

Varovalni sistem

(varna uporaba interneta)

Win 95/98/ME/NT4.0/2000/XP

Priročnik za uporabnika

Vsa navedena imena proizvodov so blagovne znamke ali zaščitene blagovne znamke posameznih podjetij. F-Secure Corporation se odreka lastniškim interesom za znamke in imena drugih čeprov, si F-Secure Corporation po najboljših močeh prizadeva za točnost teh informacij, pa ne odgovarja za morebitne vsebovane napake ali izpustitve dejstev. F-Secure Corporation si brez predhodnega obvestila pridržuje pravico do spremembe specifikacij v tem dokumentu.

Družbe, imena in podatki, ki so uporabljeni v teh primerih, so izmišljeni, če ni navedeno drugače.
Nobenega dela tega dokumenta ni dovoljeno v nikakršni obliki reproducirati ali posredovati z nobenimi sredstvi, elektronskimi ali mehanskimi, za noben namen, razen z izrecnim pisnim dovoljenjem F-Secure Corporation. Copyright © 1996-2003 F-Secure Corporation. Vse pravice pridržane.

Vsebina:

O tem vodniku.....	6
Slovar ikon.....	6
1. Namestitev varovalnega sistema (varna uporaba interneta)	7
1.1 Preden začnete	7
1.2 Koraki namestitve	7
1.3 Če morate odstraniti varovalni sistem	9
2. Začetek uporabe	10
2.1 Ko prvič uporabite varovalni sistem	10
2.2 Kaj storiti, ko se pojavi Application Control prikazovalno okno?.....	10
2.3 Ali je varovalni sistem aktiven in pravilno deluje?.....	11
2.4 Opcije za dostop do varovalnega sistema	12
3. Domača stran.....	14
4.  Zaščita pred virusi	15
4.1 Profili zaščite pred virusi	15
4.2 Pregledovanje virusov	16
4.3 Odstranjevanje virusa iz vašega računalnika	17
4.4 Kaj pa, če sumite, da ste našli nov virus?	21
4.5 Nastavitve zaščite	22
5.  Internet Shield (Internetna zaščita)	23
5.1 Profili internetne zaščite	23
5.2 Uporaba Nadzora aplikacij	24
5.3 Prirejanje pravil internetne zaščite po meri	26
5.4 Napredne nastavitve	31
6.  Samodejne posodobitve	32
7.  Moja naročnina	33
8. Kako varovalni sistem varuje vaš računalnik	34
8.1 Zaščita pred virusi	34
8.2 Internet Shield (Internetna zaščita).....	34
8.3 Kako lahko vi prispevate k izogibanju virusov in druge zlonamerne programske opreme?.....	35
Reševanje težav	36
Namestitev	36
Splošna uporaba	36
 Zaščita pred virusi	36
 Internet Shield (Internetna zaščita)	36
 Samodejne posodobitve	37
Slovar	38
Podpora in vzdrževanje	39
Tehnična pomoč	40

O tem vodniku

Ta vodnik nudi vse informacije, ki jih potrebujete za namestitev in uporabo varovalnega sistema.

Poglavje 1: *Namestitev Varovalnega sistema (varna uporaba interneta)*. Nudi vam potrebne informacije za namestitev in uporabo Varovalnega sistema.

Poglavje 2: *Začetek uporabe*. Novim uporabnikom daje informacije, bolj izkušnim pa referenco za dostop in začetek uporabe varovalnega sistema.

Poglavje 3: *Domača stran*. Omogoča vam hiter in podroben pregled vaših varnostnih nastavitev in stanje varovalnega sistema.

Poglavje 4: *Zaščita pred virusi*. Pojasni vam, kako lahko vključite ali izključite protivirusno zaščito, izbere vaš profil virusne zaščite in nadzira, kdaj ste nazadnje prejeli posodobitve definicij virusov.

Poglavje 5: *Internet Shield (Internetna zaščita)*. Pojasni, kako lahko spremenite ali uredite profile Internet Shield-a, pogledate koliko povezav je bilo dovoljenih ali zavrnjenih, in dostopate do naprednih nastavitev.

Poglavje 6: *Samodejne posodobitve*. Nudi vam informacijo o avtomatski storitvi posodabljanja, ki vam zagotavlja najnovejše informacije o virusih, verzijah programske opreme in verzijah profilov.

Poglavje 7: *Moja naročnina*. Pojasni, kako lahko preverite svoj naročniški status, obnovite naročniško razmerje in spremenite svojo naročniško številko.

Poglavje 8: *Kako varovalni sistem varuje vaš računalnik*. Definira ogroženost vašega računalnika in pojasni, kako vam varovalni sistem zaščiti vaš računalnik pred temi nevarnostmi.







Razreševanje težav - napotki za reševanje preprostih težav

Slovar - razlaga terminov, pojmov

Pomoč in vzdrževanje - vsebuje podatke za navezavo stikov oz. priklic pomoči

Slovar ikon

V varovalnem sistemu se pojavijo naslednje ikone:

	Aktiven	Možnost je aktivirana in deluje pravilno.
	Vprašanje	Vprašanje, ki od vas morda zahteva odločitev.
	Info	Informativen tekst, ki vam pomaga uporabljati varovalni sistem.
	Zaseden	Prosimo, počakajte.
	Opozorilo	Možnost v programu varovalni sistem je izključena, ali pa vaše definicije virusov niso bile posodobljene že dlje časa.
	Napaka	Pojavila se je napaka. Prosimo, pazljivo preberite sporočilo o napaki.

Pozor: Pomeni nekaterih ikon se razlikujejo od tistih na strani My Subscription (Moja naročnina). Za več informacij poiščite **Poglavje 7: *Moja naročnina***.

1. Namestitev varovalnega sistema (varna uporaba interneta)

1.1 Preden začnete

Sistemske zahteve

Vaš računalnik mora zadostiti naslednjim zahtevam za namestitev in poganjanje varovalnega sistema.

Procesor:	Intel Pentium II ali višji.
Operacijski sistem:	Win 95/98/ME/NT4.0 (zahtevan SP6)/2000/XP.
Spomin:	Windows 95/98/ME/NT4.0 -64 MB spomina. Windows 2000/XP- 128 MB spomina.
Prostor na disku:	30 MB nezasedenega prostora na disku (60 MB med namestitvijo).
Prikaz:	Najmanj 256 barv.
Povezava v internet:	Povezava v internet je pogoj za potrditev vašega naročniškega razmerja in za sprejem posodobitev.
Brskalnik:	Internet Explorer 3.0 ali novejši.

Priprava vašega računalnika na namestitev

Istočasna uporaba več različnih protivirusnih programov in požarnih zidov ni priporočljiva. Navzkrižni protivirusni programi lahko pokvarijo in poškodujejo vaše datoteke.

Odstranitev drugih protivirusnih programov / požarnih zidov

Varovalni sistem lahko samodejno nadgradi verzije F-Secure Anti-Virus 4 in 5, in F-Secure Distributed Firewall 5.

Protivirusne programe in požarne zidove drugih ponudnikov je potrebno odstraniti ločeno pred namestitvijo Varovalnega sistema. Za odstranitev programske opreme se obrnite na ustrezno dokumentacijo proizvajalca.

1.2 Koraki namestitve

Pozor: Če uporabljate Windows NT 4.0, Windows 2000 ali Windows XP in imate več kot en uporabniški račun, se morate za namestitev varovalnega sistema prijaviti s skrbniškim računom (»administrator account«).

Za namestitev varovalnega sistema sledite naslednjim navodilom:

1. del: Namestitev varovalnega sistema

1. Glede na način namestitve,
 - Vstavite varovalni sistem CD v CD-ROM enoto v vašem računalniku.Namestitev bi se morala samodejno začeti. Če se ne zažene, pobrskajte po CD-ju in poiščite datoteko **varovalni.exe** in dvakrat kliknite nanjo za zagon namestitve.

- Prenesite paket izdelka na vaš računalnik. Zaprite vse ostale programe in zaženite paket za začetek namestitve.
2. Izberite jezik, ki ga želite uporabljati za namestitev in kliknite **Next** (naprej) za nadaljevanje.
 3. Preberite dogovor o naročniškem razmerju in če se strinjate s pogoji, kliknite z miško na potrditveno polje **Sprejemem pogoje**. Kliknite **Next** (naprej) za nadaljevanje.
 4. Izberite imenik za namestitev varovalnega sistema. Kliknite **Next** (naprej) za nadaljevanje.
 5. Prenos datotek na vaš računalnik. Ko je prenos zaključen, nadaljujte z drugim delom namestitve.



Pozor: Morda boste morali ponovno zagnati vaš računalnik. Izberite **Restart Now** (ponoven zagon). Če izberete **Restart Later** (ponoven zagon kasneje), se namestitev ne bo nadaljevala dokler ne boste ponovno zagnali računalnika. Kliknite gumb **Finish** (konec) za nadaljevanje.

2. del: Izbira sestavnih delov in potrjevanje vašega naročniškega razmerja

Za potrditev vašega naročniškega razmerja vzpostavite povezavo v internet.

Vprašani boste za:

- Vnos številke vašega naročniškega razmerja za registracijo vaše naročnine. Kliknite **Next** (naprej) za nadaljevanje.
- Izberite testiranje izdelka (če nameščate v načinu vrednotenja (testiranja) - evaluation mode). Kliknite **Next** (naprej) za nadaljevanje. Izberite tip namestitve v naslednjem oknu in kliknite **Next** za nadaljevanje.

Nasvet: Poteku namestitve lahko sledite s klikom na ikono  v Windows sistemsko vrstico v desnem spodnjem vogalu vašega monitorja. To ikono bo zamenjala ikona , ko bo namestitev zaključena.

Če nalagate sestavne dele z interneta, počakajte, da mrežni namestitveni program naloži vse pakete. To navadno traja manj kot dvajset minut preko ADSL povezave, ali pa okrog uro ali več s hitrim telefonskim modemom.

1. Po namestitvi vseh sestavnih delov varovalnega sistema boste naprošeni, da ponovno zaženete računalnik. Izberite **Restart Now** (ponovni zagon). Če izberete **Restart Later** (ponoven zagon kasneje), namestitev ne bo popolna, dokler ne boste ponovno zagnali računalnika. Kliknite gumb **OK** za zaključek namestitve.

Da se prepričate o uspehu namestitve, glejte Poglavje 2. Ali je varovalni sistem aktiven in pravilno deluje?.

Pozor: Po zaključeni namestitvi se lahko pojavi sporočilo Application Control, ki vas vpraša, ali naj dovoli ali zavrne poskus katerekoli aplikacije, da vzpostavi povezavo v internet. Za navodila glejte Poglavje 2. Kaj storiti, ko se pojavi Application Control prikazovalno okno.

1.3 Če morate odstraniti varovalni sistem

Odstranite varovalni sistem z uporabo Windows opcije *Add/Remove Programs* (Dodaj ali odstrani programe) v Windows Control Panel (Windows Nadzorni plošči). Tako boste zagotovili varno in popolno odstranitev programa iz vašega računalnika. Za to naredite naslednje:

1. Odprite Start menu v Windows opravilni vrstici.
2. Izberite *Settings/Nastavitve -> Control Panel/ Nadzorna plošča -> Add/Remove Programs / Dodaj ali odstrani programe* .
3. Izberite *varovalni sistem* in kliknite **Remove**(odstrani).
4. Ponovno zaženite vaš računalnik.

2. Začetek uporabe

2.1 Ko prvič uporabite varovalni sistem

Če uporabljate varovalni sistem prvič, pogledjte naslednja poglavja, ki vam pomagajo zagotoviti, da je varovalni sistem dejansko v teku in vas varuje v skladu z vašimi varnostnimi potrebami.

- Kaj storiti, ko se pojavi Application Control prikazovalno okno?
- Ali je varovalni sistem aktiven in pravilno deluje?
- Opcije za dostop do varovalnega sistema.

2.2 Kaj storiti, ko se pojavi Application Control prikazovalno okno?

Ko ste namestili varovalni sistem, vas lahko Application Control opozori, da se aplikacija skuša povezati v internet, odvisno od vašega profila Internet Shield.

Application Control vam omogoča varno brskanje in je odlična obramba pred zlonamernimi računalniškimi programi, kot npr. trojanskimi konji (za definicijo trojanskega konja in drugih terminov glej slovar). Na začetku pa se bo pojavila cela vrsta zahtev, da zavrnete ali dovolite povezavo na določen naslov. Število zahtev se bo zmanjšalo in poredko boste videli sporočila Application Control, razen če namestite novo programsko opremo ali če se zlonamerna aplikacija skuša povezati na Internet iz vašega računalnika.

Primer: Prvi zagon vašega internetnega brskalnika po namestitvi

1. Zagon vašega internetnega brskalnika (npr. Internet Explorer, Netscape).




2. Pojavi se sporočilo Application Control, ki vas vpraša, ali naj dovoli ali zavrne poskus brskalnika *Internet Explorer*, da vzpostavi povezavo.
 - Izberite *“Zapomni si to odločitev v prihodnje”* (*remember this decision*), ker veste, da je vaš Internetni brskalnik varna aplikacija.
 - Kliknite **Allow**, ker veste, da je vaš brskalnik varen (več o tem, kaj je varno ali nevarno, najdete v Poglavju 5: Uporaba Nadzora aplikacij).

Kliknite **Help**, da boste zvedeli več o Application Control.

Pozor: Če želite izključiti možnost Application Control, pojdite na stran Internet Shield. Poleg Application Control kliknite **Change**. Statusni tekst se bo spremenil iz *Prompt* v *Allow & Log* (dovoli in beleži).

Več informacij o Application Control glej Poglavlje 5: Uporaba Nadzora aplikacij.










2.3 Ali je varovalni sistem aktiven in pravilno deluje?

Potem ko ste namestili, ali kadarkoli uporabljate varovalni sistem, lahko preverite, če je varovalni sistem aktiven in pravilno deluje, s pomočjo ikone  v sistemskem polju vaših Oken (Windows) v desnem spodnjem kotu vašega zaslona, kot je prikazano spodaj:



Pozor: V okolju Windows XP pa so ikone lahko skrite. S klikom na gumb  lahko vidite skrite ikone.

Naslednje ikone se lahko pojavijo odvisno od stanja varovalnega sistema. Glej seznam ikon in njihov pomen v spodnji tabeli:

Ikona	Pomen	Kaj storiti
	Varovalni sistem deluje pravilno. Vaš računalnik je zaščiten.	Uporabljajte elektronsko pošto in brskajte po Internetu kot običajno
	Namestitev in nadaljevanje Vaš računalnik še ni zaščiten.	Počakajte, da se postopek namestitve konča. Ikona  se pojavi, ko je namestitev zaključena.
	Stanje napake Pojavila se je napaka v varovalnem sistemu.	Položite vaš kazalec miške čez ikono  , da ugotovite vzrok za napako. Če je potrebno, ponovno zaženite vaš računalnik.
	Opozorilo Možnost zaščite je bila izključena, ali pa so vaše definicije virusov stare. Vaš računalnik ni povsem zaščiten.	Položite vaš kazalec miške čez ikono  , da vidite statusni napotek. Vključite možnost, ki je trenutno izključena, da lahko greste na varovalni sistem in preverite, ali obstajajo posodobitve.
	Unloaded (odstranjeno iz pomnilnika). Varovalni sistem ni aktiviran in vaš računalnik ni zaščiten.	Desno kliknite ikono  in izberite <i>Reload</i> , da reaktivirate varovalni sistem.
Ni ikone	Varovalni sistem ni nameščen. Vaš računalnik ni zaščiten.	Ponovno zaženite vaš računalnik in namestite varovalni sistem.

2.4 Opcije za dostop do varovalnega sistema

Obstaja več načinov za dostop do varovalnega sistema in njegovo uporabo:

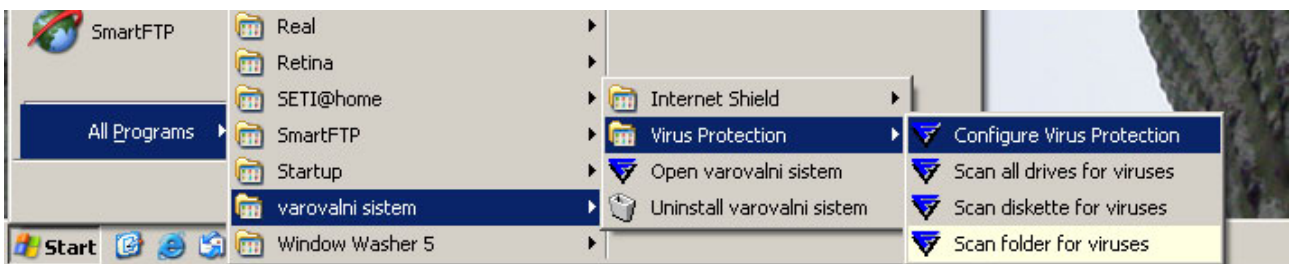
- Windows Start Menu
- Ikona F-Secure
- Varovalni sistem Windows Explorer prikazovalni meni

Windows Start Menu


Za odpiranje varovalnega sistema, dostopanje do osnovnih operacij, priročnikov in spletnih strani:


Odprite menu za zagon Oken: Windows *Start*.

1. Pojdite na meni *Programs* in pod meni varovalni sistem.
2. Kliknite Open(odpri) varovalni sistem, da lahko začnete uporabljati varovalni sistem, ali izberite drugo opcijo iz podmenija varovalni sistem.



Ikona F-Secure

Z Ikono F-Secure (), ki jo lahko vidite v sistemskem polju Windows (Oken) (v desnem spodnjem vogalu vašega monitorja), lahko odprete varovalni sistem, pogledate stanje varovalnega sistema ali uporabite prikazovalni meni za dostop do varovalnega sistema..

Za odpiranje varovalnega sistema, dvojno kliknite na ikono  z levim gumbom miške.

Varovalni sistem Status Tool-Tip

Položite vaš kazalec miške čez ikono varovalni sistem, da prikažete statusni napotek. S tem napotkom lahko v trenutku vidite, ali je kakšen problem v aplikaciji varovalnega sistema, kot prikazuje spodaj navedeni primer, kjer je bila Virus Protection (zaščita pred virusi) izključena.



Varovalni sistem Pop-Up Menu

Kliknite ikono z desnim gumbom, da dobite dostop do sporočilnega menija varovalnega sistema in njegovega seznama splošnih in pogosto uporabljenih operacij. Iz menija lahko odprete varovalni sistem ali pa takoj pregledate, če imate virus.



Spodnja tabela vam bo pomagala do boljšega razumevanja vsake postavke v meniju:

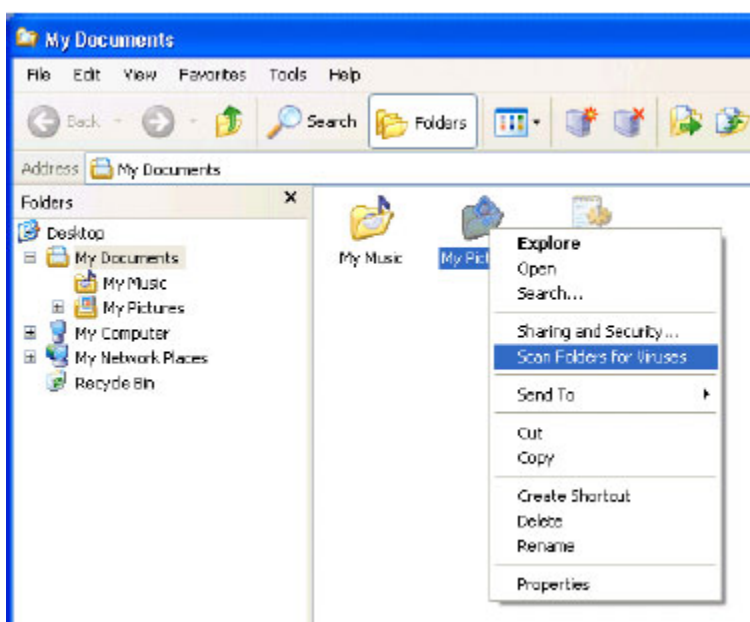
Izbira	Razlaga
Odprite varovalni sistem	Odpre varovalni sistem
Odstranitev produktov F-Secure iz pomnilnika	Odstranitev produktov F-Secure iz pomnilnika. Včasih je to potrebno, ko nameščamo programsko opremo ali opravljamo zmogljivostno kritične naloge. Ne pustite vašega računalnika v tem stanju za daljši čas, ker ni zaščiten.
Preglej vse trde diske	Virus Protection pregleduje vse razpoložljive trde diske na vašem računalniku.
Preglej disketo	Virus Protection pregleduje vsako disketo v pogonu A. drive.
Preglej cilj...	Virus Protection pregleduje ciljno datoteko po vaši izbiri. Pojavi se drevo map. Izberite vašo ciljno mapo - datoteko in kliknite OK, da se pregled začne.
Opcije ...	Odpre Advanced options (Napredne možnosti).
O ...	Prikaže informacije o varovalnem sistemu.

Varovalni sistem Windows Explorer Pop-Up Menu

Z Windows Explorerjem (Raziskovalcem) lahko pregledate diske, mape in datoteke, ali vsebujejo viruse. Zato naredite naslednje:

Namestite kazalec miške na disk, mapo ali datoteko, ki jo želite pregledati, in kliknite z desnim gumbom miške.

1. Iz prikazovalnega menija izberite Scan Folders for Viruses. Pojavi se okno *Manual Scan* in začne se pregledovanje.

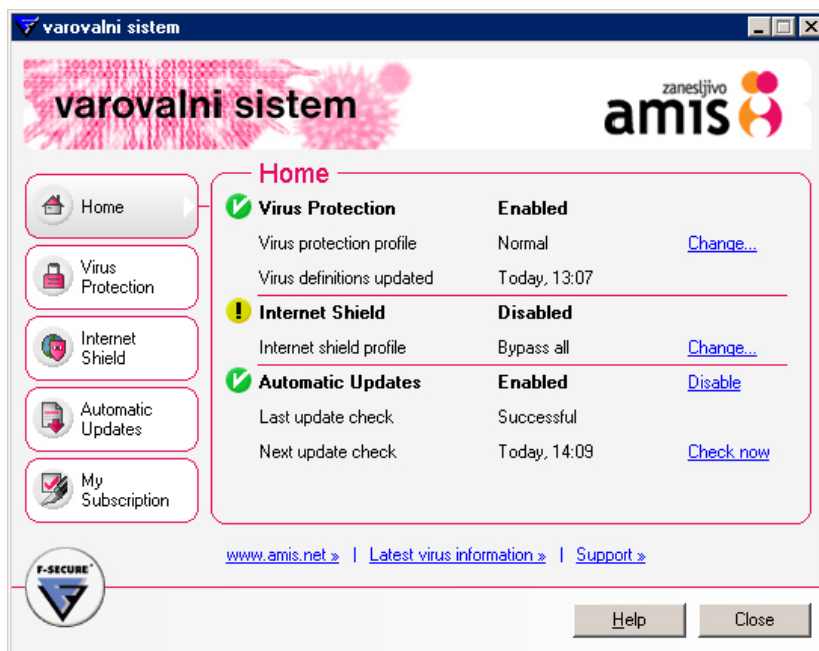


Če najde virus, glej Poglavlje 4: Odstranjevanje virusa iz vašega računalnika.

Pozor: Kadar opravite pregled, uporablja varovalni sistem nastavitve za pregledovanje iz trenutnega profila Virus Protection (zaščite pred virusi). Glej Poglavlje 4: Spreminjanje profila zaščite pred virusi.

3. Domača stran

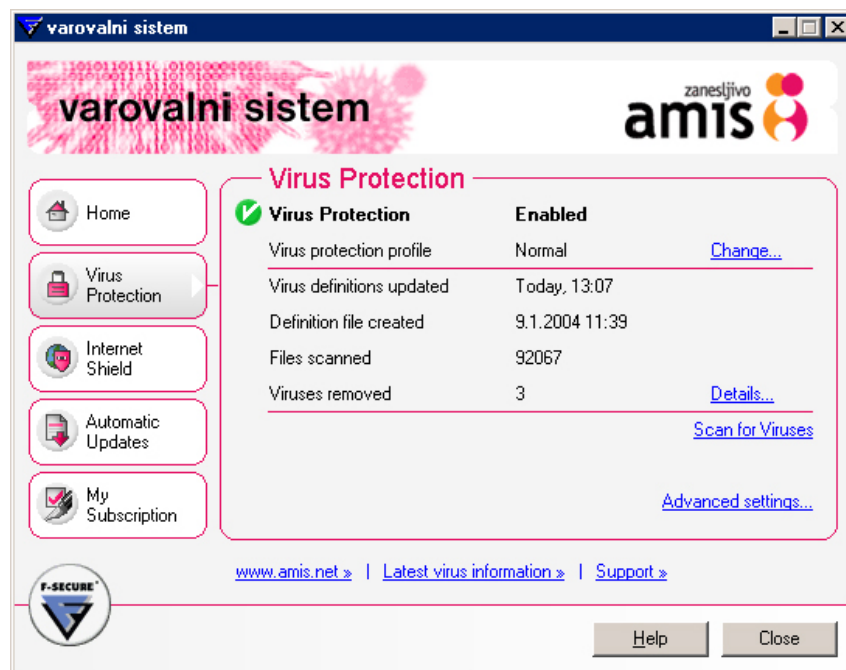
Domača stran vam omogoča hiter in podroben pregled vaših varnostnih nastavitev in status varovalnega sistema.



Na domači strani lahko:

- Izberete vaš profil protivirusne zaščite in nadzorujete stanje vaše protivirusne zaščite. Za več informacij in navodil glej Poglavje 4: Zaščita pred virusi.
- Izberite vaš profil Internet Shield (profil internetne zaščite) Za več informacij in navodil glej Poglavje 5: Internet Shield (Internetna zaščita).
- Vključite in izključite samodejne posodobitve in vidite informacije o posodobitvah, ki jih je vaš računalnik že prejel. Za več informacij in navodil glej Poglavje 6: Samodejne posodobitve.

4. Zaščita pred virusi



Na domači strani Virus Protection (zaščita pred virusi), lahko:

- Izberete vaš profil zaščite pred virusi (za več informacij glejte *Profili zaščite pred virusi*).
- Pregledate, kadar ste dobili posodobitve definicij virusov, in kadar so vaše datoteke definicij virusov ustvarili v F-Secure VirusLab-u.
- Preglejte število datotek, ki jih je varovalni sistem pregledal in koliko virusov je odstranil.
- Ročno sprožite iskanje virusov (da bi izvedeli več, glejte *Pregledovanje virusov*).

4.1 Profili zaščite pred virusi

Profili zaščite pred virusi vam omogočajo, da v trenutku spremenite vaš nivo zaščite, v skladu z vašimi potrebami. Profili se samodejno posodablajo, da se zagotovi vaša zaščita pred najnovejšimi oblikami zlonamernih računalniških programov.

Če spremenite katero nastavitev v profilu (iz naprednih nastavitev zaščite pred virusi), se bo ime profila spremenilo v User-Defined (uporabniško definiran). Za povrnitev vašega profila zaščite pred virusi, glejte *Spreminjanje profila zaščite pred virusi* spodaj.

Spreminjanje profila zaščite pred virusi

Profile lahko spremenite kadarkoli, glede na varnostno zaščito, ki jo potrebujete. Sprememba vašega izbranega profila spremeni nivo avtomatskih dejanj in poročanja.

Spremenite vaš profil zaščite pred virusi, kot sledi:

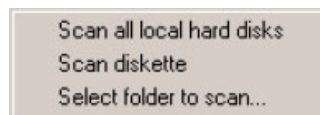
1. Kliknite **Change**.
2. Izberite profil iz spustnega seznama. Prosimo, da natančno preberite prikazan opis vsakega profila, preden ga aktivirate.
3. Kliknite gumb **OK**, da začnete uporabljati izbrani profil.

4.2 Pregledovanje virusov

Z vključeno zaščito pred virusi je vaš računalnik zaščiten. Odpiranje ali zapiranje datoteke bo vedno povzročilo pregled za viruse.

Če sumite, da neka datoteka vsebuje virus, lahko pregledate datoteko ali vaš računalnik za viruse. Za izvedbo pregledovanja virusov, storite naslednje:

- Kliknite Scan for Viruses (pregledovanje virusov).
- V meniju izberite pregledovanje vseh lokalnih trdih diskov, ene same diskete ali mape, katero boste morali določiti.



- Prikaže se okno *Manual Scan Statistics* (statistika ročnega pregledovanja) in vam pokaže statistiko pregleda. Kliknite gumb **Stop** kadarkoli za prekinitev pregledovanja.



- Po pregledovanju se ustvari poročilo. Kliknite Show Report (prikaži poročilo), da ga vidite v vašem spletnem brskalniku. Če najde virus, glej [Odstranjevanje virusa iz vašega računalnika](#).

Pozor: Kadar opravite pregled, uporablja varovalni sistem nastavitve za pregledovanje iz trenutnega profila protivirusne zaščite Virus Protection. Za izbiro drugega profila, glejte *Profili zaščite pred virusi*.

4.3 Odstranjevanje virusa iz vašega računalnika

Kako F-Secure Anti-Virus Disinfection Wizard (čarovnik za razkuževanje virusov) odstrani virus?

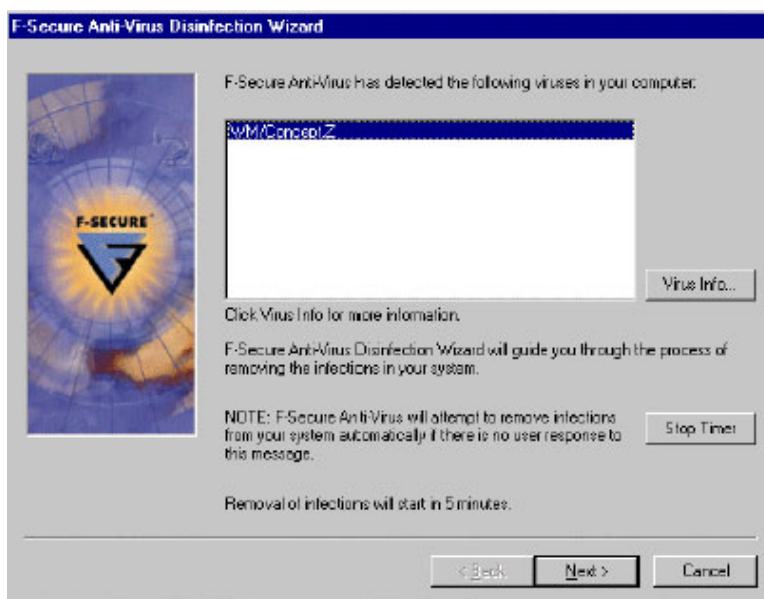
Videli boste F-Secure Anti-Virus Disinfection Wizard:

- Če je bil najden virus med pregledovanjem.
- Če je bil najden virus in je profil vaše zaščite pred virusi nastavljen na prikaz vseh ugotovitev in poročila pred razkuževanjem.
- Če je bil virus najden med samodejnim pregledom (vključena samodejna zaščita) in varovalni sistem ni mogel sam odstraniti virusa.

Naslednji koraki vam bodo pomagali pri odstranjevanju virusa.

1. korak - Zaznan virus

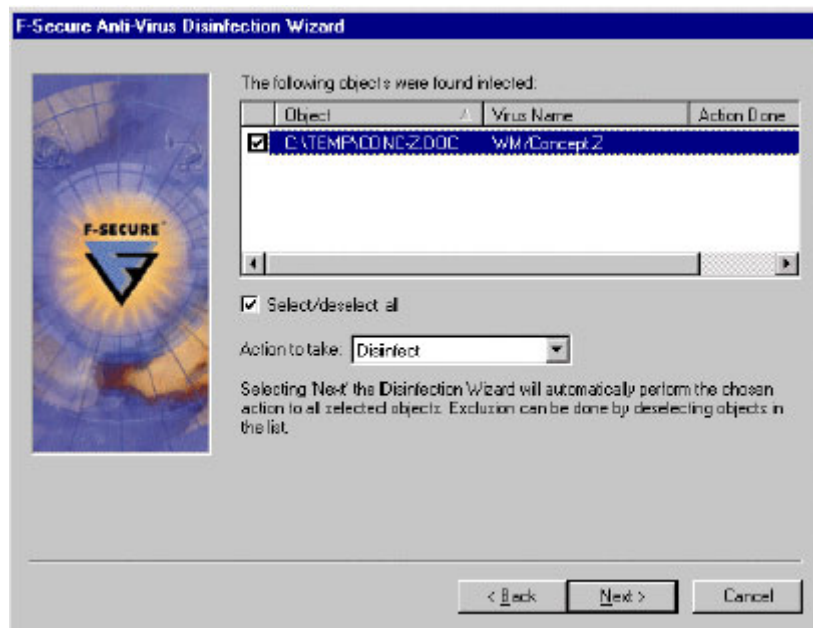
Ime zaznanega virusa se izpiše, kot je prikazano spodaj. Za nadaljevanje z razkuževanjem virusa, kliknite **Next**.



Pozor: Za več informacij o virusu, kliknite na ime virusa, nato kliknite Virus Info. Če je virus nov, lahko da opisa še ni. Preverite F-Secure Computer Virus Info Center na naslovu <http://www.f-secure.com/v-descs/> za zadnje informacije.

2. korak - Izvedeni ukrep

Izpiše se seznam okuženih datotek.



V okviru Action to Take (kako ukrepati), izberite dejanje, ki bo izvedeno na okuženi datoteki. Pregled vsakega dejanja najdete v spodnji tabeli.

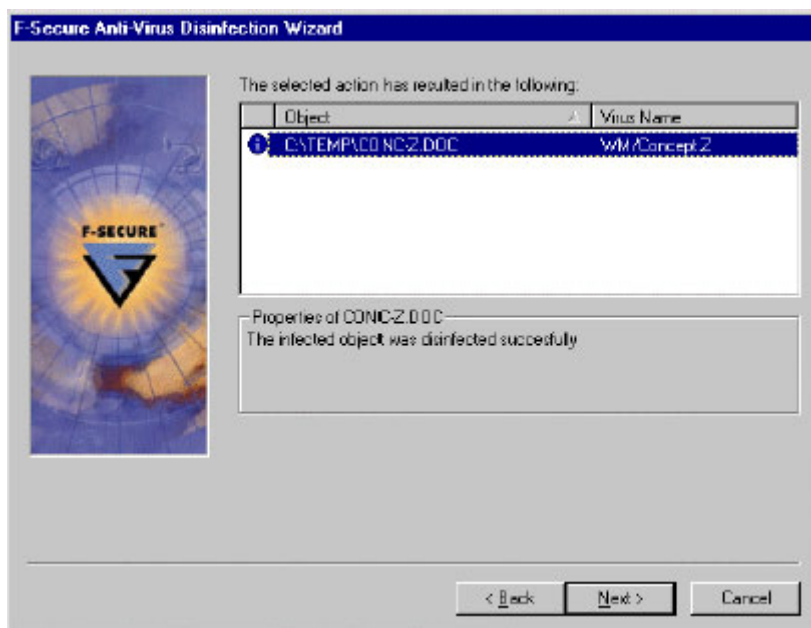
Dejanje Razlaga

Razkuži	Čarovnik za razkuževanje razkuži okuženo datoteko. Pozor: Če čarovnik za razkuževanje ne more razkužiti datoteke, jo bo avtomatsko poskusil preimenovati.
Izbriši	Čarovnik za razkuževanje izbriše datoteko, ki vsebuje virus. Vse informacije v datoteki bodo izgubljene. Opozorilo: Če izberete Delete (brisanje), bo izbrisan tudi objekt, ki je okužen.
Preimenuj	Čarovnik za razkuževanje preimenuje datoteko, ki vsebuje virus, tako da je ni mogoče zagnati. To prepreči aktiviranje virusa.

Ko ste izbrali dejanje za izvedbo, kliknite Next in čarovnik za razkuževanje bo izvedel dejanje samodejno na vseh izbranih objektih.

3. korak - Rezultat dejanja

Izpišejo se rezultati dejanja. Če izberete dejanje, ki ni uspelo, lahko greste nazaj in ponovite 2. korak in izberete drugo možnost.



Če razkuževanje in brisanje ne uspe, se lahko po izbiri odločite za preimenovanje datoteke. To je tipično dobro za okužene izvršne datoteke (.exe), saj preimenovanje spremeni končnico datoteke, tako se datoteka samodejno ne more zagnati.

Prosimo upoštevajte, da če razkuževanje ni uspelo, je čarovnik za razkuževanje lahko že avtomatsko preimenoval datoteko (glejte tabelo ukrepov zgoraj). O temu boste videli obvestilo v polju *Properties* (lastnosti).

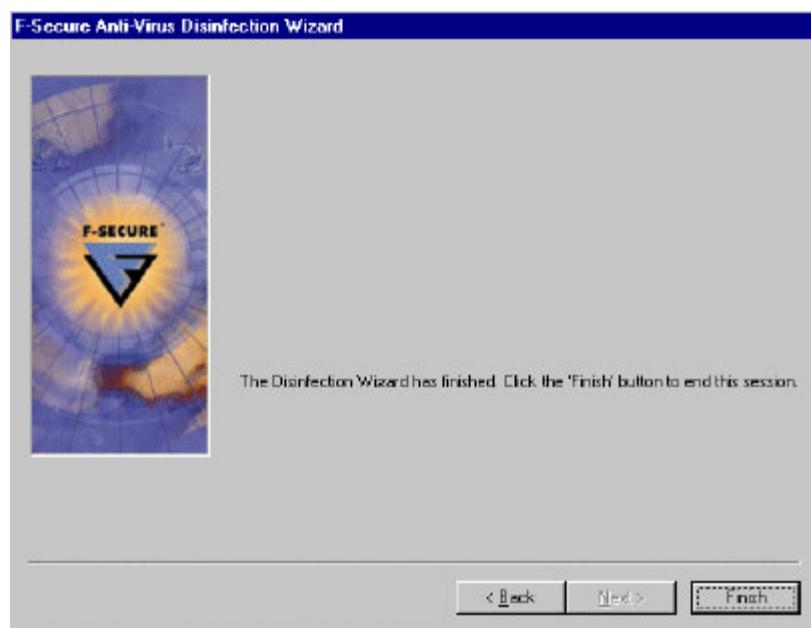
Pozor: V primeru, da je najden nov virus, stare definicije virusov ali lažni alarm, lahko razkuževanje ali brisanje ne uspe. Za navodila, kaj storiti v takem primeru, glejte [Odstranjevanje virusa, kadar Čarovnik za razkuževanje ne uspe](#).

Če je operacija uspela, kliknite **Next** za nadaljevanje.

4. korak - Pregled in konec

Po končanem procesu razkuževanja se ustvari poročilo o razkuževanju. Če ne želite ustvarjanja poročila, izpraznite potrditveno polje Generate Report. Prosimo upoštevajte, da poročilo o razkuževanju ne bo ustvarjeno za viruse, ki so bili najdeni med samodejnim pregledovanjem.

Kliknite gumb **Finish**, za izhod iz čarovnika za razkuževanje.



Poročilo o razkuževanju se prikaže v vašem privzetem spletnem brskalniku in vsebuje povezave na ustrezne opise virusov v Web Club bazi virusov.

Pozor: Če je bil virus najden v datoteki, ki jo je zaklenil drug proces takrat, ko jo je čarovnik za razkuževanje hotel odstraniti, se prikaže okno z zahtevo po ponovnem zagonu računalnika. Če vidite to okno, shranite vse odprte dokumente in nadaljujte po navodilih, ki so navedena v oknu.

Odstranjevanje virusa, kadar Čarovnik za razkuževanje ne uspe

Če čarovnik za razkuževanje ni uspel razkužiti ali izbrisati datoteke, je to morda zaradi naslednjih razlogov:

- Baza definicij virusov je zastarela. Prosimo, prepričajte se, ali imate najnovejšo definicijo datotek, in poskusite znova (glej Poglavlje 6: Samodejne posodobitve)
- Lažni alarm. Po najboljših močeh smo poskrbeli, da varovalni sistem ne misli, da je neškodljiva datoteka okužena, toda zaradi kompleksne narave datotek lahko varovalni sistem sumi tudi varno datoteko.
- Potrebno je ročno razkuževanje. V nekaterih primerih morate pognati orodje, ki razkuži datoteko in odstrani virus. To se pogosto zgodi pri modernih - najnovejših virusih, ki uporabljajo napredne tehnike skrivanja in se prilepijo k vašim datotekam.
- Odkrili ste nov virus. Morda je nova vrsta virusa okužila vaš računalnik. Ne ustrašite se. Vaše datoteke so trenutno varne, ker je varovalni sistem odkril in zaustavil virus, preden je le-ta utegnil povzročiti škodo.

Če ste prepričani, da je datoteka varna, lahko ignorirate opozorila. Lahko nastavite Automatic protection (Samodejno zaščito) in Manual scanning (Ročno pregledovanje), da v prihodnje ne pregleduje več te datoteke. To naredite tako, da pregledate Nastavitve zaščite.

Kako ročno odstranite virus?

1. Poskusite sami razkužiti datoteko. Pri odstranjevanju virusa vam bo v pomoč, če:
 - Preverite F-Secure Computer Virus Info Center na naslovu <http://www.f-secure.com/v-descs/> za informacije o virusu. Informacije o virusu vam bodo pomagale odstraniti virus in lahko vsebujejo tudi povezavo (link) na potrebno orodje za odstranitev virusa.
 - Napredni uporabniki: Pojdite direktno na <ftp://ftp.europe.f-secure.com/anti-virus/tools/>, da boste našli orodje za razkuževanje, ki vam bo v pomoč.

Orodja vsebujejo tudi vsa potrebna navodila, po katerih se ravnate pri odstranjevanju virusa iz vašega sistema.

2. Če ste poskušali s Čarovnikom za razkuževanje brez uspeha in je vaša baza definicij virusov- posodobljena-, pa kljub temu niste mogli uspešno uporabiti nobenega orodja za razkuževanje s spletne strani F-Secure tools Website, ravnajte po navodilih v Kaj pa, če sumite, da ste našli nov virus?.

4.4 Kaj pa, če sumite, da ste našli nov virus?

Če vas varovalni sistem opozarja, da imate okuženo datoteko z virusom, vendar ga ne more imenovati, razkužiti ali odstraniti, je to lahko čisto nov virus. Dokler niste prepričani, da je bil morebitni virus odstranjen ali je bil to le lažni alarm, ne poskušajte uporabljati te datoteke.

Pri odstranjevanju virusa ravnajte po naslednjih navodilih:

1. Prepričajte se, ali je vaša baza definicij virusov posodobljena. Novejša datoteka z definicijami vam lahko pove, kako ravnati pri odstranjevanju virusa iz vašega računalnika.
2. Če že imate najnovejše definicije virusov (glej Samodejne posodobitve), preverite na spletni strani F-Secure, ali obstajajo kakšna orodja za ročno odstranjevanje tega virusa (<http://www.f-secure.com/v-descs/> ali <ftp://ftp.europe.f-secure.com/anti-virus/tools/>).
3. Če vam predhodni koraki ne uspejo, pošljite datoteko v laboratorij F-Secure VirusLab. Za navodila se obrnite na: <http://www.f-secure.com/support/technical/general/samples.shtml>.

4.5 Nastavitve zaščite

V določenih primerih morda želite nastaviti zaščito pred virusi tako, da ne upošteva datotek določenega tipa, ali da ne upošteva specifičnih datotek. To so lahko primeri:

- Če ste prepričani, da datoteka ni okužena, ampak prejimate le lažne alarme.
- Vaš računalnik ima omejene vire (zmogljivosti) in bi z nastavitvijo Zaščita pred virusi za pregledovanje vseh datotek upočasnili vaš računalnik na neuporabno (premajhno) hitrost.
- Datoteka je takšnega tipa, da se nikoli ne okuži z virusom.

Nekateri profili že nastavijo samodejno pregledovanje določenih tipov datotek. To nudi dobro ravnovesje pregledovanja datotek, kjer so virusi pogosto oz. značilno odkriti, ne da bi to zavzelo preveč procesorskega časa in pomnilnika.

Opozorilo: Nastavitev zaščite pred virusi, da ignorira določene datoteke, izpostavlja te datoteke ranljive za prihodnje napade virusov in omejuje sposobnost pregledovalnika virusov, da najde in razkuži viruse. Priporočljivo je le za ekstremne primere.

Nastavljanje zaščite v realnem času ali Ročnega pregledovanja za pregled izbranih datotek

Zaščito v realnem času ali Ročnega pregledovanja za pregled izbranih datotek nastavite tako:

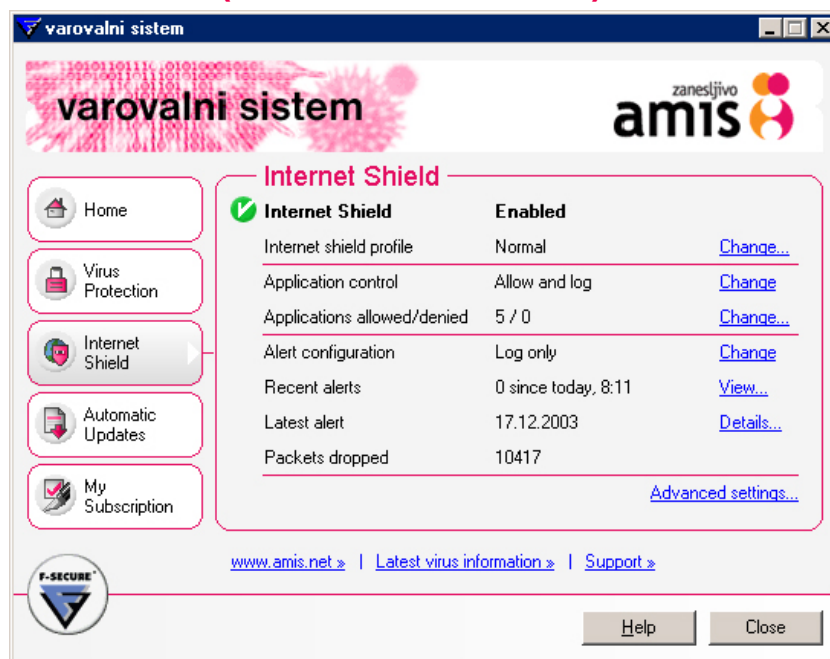
1. Odprite glavno okno varovalnega sistema .
2. Izberite stran zaščite pred virusi in kliknite na **Advanced Settings** (Napredne nastavitve). V zavihkih **Zaščita v realnem času** in **Ročno pregledovanje** se prepričajte, da se pregledajo datoteke z naslednjimi končnicami:

Nastavljanje zaščite v realnem času ali Ročnega pregledovanja za ignoriranje izbranih datotek

Zaščito v realnem času ali Ročno pregledovanje za ignoriranje izbranih datotek nastavite tako:

1. Odprite glavno okno varovalnega sistema .
2. Izberite stran zaščite pred virusi in kliknite na **Advanced Settings** . V zavihkih **Zaščita v realnem času** in **Ročno pregledovanje** se prepričajte, da:
 - je označena funkcija **Exclude files with these extensions** (Izključi datoteke z naslednjimi končnicami), in vnesite končnice datotek v tekstovno okno.
 - Označena je funkcija **Exclude Objects (files, folders...- Izključi objekte, datoteke, mape ...)**. Kliknite **Select** za brskanje po datotekah, ki jih želite izključiti in jih dodati na seznam datotek za izključitev.

5. Internet Shield (Internetna zaščita)



Na domači strani Internet Shield (internetne zaščite) lahko:

- Izberete vaš profil Internet Shield (profil internetne zaščite). Za več informacij glejte [Profili internetne zaščite](#).
- Spremenite status Application Control (nadzor aplikacij). Za to kliknite **Change** zraven obstoječega statusa Application Control.
- Preglejte, koliko aplikacij se sme, oziroma se sme povezati v internet. Za spremembo pravice do povezave za določeno aplikacijo, glejte [Spreminjanje pravice do povezave za določeno aplikacijo](#).
- Spremenite vaše nastavitve opozoril. Za to kliknite **Change** poleg tekočega statusa.
- Preglejte, koliko opozoril ste dobili od določenega datuma. Kliknite gumb **View**, da vidite seznam opozoril.
- Preglejte, koliko paketov ste zavrgli. Internet Shield (internetna zaščita) vedno zavrže znane nevarne pakete, toda tudi vi lahko vplivate na zadrževanje paketov tako, da po meri nastavite pravila internetne zaščite. (Za navodila glejte [Prirejanje pravil internetne zaščite po meri](#)).
- Preverite, kdaj ste nazadnje dobili opozorilo internetne zaščite. Kliknite gumb **Details**, da vidite podrobnosti zadnjega opozorila in pet najbolj blokiranih protokolov in strežnikov (IP naslovov).

5.1 Profili internetne zaščite

Profili internetne zaščite vam omogočajo, da v trenutku spremenite vaš nivo zaščite v skladu z vašimi potrebami. Tako, da se zagotovi zaščita pred najnovejšimi oblikami zlonamernih računalniških programov in internetnih napadov.

Spreminjanje vašega profila internetne zaščite

Profile lahko spremenite kadarkoli, glede na varnostno zaščito, ki jo potrebujete. Sprememba vašega izbranega profila spremeni nivo avtomatskih dejanj in poročanja.

Spremenite vaš profil internetne zaščite kot sledi:

1. Kliknite **Change**.
2. Izberite profil iz spustnega seznama. Prosimo preberite opis vsakega profila, preden ga aktivirate.

3. Kliknite gumb **OK**, da začnete uporabljati izbrani profil.

Za prirejanje profila po meri, glejte **Prirejanje pravil internetne zaščite po meri**.

5.2 Uporaba Nadzora aplikacij

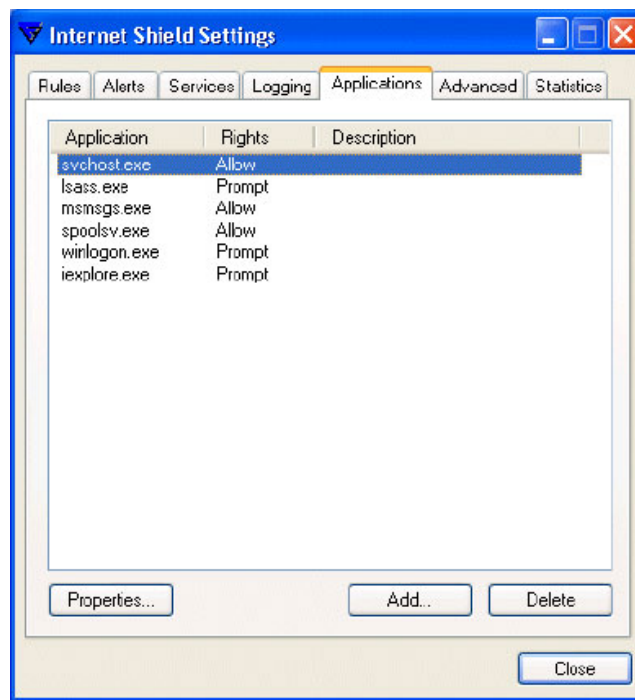
Application Control (nadzor aplikacij) je možnost varovalnega sistema, ki preverja vse aplikacije, ki se z vašega računalnika povezujejo v internet. Pojavi se sporočilo „Application Control“, ki vas vpraša, ali naj dovoli ali zavrne poskus vzpostavljanja povezave, kot je opisano v „**Kaj storiti, ko se pojavi Application Control prikazovalno okno**“. Varne in znane aplikacije bi morale imeti dovoljeno vzpostavljanje povezav v internet, zaupanja nevrednim aplikacijam pa bi morali onemogočiti povezave.

Datoteka z imenom Action Log (dnevnik dejanj) beleži vse povezave in njihove lastnosti, da lahko vidite, kam se je vaš računalnik povezal. Za dostop kliknite **Advanced Settings**, nato zavihek **Logging**.

Spreminjanje pravice do povezave za določeno aplikacijo

Za spremembo pravice do povezave za določeno aplikacijo, naredite naslednje:

1. Pojdite na stran Internet Shield (internetne zaščite) in kliknite Change zraven Applications allowed/denied (aplikacije dovoljene/zavrnjene).
2. Odpre se stran *Internet Shield Settings* (nastavitve internetne zaščite).



3. Izberite aplikacijo, katere lastnosti bi radi spremenili (tekoče pravice so navedene v stolpcu Rights (pravice)). Kliknite **Properties** (Lastnosti).
4. Izberite Deny (Zavrni), Prompt (Vprašaj), ali Allow (Dovoli). Kliknite gumb **OK** za vrnitev na stran aplikacij.
5. Nove pravice aplikacije bodo navedene poleg imena aplikacije. Kliknite **Close** (zapri) za konec.

Kaj lahko smatramo za »varno«?

- Znano aplikacijo, katero ste aktivno zagnali sami.
- Storitve sistema Windows, ki se povezujejo v internet.

Varne storitve Microsoft Windows

Nekatere storitve Microsoft Windows potrebujejo omrežni dostop za delovanje. Večina teh storitev ima avtomatski dostop, toda Application Control lahko vpraša za naslednje servise, še posebno na platformah Windows NT 4.0, Windows 2000 in Windows XP. Prosimo, da tem omogočite dostop do omrežja, sicer lahko Windows ne deluje popolnoma.

Seznam aplikacij

Pozor: %Winnt% se nanaša na imenik namestitve Windows, navadno C:\Winnt\

Izvršilna datoteka	Nahajališče	Opis	Omrežni promet
SVCHOST.EXE	%Winnt%\System32\	Generični gostiteljski proces za Win32 storitve	udp/67 ven, udp/68 notri, udp/137 ven
SPOOLSV.EXE	%Winnt%\System32\	Spooler Subsystem App	udp/137 ven, udp/138 ven
LSASS.EXE	%\Windows%\System32\	LSA izvršilna datoteka in strežniška DLL	udp/137 ven
SERVICES.EXE	%Winnt%\System32\	Services and Controller app	udp/67 ven, udp/68 notri, udp/137 ven
WINLOGON.EXE			udp/137 ven

Kaj lahko smatramo za »nevarno«?

Do katerekoli aplikacije, katero smo prejeli iz zaupanja nevrednega vira, moramo vedno postopati s sumom. Do katerekoli aplikacije, katero smo prejeli zaupanja vrednega vira, a brez predhodnega dogovora, moramo ravno tako smatrati za sumljivo.

- Katerakoli aplikacija, ki je niste aktivno namestili sami, ali ne veste zanjo.
- Aplikacija, ki jo smatrate za varno, a poskuša vzpostaviti povezavo brez da bi vi to zahtevali.
- Povezava, ki nima primerne imena cilja (spletni naslov v besedilu).

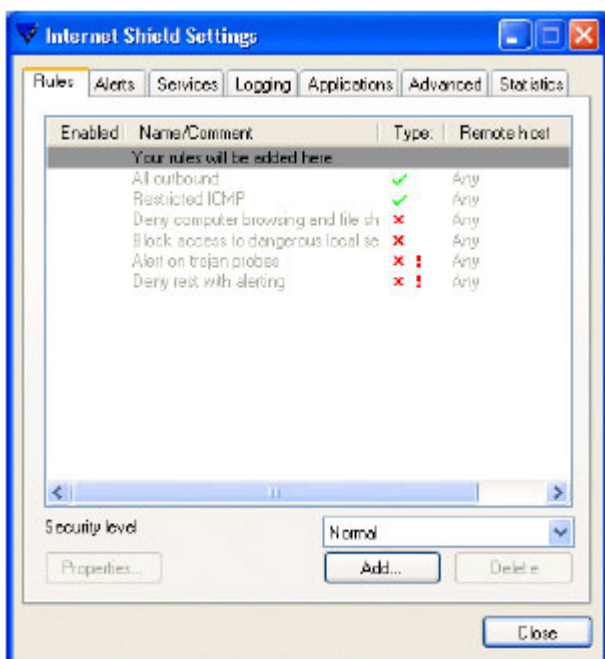
5.3 Prirejanje pravil internetne zaščite po meri

Obstajajo situacije, ko bi želeli dodati, spremeniti ali izbrisati pravila, ki določajo kaj storiti z nekaterimi povezavami. Tovrstne situacije so možne, kadar boste želeli:

- Povezava do strežnika za igranje iger ali točno določenega računalnika.
- Dovoliti splošne povezave, a blokirati povezavo do določene spletne strani ali računalnika, kateremu ne zaupate.

Za prirejanje nastavitve internetne zaščite po meri:

1. Kliknite Advanced Settings (napredne nastavitve) na strani internetne zaščite. Odpre se okno z naprednimi nastavitvami.
2. V meniju Security Level (varnostni nivo) izberite profil, ki ga želite prirediti.
3. Kliknite zavihek Rules (pravila), če ni že izbran.



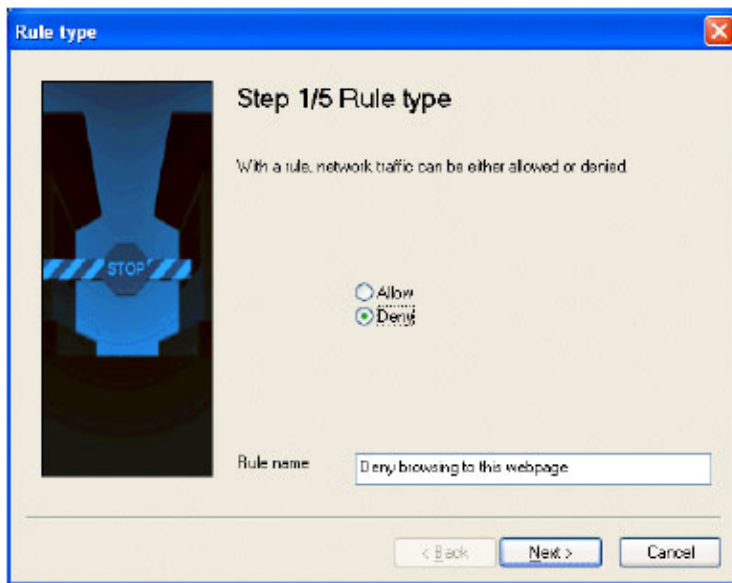
- Za spremembo obstoječega pravila, izberite pravilo s seznama in kliknite **Properties** (lastnosti).
- Za dodajanje novega pravila, kliknite **Add** (dodaj).
- Za brisanje pravila, izberite pravilo s seznama in kliknite **Delete** (izbriši).

Pozor: Prednastavljenih pravil ni mogoče spreminjati ali brisati. Lahko samo dodate nova pravila in spremenite in brišete pravila, ki ste jih sami dodali.

Ustvarjanje novega pravila internetne zaščite

1. korak - tip pravila

Pravilo poimenujte z opisnim imenom in izberite ali dovoljenje ali prepoved povezave.



2. korak - določite cilj(e)

Izberite, ali to pravilo velja za vse povezave ali samo za določene.



Lahko:

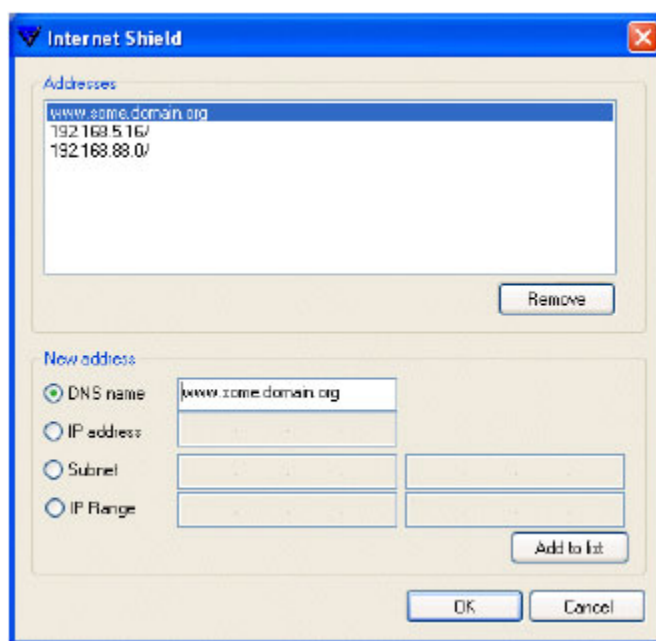
- preverite katerikoli IP naslov za uporabo pravila za vse internetne povezave, in kliknite **Next** za nadaljevanje na 3. korak ali
- odkljukajte katerikoli IP naslov in kliknite **Edit**, da odprete novo okno, kjer lahko vnesete podrobnosti o ciljih.
- cilji so lahko navedeni v kakršnem koli vrstnem redu in so lahko DNS ime, IP naslov, področje (v bitnem formatu omrežne maske) ali niz IP naslovov. Na primer:

DNS ime: www.neka.domena.org

IP naslov: 192.168.5.16

Podomrežje: 192.168.88.0/29

IP niz naslovov: 192.168.1.1-192.168.1.63

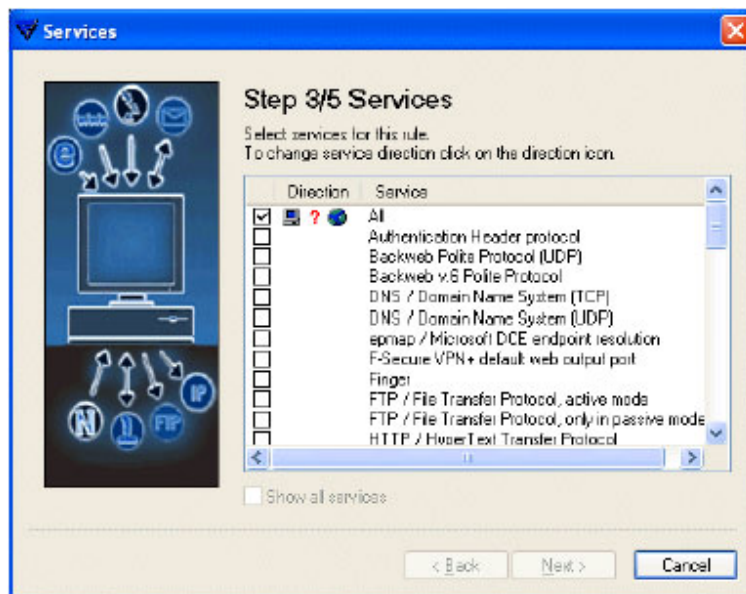


- Kliknite **Add to list** (dodaj na seznam), da dodate nov cilj na seznam ciljev, na katere se nanaša to pravilo. Za brisanje pravila, izberite pravilo s seznama in kliknite **Remove** (odstrani). Za urejanje lastnosti cilja, izberite naslov cilja s seznama. Kliknite gumb **OK** za vrnitev na stran Oddaljenih strežnikov in kliknite **Next** (naprej) za nadaljevanje.

3. korak: izberite storitev in smer pravila

Izberite storitev, na katero se bo nanašalo to pravilo s seznama storitev, ki so na voljo. Če želite, da pravilo velja za vse storitve, izberite *All* (vse) z vrha seznama.

Lahko izberete tolikšno število storitev, kot potrebujete.



Za izbrane storitve izberite smer, za katero bo pravilo veljalo, s klikom na rdeč vprašaj, ki se pojavi. Možne izbire se ciklično pojavljajo ob klikih. Za primere glejte spodnjo tabelo.

Izbira Termin Razlaga

	Nedefinirano	Smer še ni določena. Kliknite sliko za zaključek definiranja smeri.
	Prihajajoče	Storitev bo dovoljena / zavrnjena, če prihaja z interneta v vaš računalnik.
	Odhajajoče	Storitev bo dovoljena / zavrnjena, če gre iz vašega računalnika v internet.
	Oboje	Storitev bo dovoljena / zavrnjena, če gre v / iz vašega računalnika v obeh smereh.

4. korak - izberite beleženje in poročanje

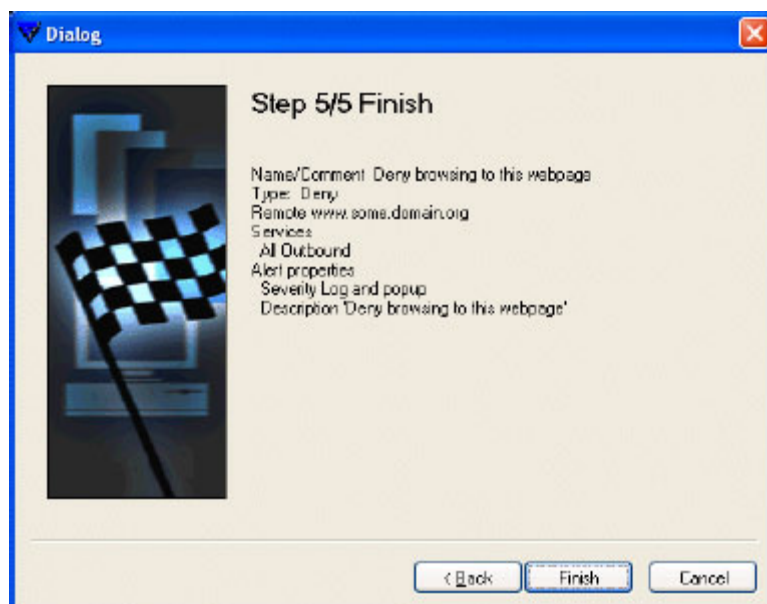
Izberete lahko, če želite biti obveščeni, kadarkoli se pravilo uporabi na poskusu povezave.



- *No alert* (ni opozorila) pomeni, da ne dobite informacije ko se pravilo uporabi nad povezavo.
- *Log* (beleženje) pomeni, da se podatki o povezavi beležijo v datoteko.
- *Log and pop-up* (beleži in opozori) pomeni, da se podatki beležijo in da dobite opozorilo, npr. kadar je povezava dovoljena / zavrnjena.

5. korak - Preglejte in odobrite pravilo

Sedaj lahko pregledate pravilo. Kliknite gumb **Back** (nazaj) v pravilu, če želite kaj spremeniti.



Če ste s pravilom zadovoljni, kliknite **Finish** (končaj). Vaše novo pravilo bo dodano na vrh seznama aktivnih pravil v zavihku Rules v nastavitvah internetne zaščite.

5.4 Napredne nastavitve

Pozor: Ta razdelek je samo za izkušene uporabnike računalnika. Internetno zaščito lahko izključite s spreminjanjem nastavitvev.

Za dostop do naprednih nastavitvev internetne zaščite, kliknite **Advanced Settings** (napredne nastavitve), na strani internetne zaščite. Kliknite zavihek Advanced v oknu, ki se pojavi.

Ko nastavljate napredne nastavitve internetne zaščite, upoštevajte naslednje postavke:

1. Zaupanja vreden vmesnik

Zaupanja vreden vmesnik se lahko uporablja, če je računalnik z varovalnim sistemom nameščen kot internetni prehod, t.j. če je vklopljena funkcija Windows Internet Connection Sharing (skupna raba povezave v internet). Omrežni vmesnik, ki se uporablja za krajevno omrežje, lahko nastavimo kot »Trusted Interface« (zaupanja vreden), tako da internetna zaščita ne velja na njem.

Pozor: Ta omrežni vmesnik bo popolnoma odprt in nezaščiten.

2. Filter paketov

Filtriranje paketov je glavno opravilo internetne zaščite. Če ga izklopite, bo večinoma neučinkovito proti vsem tipom omrežnih napadov.

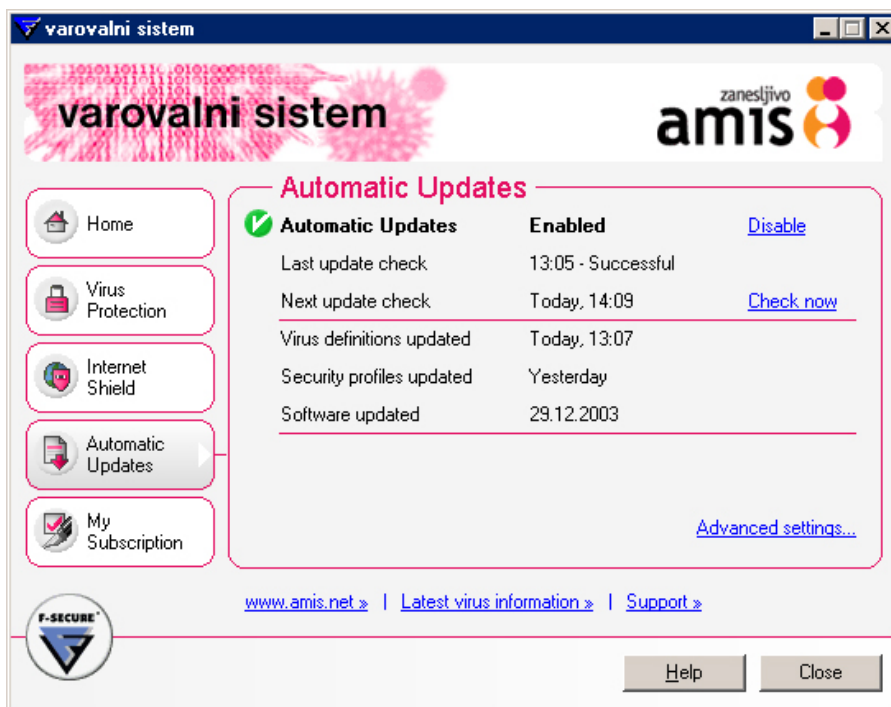
3. Nadzor aplikacij

Ne izklaplajte nadzora aplikacij v oknu naprednih nastavitvev. Izklop nadzora aplikacij poveča nevarnost napadov na osnovi programske opreme. Ne izklaplajte, razen če je potrebno za razreševanje težav ipd.

Če želite izklopiti nadzor aplikacij, pojdite na stran internetne zaščite in spremenite status nadzora aplikacij iz *Prompt* (opozori) v *Allow and log* (dovoli in beleži).

6. Samodejne posodobitve

Možnost samodejnih posodobitev se nevidno aktivira v ozadju vedno, ko se povežete na Internet, in vam zagotovi, da nevidno prejmete najnovejše posodobitve v vaš računalnik.



V poglavju o samodejnih posodobitvah lahko:

- kliknete **Enable**, da aktivirate, ali **Disable** za deaktiviranje Automatic Updates (Samodejnih posodobitev).
- Poglejte, kdaj je bil opravljen najnovejši pregled posodobitev, in/ ali kdaj se bo izvršila naslednja posodobitev.
- Če želite osebno preveriti, ali imate najnovejše definicije virusov, kliknite **Check Now** (Preveri zdaj). Če vaše definicije niso bile posodobljene, se naložijo najnovejše verzije.

Pozor: Če uporabljate modem, ali imate povezavo ISDN na Internet, mora biti povezava aktivna, da lahko pregledate posodobitve.

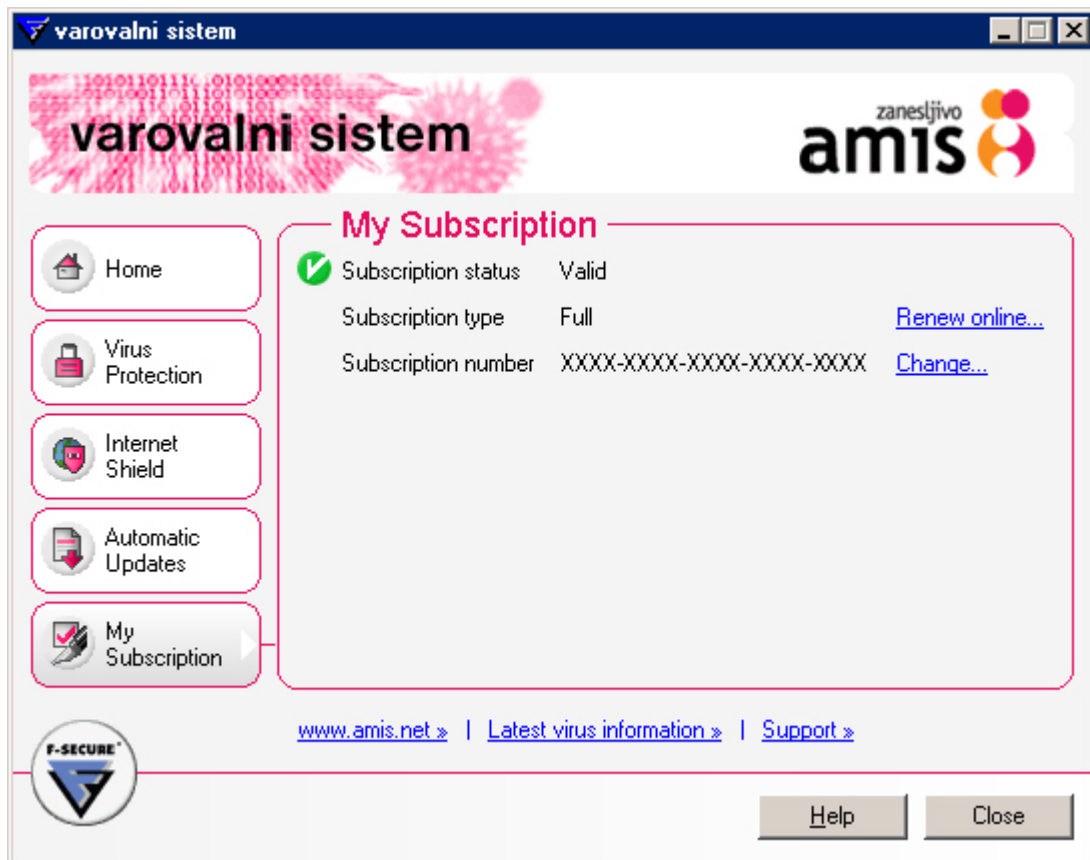
Opozorilo uporabnikom ISDN: Po privzeti vrednosti so samodejne posodobitve predvidene enkrat na uro. To pomeni, da bo zveza z Internetom vzpostavljena enkrat na vsako uro, če imate ISDN usmerjevalnik ali podobno samodejno vzpostavljanje zveze (in vsaka zveza je plačljiva). Če želite preprečiti, da vaš ISDN usmerjevalnik samodejno kliče, izključite Automatic Updates in uporabite gumb **Check now**, da preverite posodobitve.

- Preverite, kdaj je bila vsaka od spodnjih treh možnosti posodobljena.




Definicije virusov	Pogosto posodobljena baza podatkov za protivirusno zaščito. Te samodejne posodobitve se opravijo nevidno v ozadju, ne da bi vi morali karkoli storiti, in se aktivirajo vsakič, ko se povežete na Internet.
Varnostni Profili	Različni nivoji varnostnih nastavitev. Za kar največjo zaščito vašega računalnika se profili posodobijo vsakič, ko odkrijejo nove vrste napadov.
Programska oprema	Posodobitve programske opreme varovalni sistem (Varna uporaba interneta), ki se naložijo v ozadju.

7. Moja naročnina

Stran »Moja naročnina« prikazuje informacije o vašem osebnem naročniškem razmerju.



Na strani My Subscription (moja naročnina) lahko:

- Vidite status vašega naročniškega razmerja. Datum poteka vašega naročniškega razmerja je naveden s tekočim statusom, kot tudi ena od sledečih statusnih ikon:
 -  Veljavnost Vaše naročniško razmerje je veljavno.
 -  Skorajšnji potek Vaše naročniško razmerje veljavno, toda kmalu bo poteklo.
 -  Poteklo Vaše naročniško razmerje je poteklo.
- Obnovite vaše naročniško razmerje (ali če uporabljate izdelek v načinu vrednotenja, lahko naročniško razmerje sklenete).
- Spremenite vašo številko naročniškega razmerja.

8. Kako varovalni sistem varuje vaš računalnik

8.1 Zaščita pred virusi

Zlonamerna programska oprema (»malware«, iz »malicious software«) je izraz, ki se uporablja za različne oblike programov ali datotek, kot so virusi, trojanski konji, šale in potegavščine, razvite za namen povzročanja škode na vašem računalniku.



Zaščita pred virusi zazna in odstrani viruse in druge zlonamerne računalniške programe iz vašega računalnika. Ob vsakem dostopu do datoteke bodisi iz vašega trdega diska bodisi iz zunanjega pomnilnika ali iz interneta, protivirusna zaščita varovalnega sistema pregleda datoteko, če vsebuje viruse.

Aktualna protivirusna zaščita je kombinirana s samodejnim posodabljanjem definicij virusov, da vam nudi najboljšo možno zaščito pred virusi. Raziskovalni laboratorij F-Secure Anti Virus redno objavlja in posodablja definicije virusov, profilov in programsko opremo varovalnega sistema, ki jo varovalni sistem hitro in samodejno naloži kadarkoli se povežete v internet.

F-Secure protivirusna zaščita uporablja več sredstev za pregledovanje virusov, da zagotovi popolno zaščito pred virusi. Od teh, hevristična metoda pregledovanja varuje predvsem pred novimi in neznanimi virusi.

8.2 Internet Shield (Internetna zaščita)

Kadarkoli se vaš računalnik poveže v internet, je tarča internetnih napadov iz neznanih virov. V nekaterih primerih ti napadi niso napadi kot taki, temveč neškodljivo sporočanje, ki je pomotoma zašlo do vašega računalnika. Vendar pa v drugih primerih, neznan oseb ali računalnik namenoma poskuša dostopati do vašega računalnika in datotek.

Varnost vašega računalnika je lahko ogrožena na več načinov, vključujoč naslednje:

- Storitve, ki so ne namenoma ostale odprte in jih zunanji napadalci z lahkoto najdejo in zlorabijo.



Internetna zaščita varuje vaš računalnik, medtem ko ste povezani v internet. Dovolj samo povezave v in iz vašega računalnika, ki so navedene v vašem izbranem profilu. Ves ostali promet ni dovoljen, tako se učinkovito zmanjša možnost vsiljivca, da vidi / spremeni podatke na vašem računalniku.

- Vaš računalnik oddaja informacije o sebi, ko se poveže v internet. Vsakdo, ki pozna način za branje tovrstnih informacij, jih lahko uporabi kot osnovo za napad na vas.



Internetna zaščita zaustavi oddajanje informacij iz vašega računalnika v internet, kot tudi kakršnekoli odhodne povezave, skozi katere uhajajo podatki o vašem računalniku.

- Nekateri trojanski konji se skrivajo znotraj programov, ki jim navadno zaupate. To naredijo tako, da uporabljajo povezavo ali aplikacijo, za katero vi mislite, da je varna za prenos podatkov o vas ali vašemu računalniku.



Internetna zaščita prepozna poskuse trojanskih konjev po prenosu podatkov in prepreči povezavo, in s tem zavaruje vaše podatke vsakokrat pred neželenimi napadi.

8.3 Kako lahko vi prispevate k izogibanju virusov in druge zlonamerne programske opreme?

Uporaba varovalnega sistema je najboljša obrambna črta proti virusom, saj zaustavi katerikoli znan virus, preden okuži vaš računalnik. Kakorkoli, lahko tudi vi pomagate varovati vaš računalnik:

- Posodablajte vaš operacijski sistem in aplikacije ter namestite zadnje popravke, kadar so na voljo. Prepričajte se, da nalagate popravke direktno od proizvajalca.
- Vedno shranite datoteke, ki jih naložite z interneta, na trdi disk, preden jih odprete ali zaženete. Shranjevanje datoteke, ki jo prenesete k sebi, zagotavlja, da jo varovalni sistem preveri.
- Večina internetnih črvov uporablja elektronsko pošto za širjenje in ciljajo na uporabnike paketov Microsoft Outlook ali Outlook Express. Če morate uporabljati katero koli verzijo programa Outlook, redno pregledujte, prenesite in naložite zadnje varnostne popravke za Outlook od Microsofta.
- Ko dobite oglase po elektronski pošti, ostalo nezahtevano elektronsko pošto, ali če se vam zdi, da je sporočilo, ki ste ga prejeli od prijatelja nekako čudno, ne odpirajte priponk in ne sledite navedenim spletnim povezavam. Če želite videti priponko, jo shranite na vaš trdi disk, preden jo odprete. To zagotovi, da varovalni sistem preveri priponko, ali vsebuje viruse.
- Izogibajte se datotekam iz javnih novičarskih skupin in on-line sporočilnih sistemov, kot je IRC in ICQ.
- Izogibajte se posredovanja virusnih sporočil ali verižnih pisem, ki jih dobite od drugih.

Reševanje težav

Namestitev

V: Namestitev ni uspela. Kaj se je zgodilo?


O: Če ni bilo povezave v internet, varovalni sistem ni mogel potrditi vaše naročnine. Prepričajte se, da imate vzpostavljeno povezavo v internet in znova namestite varovalni sistem.

Splošna uporaba

V: Varovalni sistem deluje zelo počasi in / ali se ne odpre. Kaj je narobe?

O: Internet Explorer 3.0 ali novejši morda ni nameščen. Preverite, če imate naložen Internet Explorer in preverite številko verzije (Internet Explorer je na voljo s spletne strani podjetja Microsoft).

V: Ne morem videti ikone varovalnega sistema v sistemskem polju v spodnjem desnem vogalu zaslona.

O: V okolju Windows XP so ikone lahko skrite. Za prikaz skritih ikon, kliknite na gumb . Če ne uporabljate Windows XP, potem namestite varovalni sistem.




Zaščita pred virusi

V: Varovalni sistem ne more razkužiti/izbrisati/preimenovati okužene datoteke na mojem računalniku. Kaj storiti?

O: Glej Odstranjevanje virusa, kadar Čarovnik za razkuževanje ne uspe.

V: Med nameščanjem programske opreme me protivirusna zaščita obvesti o virusu in zaradi tega ne morem zaključiti namestitve.

O: Če ste gotovi, da programska oprema, ki jo nameščate, ne vsebuje nobenega virusa, lahko storite naslednje:

- Izberite manj strog profil protivirusne zaščite, glejte Spreminjanje profila zaščite pred virusi.
- Z desnim gumbom miške kliknite na  ikono v sistemskem polju (spodaj desno na vašem zaslonu) in izberite *Unload F-Secure products* (odstrani izdelke F-Secure iz pomnilnika). Ne pozabite ponovno zagnati izdelke po končani namestitvi.



Internet Shield (Internetna zaščita)

V: Zdi se mi, da me napada vsiljivec z interneta. Kaj storiti?

O: Pojdite na stran internetne zaščite in izberite profil Block All (blokraj vse). Za več informacij o izbiranju profilov internetne zaščite, glejte Spreminjanje vašega profila internetne zaščite.

Nadzor aplikacij

V: Kako lahko spremenim pravice aplikacije do povezave v internet? Kako dovolim povezavo aplikaciji, ki ji prej povezava v internet ni bila dovoljena?

O: Glej Spreminjanje pravice do povezave za določeno aplikacijo.

V: Moj program za elektronsko pošto (ali kakšen drugi program, npr. internetni brskalnik) je prenehal delovati.

O: Morda ste mu nehote prepovedali vzpostavljane povezave. Glejte Spreminjanje pravice do povezave za določeno aplikacijo za informacije o dovoljevanju povezave za program.

V: Katerim programom/aplikacijam lahko dovolim povezovanje v internet?

O: Glejte Uporaba Nadzora aplikacij, za pomoč pri odločanju, katerim programom naj dovolim (ali pa ne) povezovanje v internet.



Samodejne posodobitve

V: Kaj se zgodi, če moj računalnik ni priključen v internet v trenutku, ko je predvideno samodejno posodabljanje definicij virusov?

A: Ko boste naslednjič povezani v internet, bo varovalni sistem naložil zadnje samodejne posodobitve definicij virusov.

V: Kako pogosto naj bi se posodabljala baza definicij virusov?

O: Baza definicij virusov se samodejno posodablja, če imate vključeno možnost samodejnega posodabljanja. Če bi želeli ročno posodobiti bazo, potem morate to storiti vsaj enkrat na teden.

V: Želim ročno preveriti za posodobitve baze definicij virusov (s klikom na Check Now (Preveri zdaj)), a se nič ne zgodi.

O: Če uporabljate modem, ali imate povezavo ISDN na Internet, se morate ročno povezati v internet, preden kliknete **Check Now**.

Slovar

Aplikacija

Programska oprema, napisana za določen namen. Aplikacije navadno zaganjamo ročno.

Nadzor aplikacij

Application Control (Nadzor aplikacij), je možnost varovalnega sistema, da samodejno preveri aplikacijo, ki se iz vašega računalnika povezuje v internet tako, da jo preveri na seznamu varnih (vnaprej odobrenih) programov in na seznamu znanih zlonamernih programov (»trojanskih« programov).

Napadi vrste »zatajitev storitve« (Denial-of-Service)

Ekspliciten poskus napadalcev, da preprečijo legitimnim uporabnikom uporabo storitve s prekinitvijo povezave, »poplavljanjem« omrežja, ali preprečitvijo posamezniku dostop do omrežja.

DNS

Sistem domenskih imen (DNS) je metoda, ki locira in prevede imena internetnih domen v naslove internetnega protokola. Ime domene je smiselno in lahko pomnljivo »prijemališče« za internetni naslov. Internetni naslov www.neka.domena.org, je primer DNS imena.

Heuristika

Raziskovalno reševanje problemov z uporabo tehnik samodejnega učenja.

Zlonamerna programska oprema

Zlonamerna programska oprema (»malware«, iz »malicious software«) so programi ali datoteke, razvite za namen povzročanja škode. Ta vključuje računalniške viruse, internetne črve in »trojanske« programe (Trojan horses).

Paket

Paket je podatkovna enota, ki je usmerjena med izvorom in ponorom v internetu. Ko pošljemo datoteko (npr. e-poštno sporočilo) iz enega kraja do drugega v internetu, se datoteka razdeli v pakete primerne velikosti za učinkovito usmerjanje. Ko vsi paketi prispejo na cilj, se sestavijo v originalno datoteko.

Profil

Profili so prednastavljene lastnosti, ki nastavijo vaš nivo varnosti. Profili se samodejno posodabljaajo, da se zagotovi vaša zaščita pred najnovejšimi oblikami zlonamernih računalniških programov in internetnih napadov.

Podomrežje (»subnet«)

Del omrežja (angl. okrajšava za »subnetwork«). Običajno so računalniki znotraj istega podomrežja fizično blizu locirani in imajo IP naslove, ki se začnejo z istima dvema ali tremi številkami.

Trojanski konj

Program, ki namerno naredi nekaj, česar uporabnik programa ne pričakuje.

Virus

Računalniški program, ki se razširja z razmnoževanjem samega sebe.

Baza definicij virusov

Baze definicij virusov se uporabljajo za odkrivanje virusov. Kadarkoli najdejo nov virus, je potrebno posodobiti baze, da lahko protivirusna zaščita zazna ta virus.

Črv

Računalniški program, ki je sposoben razmnoževanja z vrivanjem kopij samega sebe v omrežne računalnike.

Podpora in vzdrževanje

Med trajanjem licenčnega obdobja, ki je enako vašemu naročniškemu obdobju, ste upravičeni do standardne podpore in storitev vzdrževanja, ki jih nudi F-Secure ali partner ponudnik F-Secure storitev. Po poteku licence pravice do vseh storitev, vključujoč posodobitve baze definicij virusov, potečejo in programska oprema lahko samodejno prekine delovanje, razen, če vašo licenco obnovite. Prosimo, stopite v stik z vašim ponudnikom licence za več informacij.

Ali ste kupili storitev od vašega ponudnika dostopa do interneta?

V kolikor ste storitev kupili od vašega ponudnika dostopa do interneta, boste samodejno dobili nadgradnje programske opreme in posodobitve baze definicij virusov na vaš računalnik. Za informacije o tehnični podpori in drugih storitvah vzdrževanja, prosimo glejte, vaš dogovor o storitvi z vašim ponudnikom dostopa do interneta.

Ali ste kupili storitev v trgovini ali v F-Secure spletni trgovini?

Če ste storitev kupili v trgovini, prosimo, da vašo licenco registrirate. To naredite tako, da izpolnete registracijski obrazec, vključen v škatli ali na spletni strani F-Secure na naslovu: <http://www.f-secure.com/register/>.

Z registracijo vaše licence boste imeli dostop do F-Secure storitev podpore in vzdrževanja. Če ste kupili storitev v F-Secure spletni trgovini, ste avtomatsko že registrirani.

Tehnična pomoč

Spletni center F-Secure tehnične podpore vam nudi obširno zbirko tehničnih dokumentov, ki vam nudijo rešitve na problemska vprašanja, rešitev večine pogostih težav pri nameščanju in navodila za odstranjevanje virusov. Če imate kakršne koli težave ali vprašanja, ki jih priročnik ali spletne storitve ne pokrivajo, prosimo da stopite v stik z podpornim osebjem prodajalca programa.

OPOZORILO: Brezplačna tehnična pomoč je namenjena samo registriranim uporabnikom.

Slovenija

On-line tehnična pomoč: http://www.amis.net/podpora/faq.php?CID=varovalni_sistem

E-Pošta: podpora@amis.net

Telefon: 080 20 10

Ostale države

On-line Tehnična pomoč: <http://www.f-secure.com/support/>

Vzdrževanje

Baza definicij virusov se samodejno posodablja na vašem računalniku za čas naročniškega razmerja. Če ste registrirali vašo licenco, vam lahko F-Secure od časa do časa nudi, brez dodatnih stroškov nudi nove verzije programske opreme, servisne pakete in popravke, katere lahko prenesete s spletne strani F-Secure. Za obširno zbirko z virusi povezanih informacij, prosimo, obiščite spletno stran F-Secure na naslovu: <http://www.f-secure.com/virus-info/>.