhasználóra egyformán érvényes. Védelmi egységenként (domain) engedélyezhető, illetve tiltható az írásvédelem működése és hasonlóképpen védelmi egységenként (domain) adható meg a védendő fájlok maszkjainak listája, illetve a kivételek listája is.

Védelmi egységek

A Novell NetWare jogosultságrendszeréhez hasonlóan a VirusBuster for NetWare Servers-ben a keresési és védelmi opciókat védelmi egységenként (domain) lehet megadni. Minden egyes védelmi egységhez tartozik a szerver egy alkönyvtár-struktúrája. Amennyiben ez az alkönyvtár nem tartalmaz (mélyebb szinten) újabb védelmi egységet, úgy az adott védelmi egység érvényességi köre kiterjed a megadott alkönyvtáron belüli valamennyi fájlra és alkönyvtárra, valamint azok alkönyvtáira is. Amennyiben viszont a védelmi egység alkönyvtára (mélyebb szinten) újabb védelmi egységet tartalmaz úgy az adott védelmi egység érvényességi köre már nem terjed ki az újabb védelmi egység alkönyvtárára, illetve az alatta lévő további alkönyvtárakra. Tehát minden fájl pontosan egy védelmi egységbe tartozik és egy védelmi egységen belül minden fájlra ugyanazok a védelmi beállítások érvényesek.

A program felhasználói felülete

A program funkcióit, beállításait a Novell NetWare környezetben megszokott menüszerkezeten keresztül lehet elérni. A program elindítása után annak funkcióit és beállításait menüpontokon keresztül érhetjük el.

A menürendszer használata

- Kurzor billentyűk, **PgDn**, **PgUp** - Mozgás az egyes menüpontok között.
- **Enter** billentyű - A menüpont kiválasztása.
- **ESC** billentyű - Almenüpontból, illetve a programból való kilépés.
- **F1** billentyű - Segítség megjelenítése.

A programban a konfigurálás alapegysége a lista. Egy listában lehet elemeket változtatni, törölni, felvenni, valamint egy listaelemet tovább kifejtve részletesebben konfigurálni a következőképpen:

Listák használata

- Kurzor billentyűk, **PgDn**, **PgUp** - Mozgás a listaelemek között.
- **Enter** billentyű - Egy, illetve több listabejegyzés kiválasztása.
- **F5** billentyű - Bejegyzések kijelölése, illetve a kijelölés törlése.
- **Delete** billentyű - Bejegyzés törlése.
- **Insert** billentyű - Új bejegyzés létrehozása.
- **F3** billentyű - Bejegyzés átnevezése.

Az időpont táblázat megadása során a megjelenő táblázatban a csillag (*) karakterrel kell megjelölni a kívánt időpontokat.

Időpontok megadása

- Kurzor billentyűk - Segítségükkel a táblázatban lehet mozogni.
- **F5** billentyű - Időpont intervallum kijelölése.
- **Insert**, illetve csillag (*) billentyű - Aktuális időpontot, illetve intervallum kijelölése.
- **Delete**, illetve **Space** billentyű - A kijelölés(ek) törlése.
- **Enter** billentyű - A kijelölés(ek) invertálása.

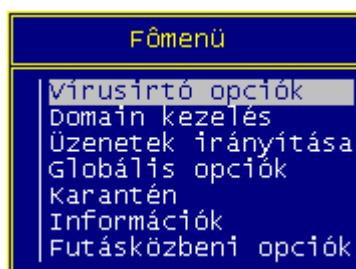
A program ismertetése

A terméket a **VBSHLD4.NLM** modul indításával aktivizálhatja. A program két képernyőt hoz létre:

- VBShield Screen - Itt követhetők nyomon a program által végzett tevékenységek, illetve az utoljára történt események.
- VBShield Console - Itt történik a program konfigurálása, itt állíthatók be az egyes opciók, illetve a periodikus ellenőrzések manuális végrehajtása is itt kezdeményezhető.

Figyelem!

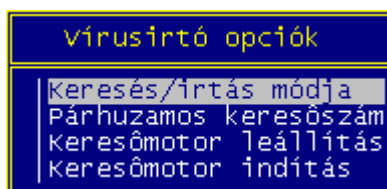
A menürendszerből való kilépés, illetve a menü bezárása egyben a programból való kilépést is eredményezi, megszűnnek az azonnali ellenőrzések és leállnak a periodikus keresések is!



A program főmenüje

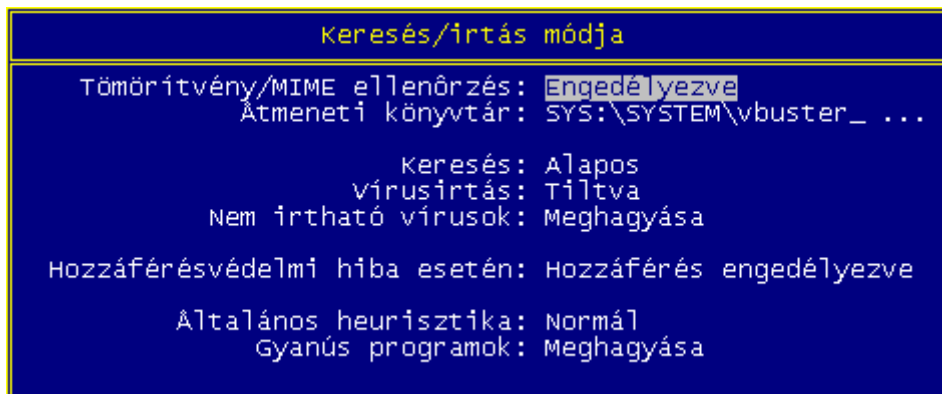
A programot az egyes menüpontokon haladva ismerheti meg részletesebben.

Vírusirtó opciók



Vírusirtó opciók

Keresés/irtás módja



Keresés/irtás módja

Tömörítvény/MIME ellenőrzés

Tömörített és MIME (levélformátumú) fájlok vírusvizsgálatának engedélyezése/tiltása.

Átmeneti könyvtár

Az itt megadott könyvtárba helyezi ideiglenesen a program a tömörített/MIME fájlok tartalmát ellenőrzéskor.

Keresés

A keresés módját állíthatja be ebben a pontban:

- *Gyors*
Szigorúan csak a fájl azon részeiben keres vírust, ahol az előfordulhat, néhány olyan vírustípust nem ismer fel, melyek megkeresése nagy erőforrást igényel (pl.: Excel FORMULA vírusok)
- *Alapos*
Optimalizált keresési mód, mely minden – az adatbázisban regisztrált – vírust felismer, a fájl azon részeiben keres vírust, ahol az előfordulhat.
- *Teljes*
Minden – az adatbázisban regisztrált – vírust felismer, a teljes fájlt leellenőrzi, azokat a részeket is, ahol normális esetben nem fordulhat elő vírus. E keresési forma erősen időigényes.

Vírusirtás

Engedélyezése után a program - amennyiben képes rá - kiírtja a vírust a fertőzött fájlból.

Nem irtható vírusok

A vírusok egy részét, bár a felismerés megtörténik, nem lehetséges eltávolítani a fájlból, mert nem lehetne már visszaállítani az eredeti fájlt, illetve vannak vírusok, melyek csak törléssel irthatóak. Itt rendelkezhet, hogy mi történjen ezzel a vírusos állománnyal:

- *Fájl átnevezése*: átnevezi a vírusos fájlt.
- *Fájl karanténba*: karantén könyvtárba mozgatja a vírusos fájlt.
- *Meghagyása*: nem nyúl a fertőzött fájlhoz.
- *Fájl törlése*: törli a fertőzött fájlt.

Hozzáférés-védelmi hiba esetén

Eldöntheti, hogy amennyiben a vírusvédelem fájl-elérési hibát talál, engedje-e érvényre jutni a kívülről érkező, a fájlra vonatkozó kérelmet vagy sem.

Általános heurisztika

A heurisztikus keresési módot kapcsolhatja ki-, illetve be, továbbá az érzékenység beállítása is ebben a pontban történik. Heurisztikus kereséskor a program megpróbálja felismerni az adatbázisában nem regisztrált, vírusokra jellemző tulajdonságokkal bíró kódrészletet, programot. Ha talál ilyen vírusgyanús fájlt, azt jelzi a felhasználónak.

A heurisztikus keresés erősségi szintjének beállítása:

- *Kikapcsolva*
Nincs heurisztikus keresés.
- *Normál*
Limitált a vizsgálat mélysége, kicsi a vakriasztások valószínűsége, de az ismeretlen vírusokat is kisebb valószínűséggel azonosítja.
- *Erős*
Nagyobb valószínűséggel azonosít ismeretlen vírusokat, de a vakriasztások valószínűsége is nagyobb.

Gyanús programok

Itt adhatja meg mi történjen a heurisztika által gyanúsaként vélt fájlokkal:

- Fájl átnevezése: átnevezi a vírusosnak vélt fájlt.
- Fájl karanténba: karantén könyvtárba mozgatja a fájlt.
- Meghagyása: nem nyúl a fertőzöttnek vélt fájlhoz.
- Fájl törlése: törli a gyanús fájlt.

Párhuzamos keresőszám

Az keresőmotorban egy időben indítható keresőszálak száma állítható be ebben a pontban.

Párhuzamos keresőszám

Összes keresőszám:
(Max.: 16, min.: 2!)

Hozzáférés-ellenőrzésre fenntartva:
(Max.: összes-1, min.: 1!)

Párhuzamos keresőszálak számának beállítása

Figyelem!

A beállított értéknek 2 és 16 között kell lennie. Az új érték mindig csak a kereső-motor újraindítása után lép érvénybe!

Alapértelmezés szerint a program négy keresőszállal dolgozik. Az engedélyezett szálak közül kettő fenn van tartva a beérkező kérések fogadására, a hozzáférési keresés céljaira. A keresőszálak számának megemlése mérlegelést kíván, mert bár egyszerre több fájl ellenőrzése történhet meg több szál aktivitása esetén, ám ez egyben a kiszolgáló gép erőforrásainak fogyasztásával jár együtt.

Keresőmotor leállítása

Viszonylag ritkán fordul elő, hogy a keresőmotort a víruskereső egészétől függetlenül kívánjuk leállítani, mégis hasznos lehet, ha a program frissítéséhez a motort leállíthatjuk, hiszen így mód nyílik "menet közbeni" keresőmotor-cserére is.

Figyelem!

A keresőmotort leállítva a védelem még aktív marad, bár vírusvizsgálat nem történhet. Ez kívülről szemlélve bizonyos fájlok elérhetetlenségét eredményezi!

Keresőmotor indítása

A keresőmotor indítása és az aktuális VDB betöltése, a beállított keresőszál számmal.

Figyelem!

Ügyeljen arra, hogy a megfelelő **VBENGINE.NLM** és vírusadatbázis fájlok rendelkezésre álljanak a search path-ban! A **VBENGINE.NLM** csak akkor indul, ha létezik a vírusadatbázis, valamint a **VBENGINE.NLM** a megfelelő verzióval!

Védelmi egység (domain) kezelés

A "Domain bejegyzések" ablakban a program megjeleníti valamennyi védelmi egység (domain) nevét. Ebben a listában lehet újabb védelmi egységeket létrehozni, a meglévőket törölni, illetve átnevezni.

A / (root) védelmi egység nem törölhető és nem nevezhető át. Egy védelmi egység átnevezése (F3 billentyű) esetén valamennyi, az adott védelmi egységre vonatkozó hivatkozás az új domain névre változik. Törlés (Delete billentyű) esetén a hivatkozások törlődnek, ha ezzel valamely üzenet irányítási egység érvényét vesztené, úgy a program figyelmeztetést ad. Amennyiben a törlendő, illetve átnevezendő védelmi egységen éppen a periodikus ellenőrzés fut, úgy az azonnal leáll. Új védelmi egység létrehozása esetén az új védelmi egység az üzenet-irányítási egységekben szereplő beállításokat örökli attól a védelmi egységtől, amelyik ki volt jelölve az **Insert** billentyű megnyomásakor.

Figyelem!

A konfigurálás időtartama alatt az adott védelmi egység inaktívvá válik, ezért üzemszerű működés közben ne hagyja nyitva a konfigurációs ablakot!

Egy védelmi egység kiválasztása esetén a következő beállításokat eszközölheti:

```

SYSTEM

A domain alkönyvtára: SYS:SYSTEM

Hozzáféréskori ellenőrzés: Engedélyezve
Teendő vírustalálatnál: Hozzáférés tiltása
Periodikus ellenőrzések: (időpont táblázat)
Ellenőrzendő file-ok: (lista)
Kivételek: (lista)

File-ok írásvédelme: Engedélyezve
Írásvédett file-ok: (lista)
Kivételek: (lista)

```

Védelmi egység beállítások

A domain alkönyvtára

Minden egyes védelmi egység rendelkezik egy alkönyvtárral. Ezt az alkönyvtárat adhatja meg ebben a pontban. Megadásakor mindig teljes útvonalat kell megadni **volume név:elérési út** alakban. Az **elérési út** megadásánál az egyes könyvtárak a "/", illetve a "\" jellel is elválaszthatók.

Hozzáféréskori ellenőrzés

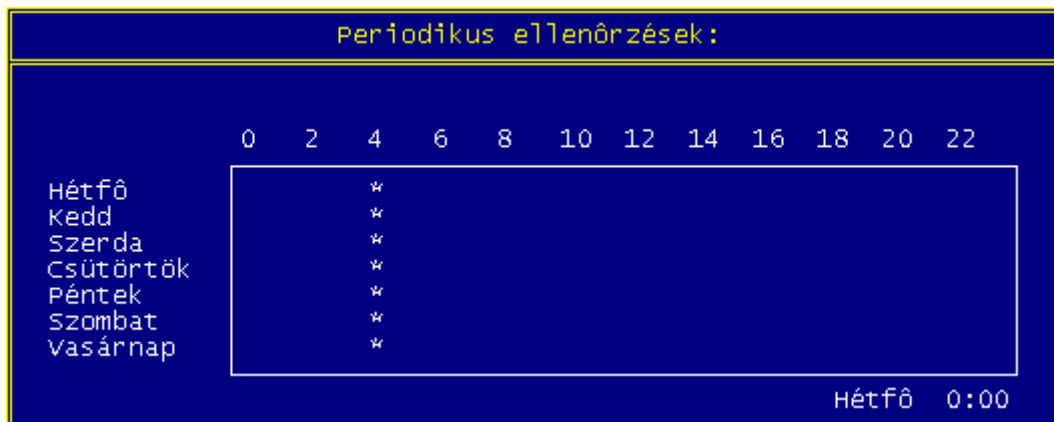
Engedélyezhető, illetve letiltható a szerveren tárolt fájlok hozzáféréskori ellenőrzése. Engedélyezése esetén egy fájl hozzáférésekor a program elvégzi a fájl vírusellenőrzését.

Teendő vírustalálatnál

Amennyiben a hozzáféréskori ellenőrzés engedélyezve van, úgy ezen opció beállításával megadható, hogy a hozzáféréskori ellenőrzés során egy esetleges vírustalálat esetén mi legyen a további teendő:

- Fájl átmozgatása: a fertőzött fájlt a Globális opciók/Vírusgyűjtő alkönyvtár mezőben megadott alkönyvtárba mozgatja.
- Hozzáférés tiltása: megakadályozza a fertőzött fájl hozzáférését.
- Semmi: nem nyúl a fertőzött fájlhoz.
- Fájl törlése: törli a fertőzött fájlt.

Periodikus ellenőrzések



Periodikus ellenőrzés beállítása

Az időponttáblázat beállításával 30 perces időközönként megadhatja, hogy heti rendszerességgel mely időpontokban történjen periodikus ellenőrzés az adott domain alkönyvtárain belül. Amennyiben a vírusvédelmi program elindulásakor azt tapasztalja, hogy egy domain-en az aktuális félórában kell periodikus ellenőrzést végezni, úgy az adott domain-en a periodikus ellenőrzést haladéktalanul elvégzi.

Ellenőrizendő fájlok

Itt adhatja meg a hozzáféréskori ellenőrzés alkalmával ellenőrizendő fájlok maszkjait (például: *.com, *.exe, *.doc).

Kivételek

Itt adhatja meg a hozzáféréskori ellenőrzés alkalmával kivételként kezelendő fájlok maszkjait (például: command.com).

Fájlok írásvédelme

Ebben a pontban engedélyezhető, illetve tiltható a vírusvédelmi program fájl szintű írásvédelmi lehetősége. A fájlok írásvédelme a speciális felhasználókra nem vonatkoznak.

Írásvédett fájlok

Itt adhatja meg az írásvédelem alá eső fájlok maszkjait.

Kivételek

Itt adhatja meg az írásvédelem alkalmával kivételként kezelendő fájlok maszkjait.

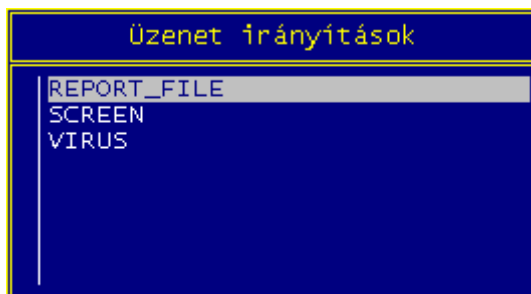
! Megjegyzés!

Amennyiben a program könyvtárában nem létezik konfigurációs fájl (VBUSTER.CFG), úgy a program indításával létrejönnek az alapértelmezés szerinti védelmi egység bejegyzések. Ezen védelmi egység bejegyzések szerint a hozzáféréskori ellenőrzés valamennyi, a szerveren elhelyezett, futtatható fájlban megtörténik. A periodikus ellenőrzést a program naponta egyszeri alkalommal 4:00-kor végzi el valamennyi domain valamennyi futtatható fájlján. Az alapértelmezés szerinti védelmi egység beállítások esetén a fájlok írásvédelme csak a SYS:LOGIN, SYS:PUBLIC és a SYS:SYSTEM alkönyvtárakban elhelyezett futtatható fájlokra vonatkozik.

Üzenetek irányítása

Az üzenetek irányítása almenüben a program megjeleníti valamennyi üzenet-irányítási egység nevét. Ezen a listában lehet újabb üzenet-irányítási egységeket létrehozni, a meglévőket törölni, illetve átnevezni. Egy üzenet-irányítási egység kiválasztása esetén az egység opciói állíthatók.

- Figyelem!**
A konfigurálás időtartama alatt az egység inaktív marad!

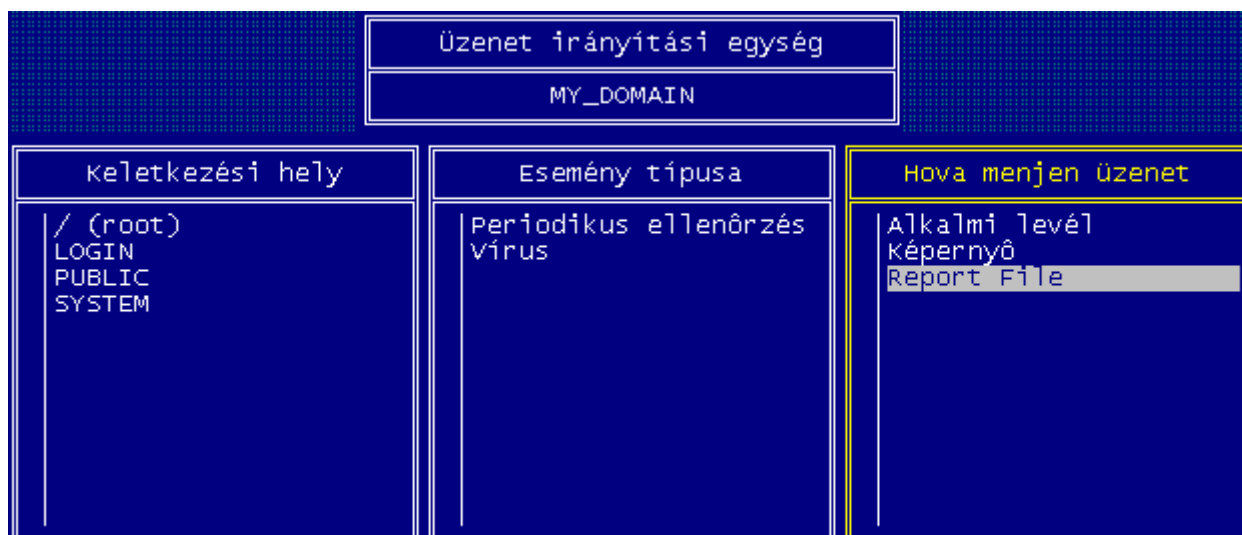


Alapértelmezett üzenet-irányítási egységek

Alapértelmezésben három üzenet-irányítási egység létezik a programban:

- Report_file - Napló fájl, melybe rögzítheti a rendszer működése során bekövetkezett események adatait.
- Screen - A VBSshield Screen képernyőüzenetei
- Virus - Vírustalálathoz aktivizálódó üzenetirányítási egység.

Egy üzenet-irányítási egység konfigurálása során meg kell adni, hogy az egység mely helyen és milyen esemény hatására keletkezett üzeneteket továbbítsa, valamint, hogy hova továbbítsa az üzeneteket.



Üzenetek panel

Üzenetek keletkezési helyei

Az üzenet irányítási egység keletkezési helye az alábbi beállításokat tartalmazhatja:

Általános

Azon üzenetek keletkezési helyét írja le, amelyek védelmi egységekhez nem köthetők. Amennyiben egy üzenet-irányítási egység tartalmazza az "általános" keletkezési hely kijelölést, úgy az üzenet irányítási egység a programon belül keletkezett, védelmi egységekhez nem köthető üzeneteket is továbbíthatja.

Domain név

Amennyiben valamely üzenet irányítási egység keletkezési hely rovatában szerepel egy védelmi egység neve, úgy az üzenet-irányítási egység a megadott védelmi egységen belül keletkezett üzenetekre is vonatkozik. Új védelmi egység létrehozása esetén az új védelmi egység az üzenet-irányítási egységben szereplő beállításokat attól a védelmi egységtől örökli, amelyik ki volt jelölve az **Insert** billentyű megnyomásakor. Természetesen ezek a beállítások módosíthatók.

Üzeneteket kiváltó események

Az üzenet irányítási egység az üzenetek keletkezését kiváltó eseményeket négy fő csoportba sorolja:

Fájl védelem

A program fájlvédelmi rendszere által kiváltott eseményeket írja le. Beállítása esetén az üzenet irányítási egység a keletkezési hely listában felsorolt védelmi egységeken belül történt illegális írási kísérlet során keletkezett üzeneteket továbbítja.

Információ

A program által kiváltott azon eseményeket írja le, amelyek a program ellenőrzési, illetve védelmi rendszerével nincsenek kapcsolatban. Beállítása esetén az üzenet-irányítási egység az alábbi üzeneteket továbbíthatja:

- Alkalmi levél elküldve: Egy alkalmi levél elküldése során a program nyugtázó üzenetet generál. Az opció beállítása esetén az üzenet-irányítási egység ezt az üzenetet is továbbítja.
- Komponens: Az opció engedélyezése esetén a külső komponens üzenetei is bejegyzésre kerülnek.
- Víruskereső motor: Az egység minden, a keresőmotorhoz kapcsolódó üzenetet továbbít az opció engedélyezése esetén.
- Fájl átmozgatva: Vírustalálat esetén, miután a fertőzött fájlt a megadott könyvtárba mozgatta, illetve átnevezte, akkor egy informális üzenetet küld. Ezen üzenetek naplózásával lehetőség nyílik a fájlok esetleges visszaállítására.
- Hiba: Bármilyen a programon belül előforduló hiba előfordulása egy üzenetet generál. Az opció beállítása esetén az üzenet irányítási egység a hibát leíró üzenetet is továbbítja.
- Víruskereső-motor hiba: Az opció engedélyezése esetén a program minden hibaüzenetet továbbít, mely a víruskereső motorhoz kapcsolódik.
- Konfiguráció változott: Az opció beállítása esetén az program konfigurációjának megváltozása esetén létrejött üzeneteket továbbítja.
- NLM elindult: Az opció beállítása esetén a program elindulásakor létrejött üzenetet továbbítja.
- NLM leállt: Az opció beállítása esetén a program leállításakor létrejött üzenetet továbbítja.
- Rendszeres levél elküldve: Egy rendszeres levél elküldése során a program nyugtázó üzenetet generál. Az opció beállítása esetén az üzenet-irányítási egység ezt az üzenetet is továbbítja.

Periodikus ellenőrzés

A program periodikus ellenőrzési rendszere által kiváltott eseményeket írja le. Beállítása esetén az üzenet irányítási egység a keletkezési hely listában felsorolt védelmi egységeken belül történő periodikus ellenőrzés állapotáról továbbíthatja az alábbi üzeneteket:

- Ellenőrizendő fájl: A program a periodikus ellenőrzés során egy új fájlhoz érkezett. Az opció beállítása esetén az üzenet-irányítási egység egy olyan üzenetet is továbbít, amely tartalmazza a védelmi egység, valamint a vizsgálandó fájl nevét.
- Ellenőrzés könyvtára: A program a periodikus ellenőrzés során egy új alkönyvtárhoz érkezett. Az opció beállítása esetén az üzenet-irányítási egység egy olyan üzenetet is továbbít, amely tartalmazza a védelmi egység, valamint a vizsgálandó alkönyvtár nevét.
- Ellenőrzés elindult: A program periodikus ellenőrzési rendszere periodikus ellenőrzést indít valamely védelmi egységen. Az opció beállítása esetén az üzenet-irányítási egység egy olyan üzenetet is továbbít, amely tartalmazza a védelmi egység nevét.
- Ellenőrzés leállt: A program periodikus ellenőrzési rendszere befejezte valamely futó periodikus ellenőrzését valamely védelmi egységen. Az opció beállítása esetén az üzenet-irányítási egység egy olyan üzenetet is továbbít, amely tartalmazza a védelmi egység nevét.
- Ellenőrzés megszakítva: A program periodikus ellenőrzési rendszere a felhasználó kérésére megszakította valamely futó periodikus ellenőrzését valamely védelmi egységen. Az opció beállítása esetén az üzenet-irányítási egység egy olyan üzenetet is továbbít, amely tartalmazza a védelmi egység nevét.

Vírus

A program vírusellenőrző rendszere által kiváltott eseményeket írja le. Beállítása esetén az üzenet-irányítási egység a keletkezési hely listában felsorolt védelmi egységeken belül történt találatok során keletkező üzeneteket továbbítja függetlenül attól, hogy azt periodikus ellenőrzés, illetve hozzáféréskori ellenőrzés váltotta ki. A lehetséges üzenetek találati jellegüktől függően a következők lehetnek:

- Gyanús: A program vírusellenőrző rendszere egy fájl ellenőrzése során vírus jelenlétére utaló gyanús kódrészletet talált.
- Immunizer: A program olyan fájlt talált, melyből egy másik vírusirtó már kiirtott egy vírust.
- Internetes féreg (I-Worm): A program vírusellenőrző rendszere internetes féreg típusú károkozóra bukkant.
- Mutáns: A program vírusellenőrző rendszere egy fájl ellenőrzése során egy ismert vírushoz hasonló kódrészletet talált.
- Szekvencia: A program vírusellenőrző rendszere egy fájl ellenőrzése során valamely vírusban is előforduló byte sorozatot talált.
- Tönkretett: A program vírusellenőrző rendszere egy olyan fájlt talált, amelyet valamilyen vírus tönkretett.
- Sűrített: A program egy tömörített fájlban talált vírust.
- Trójai program: A program trójai programot tartalmazó fájlt talált.
- Vírus: A program vírusellenőrző rendszere egy fájl ellenőrzése során vírust talált.

Az üzenetek címzettjei

Az üzenet irányítási egység a továbbítandó üzeneteket az alábbi helyekre küldheti:

Alkalmi levél

A globális opciókban megadott címekre az esemény hatására alkalmi levelet küld.

ErrorLog

Az üzenetet a Novell NetWare által kezelt hiba napló fájlba (SYS:SYSTEM/SYS\$LOG.ERR) írja.

Felhasználó

Amennyiben az üzenetet kiváltó esemény valamely felhasználóhoz köthető, úgy a program egy broadcast üzenetet küld a felhasználónak.

Képernyő

Az üzenet a szerveren, a VBShield Screen képernyőn jelenik meg.

Konzol

Az üzenet a szerveren, a System Console képernyőn jelenik meg.

Operátor

Az üzenet broadcast jelleggel valamennyi opcionálisan megadható operátornak elküldi. Az üzenet csak azokhoz az operátorokhoz jut el, akik az üzenet feldolgozásának pillanatában be vannak jelentkezve a hálózatba. Az operátorokat az operátor listába kell felvenni, mielőtt az üzenetküldő egységet aktivizálnánk.

Rendszeres levél

A globális opciókban megadott címekre rendszeresen (adott időpontokban) küldendő levélbe bejegyzik az üzenetet.

Report fájl

Az üzenetet az opcionálisan megadható (alapértelmezés szerint **vbuster.log**) fájlba írja.

Az üzenetek jellemzői

Minden egyes kimenet esetén megadható az üzenet nyelve, valamint annak részletességi foka. A részletességi fok az alábbiak egyike lehet:

Rövid

Az üzenet egysoros formában jelenik meg. A broadcast üzeneteket csak rövid üzenetként lehet továbbítani.

Normál

A megjelenített üzenet tartalmazza az eseménnyel kapcsolatos valamennyi információt az alábbi kitételekkel:

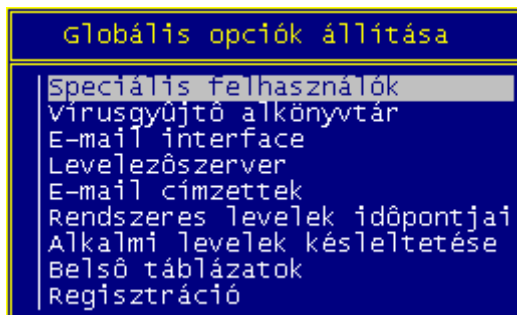
- Amennyiben az esemény valamilyen fájlhoz köthető, úgy a fájl elérési útja csak rövidített formában szerepel.
- Nem tartalmazza az esemény bekövetkezésének idejét.
- Nem tartalmazza az esetlegesen az eseményhez kötődő fizikai állomáscímet.

Részletes

A megjelenített üzenet tartalmazza az eseménnyel kapcsolatos valamennyi információt.

Globális opciók

A globális opciók almenüben a program működésével kapcsolatos általános beállítások adhatók meg.



Globális opciók

Speciális felhasználók

Itt adhatja meg azon felhasználók listáját, akik a program fájlvédelme, illetve hozzáférési tiltása ellenére írhatják, illetve olvashatják a tiltott fájlokat.

Vírusgyűjtő alkönyvtár

Vírus találata esetén, amennyiben az adott védelmi egység beállításai szerint a fertőzött fájl átmozgatásra kerül, úgy az ebbe az alkönyvtárba fog kerülni.

E-mail interfész

Az üzenet irányítási egységekben megadható azonnali, illetve periodikus levélküldési eljárás során alkalmazott levélkezelő interfészt adhatja meg ebben a menüpontban. A beállítható lehetőségek:

- Nincs: A program nem használ elektronikus levélküldési eljárást.
- Socket: Az elektronikus levelek továbbítása a socket-ek segítségével történik.

Levelezőszerver

Itt adható meg az SMTP szerver domain neve vagy IP címe, amin keresztül a levélküldés történik.

E-mail címzettek

Az üzenetirányítási egységekben megadható azonnali, illetve periodikus levélküldési eljárás során az itt felsorolt címzettek kapnak levelet.

Rendszeres levelek időpontjai

Az időpont táblázat beállításával 30 perces időközönként megadható, hogy heti rendszerességgel mely időpontokban történjen periodikus levélküldés.

Alkalmi levelek késleltetése

A megfelelő késleltetés beállításával megadható, hogy egy alkalmi levél küldése esetén a levél ne azonnal, hanem bizonyos késleltetéssel legyen elküldve. Így az összes, a késleltetés ideje alatt bekövetkező, alkalmi levélben elküldendő esemény egyetlen levélben lesz továbbítva.

Belső táblázatok

Ebben az almenüben állíthatja a program belső táblázatainak méreteit. A táblázatok méretei byte-ban értendők. A alábbi táblázatok méretei állíthatók:

- File cache: A program a hozzáféréskori ellenőrzés során vírusmentesnek ítélt fájlok neveit helyezi el a file cache táblázatban. Ismételt hozzáférés esetén, amennyiben a fájl még szerepel a táblázatban, nem történik ellenőrzés. Természetesen írási művelet esetén a fájl neve automatikusan törlődik a táblázatból. Ha nem kívánjuk használni ezt az opciót, úgy állítsuk a file cache méretét 0-ra.
- Üzenet-irányítási tábla: A tábla mérete a program által kezelt üzenet irányítási egységek tárolásához szükséges területet szabja meg.
- Domain leíró tábla: A tábla mérete a program által kezelt védelmi egységek tárolásához szükséges területet szabja meg.

Karantén

A Karantén komponens feladata - a beállításoktól függően - a vírusos, illetve vírusgyanús fájlok tárolása és azok további feldolgozása.

A karantén elemeket tartalmazó listában egy elem kiválasztása esetén információk jelennek meg a karanténba került fájlról, illetve különböző műveletek végrehajtására is lehetőség van a *Karantén műveletek* menüpont segítségével:

- Meghagy: A program a fájlra nem hajt végre semmilyen műveletet.
- Mentés másként: A fájlt a megadott néven menti el. A program a fájlt kódolja, hogy a vírus ne legyen aktív és a fájl küldhető legyen vírusellenőrzésre.
- Törlés: A program véglegesen törli a kijelölt fájlt.
- Újraellenőrzés: A program ismételt vírusellenőrzést hajt végre a kijelölt fájlra, illetve kiírja abból a vírust, amennyiben ez lehetséges.
- Visszaállítás: A program visszaállítja a fájlt eredeti helyére és állapotába, amennyiben az eredeti útvonal létezik és nem található az útvonalon azonos nevű fájl.

A beállított művelet az információs ablak bezárása után hajtódik végre!

Információk

Ebben a menüben a program által ismert egységekkel kapcsolatos információkat kérhet.

Névjegy

Kiválasztása esetén megjelennek a program forgalmazási, illetve szakmai kérdéseivel kapcsolatos címei, telefonszámai. A szokásos információkon kívül feltüntettük a program moduljaira vonatkozó adatokat is.

Futás közbeni opciók

A menüpontban az alábbi lehetőségek választhatók:

- Ellenőrzés indítása: Kiválasztása esetén megjelenik azon domain-ek listája, amelyeken indítható ellenőrzés, azaz nem fut rajta ellenőrzés és érvényes a domain bejegyzés. A domain(ek) kiválasztása után teljes ellenőrzés indul az adott domain-en.
- Ellenőrzés leállítása: Kiválasztása esetén megjelenik azon domain-ek listája, amelyeken éppen

ellenőrzés fut, illetve a periodikus ellenőrzési rendszer az ellenőrzést előjegyezte. Ez utóbbi esetben a domain név zárójelben jelenik meg. A listából kiválasztott domain(ek) ellenőrzése azonnal leáll, illetve a kiválasztott domain törlődik az előjegyzési listából.

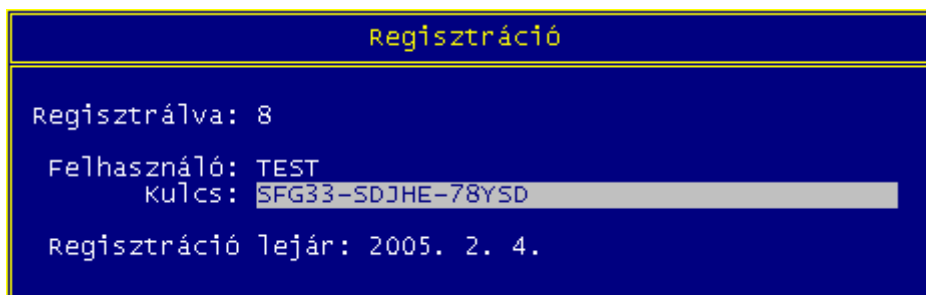
- Report fájl listázása: Kiválasztása esetén megjelenik azoknak a napló fájloknak a neve, amelyek megtekinthetők. Egy fájl kiválasztásakor megjelenik az adott fájl tartalma. Ha a megjelenítés az adott fájl legvégén áll, akkor követő üzemmódra vált, azaz az adott fájlba bekerülő új bejegyzések automatikusan megjelennek.

Regisztráció

A program csak érvényes regisztrációs adatokkal használható. Ezek nélkül nem lehet elindítani, felhasználó nevet és kulcsot mindenképpen meg kell adni.

A VirusBuster regisztrációs politikája alapján a megvásárolt programverzió teljes funkcionalitással tetszőlegesen ideig használható. Tehát a megvásárolt licenc jognak nincs időbeli korlátja, ha a regisztráció lejár, akkor a regisztrációs periódus alatt rendelkezésre álló verzió korlátlan ideig tovább használható. Amennyiben azonban a licenc lejárt után valamely programkomponens frissítésre kerül, a programot nem lehet többet elindítani (az ismételt használathoz újra regisztrálni kell). E korlátozás az adatbázis frissítéseket nem érinti, ezek tetszőlegesen időben minden következmény nélkül frissíthetők – még a regisztráció lejárt után is (de garanciát a kompatibilitás megtartására nem vállalunk).

A regisztráció lejárt után a termék leállítja az automatikus programkomponensek frissítését, hogy a periodikus frissítés ne okozzon problémát a program további használatában. Erre egy tájékoztató ablakban (és napló üzenetben) hívja fel a felhasználó figyelmét, mely minden kézi indítással kezdeményezett frissítéskor megjelenik. Lejárt regisztrációjú termékben a programkomponensek frissítése nem engedélyezett. A regisztráció megújítása után a program automatikusan visszaállítja a programkomponens-frissítéseket a korábbi állapotba.



Regisztrációs ablak

Regisztrálás menete

A regisztráció során a felhasználó az általa megadott névhez és a szerver felhasználó számához regisztrációs kulcsot kap. A név és a kapott regisztrációs kulcs a *Globális opciók/Regisztráció* menüpont kiválasztásakor megjelenő ablakban vihető be. Az ablakban megjelenő információk között láthatja a regisztráció állapotát és a program által regisztrált felhasználók számát is.

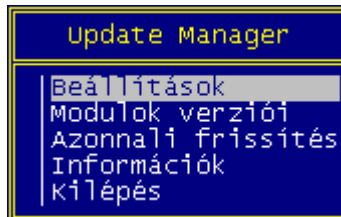
Figyelem!

A regisztrációs adatok beírásakor ügyeljen a kis- és nagybetűk használatára!

PROGRAMFRISSÍTÉS (UPDATE MANAGER)

A termék frissítése az *Update Manager* program segítségével valósítható meg. A programfrissítő telepítéséhez a védelem könyvtárába másolja fel a **VBUPDATE.NLM** és **VBUPDASC.NLM** fájlokat, illetve a **VBUSTER.INI** fájlt amennyiben ez még nem létezik a szerveren.

A programfrissítő ezek után a **load vbupdate** paranccsal indítható el. A konzol ablakban a következő lehetőségek közül választhat:



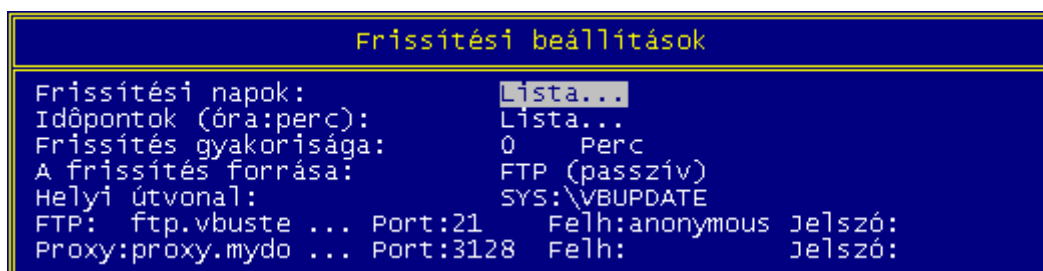
Főmenü

A termék a vírusadatbázis napra készen tartásához inkrementális adatbázis frissítési mechanizmust használ. A módszer lényege és előnye, hogy frissítéskor a programnak nem kell letöltenie mindig a teljes (több megabájt méretű) vírusadatbázis csomagot, hanem általában csak egy kisebb kiegészítő adatbázis fájlt, mely az utóbbi időben megjelent és feldolgozott károkozók felismeréséhez és eltávolításához szükséges információkat tartalmazza. Ezzel a módszerrel a napi frissítések időtartama a töredékére csökken, így lehetőség van akár naponta többször is vírusadatbázis frissítés kiadására, mely növeli a vírusvédelem hatékonyságát. Az egyes újonnan megjelenő károkozók elleni védelem a károkozók feldolgozása után szinte azonnal, minimális hálózati forgalom és letöltési idő ráfordítással eljut a felhasználókhöz.

Beállítások

Itt a program frissítésére vonatkozó általános beállítások adhatók meg, melyek mind az automatikus, mind a kézzel indított, azonnali frissítésekre érvényesek.

A termék alapértelmezett beállítása alapján két órás periódusokban próbálja meg frissíteni a program- és adatbázis komponenseket!



Frissítési beállítások

Frissítési napok

A menüpont alatt egy listára felveheti azon napokat, amikor a programnak végre kell hajtania frissítési folyamat(ka)t. Új napokat az **Insert** billentyű segítségével adhat hozzá, a listába már felvett elemeket pedig a **Delete** billentyű segítségével távolíthatja el.

Időpontok

A listába azon időpontokat veheti fel, amikor a programnak a megadott napo(ko)n a frissítést végre kell hajtania. Az időpontokat óra:perc formátumban adhatja meg (pl: 08:01). A megadott értéket a program csak abban az esetben veszi figyelembe, ha a következő *Frissítés gyakorisága* menüpontban 0 értéket ad meg.

Frissítés gyakorisága

A mezőben percekben adhatja meg a frissítés gyakoriságát, azaz a megadott időintervallum leteltével a program mindig végrehajt egy frissítési folyamatot.

A frissítés forrása

A hely típusát adhatja meg, ahonnan a program a frissítést végrehajtja. Ez lehet helyi útvonal, (passzív vagy aktív) FTP útvonal vagy Proxy-s FTP.

Helyi útvonal

Itt adhatja meg a szerveren (a megfelelő struktúrában) levő útvonalat, melyen a program a telepítő csomagokat találja.

FTP/Port/Felhasználó/Jelszó

Ebben a sorban az FTP szerver adatait adhatja meg. Alapértelmezésben a update.virusbuster.hu/pub12 szervernév 21-es port-tal történő használatát ajánljuk jelszó nélkül, *anonymous* felhasználónévvel.

Proxy/Port/Felhasználó/Jelszó

Proxy szerveren keresztül történő FTP-s frissítés esetén kell ezeket a mezőket kitölteni. Alapértelmezés szerint a 3128-as port használatát ajánljuk.

Modulok verziói

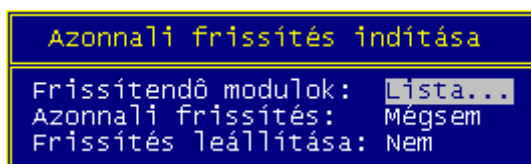
Itt a védelem egyes moduljainak verzió információit, illetve azok keletkezési dátumait tekintheti meg, illetve itt állítható be, hogy mely modulok kerüljenek frissítésre.

Az egyes feltelepített termékek neve alatt láthatók azok moduljai, illetve a modulok verziószáma és keletkezési dátuma.

A termékek neve melletti mezőre lépve kiválaszthatja, hogy az adott terméket a program frissítse-e, vagy megtartsa annak jelenlegi verzióját.

Azonnali frissítés

A menüben azonnali frissítést kezdeményezhet, illetve egy már futó frissítési folyamatot állíthat le.



Azonnali frissítés

Frissítendő modulok

A megjelenő listában tekintheti meg azon modulok listáját, melyek frissítésre kerülnek a folyamat elindításakor. Itt azon modulok kerülnek listázásra, melyeket frissítésre jelölt meg a *Modulok verziói* menüpont alatt.

Azonnali frissítés

A mezőben az indítás opciót választva elindíthatja a frissítési folyamatot. Fontos megjegyezni, hogy a folyamat csak abban az esetben indul el, ha éppen nem fut automatikus frissítési folyamat. Hasonlóképpen az automatikus frissítés sem fut le, amennyiben éppen egy azonnali frissítés van folyamatban.

Frissítés leállítása

A menüpont segítségével leállíthatja az éppen futó frissítési folyamatot.

Információk

Az *Információk* menüpont cégünk elérhetőségeit tartalmazza.

VÉGFELHASZNÁLÓI SZERZŐDÉS

A VÉGFELHASZNÁLÓI SZERZŐDÉS EGY TÖRVÉNYES MEGEGYEZÉS ÖN ÉS A VirusBuster Kft. KÖZÖTT. OLVASSA EL FIGYELMESEN, MIELŐTT FOLYTATNÁ A TELEPÍTÉST, ÉS HASZNÁLATBA VENNÉ A TERMÉKET. A SZERZŐDÉS LICENCET BIZTOSÍT A PROGRAM HASZNÁLATÁHOZ VALAMINT JÓTÁLLÁSSAL KAPCSOLATOS INFORMÁCIÓT ÉS FELELŐSSÉGI KIKÖTÉSEKET TARTALMAZ. A PROGRAM TELEPÍTÉSÉVEL ÉS HASZNÁLATÁVAL ÖN MEGERŐSÍTI A PROGRAM ÉS EZEN SZERZŐDÉS FELTÉTELEINEK ELFOGADÁSÁT. HA NEM ÉRT EGYET EZEN SZERZŐDÉS FELTÉTELEIVEL, NE TELEPÍTSE A PROGRAMOT.

FONTOS MEGJEGYZÉS: A SZOFTVER NEM HIBATŰRŐ ÉS NEM OLYAN KÖRNYEZETEKBE TÖRTÉNŐ HASZNÁLATRA LETT TERVEZVE ÉS SZÁNVA, AMELYEBEN HIBAMENTES MŰKÖDÉS SZÜKSÉGES. EZ A SZOFTVER EZÉRT NEM HASZNÁLHATÓ REPÜLŐGÉP-NAVIGÁCIÓS RENDSZEREK, NUKLEÁRIS LÉTESÍTMÉNYEK, KOMMUNIKÁCIÓS RENDSZEREK, FEGYVERRENDSZEREK, KÖZVETETT VAGY KÖZVETLEN ÉLETFENNTARTÓ RENDSZEREK, ILLETVE LÉGI IRÁNYÍTÁS MŰKÖDÉSÉBEN, VAGY BÁRMILYEN OLYAN ALKALMAZÁSBAN VAGY ESZKÖZBEN, AMELYBEN A MEGHIBÁSODÁS HALÁLÓS KIMENETELLEL, VAGY SÚLYOS, TESTI ÉPSÉGBEN VAGY VAGYONBAN KELETKEZŐ KÁRRAL JÁR HAT.

1. Meghatározások

(a) Az "Oktatási Verzió"-n a Program azon verziója értendő, mely kizárólagosan oktatási intézmények számára készült. Az "Otthoni Verzió"-n a Program azon verziója értendő, mely kizárólagosan magánszemélyek részére, egy gépen való felhasználásra készült. Az Oktatási és az Otthoni verzió nem használható fel üzleti célokra.

(b) A továbbiakban VirusBuster Kft. alatt a VirusBuster Kft. valamint, és amennyiben értelmezhető, terjesztői és értékesítői értendők.

(c) A "Nem Értékesíthető Verzió"-n a Program azon verziója értendő, mely kizárólagosan a Program bemutatására és kipróbálására használható.

(d) A "Program"-on a VirusBuster Kft. (R) VirusBuster(TM) elnevezésű szoftvere értendő, melyet a VirusBuster Kft. szolgáltat és mely tartalmaz bármely a programhoz kapcsolódó dokumentációt, kép- és hanganyagot, nyomtatott anyagot valamint on-line és elektronikus anyagot illetve dokumentációt.

2. Licenc

Ez a Végfelhasználói SZERZŐDÉS a következőkre jogosítja fel a végfelhasználót:

(a) A Program telepítésére és felhasználására egy különálló gépen, VAGY a Program telepítésére egy adattárolón, például egy hálózati szerveren, kizárólag abból a célból, hogy onnan futtatva telepíthető legyen a Program más gépekre egy belső hálózaton feltéve, hogy a végfelhasználó rendelkezik licenccel minden egyes számítógépre, melyre a Programot telepítik, vagy melyen futtatják annak adattároló eszközéről. A Program licence nem osztható meg vagy használható fel különböző számítógépeken.

(b) Csak Oktatási és Otthoni verzió. Ha az Oktatási, vagy az Otthoni verzióra vásárolt licenct, a Program telepíthető egy adattárolóra vagy tárolható azon, például egy hálózati szerveren kizárólag abból a célból, hogy onnan futtatható vagy telepíthető legyen a Program a belső hálózat más gépeire felhasználás céljából legfeljebb annyi felhasználó részére, mely szám nem haladja meg a megvásárolt licenck számát; biztosítva azt, hogy ellenőrzés alatt áll a felhasználók száma annak érdekében, hogy ezt a számot ne lépjék túl. A VirusBuster Kft. bármikor megvizsgálhatja, hogy a felhasználás megfelel-e a SZERZŐDÉSben foglaltaknak.

(c) Készíthet egy másolatot a Programról kizárólagosan biztonsági célokból. A végfelhasználó bármely másolaton köteles feltüntetni minden szerzői joggal kapcsolatos információt valamint bármely tulajdonlással kapcsolatos megjegyzést, mely a Program eredeti példányán található.

3. Licenc kikötések

(a) A második részben leírtakon kívül a Programról nem készíthető és terjeszthető semmilyen másolat valamint a Program nem küldhető egyik gépről a másikra elektronikus formában, vagy egy hálózaton belül.

(b) A Programot tilos részeire bontani, visszafejteni, vagy bármely más olyan állapotba hozni, amely ember által vizsgálható.

(c) A Program nem kölcsönözhető, nem adható el, nem adható bérbe és nem licencelhető.

(d) Tilos a Programot módosítani vagy azon alapuló munkákat készíteni.

(e) Tilos a Programot automatikus, fél-automatikus vagy manuális eszközökben víruszignatúrák, vírus-felismerő rutinok vagy más, káros kódot vagy adatot felismerő adat vagy kód létrehozására használni,

(f) Abban az esetben, ha bármilyen formában megszegi a jelen SZERZŐDÉSt, a VirusBuster Kft. megszüntetheti a licenct, és Ön köteles eltávolítani a Program minden másolatát.

4. Frissítések

Ha a Program jelen másolata a Program egy korábbi verziójának frissítése, akkor a korábbi végfelhasználói SZERZŐDÉS hatályát veszti és ez a SZERZŐDÉS lép életbe. A Program korábbi verziója nem használható a továbbiakban és nem adható át más jogi személynek.

5. Tulajdonlás

A licenc korlátozott jogokat biztosít a Program használatára. A VirusBuster Kft. minden jogot, címet és érdekeltséget fenntart

beleértve minden védjegyet a Programra és minden másolatára vonatkozóan. Minden jog, mely külön nem kerül kiemelésre jelen SZERZŐDÉSben, beleértve a nemzetközi védjegyeket is, a VirusBuster Kft. kizárólagos tulajdona.

6. KORLÁTOZOTT JÓTÁLLÁS ÉS KIKÖTÉSEK

(a) **KORLÁTOZOTT JÓTÁLLÁS.** A VirusBuster Kft. vállalja, hogy a kézhezvételtől számított (bizonyíthatóan) kilencven (90) napig az adathordozó, melyen a Program található, mentes lesz minden anyaghibától rendeltetésszerű használat esetén.

(b) **EGYÉB JÓTÁLLÁS NINCS.** KIVÉVE A FENTEBB LEÍRT KORLÁTOZOTT JÓTÁLLÁST, A VirusBuster Kft. KIZÁR BÁRMELY MÁS JÓTÁLLÁST. HA AZ ALKALMAZOTT JOG BÁRMELY JÓTÁLLÁST ÍR ELŐ A PROGRAMRA, ÚGY AZ A KÉZHEZVÉTELŐL SZÁMÍTVA CSAK KILENCVEN NAPIG ÉRVÉNYES. Bármely szóbeli vagy írásbeli információ vagy tanács, melyet a VirusBuster Kft., forgalmazói, terjesztői, ügynökei vagy alkalmazottai adnak, nem képezhet jótállást vagy szélesítheti annak körét.

7. Kizárólagos jogorvoslat

A 6-os rész alatt foglaltak úgy nyerhetnek jogorvoslatot, ha visszaviszi a Programot az értékesítés helyére a probléma leírásával és az értékesítés igazolásával. A VirusBuster Kft. kicseréli a sérült adathordozót. A VirusBuster Kft. elhárít minden felelősséget abban az esetben, ha az adathordozó sérülésének oka: baleset, nem rendeltetésszerű használat, nem megfelelő számítógép-konfiguráció alkalmazása.

8. KORLÁTOZOTT FELELŐSSÉG.

A VirusBuster Kft. NEM TARTOZIK FELELŐSSÉGGEL SEMMILYEN KÖZVETETT VAGY KÖZVETLEN KÁRÉRT SEM ÖNNEK, SEM BÁRMELY HARMADIK SZEMÉLYNEK (BELEÉRTVE KORLÁTOZÁS NÉLKÜL MINDEN NYERESÉGVESZTÉST, ÜZLETI TEVÉKENYSÉG KÉNYSZERŰ SZÜNTELELÉSÉT, INFORMÁCIÓVESZTÉST ÉS HASONLÓ KÁROKAT), AMELY A PROGRAM HASZNÁLATÁBÓL, VAGY NEM HASZNÁLHATÓSÁGÁBÓL ADÓDIK, MÉG ABBAN AZ ESETBEN SEM, HA A VirusBuster Kft.-t TÁJÉKOZTATTÁK EZEN KÁROK FELMERÜLÉSÉNEK LEHETŐSÉGÉRŐL.

9. A megegyezés alapja

A fentebb leírt korlátozott jótállás, kizárólagos jogorvoslat és korlátozott felelősség alapvető elemei a megegyezésnek, mely a VirusBuster Kft. és Ön között jön létre. A VirusBuster Kft. csak jelen alapelvek alapján értékeseíti a Programot.

10. Kizárólag fogyasztó végfelhasználók

A jelen SZERZŐDÉSben foglalt korlátozások és kizárások a jótállással és felelősséggel kapcsolatban nem befolyásolhatják a fogyasztó törvényes jogait.

11. Általános rendelkezések

Jelen SZERZŐDÉS Magyarország jogrendszerén alapul. Jelen SZERZŐDÉS tartalmazza a szerződő felek teljes megegyezését és minden más írásbeli vagy szóbeli megegyezés felett áll. A végfelhasználói SZERZŐDÉssel kapcsolatos kérdéseket a VirusBuster Kft. címére juttassa el.

A VirusBuster a VirusBuster Kft. bejegyzett védjegye Magyarországon és/vagy más országokban. Minden más elnevezés a megfelelő tulajdonosát illeti meg.

KAPCSOLAT

Jelen dokumentáció részletesen tárgyalja vírusvédelmi programunk működését, működtetését. Ennek ellenére, ha további kérdése van termékünkkel kapcsolatban, esetleg megosztaná velünk észrevételeit, javaslatait, kérjük lépjen kapcsolatba velünk. Bizalommal forduljon hozzánk az alábbi elérhetőségek egyikén! Kéréseit, megjegyzéseit, ötleteit szívesen fogadjuk.

Cím VirusBuster Kft.
Budapest 1518,
Pf. 54.
Magyarország

Telefon (+36) 1 382-7000

Fax (+36) 1 382-7007

Web <http://www.virusbuster.hu>

Támogatás <https://support.virusbuster.hu>

E-mail sales@virusbuster.hu

support@virusbuster.hu