

McAfee®

Internet Security Suite 2008

Käyttöopas

Sisältö

McAfee Internet Security	3
McAfee SecurityCenter	5
SecurityCenterin ominaisuudet	6
SecurityCenterin käyttäminen	7
SecurityCenterin päivittäminen	13
Suojausongelmien korjaaminen ja ohittaminen	17
Hälytysten käsitleminen	21
Tapahtumien näyttäminen	27
McAfee VirusScan	29
VirusScan-ohjelman ominaisuudet	30
Reaaliaikaisen virustorjunnan käynnistäminen	31
Lisäsuojauksen ottaminen käyttöön	33
Virustorjunnan määrittäminen	37
Tietokoneen tarkistaminen	55
Tarkistuksen tulosten käyttäminen	59
McAfee Personal Firewall	63
Personal Firewall -ohjelman ominaisuudet	64
Palomuurin käynnistäminen	67
Hälytysten käsitleminen	69
Tiedottavien hälytysten hallinta	73
Palomuurisuojauksen asetusten määrittäminen	75
Ohjelmien ja käyttöoikeuksien hallinta	87
Järjestelmäpalveluiden hallinta	97
Tietokoneyhteyksien hallinta	103
Kirjaus, valvonta ja analyysi	111
Perehtyminen Internet-tietoturvaan	121
McAfee Anti-Spam	123
Anti-Spamin ominaisuudet	125
Web-sähköpostitilien määrittäminen	127
Ystävien määrittäminen	131
Roskapostiviestien tunnistustavan määrittäminen	137
Sähköpostin suodatus	145
Suodatettujen sähköpostiviestien käsitleminen	149
Phishing-huijausten torjunnan asetusten määrittäminen	151
McAfee-tietosuojapalvelu	155
Privacy Service -ohjelman ominaisuudet	156
Käytönvalvonnan määrittäminen	157
Tietojen suojaaminen Internetissä	173
Salasanojen suojaaminen	175
McAfee Data Backup	179
Ominaisuudet	180
Tiedostojen arkistointi	181
Arkistoitujen tiedostojen käsitleminen	189
McAfee QuickClean	195
QuickCleanin toiminnot	196
Tietokoneen puhdistaminen	197
Tietokoneen eheyttäminen	200

Tehtävän ajoittaminen	201
McAfee Shredder.....	207
Shredderin toiminnot	208
Tiedostojen, kansioden ja levyjen tuhoaminen	209
McAfee Network Manager.....	211
Network Managerin ominaisuudet.....	212
Network Managerin kuvakkeiden toiminta	213
Hallitun verkon määrittäminen	215
Verkon etähallinta	221
McAfee EasyNetwork.....	227
EasyNetworkin ominaisuudet.....	228
EasyNetworkin asentaminen	229
Tiedostojen jakaminen ja lähettäminen.....	235
Tulostinten jakaminen.....	241
Opas	243
 Sanasto	 244
 Tietoja McAfeesta	 259
Copyright	259
Käyttöoikeus	260
Asiakaspalvelu ja tekninen tuki	261
McAfee Virtual Technician -palvelun käyttö.....	262
Tuki ja lataukset	263
 Hakemisto	 272

L U K U 1

McAfee Internet Security

McAfee Internet Security Suite with SiteAdvisor on ennakoiva kymmenvaiheinen jatkuvasti päivittyvä tietoturvaohjelmistopaketti, joka suojaa tärkeitä tietojasi, henkilötietojasi ja tietokonettasi viruksia, vakoiluohjelmia, sähköposti- ja pikaviestihuijauksia, hakkereita ja Internet-rikollisia vastaan ja varmuuskopioi tärkeät tiedostot automaattisesti. Selaa Webiä, tee ostoksia, käytä pankkipalveluja, lähetä sähköposti- ja pikaviestejä ja lataa tiedostoja turvallisesti. McAfee SiteAdvisor ja käytönvalvonta-asetukset auttavat sinua ja perheenjäseniäsi välttämään epäluotettavia Web-sivustoja. McAfeen suojauspalvelu toimittaa tietokoneeseesi jatkuvasti ja automaattisesti uusimpia ominaisuuksia, parannuksia ja uhkapäivityksiä. Lisäksi automaattiset PC-hienosäätötoiminnot poistavat turhia tiedostoja, jotta tietokone toimii parhaan suorituskykynsä mukaan.

Tässä luvussa

McAfee SecurityCenter	5
McAfee VirusScan	29
McAfee Personal Firewall	63
McAfee Anti-Spam	123
McAfee-tietosuojapalvelu.....	155
McAfee Data Backup.....	179
McAfee QuickClean.....	195
McAfee Shredder	207
McAfee Network Manager	211
McAfee EasyNetwork	227
Opas	243
Tietoja McAfeesta.....	259
Asiakaspalvelu ja tekninen tuki.....	261

L U K U 2

McAfee SecurityCenter

McAfee SecurityCenterin avulla voit valvoa tietokoneesi turvallisuustilaa, nähdä heti, ovatko tietokoneesi virus-, vakoiluohjelma- ja palomuurisuojauspalvelut ajan tasalla sekä korjata mahdollisia tietoturva-aukkoja. Se tarjoaa tarvittavat työkalut ja hallintaohjelmat tietokoneesi suojauksen kokonaisvaltaiseen koordinointiin ja hallintaan.

Ennen tietokoneesi suojauksen määrittämistä ja hallintaa tarkastele SecurityCenter-käyttöliittymää ja varmista, että ymmärrät miten suojaustila, suojausluokat ja suojauspalvelut eroavat toisistaan. Päivitä sitten SecurityCenter varmistaaksesi, että käytössäsi on viimeisin McAfeelta saatavilla oleva suoja.

Kun alkumääritykset on tehty, valvo tietokoneesi suojauksen tilaa SecurityCenterillä. Jos SecurityCenter havaitsee suojausongelman, se antaa hälytyksen. Voit joko korjata ongelman tai jättää sen huomioimatta (vakavuuden mukaan). Voit myös tarkastella SecurityCenter-tapahtumia, kuten virustarkistusasetusten muutoksia, tapahtumalokista.

Huomautus: SecurityCenter raportoi kriittiset ja ei-kriittiset suojausongelmat heti, kun se havaitsee ne. Jos tarvitset apua suojausongelmien selvittämisessä, voit käyttää McAfee Virtual Technician -palvelua.

Tässä luvussa

SecurityCenterin ominaisuudet	6
SecurityCenterin käyttäminen	7
SecurityCenterin päivittäminen.....	13
Suojausongelmien korjaaminen ja ohittaminen	17
Hälytysten käsitteleminen.....	21
Tapahtumien näyttäminen	27

SecurityCenterin ominaisuudet

SecurityCenter tarjoaa seuraavat ominaisuudet.

Yksinkertaistettu suojaustila

Voit helposti tarkastaa tietokoneesi suojaustilan, etsiä päivityksiä ja korjata mahdollisia tietoturva-aukkoja.

Automaattiset päivitykset ja uudet tuoteversiot

Lataa ja asenna rekisteröityjen ohjelmien päivitykset automaattisesti. Kun uusi McAfee-ohjelmistoversio on saatavilla, tilaajana saat sen automaattisesti ilman lisäkustannuksia, jotta suojauksesi on aina ajan tasalla.

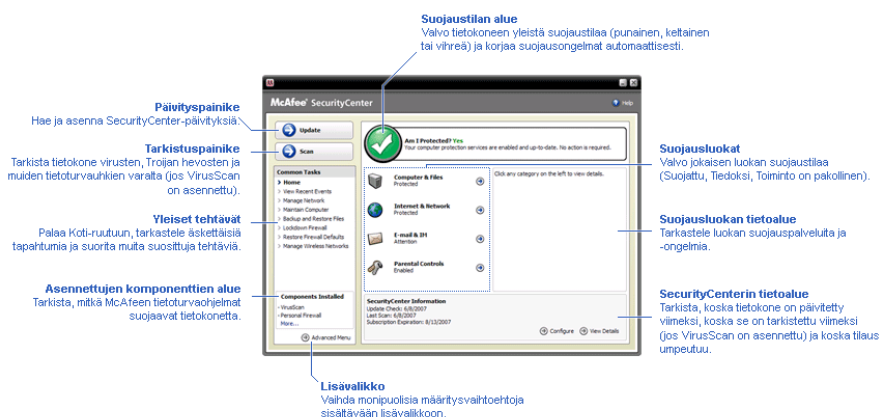
Reaaliaikaiset hälytykset

Suojahälytykset ilmoittavat virusesiintymistä ja tietoturvauhista sekä tarjoavat toimintavaihtoehtoja uhkien poistamiseen ja neutralointiin sekä lisätietoja uhista.

LUKU 3

SecurityCenterin käyttäminen

Ennen SecurityCenterin käyttöä tarkasta ne komponentit ja määrittämisalueet, joita aiot käyttää tietokoneesi suojaustilan hallintaan. Lisätietoja tässä kuvassa käytetyistä termeistä on kohdissa Suojauksen tilan toiminta (sivu 8) ja Suojausluokkien toiminta (sivu 9). Voit sitten tarkastaa McAfee-tilisi tiedot ja vahvistaa tilauksesi voimassaolon.



Tässä luvussa

Suojauksen tilan toiminta	8
Suojausluokkien toiminta	9
Suojauspalveluiden toiminta	10
McAfee-tilin hallinta	11

Suojauksen tilan toiminta

Tietokoneesi suojauksen tila näkyy SecurityCenter Koti-ikkunan suojauksen tila -kohdassa. Siitä käy ilmi, onko tietokoneesi suojattu viimeisimmiltä tietoturvaohjelmilta. Tila voi muuttua ulkoisten tietoturvahyökkäysten, muiden tietoturvaohjelmien ja Internet-yhteyttä käyttävien ohjelmien vaikutuksesta.

Tietokoneesi suojauksen tila voi olla punainen, keltainen tai vihreä.

Suojauksen tila	Kuvaus
Punainen	Tietokonetta ei ole suojattu. SecurityCenter Koti-ikkunan suojauksen tila -kohdan punainen väri tarkoittaa, että tietokonettasi ei ole suojattu. SecurityCenter ilmoittaa ainakin yhdestä kriittisestä tietoturvaongelmasta. Jokaisen suojausluokan kriittiset tietoturvaongelmat tulee korjata, jotta täydellinen suojaus on mahdollista (ongelmaluokka on asetettu Toiminto on pakollinen -tilaan, joka on myös punainen). Lisätietoja suojausongelmien korjaamisesta on kohdassa Suojausongelmien korjaaminen (sivu 18).
Keltainen	Tietokoneesi on osittain suojattu. SecurityCenter Koti-ikkunan suojauksen tila -kohdan keltainen väri tarkoittaa, että tietokonettasi ei ole suojattu. SecurityCenter ilmoittaa ainakin yhdestä ei-kriittisestä tietoturvaongelmasta. Jokaisen suojausluokan ei-kriittiset tietoturvaongelmat tulee korjata tai ohittaa, jotta täydellinen suojaus on mahdollista. Lisätietoja suojausongelmien korjaamisesta ja ohittamisesta on kohdassa Suojausongelmien korjaaminen ja ohittaminen (sivu 17).
Vihreä	Tietokoneesi on täysin suojattu. SecurityCenter Koti-ikkunan suojauksen tila -kohdan vihreä väri tarkoittaa, että tietokoneesi on suojattu. SecurityCenter ei ilmoita yhdestäkään kriittisestä tai ei-kriittisestä tietoturvaongelmasta. Jokaisessa suojausluokassa on luettelo tietokonettasi suojaavista palveluista.

Suojausluokkien toiminta

SecurityCenterin suojauspalvelut voidaan jakaa neljään luokkaan: tietokone & tiedostot, Internet & verkko, sähköposti & pikaviestit ja käytönvalvonta-asetukset. Näiden luokkien avulla voit selata tietokonettasi suojaavia tietoturvapalveluita ja määrittää niiden asetuksia.

Napsauttamalla luokan nimeä voit määrittää siihen kuuluvien palveluiden asetuksia ja tarkastella palveluiden havaitsemia tietoturvaongelmia. Jos tietokoneesi suojauksen tila on punainen tai keltainen, vähintään yhdessä luokassa on näkyvillä *Toiminto on pakollinen*- tai *Huomio*-viesti. Tämä tarkoittaa sitä, että SecurityCenter on havainnut ongelman kyseisessä luokassa. Lisätietoja suojauksen tilasta on kohdassa Suojauksen tilan toiminta (sivu 8).

Suojausluokat	Kuvaus
Tietokone & tiedostot	Tietokone & tiedostot -luokassa voit määrittää seuraavien suojauspalveluiden asetuksia: ▪ virustentorjunta ▪ PUP-suojaus ▪ järjestelmän valvontatoiminnot ▪ Windows-suojaus.
Internet & verkko	Internet & verkko -luokassa voit määrittää seuraavien suojauspalveluiden asetuksia: ▪ palomuurisuojaus ▪ henkilöllisyyden suojaus.
Sähköposti & pikaviestit	Sähköposti & pikaviestit -luokassa voit määrittää seuraavien suojauspalveluiden asetuksia: ▪ sähköpostisuojaus ▪ roskapostin torjunta.
Käytönvalvonta-asetukset	Käytönvalvonta-asetukset-luokassa voit määrittää seuraavien suojauspalveluiden asetuksia: ▪ sisällön estäminen.

Suojauspalveluiden toiminta

Suojauspalvelut ovat SecurityCenterin avainkomponentteja. Voit suojata tietokoneesi määrittämällä niiden asetuksia.

Suojauspalvelut vastaavat McAfeen ohjelmistoja. Esimerkiksi kun asennat VirusScan-ohjelman, seuraavat suojauspalvelut tulevat käyttöön: Virustentorjunta, PUP-suojaus, järjestelmän valvontatoiminnot ja Windows-suojaus. Tarkempia tietoja suojauspalveluista löytyy VirusScan-ohjeesta.

Oletusarvoisesti kaikki asennettuun ohjelmaan liittyvät suojauspalvelut ovat käytössä. Suojauspalveluita voi kuitenkin poistaa käytöstä milloin tahansa. Esimerkiksi kun asennat Tietosuojapalvelun, sisällön estäminen ja henkilöllisyyden suojaus ovat käytössä. Jos et aio käyttää sisällön estämispalvelua, voit poistaa sen käytöstä kokonaan. Voit myös poistaa suojauspalveluita käytöstä väliaikaisesti, kun teet asennus- tai huoltotoimenpiteitä.

McAfee-tilin hallinta

Voit hallita McAfee-tiliäsi SecurityCenterin avulla. Voit tarkastella tilitietojasi ja tarkastaa tilauksesi tilan helposti.

Huomautus: Jos olet asentanut McAfee-ohjelmistoja CD-levyltä, ne täytyy rekisteröidä McAfeen verkkosivuilla, jotta McAfee-tilin määrittäminen ja päivittäminen onnistuu. Vain rekisteröimällä ohjelmistot voit käyttää automaattista ohjelmistopäivitystä.

Hallitse McAfee-tiliä

Voit tarkastella McAfee-tilisi tietoja (Oma tili) helposti SecurityCenterin avulla.

- 1 Valitse **Yleiset tehtävät** -kohdasta **Oma tili**.
- 2 Kirjaudu sisään McAfee-tiliisi.

Vahvista tilaus

Voit vahvistaa tilauksesi varmistaaksesi, että se on voimassa.

- Napsauta SecurityCenter-kuvaketta  hiiren kakkospainikkeella tehtäväpalkin oikeassa reunassa olevalla Windowsin ilmaisinalueella ja napsauta sitten **Vahvista tilaus**-kohtaa.

LUKU 4

SecurityCenterin päivittäminen

SecurityCenter varmistaa, että rekisteröimäsi McAfee-ohjelmistot ovat ajan tasalla, tarkistamalla ja asentamalla uusimmat Internet-päivitykset neljän tunnin välein. Asennettujen ja rekisteröityjen ohjelmistojen mukaan Internet-päivityksiin saattavat kuulua uusimmat virusmääritykset sekä tietomurto-, roskaposti-, vakoiluohjelma- ja tietoturvasuojauspäivitykset. Jos haluat tarkistaa päivitykset oletuksena asetettua neljää tuntia aikaisemmin, voit tehdä sen koska tahansa. Sillä välin kun SecurityCenter tarkistaa päivityksiä, voit suorittaa muita tehtäviä.

Voit myös muuttaa SecurityCenterin päivitysten tarkistus- ja asennusasetuksia. Tämä ei kuitenkaan ole suositeltavaa. Voit esimerkiksi muuttaa asetuksia niin, että SecurityCenter lataa päivitykset, mutta ei asenna niitä. Halutessasi SecurityCenter voi myös antaa huomautuksen ennen päivitysten lataamista ja asentamista. Voit myös kytkeä automaattisen päivityksen pois käytöstä.

Huomautus: Jos olet asentanut McAfee-ohjelmistoja CD-levyltä, ne täytyy rekisteröidä McAfeen verkkosivuilla, jotta automaattinen päivitys on mahdollista.

Tässä luvussa

Tarkista päivitykset	13
Määritä automaattiset päivitykset	14
Poista automaattiset päivitykset käytöstä	14

Tarkista päivitykset

Oletusasetuksena SecurityCenter tarkistaa päivitykset neljän tunnin välein, kun tietokone on liitetty Internetiin. Voit myös halutessasi tarkistaa päivitykset ennen kuin neljä tuntia on kulunut edellisestä tarkistuksesta. Jos olet kytkenyt automaattisen päivityksen pois käytöstä, on säännöllinen päivitysten tarkistus omalla vastuullasi.

- Valitse SecurityCenterin Koti-ikkunan kohta **Päivitä**.

Vihje: Voit tarkistaa päivitykset käynnistämättä SecurityCenteriä. Napsauta tehtäväpalkin oikeassa reunassa olevan ilmaisinalueen SecurityCenter-kuvaketta  hiiren oikealla painikkeella ja valitse **Päivitykset**.

Määritä automaattiset päivitykset

Oletusasetuksena SecurityCenter tarkistaa ja asentaa päivitykset neljän tunnin välein, kun tietokoneesi on liitettyä Internetiin. Jos haluat muuttaa oletusasetuksia, voit määrittää SecurityCenterin lataamaan päivitykset automaattisesti ja ilmoittamaan, kun päivitykset voidaan asentaa. Voit myös määrittää SecurityCenterin antamaan huomautuksen ennen päivitysten lataamista.

Huomautus: SecurityCenter ilmoittaa valmiista päivityksistä antamalla hälytyksen. Hälytyksen jälkeen voit joko ladata tai asentaa päivitykset tai lykätä niitä. Jos päivität ohjelmistoja hälytyksen yhteydessä, sinua voidaan pyytää vahvistamaan tilauksesi ennen päivitysten lataamista ja asentamista. Lisätietoja on kohdassa Hälytysten käsittelyminen (sivu 21).

- 1 Avaa SecurityCenter-asetusikkuna.
Miten?
 1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
 2. Valitse oikeanpuoleisen ruudun **SecurityCenterin tiedot** -kohdasta **Määritä**.
- 2 Napsauta SecurityCenter-asetusikkunan **Automaattiset päivitykset eivät ole käytössä** -kohdasta **Käytössä** ja sitten **Lisäasetukset**.
- 3 Napsauta yhtä seuraavista painikkeista:
 - **Asenna päivitykset automaattisesti ja ilmoita, kun palvelut päivitetään (suositus)**
 - **Lataa päivitykset automaattisesti ja ilmoita, kun ne ovat valmiina asennettaviksi**
 - **Ilmoita ennen päivitysten lataamista.**
- 4 Valitse **OK**.

Poista automaattiset päivitykset käytöstä

Jos kytket automaattisen päivityksen pois käytöstä, on säännöllinen päivitysten tarkistus omalla vastuullasi. Ilman päivityksiä tietokoneessasi ei ole uusinta tietoturvasuojaa. Lisätietoja manuaalisesta päivitysten tarkistamisesta on kohdassa Etsi päivityksiä (sivu 13).

- 1 SecurityCenter-asetusikkunan avaaminen
Miten?

1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
 2. Valitse oikeanpuoleisen ruudun **SecurityCenterin tiedot** -kohdasta **Määritä**.
- 2** Napsauta SecurityCenter-asetusikkunan **Automaattiset päivitykset ovat käytössä** -kohdasta **Ei käytössä**.

Vihje: Voit kytkeä automaattisen päivityksen käyttöön napsauttamalla **Käytössä**-painiketta tai poistamalla Päivitysvalinnat-ikkunan valinnan **Poista automaattinen päivitystoiminto käytöstä ja anna minun tarkistaa päivitykset manuaalisesti**.

L U K U 5

Suojausongelmien korjaaminen ja ohittaminen

SecurityCenter raportoi kriittiset ja ei-kriittiset suojausongelmat heti, kun se havaitsee ne. Kriittiset suojausongelmat vaativat välittömiä toimenpiteitä ja vaarantavat suojauksen tilan (väri muuttuu punaiseksi). Ei-kriittiset ongelmat eivät vaadi välittömiä toimenpiteitä, mutta ne voivat vaarantaa suojauksen tilan (ongelmatyypin mukaan). Jotta saat suojauksen tilan vihreäksi, sinun täytyy ratkaista kaikki kriittiset ongelmat ja joko ratkaista tai ohittaa kaikki ei-kriittiset ongelmat. Jos tarvitset apua suojausongelmien selvittämisessä, voit käyttää McAfee Virtual Technician -palvelua. Lisätietoja McAfee Virtual Technician -palvelusta löydät McAfee Virtual Technician -ohjeesta.

Tässä luvussa

Suojausongelmien korjaaminen	18
Suojausongelmien ohittaminen.....	20

Suojausongelmien korjaaminen

Suurin osa turvallisuusongelmista voidaan korjata automaattisesti. Jotkin ongelmat saattavat kuitenkin vaatia toimenpiteitä. Esimerkiksi jos palomuurisuojaus on kytketty pois käytöstä, SecurityCenter voi kytkeä sen automaattisesti takaisin käyttöön, mutta jos palomuurisuojausta ei ole asennettu, se täytyy asentaa. Seuraavassa taulukossa on esitetty joitakin mahdollisia toimenpiteitä, joilla vikoja voidaan korjata manuaalisesti.

Ongelma	Toimenpide
Tietokoneelle ei ole suoritettu täydellistä tarkistusta viimeisen 30 päivän aikana.	Tarkista tietokone manuaalisesti. Lisätietoja on VirusScan-ohjeessa.
DAT-virusmäärittystiedostot ovat vanhentuneet.	Päivitä suoja manuaalisesti. Lisätietoja on VirusScan-ohjeessa.
Ohjelmaa ei ole asennettu.	Asenna ohjelma McAfee-verkkosivuilta tai CD-levyltä.
Ohjelmasta puuttuu komponentteja.	Asenna ohjelma uudelleen McAfee-verkkosivuilta tai CD-levyltä.
Ohjelmaa ei ole rekisteröity, eikä se tarjoa täydellistä suojaa.	Rekisteröi ohjelma McAfee-verkkosivuilla.
Ohjelma on vanhentunut.	Tarkista tilisi tilanne McAfee-verkkosivuilta.

Huomautus: Yksittäinen suojausongelma saattaa usein vaikuttaa useampaan suojausluokkaan. Tällaisessa tilanteessa ongelman korjaaminen yhdessä suojausluokassa poistaa sen myös muista luokista.

Korjaa suojausongelmat automaattisesti

SecurityCenter voi korjata useimmat suojausongelmat automaattisesti. SecurityCenterin automaattisen korjauksen yhteydessä tekemät muutokset asetuksiin eivät kirjaudu tapahtumalokiin. Lisätietoja tapahtumista on kohdassa Tapahtumien tarkastelu (sivu 27).

- 1 Valitse **Yleiset tehtävät** -kohdasta **Koti**.
- 2 Napsauta SecurityCenterin Koti-ikkunan suojauksen tila -kohdan **Korjaa**-painiketta.

Korjaa suojausongelmat manuaalisesti

Jos ongelman korjaus ei onnistu automaattisesti, voit korjata sen manuaalisesti.

- 1 Valitse **Yleiset tehtävät** -kohdasta **Koti**.
- 2 Napsauta SecurityCenterin Koti-ikkunassa sitä suojausluokkaa, jossa SecurityCenter ilmoittaa ongelman olevan.
- 3 Napsauta ongelman kuvauksen perässä olevaa linkkiä.

Suojausongelmien ohittaminen

Jos SecurityCenter havaitsee ei-kriittisen ongelman, sen voi joko korjata tai ohittaa. Muut ei-kriittiset ongelmat (jos esimerkiksi roskapostinesto- tai tietosuojapalvelua ei ole asennettu) ohitetaan automaattisesti. Ohitetut ongelmat eivät näy SecurityCenterin Koti-ikkunan suojausluokan tietoa-alueessa, ellei tietokoneesi suojauksen tila ole vihreä. Jos ohitat ongelman, saat sen halutessasi myöhemmin näkyviin suojausluokan tietoa-alueeseen, vaikka tietokoneen suojauksen tila ei olisikaan vihreä.

Ohita suojausongelma

Jos SecurityCenter havaitsee ei-kriittisen ongelman, jota et aio korjata, voit ohittaa sen. Ongelman ohittaminen poistaa ongelman SecurityCenterin suojausluokan tietoa-alueesta.

- 1 Valitse **Yleiset tehtävät** -kohdasta **Koti**.
- 2 Napsauta SecurityCenterin Koti-ikkunassa sitä suojausluokkaa, jossa SecurityCenter ilmoittaa ongelman olevan.
- 3 Napsauta suojausongelman vieressä olevaa **Ohita**-linkkiä.

Ohitettujen ongelmien näyttäminen tai piilottaminen

Ongelman vakavuuden mukaan voit näyttää tai piilottaa ohitetun suojausongelman.

- 1 Avaa Hälytysasetukset-ikkuna.
Miten?
 1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
 2. Valitse oikeanpuoleisen ruudun **SecurityCenterin tiedot** -kohdasta **Määritä**.
 3. Valitse **Hälytykset**-kohdasta **Lisäasetukset**.
- 2 Valitse SecurityCenter-asetusikkunasta **Ohitetut ongelmat**.
- 3 Toimi Ohitetut ongelmat -ikkunassa seuraavasti:
 - Voit ohittaa ongelman valitsemalla sen valintaruudun.
 - Voit ilmoittaa ongelmasta suojausluokan tietoa-alueessa poistamalla kyseisen valintaruudun valinnan.
- 4 Valitse **OK**.

Vihje: Voit ohittaa ongelman myös napsauttamalla suojausluokan tietoa-alueessa ilmoitetun ongelman vieressä olevaa **Ohita**-linkkiä.

LUKU 6

Hälytysten käsitleminen

Hälytykset ovat pieniä ponnahdusikkunoita, jotka näkyvät näytön oikeassa alareunassa tiettyjen SecurityCenter-tapahtumien yhteydessä. Hälytyksessä on yksityiskohtaista tietoa tapahtumasta sekä suosituksia ja ongelmien ratkaisuja, jotka saattavat liittyä tapahtumaan. Joissakin hälytyksissä on myös linkkejä tapahtuman lisätietoihin. Näiden linkkien avulla voit ladata McAfeen yleisen Web-sivuston tai lähettää McAfeelle tietoja vianmäärittystä varten.

Hälytyksiä on kolmea eri tyyppiä: punainen, keltainen ja vihreä.

Hälytystyyppi	Kuvaus
Punainen	Punainen hälytys on kriittinen ilmoitus, joka vaatii käyttäjän antaman vastauksen. Tämä hälytys esiintyy silloin, kun SecurityCenter ei voi määrittää suojausongelman korjausta automaattisesti.
Keltainen	Keltainen hälytys on ei-kriittinen ilmoitus, joka yleensä vaatii käyttäjän antaman vastauksen.
Vihreä	Vihreä hälytys on ei-kriittinen ilmoitus, joka ei yleensä vaadi käyttäjän antamaa vastausta. Vihreät hälytykset välittävät perustietoa tapahtumasta.

Koska hälytykset ovat tärkeitä suojaustilan valvonnassa ja hallinnassa, käyttäjä ei voi poistaa niitä käytöstä. Käyttäjä voi kuitenkin määrittää, minkä tyyppiset tiedottavat hälytykset tulevat näkyviin. Lisäksi käyttäjä voi määrittää joitakin hälytysasetuksia (esimerkiksi soittaako SecurityCenter äänen hälytyksen esiintyessä tai näyttääkö se McAfee-aloitusnäytön käynnistyksen yhteydessä).

Tässä luvussa

Tiedottavien hälytysten näyttäminen ja piilottaminen	22
Hälytysasetusten määrittäminen	24

Tiedottavien hälytysten näyttäminen ja piilottaminen

Tiedottavat hälytykset ilmoittavat tapahtumista, jotka eivät ole uhkia tietokoneen turvallisuudelle. Jos käytössä on esimerkiksi palomuurisuojaus, näyttöön tulee oletusarvoisesti tiedottava hälytys aina, kun tietokoneessa oleva ohjelma on myöntänyt luvan Internet-yhteyden muodostamiseen. Jos et halua nähdä tietyn tyyppisiä tiedottavia hälytyksiä, voit piilottaa ne. Voit myös piilottaa kaikki tiedottavat hälytykset. Voit piilottaa kaikki tiedottavat hälytykset myös silloin, kun pelaat peliä tietokoneen koko näyttöruudulla. Kun lopetat pelin palaamisen ja palaat koko näytön tilasta normaaliin tilaan, SecurityCenter alkaa taas näyttää tiedottavia hälytyksiä.

Jos piilotat tiedottavat hälytykset vahingossa, voit palauttaa ne milloin tahansa. Oletuksen mukaan SecurityCenter näyttää kaikki tiedottavat hälytykset.

Näytä tai piilota tiedottavat hälytykset

Voit määrittää SecurityCenterin siten, että tietyt tiedottavat hälytykset näytetään ja muuntyyppiset tiedottavat hälytykset piilotetaan tai että kaikki tiedottavat hälytykset piilotetaan.

1 Avaa Hälytysasetukset-ikkuna.

Miten?

1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
2. Valitse oikeanpuoleisen ruudun **SecurityCenterin tiedot** -kohdasta **Määritä**.
3. Valitse **Hälytykset**-kohdasta **Lisäasetukset**.

2 Valitse SecurityCenter-asetusikkunasta **Tiedottavat hälytykset**.

3 Toimi Tiedottavat hälytykset -ikkunassa seuraavasti:

- Saat tiedottavan hälytyksen näkyviin poistamalla sen valintaruudun valinnan.
- Voit piilottaa tiedottavan hälytyksen valitsemalla sen valintaruudun.
- Voit piilottaa kaikki tiedottavat hälytykset valitsemalla **Älä näytä tiedottavia hälytyksiä** -valintaruudun.

4 Valitse **OK**.

Vihje: Voit piilottaa tiedottavan hälytyksen myös valitsemalla hälytysikkunan **Älä näytä tätä hälytystä uudelleen** -valintaruudun. Saat tiedottavan hälytyksen uudelleen näkyviin poistamalla Tiedottavat hälytykset -ikkunan kyseisen valintaruudun valinnan.

Näytä tai piilota tiedottavat hälytykset pelejä pelattaessa

Voit piilottaa tiedottavat hälytykset, kun pelaat peliä tietokoneen koko näyttöruudulla. Kun lopetat pelin palaamisen ja palaat koko näytön tilasta normaaliin tilaan, SecurityCenter alkaa taas näyttää tiedottavia hälytyksiä.

1 Avaa Hälytysasetukset-ikkuna.

Miten?

1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
2. Valitse oikeanpuoleisen ruudun **SecurityCenterin tiedot** -kohdasta **Määritä**.
3. Valitse **Hälytykset**-kohdasta **Lisäasetukset**.

2 Valitse Hälytysasetukset-ikkunasta **Näytä tiedottavat hälytykset, kun tietokoneen havaitaan olevan pelitilassa** -valintaruutu tai poista sen valinta.

3 Valitse **OK**.

Hälytysasetusten määrittäminen

SecurityCenter määrittää hälytysten ilmestymisen ja toistumistiheyden. Käyttäjä voi kuitenkin määrittää joitakin perushälytysasetuksia. Voit esimerkiksi määrittää, että SecurityCenter soittaa äänen hälytyksen esiintyessä tai että aloitusnäyttövaroitusta piilotetaan Windowsin käynnistyksen yhteydessä. Voit myös piilottaa hälytykset, jotka ilmoittavat online-yhteisön virusesiintymistä ja muista tietoturvauhista.

Soita ääni hälytyksen esiintyessä

Jos haluat kuulla äänimerkin hälytyksen yhteydessä, voit määrittää SecurityCenterin soittamaan hälytysäänen.

- 1 Avaa Hälytysasetukset-ikkuna.
Miten?
 1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
 2. Valitse oikeanpuoleisen ruudun **SecurityCenterin tiedot** -kohdasta **Määritä**.
 3. Valitse **Hälytykset**-kohdasta **Lisäasetukset**.
- 2 Valitse Hälytysasetukset-ikkunan **Ääni**-kohdasta **Soita ääni hälytyksen esiintyessä** -valintaruutu.

Piilota aloitusnäyttö käynnistyksessä

Oletusasetuksena McAfeen aloitusnäyttö on hetken aikaa näytöllä Windowsin käynnistyksen yhteydessä merkinä siitä, että SecurityCenter suojaa tietokonettasi. Voit kuitenkin piilottaa aloitusnäytön halutessasi.

- 1 Avaa Hälytysasetukset-ikkuna.
Miten?
 1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
 2. Valitse oikeanpuoleisen ruudun **SecurityCenterin tiedot** -kohdasta **Määritä**.
 3. Valitse **Hälytykset**-kohdasta **Lisäasetukset**.
- 2 Poista Hälytysasetukset-ikkunan **Aloitusnäyttö**-kohdasta valinta **Näytä McAfee-aloitusnäyttö Windowsin käynnistyessä**.

Vihje: Saat aloitusnäytön taas näkyviin milloin tahansa valitsemalla **Näytä McAfee-aloitusnäyttö Windowsin käynnistyessä**.

Piilota virusesiintymähälytykset

Voit piilottaa hälytykset, jotka ilmoittavat online-yhteisön virusesiintymistä ja muista tietoturvauhista.

1 Avaa Hälytysasetukset-ikkuna.

Miten?

1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
2. Valitse oikeanpuoleisen ruudun **SecurityCenterin tiedot** -kohdasta **Määritä**.
3. Valitse **Hälytykset**-kohdasta **Lisäasetukset**.

2 Poista Hälytysasetukset-ikkunasta valinta **Hälytä virus- tai tietoturvauhista**.

Vihje: Saat virusesiintymähälytykset takaisin näkyviin valitsemalla **Hälytä virus- tai tietoturvauhista**.

LUKU 7

Tapahtumien näyttäminen

Tapahtuma on toimenpide tai asetusmuutos, joka tehdään suojausluokassa ja luokkaan liittyvissä palveluissa. Suojauspalvelut tallentavat erityyppisiä tapahtumia. Esimerkiksi SecurityCenter tallentaa tapahtuman, kun suojauspalvelu otetaan käyttöön tai poistetaan käytöstä. Virussuojaus tallentaa tapahtuman aina, kun virus havaitaan tai poistetaan. Palomuurisuojaus taas tallentaa tapahtuman aina, kun Internet-yhteysyritys estetään. Lisätietoja suojausluokista on kohdassa Suojausluokkien toiminta (sivu 9).

Voit tarkastella tapahtumia etsiessäsi ratkaisuja asetusongelmiin, tai kun tarkastat muiden käyttäjien tekemiä toimintoja. Monet vanhemmat valvovat lastensa Internetin käyttöä tapahtumalokin avulla. Voit tarkastella äskettäisiä tapahtumia, jos haluat nähdä viimeisten 30 päivän tapahtumat. Voit tarkastella kaikkia tapahtumia, jos haluat nähdä kattavan luettelon kaikista tapahtumista. Kun tarkastelet kaikkia tapahtumia, SecurityCenter käynnistää tapahtumalokin, joka järjestee tapahtumat suojausluokkien mukaan.

Tässä luvussa

Tarkastele äskettäisiä tapahtumia	27
Tarkastele kaikkia tapahtumia	27

Tarkastele äskettäisiä tapahtumia

Voit tarkastella äskettäisiä tapahtumia, jos haluat nähdä vain viimeisten 30 päivän tapahtumat.

- Napsauta **Yleiset tehtävät** -kohdasta **Tarkastele äskettäisiä tapahtumia**.

Tarkastele kaikkia tapahtumia

Voit tarkastella kaikkia tapahtumia, jos haluat nähdä kattavan luettelon kaikista tapahtumista.

- 1 Napsauta **Yleiset tehtävät** -kohdasta **Tarkastele äskettäisiä tapahtumia**.
- 2 Valitse Viimeisimmät tapahtumat -ruudun kohta **Näytä loki**.
- 3 Napsauta haluamaasi tapahtumatyyppiä tapahtumalokin vasemmassa ikkunassa.

LUKU 8

McAfee VirusScan

VirusScan-ohjelman edistykselliset tunnistus- ja suojapalvelut antavat tietokoneellesi suojan uusimpia turvallisuushahkia, kuten viruksia, troijalaisia, seurantaevästeitä, vakoiluohjelmia, mainosohjelmia ja muita ei-toivottuja ohjelmia vastaan. VirusScan suojaa pöytä- tai kannettavaa tietokonettasi tiedostojen ja kansioiden lisäksi myös muiden tulokohtien, kuten sähköpostin, pikaviestien ja Web-sivustojen kautta tulevalta uhilta.

VirusScan suojaa tietokonettasi välittömästi ja jatkuvasti (ilman hankalaa valvontaa). VirusScan valvoo, tarkistaa ja havaitsee mahdolliset vahingot reaaliajassa samalla, kun työskentelet, selaat Webiä tai luet sähköpostia. Perusteelliset, kehittyneempiä asetuksia käyttävät tarkistukset tehdään säännöllisen aikataulun mukaan. Voit muuttaa VirusScanin toimintaa haluamaksesi. Jos et kuitenkaan halua tehdä muutoksia, tietokoneesi pysyy suojattuna.

Virukset, madot ja muut mahdolliset uhat voivat tunkeutua tietokoneeseesi normaalissa käyttötilanteessa. Jos näin tapahtuu, VirusScan ilmoittaa uhasta, mutta huolehtii siitä yleensä puolestasi. Se joko puhdistaa saastuneet kohteet tai siirtää ne karanteeniin, ennen kuin vahinkoa tapahtuu. Joskus, vaikkakin harvoin, saattaa olla tarvetta jatkotoimenpiteille. Tällaisessa tilanteessa VirusScan antaa sinun päättää, mitä tehdään (tarkistetaanko uudelleen käynnistuksen yhteydessä, säilytetäänkö havaittu kohde vai poistetaanko havaittu kohde).

Huomautus: SecurityCenter raportoi kriittiset ja ei-kriittiset suojausongelmat heti, kun se havaitsee ne. Jos tarvitset apua suojausongelmien selvittämisessä, voit käyttää McAfee Virtual Technician -palvelua.

Tässä luvussa

VirusScan-ohjelman ominaisuudet	30
Reaaliaikaisen virustorjunnan käynnistäminen	31
Lisäsuojauksen ottaminen käyttöön.....	33
Virustorjunnan määrittäminen.....	37
Tietokoneen tarkistaminen	55
Tarkistuksen tulosten käyttäminen	59

VirusScan-ohjelman ominaisuudet

VirusScan tarjoaa seuraavat ominaisuudet.

Perusteellinen virussuoja

VirusScan-ohjelman edistyneet tunnistus- ja suojapalvelut antavat tietokoneellesi suojan uusimpia turvallisuusuhkia, kuten viruksia, troijalaisia, seurantaevästeitä, vakoiluohjelmia, mainosohjelmia ja muita ei-toivottuja ohjelmia vastaan. VirusScan suojaa pöytä- tai kannettavaa tietokonettasi tiedostojen ja kansioiden lisäksi myös muiden tulokohtien, kuten sähköpostin, pikaviestien ja Web-sivustojen kautta tulevilta uhilta. Hankalaa valvontaa ei tarvita.

Resurssitietoiset tarkistusasetukset

Jos tarkistusnopeus on hidas, voit kytkeä mahdollisimman vähäisen resurssien kulutuksen pois käytöstä. Huomaa kuitenkin, että tällöin virussuojaukseen käytetään enemmän resursseja kuin muihin tehtäviin. Voit halutessasi muuttaa VirusScanin reaaliaikaisia ja manuaalisia tarkistusasetuksia. Jos et kuitenkaan halua tehdä muutoksia, tietokoneesi pysyy suojattuna.

Automaattinen korjaus

Jos VirusScan havaitsee turvallisuusuhan reaaliaikaisen tai manuaalisen tarkistuksen aikana, se yrittää käsitellä uhan automaattisesti uhkatyyppin mukaan. Näin useimmat uhat voidaan havaita ja neutraloida ilman käyttäjän toimenpiteitä. Joskus, vaikkakin harvoin, VirusScan ei välttämättä pysty neutraloimaan uhkaa itse. Tällaisessa tapauksessa VirusScan antaa sinun päättää, mitä tehdään (tarkistetaanko uudelleen käynnistyksen yhteydessä, säilytetäänkö havaittu kohde vai poistetaanko havaittu kohde).

Tehtävien pysäyttäminen koko näytön tilassa

Kun katsot elokuvia, pelaat pelejä tai käytät jotain muuta toimintoa, joka käyttää tietokoneen koko näyttöruutua, VirusScan pysäyttää tietyt tehtävät, kuten automaattisen päivityksen ja manuaalisen tarkistuksen.

Reaaliaikaisen virustorjunnan käynnistäminen

VirusScan tarjoaa kahdentyyppistä virustorjuntaa: reaaliaikaista ja manuaalista. Reaaliaikainen virustorjunta valvoo virustoimintaa tietokoneessasi jatkuvasti. Se tarkistaa tiedostot aina, kun niitä avataan. Manuaalisella virustorjunnalla voit tarkistaa tiedostoja halutessasi. Jos haluat varmistaa, että tietokoneesi pysyy suojattuna uusimmilta turvallisuushilta, pidä reaaliaikainen virustorjunta käytössä ja laadi säännöllinen aikataulu perusteellisempia manuaalisia tarkistuksia varten. Oletusasetuksena VirusScan suorittaa aikataulunmukaisen tarkistuksen kerran viikossa. Lisätietoja reaaliaikaisesta ja manuaalisesta tarkistuksesta löytyy kohdasta Tietokoneen tarkistaminen (sivu 55).

Joissakin tilanteissa reaaliaikainen tarkistus voi olla tarpeen pysäyttää (esimerkiksi kun joitakin tarkistusasetuksia muutetaan, tai kun etsitään ratkaisua suorituskykyongelmaan). Kun reaaliaikainen virustorjunta on pois käytöstä, tietokoneesi ei ole suojattu ja SecurityCenterin suojauksen tila on punainen. Lisätietoja suojauksen tilasta löytyy SecurityCenter-ohjeen kohdasta Suojauksen tilan toiminta.

Käynnistä reaaliaikainen virustorjunta

Oletusasetuksena reaaliaikainen virustorjunta on käytössä ja suojaa tietokonettasi viruksilta, troijalaisilta ja muilta turvallisuushilta. Jos poistat reaaliaikaisen virustorjunnan käytöstä, se pitää ottaa taas käyttöön, jotta tietokoneesi pysyy suojattuna.

- 1 Avaa Tietokone ja tiedostot -asetusikkuna.
Miten?
 1. Valitse vasemmanpuoleisesta ruudusta **Lisävalikko**.
 2. Valitse **Määritä**.
 3. Valitse Määritä-ruudusta **Tietokone ja tiedostot**.
- 2 Valitse **Virustorjunta**-kohdassa **Käytössä**.

Lopeta reaaliaikainen virustorjunta

Voit poistaa reaaliaikaisen virustorjunnan tilapäisesti käytöstä ja määrittää ajankohdan, jolloin se otetaan taas käyttöön. Voit jatkaa virustorjuntaa automaattisesti 15, 30, 45 tai 60 minuutin kuluttua tai tietokoneen uudelleenkäynnistyksen jälkeen. Voit myös valita, että virustentorjuntaa ei oteta käyttöön koskaan.

- 1 Avaa Tietokone ja tiedostot -asetusikkuna.
Miten?

1. Valitse vasemmanpuoleisesta ruudusta **Lisävalikko**.
2. Valitse **Määritä**.
3. Valitse Määritä-ruudusta **Tietokone ja tiedostot**.
- 2** Valitse **Virustorjunta**-kohdasta **Ei käytössä**.
- 3** Valitse valintaikkunassa ajankohta, jolloin reaaliaikaista tarkastusta jatketaan.
- 4** Valitse **OK**.

L U K U 9

Lisäsuojauksen ottaminen käyttöön

Reaaliaikaisen virustorjunnan lisäksi VirusScan antaa lisäsuojaa komentosarjoja, vakoiluohjelmia ja mahdollisesti haitallisia sähköposti- ja pikaviestien liitetiedostoja vastaan. Oletuksen mukaan komentosarjojen tarkistus sekä vakoiluohjelma-, sähköposti- ja pikaviestisuojaus on käytössä ja suojaa tietokonetta.

Komentosarjatarkistussuojaus

Komentosarjatarkistussuojaus havaitsee mahdollisesti haitalliset komentosarjat ja estää niiden suorittamisen tietokoneessa. Se valvoo komentosarjan epäilyttävää toimintaa (esimerkiksi kun komentosarjan suorittaminen johtaa tiedostojen luomiseen, kopiointiin ja poistamiseen tai Windows-rekisterin avaamiseen) ja varoittaa, ennen kuin vahinkoja pääsee tapahtumaan.

Vakoiluohjelmien torjunta

Vakoiluohjelmien torjunta havaitsee vakoilu- ja mainosohjelmat sekä muut mahdolliset ei-toivotut ohjelmat. Vakoiluohjelma on tietokoneeseen salaa asennettu ohjelma, joka tarkkailee tietokoneen käyttöä, kerää henkilökohtaisia tietoja ja häiritsee jopa tietokoneen toimintaa asentamalla lisäohjelmia tai ohjaamalla selaimen toimintaa.

Sähköpostisuojaus

Sähköpostisuojaus valvoo lähtevien ja saapuvien sähköpostiviestien ja liitetiedostojen epäilyttävää toimintaa.

Pikaviestisuojaus

Pikaviestisuojaus tunnistaa saapuvien pikaviestien liitetiedostojen potentiaaliset suojausuhat. Se myös estää pikaviestiohjelmia jakamasta henkilökohtaisia tietoja.

Tässä luvussa

Käynnistä komentosarjatarkistussuojaus	34
Käynnistä vakoiluohjelmasuojaus	34
Käynnistä sähköpostisuojaus	34
Käynnistä pikaviestisuojaus	35

Käynnistä komentosarjatarkistussuojaus

Kun otat komentosarjatarkistussuojauksen käyttöön, virustorjuntaohjelmisto havaitsee mahdollisesti haitalliset komentosarjat ja estää niiden suorittamisen tietokoneessa. Komentosarjatarkistussuojaus hälyttää, kun komentosarja yrittää luoda, kopioida tai poistaa tiedostoja tai yrittää muuttaa Windowsin rekisteriä.

1 Avaa Tietokone ja tiedostot -asetusikkuna.

Miten?

1. Valitse vasemmanpuoleisesta ruudusta **Lisävalikko**.
2. Valitse **Määritä**.
3. Valitse Määritä-ruudusta **Tietokone ja tiedostot**.

2 Valitse **Komentosarjatarkistussuojaus**-kohdassa **Käytössä**.

Huomaa: Voit poistaa komentosarjatarkistussuojauksen käytöstä milloin tahansa. Tämä ei kuitenkaan ole suotavaa, sillä tällöin tietokone altistuu haitallisille komentosarjoille.

Käynnistä vakoiluohjelasuojaus

Kun otat vakoiluohjelasuojauksen käyttöön, virustorjuntaohjelmisto havaitsee ja poistaa vakoilu- ja mainosohjelmat sekä muut mahdolliset ei-toivotut ohjelmat, jotka keräävät ja lähettävät tietoja käyttäjän tietämättä.

1 Avaa Tietokone ja tiedostot -asetusikkuna.

Miten?

1. Valitse vasemmanpuoleisesta ruudusta **Lisävalikko**.
2. Valitse **Määritä**.
3. Valitse Määritä-ruudusta **Tietokone ja tiedostot**.

2 Valitse **Komentosarjatarkistussuojaus**-kohdassa **Käytössä**.

Huomaa: Voit poistaa vakoiluohjelasuojauksen käytöstä milloin tahansa. Tämä ei kuitenkaan ole suotavaa, sillä tällöin tietokone altistuu mahdollisille haittaohjelmille.

Käynnistä sähköpostisuojaus

Kun otat sähköpostisuojauksen käyttöön, virustorjuntaohjelma havaitsee lähtevien (SMTP) ja saapuvien (POP3) sähköpostiviestien ja tiedostoliitteiden sisältämät madot ja mahdolliset uhat.

1 Avaa Sähköposti ja pikaviesti -asetusikkuna.

Miten?

1. Valitse vasemmanpuoleisesta ruudusta **Lisävalikko**.
2. Valitse **Määritä**.
3. Valitse Määritä-ruudusta **Sähköposti ja pikaviestit**.

2 Valitse **Sähköpostisuojaus**-kohdasta **Käytössä**.

Huomaa: Voit poistaa sähköpostisuojaus käytöstä milloin tahansa. Tämä ei kuitenkaan ole suotavaa, sillä tällöin tietokone altistuu sähköpostiuhille.

Käynnistä pikaviestisuojaus

Kun otat pikaviestisuojaus käyttöön, virustorjuntaohjelmisto havaitsee saapuvien pikaviestien liitetiedostoihin liittyvät tietoturvaohat.

1 Avaa Sähköposti ja pikaviestit -asetusikkuna.

Miten?

1. Valitse vasemmanpuoleisesta ruudusta **Lisävalikko**.
2. Valitse **Määritä**.
3. Valitse Määritä-ruudusta **Sähköposti ja pikaviestit**.

2 Valitse **Pikaviestisuojaus**-kohdasta **Käytössä**.

Huomaa: Voit poistaa pikaviestisuojaus käytöstä milloin tahansa. Tämä ei kuitenkaan ole suotavaa, sillä tällöin tietokone altistuu haitallisille pikaviestien liitetiedostoille.

L U K U 10

Virustorjunnan määrittäminen

VirusScan tarjoaa kahdentyyppistä virustorjuntaa: reaaliaikaista ja manuaalista. Reaaliaikainen virustorjunta tarkistaa tiedostot joka kerta, kun käyttäjä tai tietokone käyttää niitä. Manuaalisella virustorjunnalla voit tarkistaa tiedostoja halutessasi. Voit määrittää kullekin suojaustyypille asetuksia. Esimerkki: Koska reaaliaikainen suojaus valvoo tietokonetta jatkuvasti, voit valita sille tietyt perustarkistusasetukset. Voit määrittää kattavammat tarkistusasetukset manuaaliselle, tarvittaessa suoritettavalle suojaukselle.

Tässä luvussa

Reaaliaikaisen tarkistuksen asetusten määrittäminen	38
Manuaalisen tarkistuksen asetusten määrittäminen	40
SystemGuards-toimintojen asetukset	44
Luotettujen luetteloiden käyttäminen.....	51

Reaaliaikaisen tarkistuksen asetusten määrittäminen

Kun käynnistät reaaliaikaisen virustorjunnan, VirusScan käyttää vakioasetuksia tiedostojen tarkistukseen. Voit kuitenkin muuttaa vakioasetuksia tarpeittesi mukaan.

Kun muutat reaaliaikaisen tarkistuksen asetuksia, sinun täytyy päättää, mitä tarkistuksia VirusScan tekee sekä mitä sijaintipaikkoja ja tiedostotyypppejä tarkistetaan. Voit esimerkiksi määrittää, etsiikö VirusScan tuntemattomia viruksia tai evästeitä, joilla verkkosivut seuraavat Internetin käyttöäsi, tai tarkistaako se tietokoneeseesi yhdistettyjä verkkoasemia vai ainoastaan paikallisia asemia. Voit myös määrittää, mitä tiedostotyypppejä tarkistetaan (kaikki tiedostot tai vain ohjelmatiedostot ja asiakirjat, joissa virukset useimmin havaitaan).

Reaaliaikaisen virustorjunnan asetuksissa on myös valinta sille, onko tietokoneesi puskurin ylivuotosuojaus tarpeellinen. Puskuri on muistin osa, jota käytetään tallentamaan tietokoneen tietoja väliaikaisesti. Puskurin ylivuoto voi tapahtua, jos ohjelmien tai prosessien käyttämä puskurin määrä ylittää puskurin kapasiteetin. Puskurin ylivuototilanteessa tietokoneesi on altis tietoturvahyökkäyksille.

Määritä reaaliaikaisen tarkistuksen asetukset

Voit määrittää, mitä VirusScan etsii reaaliaikaisen tarkistuksen aikana. Lisäksi voit määrittää tarkistettavat tiedostojen sijaintipaikat ja tiedostotyyppit. Asetuksiin kuuluu esimerkiksi tuntemattomien virusten ja seurantaevästeiden tarkistus sekä puskurin ylivuotosuoja. Voit myös määrittää reaaliaikaisen tarkistuksen käsittämään tietokoneeseesi yhdistetyt verkkoasemat.

- 1 Avaa Reaaliaikainen tarkistus -ikkuna.
Miten?

1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
2. Napsauta SecurityCenterin Koti-ikkunan **Tietokone ja tiedostot** -painiketta.
3. Napsauta Internet ja verkko -tietoalueen **Määritä**-painiketta.
4. Varmista Tietokone ja tiedostot -määritysikkunasta, että virustorjunta on käytössä, ja napsauta **Lisäasetukset**-painiketta.

2 Määritä reaaliaikaisen tarkistuksen asetukset ja napsauta OK.

Jos haluat...	Tee näin...
havaita tuntemattomat virukset ja tunnettujen virusten uudet muunnelmät	valitse Tarkista tuntemattomat virukset heuristiikan avulla -valintaruutu.
havaita evästeet	valitse Tarkista ja poista seurantaevästeet -valintaruutu.
havaita virukset ja mahdolliset uhat verkkoasemilta	valitse Tarkista verkkoasemat -valintaruutu.
suojata tietokoneesi puskurin ylivuodoilta	valitse Ota käyttöön puskurin ylivuotosuojaus -valintaruutu.
määrittää tarkistettavat tiedostotyytit	valitse joko Kaikki tiedostot (suositus) tai Vain ohjelmatiedostot ja asiakirjat .

Manuaalisen tarkistuksen asetusten määrittäminen

Manuaalisella virustorjunnalla voit tarkistaa tiedostoja halutessasi. Kun aloitat manuaalisen tarkistuksen, VirusScan etsii tietokoneestasi viruksia ja muita mahdollisesti haitallisia kohteita käyttäen kattavia tarkistusasetuksia. Kun muutat manuaalisen tarkistuksen asetuksia, sinun täytyy päättää, mitä tarkistuksia VirusScan tekee. Voit esimerkiksi määrittää, etsiikö VirusScan tuntemattomia viruksia, ei-toivottuja ohjelmia (vakoilu- ja mainosohjelmat), vaikeasti havaittavia ohjelmia (tietomurto-ohjelmistot, jotka mahdollistavat tietokoneen luvattoman käytön) tai seurantaevästeitä. Sinun täytyy myös päättää, minkä tyyppiset tiedostot tarkistetaan. Voit esimerkiksi määrittää, tarkistaako VirusScan kaikki tiedostot vai vain ohjelmatiedostot ja asiakirjat (virukset havaitaan yleensä näissä tiedostoissa). Voit myös määrittää, tarkistetaanko arkistotiedostot (kuten .zip-tiedostot).

Oletusasetuksena VirusScan tarkistaa kaikki tietokoneesi asemat ja hakemistot jokaisen manuaalisen tarkistuksen yhteydessä. Voit kuitenkin muuttaa tarkistuskohteita tarpeittesi mukaan. Voit esimerkiksi tarkistaa vain tärkeimmät järjestelmätiedostot, työpöydällä olevat tiedostot tai Ohjelmatiedostot-kansiossa olevat tiedostot. Jos et halua olla itse vastuussa jokaisen manuaalisen tarkistuksen aloittamisesta, voit myös laatia säännöllisen tarkistusaikataulun. Aikataulunmukaiset tarkistukset tarkistavat aina koko tietokoneen käyttäen oletusasetuksia. Oletusasetuksena VirusScan suorittaa aikataulunmukaisen tarkistuksen kerran viikossa.

Jos tarkistusnopeus on hidas, voit kytkeä mahdollisimman vähäisen resurssien kulutuksen pois käytöstä. Huomaa kuitenkin, että tällöin virussuojaukseen käytetään enemmän resursseja kuin muihin tehtäviin.

Huomaa: Kun katsot elokuvia, pelaat pelejä tai käytät jotain muuta toimintoa, joka käyttää tietokoneen koko näyttöruutua, VirusScan pysäyttää tietyt tehtävät, kuten automaattisen päivityksen ja manuaalisen tarkistuksen.

Määritä manuaalisen tarkistuksen asetukset

Voit määrittää, mitä VirusScan etsii manuaalisen tarkistuksen aikana. Lisäksi voit määrittää tarkistettavat tiedostojen sijaintipaikat ja tiedostotyytit. Asetuksiin kuuluu esimerkiksi tuntemattomien virusten, arkistotiedostojen, vakoiluohjelmien, ei-toivottujen ohjelmien, seurantaevästeiden, tietomurto-ohjelmistojen ja vaikeasti havaittavien ohjelmien tarkistus.

1 Avaa Manuaalinen tarkistus -ikkuna.

Miten?

1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
 2. Napsauta SecurityCenterin Koti-ikkunan **Tietokone ja tiedostot** -painiketta.
 3. Napsauta Internet ja verkko -tietoalueen **Määritä**-painiketta.
 4. Varmista Tietokone ja tiedostot -määritysikkunasta, että virustorjunta on käytössä, ja napsauta **Lisäasetukset**-painiketta.
 5. Napsauta Virustorjunta-ikkunan kohtaa **Manuaalinen tarkistus**.
- 2 Määritä manuaalisen tarkistuksen asetukset ja napsauta **OK**.

Jos haluat...	Tee näin...
havaita tuntemattomat virukset ja tunnettujen virusten uudet muunnelmat	valitse Tarkista tuntemattomat virukset heuristiikan avulla -valintaruutu.
tunnistaa ja poistaa viruksia .zip-tiedostoista ja muista pakatuista tiedostoista	valitse Tarkista .zip- ja muut pakatut tiedostot -valintaruutu.
havaita vakoilu- ja mainosohjelmat sekä muut mahdolliset ei-toivotut ohjelmat	valitse Tarkista vakoiluohjelmat ja mahdolliset haittaohjelmat -valintaruutu.
havaita evästeet	valitse Tarkista ja poista seurantaevästeet -valintaruutu.
havaita tietomurto-ohjelmistot ja vaikeasti havaittavat ohjelmat, jotka voivat muuttaa ja käyttää hyväkseen Windowsin järjestelmätiedostoja	valitse Tarkista tietomurto-ohjelmistot ja muut vaikeasti havaittavat ohjelmat -valintaruutu.
käyttää vain vähän prosessoritehoa tarkistuksiin ja enemmän muihin tehtäviin (kuten Web-selaukseen ja asiakirjojen avaamiseen)	valitse Tarkista minimiresursseilla -valintaruutu.
määrittää tarkistettavat tiedostotyyppit	valitse joko Kaikki tiedostot (suositus) tai Vain ohjelmatiedostot ja asiakirjat .

Määritä manuaalisen tarkistuksen kohteen sijainti

Voit määrittää paikan, mistä VirusScan etsii viruksia ja muita vahingollisia kohteita manuaalisen tarkistuksen aikana. Voit tarkistaa kaikki tietokoneesi tiedostot, kansiot ja asemat, tai voit rajoittaa tarkistuksen tiettyihin kansioihin ja asemiin.

1 Avaa Manuaalinen tarkistus -ikkuna.

Miten?

1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
2. Napsauta SecurityCenterin Koti-ikkunan **Tietokone ja tiedostot** -painiketta.
3. Napsauta Internet ja verkko -tietoa-alueen **Määritä**-painiketta.
4. Varmista Tietokone ja tiedostot -määritysikkunasta, että virustorjunta on käytössä, ja napsauta **Lisäasetukset**-painiketta.
5. Napsauta Virustorjunta-ikkunan kohtaa **Manuaalinen tarkistus**.

2 Napsauta **Oletustarkistussijainti**.

3 Määritä manuaalisen tarkistuksen kohteen sijainti ja napsauta **OK**.

Jos haluat...	Tee näin...
tarkistaa kaikki tietokoneesi tiedostot ja kansiot	valitse (Oma) Tietokone -valintaruutu.
tarkistaa tietyt tiedostot, kansiot ja asemat	poista (Oma) Tietokone -valinta ja valitse vähintään yksi kansio tai asema.
tarkistaa tärkeimmät järjestelmätiedostot	poista (Oma) Tietokone -valinta ja valitse Tärkeät järjestelmätiedostot -valintaruutu.

Laadi tarkistusaikataulu

Voit laatia tarkistusaikataulun, jonka mukaan ajoitettu tarkistus voidaan tehdä minä päivänä ja mihin aikaan tahansa. Ajoitetut tarkistukset tarkistavat aina koko tietokoneen käyttäen oletusasetuksia. Oletusasetuksena VirusScan suorittaa ajoitetun tarkistuksen kerran viikossa. Jos tarkistusnopeus on hidas, voit kytkeä mahdollisimman vähäisen resurssien kulutuksen pois käytöstä. Huomaa kuitenkin, että tällöin virussuojaukseen käytetään enemmän resursseja kuin muihin tehtäviin.

1 Avaa Ajoitettu tarkistus -ikkuna.

Miten?

1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
2. Napsauta SecurityCenterin Koti-ikkunan **Tietokone ja tiedostot** -painiketta.
3. Napsauta Internet ja verkko -tietoalueen **Määritä**-painiketta.
4. Varmista Tietokone ja tiedostot -määrittämissivun, että virustorjunta on käytössä, ja napsauta **Lisäasetukset**-painiketta.
5. Napsauta Virustorjunta-ikkunan kohtaa **Ajoitettu tarkistus**.

2 Valitse **Ota käyttöön ajoitettu tarkistus**.

3 Voit vähentää tarkistukseen käytettävää prosessoritehoa valitsemalla **Tarkista minimiresursseilla**.

4 Valitse vähintään yksi päivä.

5 Määritä aloitusaika.

6 Valitse **OK**.

Vihje: Voit palauttaa oletusasetukset valitsemalla **Palauta**.

SystemGuards-toimintojen asetukset

SystemGuards-toiminnot valvovat, kirjaavat, raportoivat ja hallitsevat Windowsin rekisteriin tai tärkeimpiin järjestelmätiedostoihin tehtyjä mahdollisesti luvattomia muutoksia. Luvattomat rekisteri- ja tiedostomuutokset voivat vahingoittaa tietokonettasi ja arvokkaita järjestelmätiedostoja sekä vaarantaa tietokoneesi tietoturvan.

Rekisteri- ja tiedostomuutokset ovat tavallisia, ja niitä tapahtuu tietokoneessasi säännöllisesti. Koska suurin osa muutoksista on vaarattomia, SystemGuardsin oletusasetukset on määritetty suojaamaan tietokonettasi älykkäästi ja luotettavasti mahdollisesti vaarallisilta luvattomilta muutoksilta. Esimerkiksi havaitessaan tavallisesta poikkeavia ja mahdollisesti vaarallisia muutoksia SystemGuards raportoi niistä ja kirjaa ne lokiin. Tavalliset, mutta mahdollisesti vaaralliset muutokset kirjataan vain lokiin. Oletusasetuksena kuitenkin tavallisten ja matalan riskitason muutosten valvonta on pois käytöstä. SystemGuards-teknologia voidaan määrittää suojaamaan mitä tahansa ympäristöä.

SystemGuards-toimintoja on kolmea eri tyyppiä: ohjelmien, Windowsin ja selainten SystemGuards-toiminnot.

Ohjelmien SystemGuards-toiminnot

Ohjelmien SystemGuards-toiminnot havaitsevat tietokoneesi rekisterin ja muiden tärkeiden Windowsin tiedostojen mahdollisesti luvattomat muutokset. Tärkeitä rekisterimerkintöjä ja tiedostoja ovat esimerkiksi ActiveX-asennusmerkinnät, käynnistysmerkinnät, Windows Shell Execute Hook -ohjelmat sekä Shell Service Object Delay Load -luettelot. Ohjelmien SystemGuards-toiminnot valvovat niitä ja pysäyttävät epäilyttävät ActiveX-ohjelmat (Internetistä ladatut), vakoiluohjelmat ja ei-toivotut ohjelmat, jotka voivat käynnistyä automaattisesti Windowsin käynnistyksen yhteydessä.

Windowsin SystemGuards-toiminnot

Windowsin SystemGuards-toiminnot havaitsevat tietokoneesi rekisterin ja muiden tärkeiden Windowsin tiedostojen mahdollisesti luvattomat muutokset. Tärkeitä rekisterimerkintöjä ja tiedostoja ovat esimerkiksi pikavalikon käsittelijät, AppInit DLL-tiedostot sekä Windowsin Hosts-tiedostot. Windowsin SystemGuards-toiminnot valvovat niitä ja estävät tietokonettasi lähettämästä tai vastaanottamasta luvattomia ja henkilökohtaisia tietoja Internetin välityksellä. Suojaukset auttavat myös pysäyttämään ohjelmia, jotka voivat muuttaa tärkeitten ohjelmiesi ulkonäköä ja toimintaa.

Selaimen SystemGuards-toiminnot

Ohjelmien ja Windowsin SystemGuards-toimintojen tavoin myös selainten SystemGuards-toiminnot havaitsevat tietokoneesi rekisterin ja muiden tärkeiden Windowsin tiedostojen mahdollisesti luvattomat muutokset. Selaimen SystemGuards-toiminnot valvovat muutoksia tärkeisiin rekisterimerkintöihin ja tiedostoihin, kuten Internet Explorerin laajennuksiin, Internet Explorerin URL-osoitteisiin ja Internet Explorerin suojausvyöhykkeisiin. SystemGuards-teknologia auttaa estämään selaimen luvattonta toimintaa, kuten käyttäjän ohjaamista epäilyttäviin Web-sivustoihin, selaimen asetusten ja määritysten luvattonta muuttamista ja epäilyttävien sivustojen tulkintaa luotettaviksi.

Ota SystemGuards-suojaus käyttöön

Kun SystemGuards-suojaus on käytössä, se havaitsee ja varoittaa Windowsin rekisterin ja tiedostojen mahdollisesti luvattomista muutoksista. Luvattomat rekisteri- ja tiedostomuutokset voivat vahingoittaa tietokonettasi ja arvokkaita järjestelmätiedostoja sekä vaarantaa tietokoneesi tietoturvan.

1 Avaa Tietokone ja tiedostot -asetusikkuna.

Miten?

1. Valitse vasemmanpuoleisesta ruudusta **Lisävalikko**.
2. Valitse **Määritä**.
3. Valitse Määritä-ruudusta **Tietokone ja tiedostot**.

2 Valitse **SystemGuard-suojaus**-kohdassa **Käytössä**.

Huomautus: Voit poistaa SystemGuard-suojauksen käytöstä valitsemalla **Ei käytössä**.

Määritä SystemGuards-asetukset

Voit määrittää Windowsin tiedostoihin, ohjelmiin ja Internet Exploreriin liittyvien luvattomien rekisteri- ja tiedostomuutosten suojaus-, kirjaus- ja hälytysasetukset SystemGuards-ikkunassa. Luvattomat rekisteri- ja tiedostomuutokset voivat vahingoittaa tietokonettasi ja arvokkaita järjestelmätiedostoja sekä vaarantaa tietokoneesi tietoturvan.

1 Avaa SystemGuards-ikkuna.

Miten?

1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
2. Napsauta SecurityCenterin Koti-ikkunan **Tietokone ja tiedostot** -painiketta.
3. Napsauta Internet ja verkko -tietoalueen **Määritä**-painiketta.
4. Varmista Tietokone ja tiedostot -määrittämissivusta, että SystemGuard-suojauksen käyttö on käytössä, ja napsauta **Lisäasetukset**-painiketta.

2 Valitse luettelosta SystemGuards-tyyppi.

- **Ohjelmien SystemGuards-toiminnot**
- **Windowsin SystemGuards-toiminnot**
- **Selaimen SystemGuards-toiminnot**

3 Suorita jokin seuraavista toimenpiteistä **Haluan**-kohdassa:

- Jos haluat havaita, kirjata ja raportoida ohjelmien, Windowsin ja selainten SystemGuards-toimintoihin liittyviä luvattomia rekisteri- ja tiedostomuutoksia, valitse **Näytä hälytykset**.
- Jos haluat havaita ja kirjata ohjelmien, Windowsin ja selainten SystemGuards-toimintoihin liittyviä luvattomia rekisteri- ja tiedostomuutoksia, valitse **Muutokset ainoastaan kirjataan lokiin**.
- Jos haluat poistaa käytöstä ohjelmien, Windowsin ja selainten SystemGuards-toimintoihin liittyvien luvattomien rekisteri- ja tiedostomuutosten havaitsemisen, valitse **Muutokset ainoastaan kirjataan lokiin**.

Huomaa: Katso lisätietoja SystemGuards-tyypeistä kohdasta Tietoja SystemGuards-tyypeistä (sivu 47).

Tietoja SystemGuards-tyypeistä

SystemGuards-toiminnot havaitsevat tietokoneesi rekisterin ja muiden tärkeiden Windowsin tiedostojen mahdollisesti luvattomat muutokset. SystemGuards-toimintoja on kolmea eri tyyppiä: ohjelmien, Windowsin ja selainten SystemGuards-toiminnot.

Ohjelmien SystemGuards-toiminnot

Ohjelmien SystemGuards-toiminnot pysäyttävät epäilyttävät ActiveX-ohjelmat (Internetistä ladatut), vakoiluohjelmat ja ei-toivotut ohjelmat, jotka voivat käynnistyä automaattisesti Windowsin käynnistyksen yhteydessä.

SystemGuard -toiminto	Havaitsee...
ActiveX-asennukset	Luvattomat ActiveX-asennusten rekisterimuutokset, jotka voivat vahingoittaa tietokonettasi ja arvokkaita järjestelmätiedostoja sekä vaarantaa tietokoneesi tietoturvan.
Käynnistettävät kohteet	Vakoilu-, mainos-, ja muut haittaohjelmat, jotka voivat muuttaa käynnistettäviä kohteita, mikä mahdollistaa epäilyttävien ohjelmien suorittamisen Windowsin käynnistyksen yhteydessä.
Windows Shell Execute Hook -ohjelmat	Vakoilu- ja mainosohjelmat tai muut mahdolliset haittaohjelmat, jotka voivat asentaa Shell Execute Hook -ohjelmia estääkseen tietoturvaohjelmia toimimasta.
Shell Service Object Delay Load -luettelo	Vakoilu-, mainos- ja muut haittaohjelmat, jotka voivat muuttaa rekisterin Shell Service Object Delay Load -toimintoja, mikä mahdollistaa epäilyttävien ohjelmien suorittamisen Windowsin käynnistyksen yhteydessä.

Windowsin SystemGuards-toiminnot

Windowsin SystemGuards-toiminnot estävät tietokoneettasi lähettämästä tai vastaanottamasta luvattomia ja henkilökohtaisia tietoja Internetin välityksellä. Suojaukset auttavat myös pysäyttämään ohjelmia, jotka voivat muuttaa tärkeitten ohjelmiesi ulkonäköä ja toimintaa.

SystemGuard -toiminto	Kohde
Pikavalikon käsittelijät	Luvattomat pikavalikon käsittelijöiden muutokset, jotka voivat muuttaa Windowsin valikoiden ulkoasua ja toimintaa. Pikavalikot mahdollistavat erilaiset tietokoneen toiminnot, kuten tiedostojen napsauttamisen hiiren kakkospainikkeella.
AppInit DLL -tiedostot	Windowsin appInit DLL -tiedostojen luvattomat rekisterimuutokset saattavat mahdollistaa haitallisten ohjelmien suorittamisen tietokoneen käynnistyksen yhteydessä.
Windowsin Hosts-tiedosto	Vakoilu-, mainos- ja muut haittaohjelmat voivat muuttaa Windowsin Hosts-tiedostoa, mikä mahdollistaa selaimen ohjaamisen epäilyttäville Web-sivustoille ja ohjelmistopäivitysten estämisen.
Winlogon-käyttöliittymä	Vakoilu-, mainos- ja muut haittaohjelmat voivat muuttaa Winlogon-käyttöliittymän rekisteriä, mikä mahdollistaa sen, että toiset ohjelmat korvaavat Windowsin Resurssienhallinnan.
Winlogon User Init -asetukset	Vakoilu-, mainos- ja muut haittaohjelmat voivat muuttaa Winlogon User Init -rekisteriasetuksia, mikä mahdollistaa epäilyttävien ohjelmien suorittamisen Windowsiin kirjautumisen yhteydessä.
Windows-protokollat	Vakoilu-, mainos- ja muut haittaohjelmat voivat muuttaa Windows-protokollien rekisteriasetuksia, mikä vaikuttaa siihen, miten tietokoneesi lähettää ja vastaanottaa tietoja Internetistä.
Winsock-kerrostettujen palvelujen tarjoajat	Vakoilu-, mainos- ja muut haittaohjelmat voivat asentaa Winsock LSP:n rekisterimuutoksia, mikä mahdollistaa Internetiin lähettämiesi ja sieltä vastaanottamiesi tietojen kaappaamisen ja muuttamisen.
Windows-käyttöliittymän avoimet komennot	Luvattomat muutokset Windows-käyttöliittymän avoimiin komentoihin voivat mahdollistaa matojen ja muiden haittaohjelmien suorittamisen tietokoneellasi.

Shared Task Scheduler -rekisteriavain	Vakoilu-, mainos- ja muut haittaohjelmat voivat tehdä muutoksia Shared Task Scheduler -rekisteriavaimeen, mikä mahdollistaa vahingollisten ohjelmien suorittamisen tietokoneen käynnistyksen yhteydessä.
Windows Messenger -palvelu	Vakoilu-, mainos- ja muut haittaohjelmat voivat muuttaa Windows Messenger -palvelun rekisteriasetuksia, mikä mahdollistaa ei-toivotut mainosten esittämisen ja ohjelmien etäsuorittamisen tietokoneellasi.
Windowsin Win.ini-tiedosto	Vakoilu-, mainos- ja muut haittaohjelmat voivat muuttaa Win.ini-tiedostoa, mikä mahdollistaa epäilyttävien ohjelmien suorittamisen tietokoneen käynnistyksen yhteydessä.

Selaimen SystemGuards-toiminnot

Selainten SystemGuards-teknologia auttaa estämään selaimen luvaton toimintaa, kuten käyttäjän ohjaamista epäilyttäviin Web-sivustoihin, selaimen asetusten ja määritysten luvaton muuttamista ja epäilyttävien sivustojen tulkintaa luotettaviksi.

SystemGuard-toiminto	Havaitsee...
Selainapuohjelman objektit	Vakoilu-, mainos- ja muut haittaohjelmat, jotka voivat käyttää selainapuohjelmien objekteja Web-selauksen seuraamiseen ja ei-toivottujen mainosten esittämiseen.
Internet Explorerin palkit	Internet Explorerin palkkiohjelmien (kuten Haku ja Suosikit) luvattomat rekisterimuutokset, jotka voivat muuttaa Internet Explorerin ulkonäköä ja toimintaa.
Internet Explorerin laajennukset	Vakoilu-, mainos- ja muut haittaohjelmat, jotka voivat asentaa Internet Explorerin laajennuksia. Laajennukset seuraavat Web-selausta ja esittävät ei-toivottuja mainoksia.
Internet Explorer ShellBrowser	Internet Explorer ShellBrowserin luvattomat rekisterimuutokset, jotka voivat muuttaa Web-selaimesi ulkonäköä ja toimintaa.
Internet Explorer WebBrowser	Internet Explorer WebBrowserin luvattomat rekisterimuutokset, jotka voivat muuttaa Web-selaimesi ulkonäköä ja toimintaa.
Internet Explorer URL Search Hook -objektit	Vakoilu-, mainos- ja muut haittaohjelmat, jotka voivat tehdä muutoksia Internet Explorer URL Search Hook -objektien rekistereihin, mikä mahdollistaa selaimesi ohjaamisen epäilyttäville Web-sivustoille, kun haet tietoja Webistä.

Internet Explorerin URL-osoitteet	Vakoilu-, mainos- ja muut haittaohjelmat, jotka voivat muuttaa Internet Explorerin URL-osoitteiden rekisteriä, mikä vaikuttaa selaimen asetuksiin.
Internet Explorerin rajoitukset	Vakoilu-, mainos- ja muut haittaohjelmat, jotka voivat muuttaa Internet Explorerin rajoitusten rekisteriä, mikä vaikuttaa selaimen asetuksiin.
Internet Explorerin suojausvyöhykkeet	Vakoilu-, mainos- ja muut haittaohjelmat, jotka voivat tehdä muutoksia Internet Explorerin suojausvyöhykkeisiin, mikä mahdollistaa vahingollisten ohjelmien suorittamisen tietokoneen käynnistyksen yhteydessä.
Internet Explorerin luotettavat sivustot	Vakoilu-, mainos- ja muut haittaohjelmat, jotka voivat muuttaa Internet Explorerin luotettavien sivustojen rekisteriasetuksia niin, että selaimesi luottaa epäilyttäviin Web-sivustoihin.
Internet Explorer -käytäntö	Vakoilu-, mainos- ja muut haittaohjelmat, jotka voivat muuttaa Internet Explorer -käytäntöjen rekisteriä, mikä vaikuttaa selaimen ulkonäköön ja toimintaan.

Luotettujen luetteloiden käyttäminen

Jos VirusScan havaitsee tiedosto- tai rekisterimuutoksen (SystemGuard), ohjelman tai puskurin ylivuodon, se pyytää joko luottamaan kohteeseen tai poistamaan sen. Jos luotat kohteeseen etkä halua, että siitä ilmoitetaan jatkossa, kohde lisätään luotettujen luetteloon. Luotettujen luettelossa olevan kohteen toiminnan estäminen on myös mahdollista. Estäminen estää kohteen suorittamisen ja sen tekemät muutokset tietokoneeseesi ilman, että yrityksistä ilmoitetaan. Voit myös poistaa kohteen luotettujen luettelosta. Kun kohde on poistettu luettelosta, VirusScan voi taas havaita sen toiminnan.

Luotettujen luetteloiden hallinta

Luotetut luettelot -ikkunassa voit merkitä kohteita luotetuiksi tai estää aikaisemmin luotetuiksi merkittyjä kohteita. Voit myös poistaa kohteen luotettujen luettelosta, jotta VirusScan havaitsee kohteen.

1 Avaa Luotetut luettelot -ikkuna.

Miten?

1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
2. Napsauta SecurityCenterin Koti-ikkunan **Tietokone ja tiedostot** -painiketta.
3. Napsauta Internet ja verkko -tietoalueen **Määritä** -painiketta.
4. Varmista Tietokone ja tiedostot -määritysikkunasta, että virustorjunta on käytössä, ja napsauta **Lisäasetukset** -painiketta.
5. Napsauta Virustorjunta-ikkunan kohtaa **Luotetut luettelot**.

2 Valitse yksi seuraavista luettelotyypeistä:

- **Ohjelmien SystemGuards-suojaukset**
- **Windows SystemGuards-suojaukset**
- **Selaimen SystemGuards-toiminnot**
- **Luotetut ohjelmat**
- **Luotetut puskurin ylivuodot**

3 Suorita jokin seuraavista toimenpiteistä **Haluan**-kohdassa:

- Jotta havaittu ohjelma voi tehdä muutoksia Windowsin rekisteritietoihin tai kriittisiin järjestelmätiedostoihin ilmoittamatta käyttäjälle, valitse **Luota**.
- Voit estää havaittua ohjelmaa tekemästä muutoksia Windowsin rekisteritietoihin tai kriittisiin järjestelmätiedostoihin valitsemalla **Estä**.

- Voit poistaa havaitun ohjelman luotettujen luettelosta valitsemalla **Poista**.

4 Valitse **OK**.

Huomaa: Lisätietoja luotettujen luetteloiden tyypeistä on kohdassa Tietoja luotettujen luetteloiden tyypeistä (sivu 52).

Tietoja luotettujen luetteloiden tyypeistä

Luotetut luettelot -ikkunan SystemGuards-toiminnot ilmaisevat VirusScan-ohjelman aiemmin havaitsemia luvattomia rekisteri- ja tiedostomuutoksia, jotka olet hyväksynyt hälytyksessä tai Tarkistuksen tulokset -ikkunassa. Luotetut luettelot -ikkunassa on viisi erityyppistä ja hallittavaa luotettua luetteloa: Ohjelmien SystemGuard-toiminnot, Windows SystemGuards, Selaimen SystemGuards, Luotetut ohjelmat ja Luotetut puskurin ylivuodot.

Toiminto	Kuvaus
Ohjelmien SystemGuards -suojaukset	Luotetut luettelot -ikkunan ohjelmien SystemGuards-toiminnot ilmaisevat VirusScan-ohjelman aiemmin havaitsemia luvattomia rekisteri- ja tiedostomuutoksia, jotka olet hyväksynyt hälytyksessä tai Tarkistuksen tulokset -ikkunassa. Ohjelmien SystemGuards-toiminnot havaitsevat ActiveX-asennusmerkintöihin, käynnistysmerkintöihin, Windows shell execute hook -ohjelmiin ja Shell Service Object Delay Load -toimintoihin liittyvät luvattomat rekisteri- ja tiedostomuutokset. Tämän tyyppiset luvattomat rekisteri- ja tiedostomuutokset voivat vahingoittaa tietokonettasi ja arvokkaita järjestelmätiedostoja sekä vaarantaa tietokoneesi tietoturvan.
Windows SystemGuards -suojaukset	Luotetut luettelot -ikkunan Windows SystemGuards-toiminnot ilmaisevat VirusScan-ohjelman aiemmin havaitsemia luvattomia rekisteri- ja tiedostomuutoksia, jotka olet hyväksynyt hälytyksessä tai Tarkistuksen tulokset -ikkunassa. Windows SystemGuards -toiminnot havaitsevat pikavalikon käsittelijöihin, AppInit DLL -tiedostoihin, Windowsin Hosts-tiedostoihin, Winlogon-käyttöliittymään, Winsock LSP:hen ym. liittyvät luvattomat rekisteri- ja tiedostomuutokset. Tämän tyyppiset luvattomat rekisteri- ja tiedostomuutokset voivat muuttaa ohjelmien ulkoasua ja toimintaa, vaikuttaa siihen, miten tietokone lähettää tietoja Internetiin ja miten tietokone vastaanottaa tietoja, sekä sallia epäilyttävien ohjelmien suorittamisen tietokoneessa.

Selaimen SystemGuards-toiminnot	Luotetut luettelot -ikkunan selaimen SystemGuards-toiminnot ilmaisevat VirusScan-ohjelman aiemmin havaitsemia luvattomia rekisteri- ja tiedostomuutoksia, jotka olet hyväksynyt hälytysikkunassa tai Tarkistuksen tulokset -ikkunassa. Selaimen SystemGuards-toiminnot havaitsevat selainapuohjelmien objekteihin, Internet Explorerin laajennuksiin, Internet Explorerin URL-osoitteisiin, Internet Explorerin suojausvyöhykkeisiin ym. liittyvät luvattomat rekisteri- ja tiedostomuutokset. Tämän tyyppiset luvattomat rekisteri- ja tiedostomuutokset voivat muuttaa selaimen asetuksia ja määrittämiä ja vaikuttaa selaimen toimintaan niin, että käyttäjä ohjataan epäilyttäviin Web-sivustoihin ja että selain tulkitsee epäilyttävät sivustot luotettaviksi.
Luotetut ohjelmat	Luotetut ohjelmat ovat VirusScan-ohjelman aiemmin havaitsemia mahdollisesti ei-toivottuja ohjelmia, jotka olet hyväksynyt hälytysikkunassa tai Tarkistuksen tulokset -ikkunassa.
Luotetut puskurin ylivuodot	Luotetut puskurin ylivuodot ovat VirusScan-ohjelman aiemmin havaitsemia luvattomia toimenpiteitä, jotka olet hyväksynyt hälytysikkunassa tai Tarkistuksen tulokset -ikkunassa. Puskurin ylivuodot voivat vahingoittaa tietokonetta ja tiedostoja. Puskurin ylivuoto tapahtuu, jos ohjelmien tai prosessien käyttämä puskurin määrä ylittää puskurin kapasiteetin.

L U K U 1 1

Tietokoneen tarkistaminen

Kun käynnistät SecurityCenterin ensimmäistä kertaa, VirusScanin reaaliaikainen virustorjunta alkaa suojella tietokonetta mahdollisesti haitallisilta viruksilta, troijalaisilta ja muilta tietoturvauhilta. Ellet poista reaaliaikaista virustorjuntaa käytöstä, VirusScan tarkkailee tietokonetta jatkuvasti mahdollisten virusten varalta ja tarkistaa tiedostot aina määrittämiesi reaaliaikaisten tarkistusasetusten avulla, kun tiedostoja käytetään. Jos haluat varmistaa, että tietokoneesi pysyy suojattuna uusimmilta turvallisuushilta vastaan, pidä reaaliaikainen virustorjunta käytössä ja laadi säännöllinen aikataulu perusteellisempia manuaalisia tarkistuksia varten. Lisätietoja reaaliaikaisen ja manuaalisen tarkistuksen määrittämisestä on kohdassa Virustorjunnan määrittäminen (sivu 37).

VirusScanin manuaalisessa tarkistuksessa on reaaliaikaista tarkistusta kattavammat tarkistusasetukset, joiden avulla voit ajoittain tarkistaa tietokoneen reaaliaikaista tarkistusta tarkemmin. Voit käynnistää manuaalisen tarkistuksen SecurityCenteristä ja ajoittaa tiettyjen kohteiden tarkistuksen. Voit myös käynnistää manuaalisen tarkistuksen Windowsin Resurssienhallinnasta työskennellessäsi. Kun suoritat tarkistuksen SecurityCenterissä, voit muuttaa tarkistusasetuksia käytön aikana. Windowsin Resurssienhallinnassa sen sijaan on kätevät tietoturvatoiminnot.

Voit tarkastella molemmissa tapauksissa tarkistuksen tuloksia tarkistuksen jälkeen. Tarkistuksen tuloksissa näkyy, onko VirusScan havainnut, korjannut tai eristänyt viruksia, troijalaisia, vakoiluohjelmia, mainosohjelmia, evästeitä tai muita mahdollisia haittaohjelmia. Voit tarkastella tarkistuksen tuloksia useissa muodoissa. Voit esimerkiksi valita tarkistuksen tulosten perusyhteenvedon tai yksityiskohtaiset tiedot, kuten tartunnan tilan ja tyypin. Voit myös tarkastella yleisiä tarkistustilastoja.

Tässä luvussa

Tietokoneen tarkistaminen	56
Näytä tarkistuksen tulokset	56

Tietokoneen tarkistaminen

Voit käynnistää manuaalisen tarkistuksen SecurityCenterin Perus- tai Lisävalikosta. Jos käynnistät tarkistuksen Lisävalikosta, voit vahvistaa manuaalisen tarkistuksen asetukset ennen tarkistusta. Jos käynnistät tarkistuksen Perusvalikosta, VirusScan käynnistää tarkistuksen heti ja käyttää aiemmin määritettyjä tarkistusasetuksia. Voit käynnistää tarkistuksen myös Windowsin Resurssienhallinnasta, jolloin järjestelmä käyttää aiemmin määritettyjä asetuksia.

- Valitse jompikumpi seuraavista:

Tarkistaminen SecurityCenterissä

Jos haluat...	Tee näin...
suorittaa tarkistuksen nykyisiä asetuksia käyttäen	valitse Perusvalikosta Tarkista .
muuttaa asetuksia ennen tarkistusta	valitse Lisävalikosta Tarkista , valitse tarkistettavat kohteet, valitse tarkistuksen asetukset ja valitse sitten Tarkista nyt .

Tarkistaminen Windowsin Resurssienhallinnassa

1. Avaa Windowsin Resurssienhallinta.
2. Napsauta tiedostoa, kansiota tai asemaa hiiren kakkospainikkeella ja valitse sitten **Tarkista**.

Huomautus: Tarkistuksen tulokset näkyvät Tarkistus on päättynyt -ikkunassa. Tuloksissa näkyvät tarkistettujen, havaittujen, korjattujen, eristettyjen ja poistettujen kohteiden lukumäärät. Lisätietoja tarkistuksen tuloksista ja saastuneiden kohteiden käsittelemisestä saat valitsemalla **Näytä tarkistuksen lisätiedot**.

Näytä tarkistuksen tulokset

Kun manuaalinen tarkistus on suoritettu, voit tarkastella tuloksia ja määrittää tietokoneen suojauksen tilan. Tarkistuksen tuloksissa näkyy, onko VirusScan havainnut, korjannut tai eristänyt viruksia, troijailasia, vakoiluohjelmia, mainosohjelmia, evästeitä tai muita mahdollisia haittaohjelmia.

- Valitse Perus- tai Lisävalikosta **Tarkista** ja valitse yksi seuraavista vaihtoehdoista:

Jos haluat...	Tee näin...
tarkastella tarkistuksen tuloksia hälytysikkunassa	tarkastele tuloksia Tarkistus on päättynyt -ikkunassa.

lisätietoja tarkistuksen tuloksista	valitse Tarkistus on päättynyt -ikkunassa Näytä tarkistuksen lisätiedot.
tarkastella tarkistuksen tulosten yhteenvetoa	napsauta tehtäväpalkin ilmaisinalueen Tarkistus on päättynyt -kuvaketta.
tarkastella tarkistustilastoja	kaksoisnapsauta ilmaisinalueen Tarkistus on päättynyt -kuvaketta.
tarkastella havaittujen kohteiden, tartunnan tilan ja tartunnan tyyppin tietoja	kaksoisnapsauta ilmaisinalueen Tarkistus on suoritettu -kuvaketta ja valitse sitten Tarkistuksen edistyminen: Manuaalinen tarkistus -ikkunassa Näytä tulokset.

LUKU 12

Tarkistuksen tulosten käyttäminen

Jos VirusScan havaitsee turvallisuusuhan reaaliaikaisen tai manuaalisen tarkistuksen aikana, se yrittää käsitellä uhan automaattisesti uhkatyypin mukaan. Jos VirusScan esimerkiksi havaitsee viruksen, troijalaisen tai seurantaevästeen, VirusScan yrittää puhdistaa saastuneen tiedoston. Jos VirusScan ei pysty puhdistamaan tiedostoa, ohjelma eristää tiedoston.

Joidenkin tietoturvaohjelmien tapauksessa VirusScan ei ehkä voi puhdistaa tai eristää tiedostoa. Tällaisissa tapauksissa VirusScan kehottaa käyttäjää käsittelemään uhan. Voit toimia eri tavoin uhan tyyppin mukaan. Jos VirusScan esimerkiksi havaitsee tiedostossa viruksen, muttei onnistu puhdistamaan tai eristämään tiedostoa, VirusScan estää tiedoston käyttämisen. Jos VirusScan havaitsee seurantaevästeitä, muttei onnistu puhdistamaan tai eristämään evästeitä, voit poistaa evästeet tai määrittää ne luotettaviksi. Jos VirusScan havaitsee mahdollisia haittaohjelmia, VirusScan ei suorita automaattisia toimia. Voit itse eristää ohjelmat tai määrittää ne luotettaviksi.

Kun VirusScan eristää kohteita, se salaa kohteet ja eristää ne sitten kansioon, jotta tiedostot, ohjelmat tai evästeet eivät voi vahingoittaa tietokonetta. Voit palauttaa tai poistaa eristettyjä kohteita. Useimmissa tapauksissa eristetyn evästeen poistaminen ei vaikuta järjestelmään. Jos VirusScan on kuitenkin eristänyt ohjelman, jonka tunnistat ja jota käytät, on suositeltavaa palauttaa ohjelma.

Tässä luvussa

Virusten ja troijalaisten käsitleminen.....	59
Mahdollisten haittaohjelmien käsitleminen.....	60
Eristettyjen tiedostojen käsitleminen.....	60
Eristettyjen ohjelmien ja evästeiden käsitleminen	61

Virusten ja troijalaisten käsitleminen

Jos VirusScan havaitsee reaaliaikaisen tai manuaalisen tarkistuksen aikana tietokoneessa viruksen tai troijalaisen, VirusScan yrittää puhdistaa tiedoston. Jos VirusScan ei pysty puhdistamaan tiedostoa, ohjelma yrittää eristää tiedoston. Jos myös eristäminen epäonnistuu, VirusScan estää tiedoston käyttämisen (vain reaaliaikaista tarkistusta käytettäessä).

1 Avaa Tarkistuksen tulokset -ikkuna.

Miten?

1. Kaksoisnapsauta tehtäväpalkin oikeassa reunassa olevalla ilmaisinalueella sijaitsevaa **Tarkistus on päättynyt** -kuvaketta.
 2. Valitse Tarkistuksen edistymisen: Manuaalinen tarkistus -ikkunassa **Näytä tulokset**.
- 2 Valitse tarkistuksen tulosten luettelosta **Viruses and Trojans** (Virukset ja troijalaiset).

Huomautus: Lisätietoja VirusScanin eristämien tiedostojen käsittelemisestä on kohdassa Eristettyjen tiedostojen käsitteleminen (sivu 60).

Mahdollisten haittaohjelmien käsitteleminen

Jos VirusScan havaitsee reaaliaikaisen tai manuaalisen tarkistuksen aikana tietokoneessa mahdollisen haittaohjelman, voit joko poistaa ohjelman tai määrittää sen luotettavaksi. Mahdollisen haittaohjelman poistaminen ei poista ohjelmaa järjestelmästä. Poistaminen eristää ohjelman, jotta se ei voi vahingoittaa tietokonetta tai tiedostoja.

- 1 Avaa Tarkistuksen tulokset -ikkuna.
Miten?
 1. Kaksoisnapsauta tehtäväpalkin oikeassa reunassa olevalla ilmaisinalueella sijaitsevaa **Tarkistus on päättynyt** -kuvaketta.
 2. Valitse Tarkistuksen edistymisen: Manuaalinen tarkistus -ikkunassa **Näytä tulokset**.
- 2 Valitse tarkistuksen tulosten luettelosta **Mahdolliset haittaohjelmat**.
- 3 Valitse mahdollinen haittaohjelma.
- 4 Valitse **Haluan**-kohdassa **Poista** tai **Luota**.
- 5 Vahvista valinta.

Eristettyjen tiedostojen käsitteleminen

Kun VirusScan eristää saastuneita tiedostoja, se salaa tiedostot ja eristää ne sitten kansioon, jotta tiedostot eivät voi vahingoittaa tietokonetta. Voit palauttaa tai poistaa eristettyjä tiedostoja.

- 1 Avaa Eristetyt tiedostot -ikkuna.
Miten?

1. Valitse vasemmanpuoleisesta ruudusta **Lisävalikko**.
2. Valitse **Palauta**.
3. Valitse **Tiedostot**.
- 2 Valitse eristetty tiedosto.
- 3 Valitse jokin seuraavista:
 - Jos haluat korjata eristetyn tiedoston ja palauttaa sen alkuperäiseen kansioon, valitse **Palauta**.
 - Jos haluat poistaa saastuneet tiedostot tietokoneesta, valitse **Poista**.
- 4 Vahvista valinta valitsemalla **Kyllä**.

Vihje: Voit palauttaa tai poistaa useita tiedostoja samanaikaisesti.

Eristettyjen ohjelmien ja evästeiden käsitteleminen

Kun VirusScan eristää mahdollisia haittaohjelmia tai seurantaevästeitä, se salaa tiedostot ja eristää ne sitten kansioon, jotta ohjelmat tai evästeet eivät voi vahingoittaa tietokonetta. Voit sitten palauttaa tai poistaa eristettyjä kohteita. Useimmissa tapauksissa eristetyn evästeen tai ohjelman poistaminen ei vaikuta järjestelmään.

- 1 Avaa eristetyt ohjelmat ja seurantaevästeet -ikkuna.
Miten?
 1. Valitse vasemmanpuoleisesta ruudusta **Lisävalikko**.
 2. Valitse **Palauta**.
 3. Valitse **Ohjelmat ja evästeet**.
- 2 Valitse eristetty ohjelma tai eväste.
- 3 Valitse jokin seuraavista:
 - Jos haluat korjata eristetyn tiedoston ja palauttaa sen alkuperäiseen kansioon, valitse **Palauta**.
 - Jos haluat poistaa saastuneet tiedostot tietokoneesta, valitse **Poista**.
- 4 Vahvista toiminto valitsemalla **Kyllä**.

Vihje: Voit palauttaa tai poistaa useita ohjelmia tai evästeitä samanaikaisesti.

L U K U 13

McAfee Personal Firewall

Personal Firewall on edistynyt tapa suojata tietokonetta ja henkilökohtaisia tietoja. Personal Firewall muodostaa muurin tietokoneen ja Internetin välille ja valvoo Internet-tietoliikennettä taustalla epäilyttävien tapahtumien varalta.

Huomautus: SecurityCenter raportoi kriittiset ja ei-kriittiset suojausongelmat heti, kun se havaitsee ne. Jos tarvitset apua suojausongelmien selvittämisessä, voit käyttää McAfee Virtual Technician -palvelua.

Tässä luvussa

Personal Firewall -ohjelman ominaisuudet	64
Palomuurin käynnistäminen	67
Hälytysten käsitteleminen	69
Tiedottavien hälytysten hallinta	73
Palomuurisuojauksen asetusten määrittäminen	75
Ohjelmien ja käyttöoikeuksien hallinta	87
Järjestelmäpalveluiden hallinta	97
Tietokoneyhteyksien hallinta	103
Kirjaus, valvonta ja analyysi	111
Perehtyminen Internet-tietoturvaan	121

Personal Firewall -ohjelman ominaisuudet

Personal Firewall sisältää seuraavat ominaisuudet.

Vakio ja mukautettu tietoturvasuojaus

Suojaudu tunkeutumiselta ja epäilyttäviltä tapahtumilta palomuurin vakioasetusten tai mukautettujen suojausasetusten avulla.

Reaaliaikaisia suosituksia

Saat halutessasi toiminnallisia suosituksia, jotka auttavat sinua päättämään, pitääkö ohjelmille myöntää oikeus muodostaa yhteys Internetiin tai voiko tietoliikenteeseen luottaa.

Ohjelmien käytön älykäs hallinta

Ohjelmien käytön älykäs hallinta ohjaa ohjelmien Internet-yhteyksiä, antaa hälytyksiä ja tapahtumalokeja sekä määrittää yksittäisten ohjelmien käyttöoikeuksia.

Pelaamisen suojaus

Pelaamisen suojaus estää tietomurtoyrityksiä ja epäilyttäviä tapahtumia koskevia hälytyksiä häiritsemästä sinua pelatessasi koko näytön tilassa.

Tietokoneen käynnistyssuojaus

Tietokoneen käynnistyssuojaus suojaa tietokonetta tietomurtoyrityksiltä, ei-toivotuilta ohjelmilta ja tietoliikenteeltä ennen Windowsin® käynnistymistä.

Järjestelmäpalveluporttien valvonta

Hallitse avattuja ja suljettuja järjestelmäpalveluportteja, joita jotkin ohjelmat vaativat.

Tietokoneyhteyksien hallinta

Salli ja estä etäyhteyksiä oman tietokoneesi ja muiden tietokoneiden välillä.

HackerWatchin yhdistetyt tiedot

Seuraa hakkereiden toimintaa ja tietomurtoja HackerWatch-verkkosivuston kautta. Sivusto tarjoaa aina ajan tasalla olevia tietoja tietokoneesi ohjelmista, maailmanlaajuisista tietoturvatapahtumista ja Internet-porttitilastoista.

Lukitse palomuuuri

Voit estää kaiken tietokoneesi ja Internetin välisen saapuvan ja lähtevän tietoliikenteen välittömästi.

Palomuurin palauttaminen

Voit palauttaa palomuurin alkuperäiset suojasetukset välittömästi.

Trojajalaisten tehokas tunnistaminen

Havaitse ja estä mahdollisesti haitallisia sovelluksia, kuten troijalaisia, lähettämistä henkilökohtaisia tietojasi Internetiin.

Tapahtumien kirjaus

Seuraa äskettäistä tulevaa ja lähtevää tietoliikennettä sekä tietomurtotapahtumia.

Internet-tietoliikenteen valvonta

Voit tarkastella maailmanlaajuisia kartoja, jotka kuvaavat vihamielisiä hyökkäyksiä ja tietoliikennettä. Lisäksi voit hakea yksityiskohtaisia tietoja IP-lähdeosoitteiden omistajista ja niiden maantieteellisestä sijainnista. Analysoi saapuvaa ja lähtevää tietoliikennettä, valvo ohjelmien käyttämää kaistanleveyttä ja ohjelmatapahtumia.

Tietomurtojen estäminen

Suojaa yksityisyyttäsi mahdollisilta Internet-uhkilta. McAfee tarjoaa kolmannen suojaukerroksen käyttämällä heuristista menetelmää, joka estää hyökkäyksiä ja tietomurtoyrityksiä muistuttavia kohteita.

Kehittynyt tietoliikenneanalyysi

Tarkastele saapuvaa ja lähtevää Internet-tietoliikennettä sekä ohjelmien muodostamia yhteyksiä, myös niitä, jotka kuuntelevat aktiivisesti avoimia yhteyksiä. Näin voit tunnistaa tietomurtoille alttiit ohjelmat ja ryhtyä tarvittaviin toimenpiteisiin.

LUKU 14

Palomuurin käynnistäminen

Palomuurin käynnistämisen jälkeen tietokone on suojattu tietomurroilta ja ei-toivotulta tietoliikenteeltä. Olet lisäksi valmis käsittelemään hälytyksiä ja hallitsemaan tunnettujen ja tuntemattomien ohjelmien saapuvaa ja lähtevää Internet-käyttöä. Suositukset ja Luottava suojaustaso (jossa ohjelmille on sallittu vain lähtevä Internet-liikenne) ovat automaattisesti käytössä.

Voit poistaa Firewallin käytöstä Internet- ja verkkomäärittelyt -ikkunasta, mutta tällöin tietokone ei ole suojassa tietomurroilta ja ei-toivotulta tietoliikenteeltä, etkä myöskään voi hallita saapuvia ja lähteviä Internet-yhteyksiä tehokkaasti. Jos sinun on poistettava palomuurisuojaus käytöstä, tee se väliaikaisesti ja vain silloin, kun se on aivan välttämätöntä. Voit myös ottaa Firewallin käyttöön Internet- ja verkkomäärittelyt -ikkunassa.

Firewall poistaa Windowsin® palomuurin automaattisesti käytöstä ja asettaa itsensä oletuspalomuuriksi.

Huomaa: Määritä palomuuuri avaamalla Internet ja verkko -asetusikkuna.

Tässä luvussa

Palomuurisuojauksen käynnistäminen.....	67
Palomuurisuojauksen pysäyttäminen.....	68

Palomuurisuojauksen käynnistäminen

Voit ottaa palomuurin käyttöön suojaamaan tietokoneettasi tietomurroilta ja ei-toivotulta tietoliikenteeltä sekä auttamaan sinua hallitsemaan saapuvia ja lähteviä Internet-yhteyksiä.

- 1 Valitse McAfee SecurityCenter -ikkunassa **Internet ja verkko** ja valitse sitten **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelyt -ikkunan **Palomuurisuojaus ei ole käytössä** -kohdasta **Käytössä**.

Palomuurisuojaus pysäyttäminen

Voit poistaa palomuurin käytöstä, jos et halua suojata tietokonetta tietomurroilta ja ei-toivotulta tietoliikenteeltä. Kun palomuurisuojaus on poistettu käytöstä, et voi hallita saapuvia ja lähteviä Internet-yhteyksiä.

- 1 Valitse McAfee SecurityCenter -ikkunassa **Internet ja verkko** ja valitse sitten **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Ei käytössä**.

LUKU 15

Hälytysten käsitteleminen

Palomuuuri käyttää erilaisia hälytyksiä auttaakseen sinua hallitsemaan tietoturvaa. Nämä hälytykset voidaan jakaa kolmeen eri ryhmään:

- Punaiset hälytykset
- Keltaiset hälytykset
- Vihreät hälytykset

Hälytyksissä on myös tietoja, jotka auttavat käyttäjää päättämään, miten hälytyksiä pitää käsitellä tai miten tietokoneessa käytettävistä ohjelmista voi saada tietoja.

Tässä luvussa

Tietoja hälytyksistä 70

Tietoja hälytyksistä

Palomuurissa on kolme perushälytystyyppiä. Joissakin hälytyksissä on myös tietoja, jotka helpottavat tietokoneessa suoritettavien ohjelmien käytön oppimista tai niihin liittyvien tietojen hankkimista.

Punaiset hälytykset

Punainen hälytys tarkoittaa, että palomuuuri havaitsee ja estää tietokoneessa olevan troijalaisen ja suosittelee tietokoneen tarkistamista uusien uhkien välttämiseksi. Troijan hevonen näyttää luvalliselta ohjelmalta, mutta se voi aiheuttaa tietokoneelle vahinkoa tai sallia tietokoneen luvattoman käytön. Hälytys esiintyy kaikilla tietoturvasoilla paitsi Avoin-tasolla.

Keltaiset hälytykset

Keltainen hälytys on yleisin hälytystyyppi. Se ilmoittaa palomuurin havaitsemista ohjelmatoiminnoista ja verkkotapahtumista. Keltainen hälytys kuvaa ohjelmatoiminnon tai verkkotapahtuman ja ehdottaa yhtä tai useita menettelytapoja. Näyttöön tulee esimerkiksi **Havaittu uusi verkko** -hälytys, kun tietokone, johon palomuuuri on asennettu, kytketään uuteen verkkoon. Voit itse päättää, haluatko luottaa verkkoon vai et. Jos verkkoon luotetaan, palomuuuri sallii tietoliikenteen kaikista muista verkossa olevista tietokoneista, ja verkko lisätään luotettavien IP-osoitteiden luetteloon. Jos suositukset on otettu käyttöön, ohjelmat lisätään Ohjelmien käyttöoikeudet -ikkunaan.

Vihreät hälytykset

Useimmissa tapauksissa vihreä hälytys antaa perustietoja tapahtumasta eikä vaadi käyttäjän vastausta. Vihreät hälytykset on oletusarvoisesti poistettu käytöstä, ja ne esiintyvät yleensä vain, kun käytössä on tietoturvaso Normaali, Luottava, Tiukka tai Vaikeasti havaittava.

Käyttäjätuki

Monissa palomuurin hälytyksissä on lisätietoja, jotka auttavat sinua hallitsemaan tietokoneen tietoturvaa. Niihin kuuluvat muun muassa seuraavat:

- **Lisää tietoja tästä ohjelmasta:** Avaa McAfeen maailmanlaajuinen tietoturvaa käsittelevä Web-sivusto, jos haluat saada lisätietoja ohjelmasta, jonka palomuuuri on havainnut tietokoneessa.

- **Kerro McAfeelle tästä ohjelmasta:** Lähetä McAfeelle tietoja tuntemattomasta tiedostosta, jonka palomuuuri on havainnut tietokoneessa.
- **McAfee suosittelee:** Hälytysten käsittelyyn liittyviä neuvoja. Hälytys voi esimerkiksi suositella, että myönnät ohjelmalle käyttöoikeudet.

LUKU 16

Tiedottavien hälytysten hallinta

Voit määrittää, näytetäänkö vai piilotetaan tiedottavat hälytykset, jotka palomuuuri lähettää havaittuaan tietomurtoyrityksiä tai epäilyttäviä tapahtumia tiettyjen tapahtumien aikana, kuten pelattaessa koko näytön tilassa.

Tässä luvussa

Näytä hälytykset pelaamisen aikana.....	73
Piilota tiedottavat hälytykset	74

Näytä hälytykset pelaamisen aikana

Voit määrittää, näytetäänkö tiedottavat hälytykset, jotka palomuuuri lähettää havaittuaan tietomurtoyrityksiä tai epäilyttäviä tapahtumia, kun tietokoneella pelataan koko näytön tilassa.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Lisävalikko**.
- 2 Valitse **Määritä**.
- 3 Valitse SecurityCenter-asetusikkunan **Hälytykset**-kohdasta **Lisäasetukset**.
- 4 Valitse Hälytysasetukset-ikkunasta **Näytä tiedottavat hälytykset, kun tietokoneen havaitaan olevan pelitilassa**.
- 5 Valitse **OK**.

Piilota tiedottavat hälytykset

Voit piilottaa tiedottavat hälytykset, jotka palomuuuri lähettää havaittuaan tietomurtoyrityksen tai epäilyttävän tapahtuman.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Lisävalikko**.
- 2 Valitse **Määritä**.
- 3 Valitse SecurityCenter-asetusikkunan **Hälytykset**-kohdasta **Lisäasetukset**.
- 4 Valitse SecurityCenter-asetusikkunasta **Tiedottavat hälytykset**.
- 5 Toimi Tiedottavat hälytykset -ikkunassa seuraavasti:
 - Piilota tiedottavat hälytykset valitsemalla **Älä näytä tiedottavia hälytyksiä**.
 - Tyhjennä poistettava viesti.
- 6 Valitse **OK**.

L U K U 17

Palomuurisuojauksen asetusten määrittäminen

Palomuurin avulla voit hallita tietoturvaa eri tavoilla sekä mukauttaa tapaa, jolla tietoturvatapahtumiin ja hälytyksiin vastataan.

Kun olet asentanut palomuurin ensimmäisen kerran, tietokoneen suojaustasoksi on määritetty Luottava ja ohjelmien vain lähtevät yhteydet on sallittu. Palomuurissa on kuitenkin myös muita tasoja, jotka vaihtelevat erittäin rajoittavista erittäin salliviin.

Halutessasi voit saada palomuurilta myös hälytyksiin ja ohjelmien Internet-käyttöön liittyviä suosituksia.

Tässä luvussa

Palomuurin tietoturvasojen hallinta	76
Hälytyksiin liittyvien suositusten asetusten määrittäminen	80
Palomuurin suojauksen optimointi.....	82
Firewallin lukitseminen ja palauttaminen	85

Palomuurin tietoturvasojen hallinta

Palomuurin suojaustasojen avulla voit määrittää, kuinka paljon haluat hallita hälytyksiä ja miten haluat vastata hälytyksiin. Nämä hälytykset tulevat näkyviin, kun palomuuari havaitsee ei-toivottua tietoliikennettä tai saapuvia ja lähteviä Internet-yhteyksiä. Oletuksena palomuurin suojausasetuksiksi on määritetty Luottava ja lähtevän tietoliikenteen sallivat käyttöoikeudet.

Kun Luottava-tietoturvaso on asetettu ja suositukset on otettu käyttöön, keltaiset hälytykset antavat mahdollisuuden sallia käyttöoikeudet tuntemattomille, saapuvaa yhteyttä tarvitseville ohjelmille tai estää ne. Kun palomuuari havaitsee tunnettuja ohjelmia, näyttöön ilmestyy vihreitä, tiedottavia hälytyksiä ja käyttöoikeudet myönnetään automaattisesti. Kun käyttöoikeudet on myönnetty, ohjelma voi muodostaa lähteviä yhteyksiä ja kuunnella pyytämättömiä saapuvia yhteyksiä.

Yleisesti voidaan sanoa, että rajoittavien tietoturvasojen (Vaikeasti havaittava ja Tiukka) kohdalla käytetään enemmän asetuksia ja näytetään enemmän hälytyksiä, joihin käyttäjän on vastattava.

Seuraavassa taulukossa kuvataan palomuurin kuusi suojaustasoa erittäin rajoittavasta vähiten rajoittavaan:

Taso	Kuvaus
Lukitus	Estää kaikki lähtevät ja saapuvat verkkoyhteydet, mukaan lukien yhteydet Web-sivustoihin, sähköpostiin ja tietoturvapäivityksiin. Tällä tietoturvasolla on sama vaikutus kuin Internet-yhteyden katkaisemisella. Tätä asetusta käyttämällä voit estää portit, jotka olet valinnut avattaviksi Järjestelmäpalvelut-ikkunassa.
Vaikeasti havaittava	Estää kaikki saapuvat Internet-yhteydet (paitsi avoimet portit) ja estää muita näkemästä tietokonettasi Internetissä. Palomuuari hälyttää, kun uudet ohjelmat yrittävät muodostaa yhteyden Internetiin tai vastaanottavat saapuvia yhteyspyyntöjä. Estetyt ja lisätyt ohjelmat näkyvät Ohjelmien käyttöoikeudet -ikkunassa.
Tiukka	Palomuuari hälyttää, kun uudet ohjelmat yrittävät muodostaa yhteyden Internetiin tai vastaanottavat saapuvia yhteyspyyntöjä. Estetyt ja lisätyt ohjelmat näkyvät Ohjelmien käyttöoikeudet -ikkunassa. Kun tietoturvasoksi on asetettu Tiukka, ohjelma pyytää vain kulloinkin tarvittavaa käyttöoikeutta, esimerkiksi oikeutta vain lähtevään tietoliikenteeseen, jonka voit sallia tai estää. Jos ohjelma tarvitsee myöhemmin sekä saapuvaa että lähtevää yhteyttä, voit sallia ohjelmalle täydet käyttöoikeudet Ohjelmien käyttöoikeudet -ikkunassa.
Standardi	Palomuuari valvoo saapuvia ja lähteviä verkkoyhteyksiä ja ilmoittaa käyttäjälle, kun uudet ohjelmat yrittävät muodostaa yhteyden Internetiin. Estetyt ja lisätyt ohjelmat näkyvät Ohjelmien käyttöoikeudet -ikkunassa.

Luottava	Palomuuuri sallii joko saapuvat ja lähtevät tai vain lähtevät Internet-yhteydet. Oletussuojaustaso on Luottava ja vain ohjelmien lähtevät yhteydet on sallittu. Jos ohjelmalle on myönnetty täydet käyttöoikeudet, palomuuuri luottaa automaattisesti kyseiseen ohjelmaan ja lisää sen Ohjelmien käyttöoikeudet -ikkunan sallittujen ohjelmien luetteloon. Jos ohjelmalle on myönnetty vain lähtevän liikenteen käyttöoikeudet, palomuuuri luottaa automaattisesti kyseiseen ohjelmaan silloin, kun se muodostaa lähtevän Internet-yhteyden. Saapuville yhteyksille ei myönnetä automaattisesti käyttöoikeuksia.
Avaa	Palomuuuri sallii kaikki saapuvat ja lähtevät Internet-yhteydet.

Palomuuuri antaa sinulle myös mahdollisuuden palauttaa tietoturvaso välittömästi Luotettava-tasoksi (ja myöntää vain lähtevien yhteyksien käyttöoikeudet) Palauta palomuurisuojausten oletusasetukset -ikkunassa.

Aseta tietoturvasoksi Lukitus

Voit estää kaiken lähtevän ja saapuvan verkkoliikenteen määrittämällä palomuurin suojaustasoksi Lukitus.

- 1 Valitse McAfee SecurityCenter -ikkunassa **Internet ja verkko** ja valitse sitten **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Siirrä Tietoturvaso-ikkunan liukusäädintä siten, että sen nykyisenä tasona on **Lukitus**.
- 4 Valitse **OK**.

Suojaustason määrittäminen Vaikeasti havaittava -tasolle

Voit estää kaikki saapuvat yhteydet määrittämällä palomuurin tietoturvasoksi Vaikeasti havaittava, jos haluat estää muita näkemästä tietokonetta Internetissä.

- 1 Valitse McAfee SecurityCenter -ikkunassa **Internet ja verkko** ja valitse sitten **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Siirrä Tietoturvaso-ikkunan liukusäädintä siten, että sen nykyisenä tasona on **Vaikeasti havaittava**.
- 4 Valitse **OK**.

Huomautus: Piilotustilassa palomuuuri ilmoittaa, kun uudet ohjelmat pyytävät lähtevän yhteyden sallimista tai vastaanottavat saapuvan liikenteen pyyntöjä.

Suojaustason määrittäminen Tiukka-tasolle

Voit määrittää suojaustasoksi Tiukka, jos haluat palomuurin ilmoittavan, kun uudet ohjelmat yrittävät muodostaa lähteviä Internet-yhteyksiä tai saavat saapuvia yhteyspyyntöjä.

- 1 Valitse McAfee SecurityCenter -ikkunassa **Internet ja verkko** ja valitse sitten **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelyt -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Siirrä Tietoturvaso-ikkunan liukusäädintä siten, että sen nykyisenä tasona on **Tiukka**.
- 4 Valitse **OK**.

Huomautus: Kun tietoturvasoksi on asetettu Tiukka, ohjelma pyytää vain kulloinkin tarvittavaa käyttöoikeutta, esimerkiksi oikeutta vain lähtevään tietoliikenteeseen, jonka voit myöntää tai estää. Jos ohjelma tarvitsee myöhemmin sekä saapuvaa että lähtevää yhteyttä, voit myöntää ohjelmalle täydet käyttöoikeudet Ohjelmien käyttöoikeudet -ikkunassa.

Suojaustason määrittäminen Normaali-tasolle

Voit määrittää palomuurin suojaustasoksi Normaali, jos haluat palomuurin valvovan saapuvia ja lähteviä yhteyksiä ja hälyttävän, kun uudet ohjelmat yrittävät käyttää Internetiä.

- 1 Valitse McAfee SecurityCenter -ikkunassa **Internet ja verkko** ja valitse sitten **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelyt -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Siirrä Tietoturvaso-ikkunan liukusäädintä siten, että sen nykyisenä tasona on **Normaali**.
- 4 Valitse **OK**.

Suojaustason määrittäminen Luottava-tasolle

Voit määrittää palomuurin suojaustasoksi Luottava, jos haluat sallia täydet käyttöoikeudet tai vain lähtevän verkkoliikenteen.

- 1 Valitse McAfee SecurityCenter -ikkunassa **Internet ja verkko** ja valitse sitten **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelyt -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Siirrä Tietoturvaso-ikkunan liukusäädintä siten, että sen nykyisenä tasona on **Luottava**.
- 4 Valitse jokin seuraavista:
 - Voit sallia saapuvan ja lähtevän liikenteen valitsemalla **Salli kaikki käyttö**.

- Voit sallia pelkästään lähtevän liikenteen valitsemalla **Myönnä lähtevien yhteyksien käyttöoikeudet**.

5 Valitse **OK**.

Huomautus: Myönnä lähtevien yhteyksien käyttöoikeudet on oletusasetus.

Suojaustason määrittäminen Avoin-tasolle

Voit sallia kaiken lähtevän ja saapuvan verkkoliikenteen määrittämällä palomuurin suojaustasoksi Avoin.

- 1 Valitse McAfee SecurityCenter -ikkunassa **Internet ja verkko** ja valitse sitten **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelyt -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Siirrä Tietoturvaso-ikkunan liukusäädintä siten, että sen nykyisenä tasona on **Avoin**.
- 4 Valitse **OK**.

Hälytyksiin liittyvien suositusten asetusten määrittäminen

Voit määrittää, miten haluat Firewallin hälyttävän ohjelmista, jotka yrittävät muodostaa Internet-yhteyden. Firewall voi lisätä suosituksia hälytyksiin, jättää ne pois tai näyttää ne. Suositusten ottaminen käyttöön auttaa sinua päättämään, miten hälytyksiä kannattaa käsitellä.

Kun suositukset on otettu käyttöön (ja tietoturvasoksi on asetettu Luottava ja vain lähtevät yhteydet on sallittu), palomuuuri myöntää tai estää tunnettujen ohjelmien käyttöoikeudet automaattisesti sekä antaa hälytyksissä toimenpidesuosituksia, kun se kohtaa mahdollisesti vaarallisia ohjelmia.

Kun suositukset on poistettu käytöstä, palomuuuri ei myönnä eikä estä Internetin käyttöä eikä se myöskään anna toimenpidesuosituksia.

Kun suositusten arvoksi on asetettu Vain näyttö, palomuuuri kehottaa sallimaan tai estämään yhteyksiä, ja se suosittelee toimenpiteitä.

Suosituksien käyttöönotto

Voit ottaa suositukset käyttöön, jotta palomuuuri voi myöntää tai estää ohjelmien käyttöoikeudet sekä hälyttää tunnistamattomista ja mahdollisesti vaarallisista ohjelmista.

- 1 Valitse McAfee SecurityCenter -ikkunassa **Internet ja verkko** ja valitse sitten **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelyt -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Tietoturvaso-ikkunan **Suosituksien** -kohdasta **Ota suositukset käyttöön**.
- 4 Valitse **OK**.

Poista suositukset käytöstä

Voit poistaa suositukset käytöstä, jotta Firewall voi myöntää tai estää ohjelmien käyttöoikeudet sekä hälyttää tunnistamattomista ja mahdollisesti vaarallisista ohjelmista. Et kuitenkaan saa hälytyksiä ohjelmien käyttöoikeuksien käsittelyyn liittyvistä suosituksista. Jos Firewall havaitsee uuden ohjelman, jota se pitää epäilyttävänä tai jonka tiedetään olevan mahdollisesti vaarallinen, se estää automaattisesti ohjelmaa käyttämästä Internetiä.

- 1 Valitse McAfee SecurityCenter -ikkunassa **Internet ja verkko** ja valitse sitten **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Tietoturvasuojatason ikkunan **Suosituksien** -kohdasta **Poista suositukset käytöstä**.
- 4 Valitse **OK**.

Näytä vain suositukset

Voit määrittää, että vain hälytysten suositukset tulevat näkyviin, jotta voit päättää, myönnetäänkö vai estetäänkö tunnistamattomat sekä mahdollisesti vaaralliset ohjelmat.

- 1 Valitse McAfee SecurityCenter -ikkunassa **Internet ja verkko** ja valitse sitten **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Tietoturvasuojatason ikkunan **Suosituksien** -kohdasta **Vain näyttö**.
- 4 Valitse **OK**.

Palomuurin suojauksen optimointi

Tietokoneen suojaus voi pettää monesta syystä. Jotkin ohjelmat voivat esimerkiksi yrittää muodostaa Internet-yhteyden ennen Windowsin® käynnistymistä. Kokeneet tietokoneen käyttäjät voivat määrittää, onko tietokoneesi verkossa, lähettämällä tietokoneeseesi ping-pyynnön. Firewallin avulla voit puolustautua molempia tietomurtoyrityksiä vastaan sallimalla käynnistyssuojauksen käyttöönoton ja estämällä ping-pyyntöjä. Ensimmäinen asetus estää ohjelmia pääsemästä Internetiin Windowsin käynnistyessä ja toinen estää ping-pyyntöjä, jotka auttavat muita käyttäjiä havaitsemaan tietokoneesi verkossa.

Vakioasennusasetuksiin kuuluu muun muassa tavallisimpien tietomurtoyritysten, kuten palvelunestohyökkäysten tai tietoturva-aukkojen, automaattinen tunnistaminen. Käyttämällä vakioasennusasetuksia voit varmistaa, että tietokoneesi on suojattu näitä hyökkäyksiä ja tarkistuksia vastaan. Tietomurtojen havainnointi -ikkunassa voit kuitenkin myös poistaa yhden tai usean hyökkäyksen tai tarkistuksen automaattisen tunnistuksen käytöstä.

Suojaa tietokonetta käynnistyksen aikana

Voit suojata tietokonetta Windowsin käynnistyessä ja estää uusia ohjelmia, joilla ei ole – mutta jotka nyt tarvitsevat – Internetin käyttöoikeuksia käynnistyksen aikana. Firewall näyttää niitä ohjelmia koskevat hälytykset, jotka pysyivät Internetin käyttöoikeuksia. Voit päättää, myönnätkö vai estätkö oikeudet. Jos haluat käyttää tätä toimintoa, tietoturvasen asetuksena on oltava jokin muu kuin Avoin tai Lukitus.

- 1 Valitse McAfee SecurityCenter -ikkunassa **Internet ja verkko** ja valitse sitten **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Tietoturvasen -ikkunan **Suojausasetukset** -kohdasta **Salli käynnistyssuojaus**.
- 4 Valitse **OK**.

Huomaa: Estettyjä yhteyksiä ja tietomurtoja ei kirjata, jos käynnistyssuojaus on käytössä.

Määritä ping-pyyntöjen asetukset

Voit sallia tai estää sen, onko tietokoneesi verkossa muiden tietokonekäyttäjien tunnistettavissa.

- 1 Valitse McAfee SecurityCenter -ikkunassa **Internet ja verkko** ja valitse sitten **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Tietoturvasuojaus-ikkunan **Suojausasetukset**-kohdasta jompikumpi seuraavista:
 - Valitse **Salli ICMP ping -pyynnöt**, jos haluat sallia verkossa olevan tietokoneen havaitsemisen ping-pyyntöjen avulla.
 - Poista **Salli ICMP ping -pyynnöt** -kohdan valinta, jos haluat estää verkossa olevan tietokoneen havaitsemisen ping-pyyntöjen avulla.
- 4 Valitse **OK**.

Määritä tietomurtojen havainnoinnin asetukset

Tietomurtoja havainnoimalla voit suojata tietokonetta hyökkäyksiltä ja luvattomilta tarkistuksilta. Palomuurin vakioasetuksiin kuuluu yleisimpien tietomurtoyritysten (esimerkiksi palvelunestohyökkäysten ja tietoturva-aukkojen) automaattinen tunnistus. Voit kuitenkin myös poistaa yhden tai usean hyökkäyksen tai tarkistuksen automaattisen tunnistuksen käytöstä.

- 1 Valitse McAfee SecurityCenter -ikkunassa **Internet ja verkko** ja valitse sitten **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Firewall-ikkunasta **Tietomurtojen havainnointi**.
- 4 Valitse **Tunnista tietomurtoyritykset** -kohdasta jompikumpi seuraavista:
 - Valitse nimi hyökkäyksen tai tarkistuksen automaattista havainnointia varten.
 - Poista nimi, jos haluat poistaa hyökkäyksen tai tarkistuksen automaattisen havainnoinnin käytöstä.
- 5 Valitse **OK**.

Määritä palomuurin suojauksen tilan asetukset

Voit määrittää palomuurin asetukset niin, että tiettyjä tietokoneen ongelmia ei raportoida SecurityCenteriin.

- 1 Valitse McAfee SecurityCenter -ikkunan **SecurityCenterin tiedot** -kohdasta **Määritä**.
- 2 Valitse SecurityCenter-asetusikkunan **Suojauksen tila** -kohdasta **Lisäasetukset**.
- 3 Valitse Ohitetut ongelmat -ikkunasta vähintään yksi seuraavista vaihtoehdoista:
 - **Palomuurisuojaus ei ole käytössä.**
 - **Palomuurin suojaustasoksi on määritetty Avoin.**
 - **Palomuuripalvelu ei ole käytössä.**
 - **Palomuurisuojausta ei ole asennettu tietokoneeseen.**
 - **Windowsin palomuuri on poistettu käytöstä.**
 - **Lähtevää palomuuria ei ole asennettu tietokoneeseen.**
- 4 Valitse **OK**.

Firewallin lukitseminen ja palauttaminen

Lukituksella voit välittömästi estää kaiken saapuvan ja lähtevän verkkoliikenteen, mikä auttaa sinua eristämään ja ratkaisemaan tietokoneessa olevan ongelman.

Lukitse Firewall välittömästi

Firewallin lukitseminen estää välittömästi kaiken tietokoneen ja Internetin välisen tietoliikenteen.

- 1 Valitse McAfee SecurityCenter -ikkunan **Yleiset tehtävät** -kohdasta **Firewallin lukitseminen**.
- 2 Valitse Firewallin lukitseminen -ikkunasta **Lukitus**.
- 3 Vahvista valintasi valitsemalla **Kyllä**.

Vihje: Voit lukita Firewallin myös napsauttamalla tehtäväpalkin oikeassa reunassa sijaitsevalla ilmaisinalueella olevaa SecurityCenter-kuvaketta  hiiren kakkospainikkeella, valitsemalla **Pikalinkit** ja napsauttamalla **Firewallin lukitseminen**.

Poista Firewallin lukitus välittömästi

Firewallin lukituksen poistaminen sallii kaiken tietokoneen ja Internetin välisen tietoliikenteen.

- 1 Valitse McAfee SecurityCenter -ikkunan **Yleiset tehtävät** -kohdasta **Firewallin lukitseminen**.
- 2 Valitse Lukitse Firewall -ikkunasta **Poista lukitus**.
- 3 Vahvista valintasi valitsemalla **Kyllä**.

Palauta Firewallin asetukset

Voit palauttaa Firewallin alkuperäiset suojausasetukset nopeasti. Tämä muuttaa suojaustason takaisin Luottavaksi ja sallii vain lähtevän tietoliikenteen, ottaa Suositukset käyttöön, palauttaa oletusarvoisten ohjelmien luettelon ja niiden käyttöoikeudet Ohjelmien käyttöoikeudet -ruudussa, poistaa luotettavat ja estetyt IP-osoitteet sekä palauttaa järjestelmäpalvelut, tapahtumalokin asetukset ja tietomurtojen havainnoinnin.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Palauta Firewallin oletusasetukset**.
- 2 Valitse Palauta Firewallin oletusasetukset -ikkunasta **Palauta oletusasetukset**.
- 3 Vahvista valintasi valitsemalla **Kyllä**.

Vihje: Voit palauttaa Firewallin oletusasetukset myös napsauttamalla tehtäväpalkin oikeassa reunassa sijaitsevalla ilmaisinalueella olevaa SecurityCenter-kuvaketta  hiiren kakkospainikkeella, valitsemalla **Pikalinkit** ja napsauttamalla **Palauta Firewallin oletusasetukset**.

LUKU 18

Ohjelmien ja käyttöoikeuksien hallinta

Firewallin avulla voit luoda käyttöoikeuksia nykyisille ja uusille ohjelmille, jotka vaativat saapuvia ja lähteviä Internet-yhteyksiä, ja hallita niitä. Firewallin avulla voit hallita ohjelmien kaikkea tai vain lähtevää tietoliikennettä. Ohjelmien käyttöoikeudet voidaan myös estää.

Tässä luvussa

Ohjelmien Internet-käyttöoikeuden salliminen	88
Vain lähtevän tietoliikenteen käyttöoikeuksien myöntäminen	91
Ohjelmien Internet-käyttöoikeuden estäminen	93
Ohjelmien käyttöoikeuksien poistaminen	95
Perehtyminen ohjelmiin	96

Ohjelmien Internet-käyttöoikeuden salliminen

Jotkin ohjelmat, kuten Internet-selaimet, vaativat Internet-käyttöoikeutta toimiakseen kunnolla.

Firewallin Ohjelmien käyttöoikeudet -sivulla voit

- sallia ohjelmien käytön
- sallia vain lähtevän tietoliikenteen
- estää ohjelmien käytön.

Voit myöntää ohjelmille täydelliset tai vain lähtevän tietoliikenteen käyttöoikeudet myös lähtevien ja äskettäisten tapahtumien lokeista.

Myönnä ohjelmalle täydet käyttöoikeudet

Voit myöntää tietokoneessa olevalle estetylle ohjelmalle täydelliset ja lähtevän tietoliikenteen käyttöoikeudet.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet & verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Firewall-ikkunasta **Ohjelmien käyttöoikeudet**.
- 4 Valitse **Ohjelmien käyttöoikeudet** -kohdasta ohjelma, jonka asetuksena on **Estetty** tai **Vain lähtevien yhteyksien käyttöoikeudet**.
- 5 Valitse **Toiminto**-kohdasta **Myönnä käyttöoikeudet**.
- 6 Valitse **OK**.

Myönnä uudelle ohjelmalle täydet käyttöoikeudet

Voit myöntää tietokoneessa olevalle uudelle ohjelmalle täydelliset saapuvan ja lähtevän tietoliikenteen käyttöoikeudet.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet & verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Firewall-ikkunasta **Ohjelmien käyttöoikeudet**.
- 4 Valitse **Ohjelmien käyttöoikeudet** -kohdasta **Lisää sallittu ohjelma**.
- 5 Hae ja valitse **Lisää ohjelma** -valintaikkunasta ohjelma, jonka haluat lisätä, ja valitse **Avaa**.

Huomautus: Voit muuttaa juuri lisätyn ohjelman käyttöoikeuksia samalla tavalla kuin nykyisen ohjelman käyttöoikeuksia: valitse ohjelma ja sitten **Toiminto**-kohdasta **Myönnä vain lähtevien yhteyksien käyttöoikeudet** tai **Estä käyttöoikeudet**.

Myönnä täydet käyttöoikeudet äskettäisten tapahtumien lokista

Voit myöntää äskettäisten tapahtumien lokissa olevalle estetyille ohjelmalle täydelliset saapuvan ja lähtevän tietoliikenteen käyttöoikeudet.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Lisävalikko**.
- 2 Valitse **Raportit ja lokit**.
- 3 Valitse ensin tapahtuman kuvaus **Äskettäiset tapahtumat** -ikkunasta ja sitten **Myönnä käyttöoikeudet**.
- 4 Vahvista valintasi Ohjelmien käyttöoikeudet -valintaikkunassa valitsemalla **Kyllä**.

Liittyvät aiheet

- Tarkastele lähteviä tapahtumia (sivu 113)

Myönnä täydet käyttöoikeudet lähtevien tapahtumien lokista

Voit myöntää lähtevien tapahtumien lokissa olevalle estetyille ohjelmalle täydelliset saapuvan ja lähtevän tietoliikenteen käyttöoikeudet.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Lisävalikko**.
- 2 Valitse **Raportit ja lokit**.
- 3 Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
- 4 Valitse **Internet & verkko** ja valitse sitten **Lähtevät tapahtumat**.
- 5 Valitse ohjelma ja napsauta **Haluan**-kohdassa **Myönnä käyttöoikeudet**.
- 6 Vahvista valintasi Ohjelmien käyttöoikeudet -valintaikkunassa valitsemalla **Kyllä**.

Vain lähtevän tietoliikenteen käyttöoikeuksien myöntäminen

Jotkin tietokoneeseen asennetut ohjelmat vaativat lähteviä Internet-yhteyksiä. Firewallin avulla voit myöntää ohjelmille vain lähtevän tietoliikenteen käyttöoikeudet.

Myönnä ohjelmalle vain lähtevän tietoliikenteen käyttöoikeudet

Voit myöntää ohjelmalle vain lähtevän tietoliikenteen käyttöoikeudet.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet & verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Firewall-ikkunasta **Ohjelmien käyttöoikeudet**.
- 4 Valitse **Ohjelmien käyttöoikeudet** -kohdasta ohjelma, jonka asetuksena on **Estetty** tai **Täydet käyttöoikeudet**.
- 5 Valitse **Toiminto**-kohdasta **Myönnä vain lähtevien yhteyksien käyttöoikeudet**.
- 6 Valitse **OK**.

Myönnä vain lähtevän tietoliikenteen oikeudet äskettäisten tapahtumien lokista

Voit myöntää äskettäisten tapahtumien lokissa olevalle estetylle ohjelmalle vain lähtevän tietoliikenteen käyttöoikeudet.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Lisävalikko**.
- 2 Valitse **Raportit ja lokit**.
- 3 Valitse ensin tapahtuman kuvaus **Äskettäiset tapahtumat** -ikkunasta ja sitten **Myönnä vain lähtevien yhteyksien käyttöoikeudet**.
- 4 Vahvista valintasi Ohjelmien käyttöoikeudet -valintaikkunassa valitsemalla **Kyllä**.

Myönnä vain lähtevän tietoliikenteen käyttöoikeudet lähtevien tapahtumien lokista

Voit myöntää lähtevien tapahtumien lokissa olevalle estetyille ohjelmalle vain lähtevän tietoliikenteen käyttöoikeudet.

- 1** Valitse McAfee SecurityCenter -ikkunasta **Lisävalikko**.
- 2** Valitse **Raportit ja lokit**.
- 3** Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
- 4** Valitse **Internet & verkko** ja valitse sitten **Lähtevät tapahtumat**.
- 5** Valitse ohjelma ja **Haluan**-kohdasta **Myönnä vain lähtevien yhteyksien käyttöoikeudet**.
- 6** Vahvista valintasi Ohjelmien käyttöoikeudet -valintaikkunassa valitsemalla **Kyllä**.

Ohjelmien Internet-käyttöoikeuden estäminen

Firewall antaa sinulle mahdollisuuden estää ohjelmia käyttämästä Internetiä. Varmista, että ohjelman estäminen ei vaikuta häiritsevästi verkkoyhteyteen tai johonkin muuhun ohjelmaan, joka vaatii Internet-käyttöoikeutta toimiakseen kunnolla.

Estä ohjelman käyttöoikeudet

Voit estää ohjelman saapuvan ja lähtevän tietoliikenteen.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet & verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelyt -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Firewall-ikkunasta **Ohjelmien käyttöoikeudet**.
- 4 Valitse **Ohjelmien käyttöoikeudet** -kohdasta ohjelma, jonka asetuksena on **Täydet käyttöoikeudet** tai **Vain lähtevien yhteyksien käyttöoikeudet**.
- 5 Valitse **Toiminto**-kohdasta **Estä käyttöoikeudet**.
- 6 Valitse **OK**.

Estä uuden ohjelman käyttöoikeudet

Voit estää uuden ohjelman saapuvan ja lähtevän tietoliikenteen.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet & verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelyt -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Firewall-ikkunasta **Ohjelmien käyttöoikeudet**.
- 4 Valitse **Ohjelmien käyttöoikeudet** -kohdasta **Lisää estetty ohjelma**.
- 5 Hae ja valitse **Lisää ohjelma** -valintaikkunasta ohjelma, jonka haluat lisätä, ja valitse **Avaa**.

Huomautus: Voit muuttaa juuri lisätyn ohjelman käyttöoikeuksia valitsemalla ohjelman ja napsauttamalla **Toiminto**-kohdassa **Myönnä vain lähtevien yhteyksien käyttöoikeudet** tai **Myönnä käyttöoikeudet**.

Estä käyttöoikeudet äskettäisten tapahtumien lokista

Voit estää äskettäisten tapahtumien lokissa olevan ohjelman saapuvan ja lähtevän tietoliikenteen käyttöoikeudet.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Lisävalikko**.
- 2 Valitse **Raportit ja lokit**.
- 3 Valitse ensin tapahtuman kuvaus **Äskettäiset tapahtumat** -ikkunasta ja sitten **Estä käyttöoikeudet**.
- 4 Vahvista valintasi Ohjelmien käyttöoikeudet -valintaikkunassa valitsemalla **Kyllä**.

Ohjelmien käyttöoikeuksien poistaminen

Varmista ennen ohjelman käyttöoikeuksien poistamista, että tämä ei vaikuta tietokoneen toimintaan tai verkkoyhteyteen.

Poista ohjelman käyttöoikeudet

Voit poistaa ohjelman saapuvan ja lähtevän tietoliikenteen käyttöoikeudet.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet & verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelyt -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Firewall-ikkunasta **Ohjelmien käyttöoikeudet**.
- 4 Valitse **Ohjelmien käyttöoikeudet** -kohdasta ohjelma.
- 5 Valitse **Toiminto**-kohdasta **Poista ohjelman käyttöoikeudet**.
- 6 Valitse **OK**.

Huomautus: Firewall estää muuttamasta joitakin ohjelmia himmentämällä tai poistamalla käytöstä joitakin toimintoja.

Perehtyminen ohjelmiin

Jos et ole varma, mitä ohjelmien käyttöoikeuksia kannattaa käyttää, saat lisätietoja ohjelmasta McAfeen HackerWatch-sivustosta.

Hanki ohjelmatietoja

Saat ohjelmatietoja McAfeen HackerWatch-sivustosta, joiden avulla voit päättää, haluatko myöntää vai estää ohjelmien saapuvan ja lähtevän tietoliikenteen käyttöoikeudet.

Huomautus: Varmista, että olet muodostanut Internet-yhteyden ja että selain käynnistää McAfeen HackerWatch-sivuston. Siinä on ajan tasalla olevia tietoja ohjelmista, Internet-käytön vaatimuksista ja tietoturvaohjeista.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet & verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Firewall-ikkunasta **Ohjelmien käyttöoikeudet**.
- 4 Valitse **Ohjelmien käyttöoikeudet** -kohdasta ohjelma.
- 5 Valitse **Toiminto**-kohdasta **Lisätietoja**.

Hae ohjelmatietoja lähtevien tapahtumien lokista

Lähtevien tapahtumien lokista saat ohjelmatietoja McAfeen HackerWatch-sivustosta. Niiden avulla voit päättää, haluatko myöntää vai estää tiettyjen ohjelmien saapuvan ja lähtevän tietoliikenteen käyttöoikeudet.

Huomautus: Varmista, että olet muodostanut Internet-yhteyden ja että selain käynnistää McAfeen HackerWatch-sivuston. Siinä on ajan tasalla olevia tietoja ohjelmista, Internet-käytön vaatimuksista ja tietoturvaohjeista.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Lisävalikko**.
- 2 Valitse **Raportit ja lokit**.
- 3 Valitse Äskettäiset tapahtumat -kohdasta tapahtuma ja napsauta **Tarkastele lokia**.
- 4 Valitse **Internet & verkko** ja valitse sitten **Lähtevät tapahtumat**.
- 5 Valitse ensin IP-osoite ja sitten **Lisätietoja**.

LUKU 19

Järjestelmäpalveluiden hallinta

Toimiakseen kunnolla tiettyjen ohjelmien (muun muassa Web-palvelinten ja tiedostonjakelupalvelinten ohjelmien) täytyy hyväksyä pyytämättömiä yhteyksiä muista tietokoneista tähän tarkoitukseen varattujen järjestelmäpalveluporttien kautta. Tavallisesti Firewall sulkee nämä järjestelmäpalveluportit, sillä järjestelmän haavoittuvuus johtuu useimmiten juuri niistä. Etätietokoneyhteydet edellyttävät kuitenkin, että nämä järjestelmäpalveluportit ovat auki.

Tässä luvussa

Järjestelmäpalveluporttien asetusten määrittäminen
.....98

Järjestelmäpalveluporttien asetusten määrittäminen

Järjestelmäpalveluportit voidaan määrittää tietokoneen verkkopalvelun etäkäytön sallimiseksi tai estämiseksi.

Alla oleva luettelo sisältää yleisimmät järjestelmäpalvelut ja niiden portit:

- Tiedonsiirtoprotokolla (FTP), portit 20-21
- Postipalvelin (IMAP), portti 143
- Postipalvelin (POP3), portti 110
- Postipalvelin (SMTP), portti 25
- Microsoftin hakemistopalvelin (MSFT DS), portti 445
- Microsoftin SQL-palvelin (MSFT SQL), portti 1433
- Network Time Protocol, portti 123
- Etätyöpöytä / Etätuki / Päätepalvelin (RDP), portti 3389
- Etäproseduurikutsut (RPC), portti 135
- Suojattu Web-palvelin (HTTPS), portti 443
- Universal Plug and Play (UPNP), portti 5000
- Web-palvelin (HTTP), portti 80
- Windows File Sharing (NETBIOS), portit 137–139

Järjestelmäpalveluportit voidaan määrittää myös siten, että tietokone voi jakaa Internet-yhteytensä muiden samaan verkkoon liittyneiden tietokoneiden kanssa. Tämä Internet Connection Sharing (ICS) -yhteys antaa yhteyden jakavalle tietokoneelle mahdollisuuden toimia Internet-yhdyskätävänä, jota muut verkossa olevat tietokoneet voivat käyttää.

Huomautus: Jos tietokoneessa on sovellus, joka sallii sekä Web-että FTP-palvelinyhteydet, yhteyden jakavan tietokoneen on mahdollisesti avattava siihen liittyvä järjestelmäpalveluportti ja sallittava saapuvien yhteyksien siirtäminen kyseisiin portteihin.

Salli olemassa olevan järjestelmäpalveluportin käyttö

Voit avata tai sulkea olemassa olevan portin ja sallia tietokoneen verkkopalvelun etäkäytön.

Huomautus: Avattu järjestelmäpalveluportti voi saattaa tietokoneen alttiiksi Internetin tietoturvauhille, joten avaa portti vain silloin, kun se on välttämätöntä.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet & verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelyt -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Firewall-ikkunasta **Järjestelmäpalvelut**.
- 4 Valitse **Avaa järjestelmäpalveluportti** -kohdasta järjestelmäpalvelu portin avaamiseksi.
- 5 Valitse **OK**.

Estä olemassa olevan järjestelmäpalveluportin käyttö

Voit sulkea olemassa olevan portin ja estää tietokoneen verkkopalvelun etäkäytön.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet & verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelyt -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Firewall-ikkunasta **Järjestelmäpalvelut**.
- 4 Poista **Avaa järjestelmäpalveluportti** -kohdasta järjestelmäpalvelu portin sulkemiseksi.
- 5 Valitse **OK**.

Määritä uuden järjestelmäpalveluportin asetukset

Voit määrittää tietokoneeseen uuden verkkopalveluportin, jonka avaamalla tai sulkemalla voit puolestaan sallia tai estää tietokoneen verkkopalvelun etäkäytön.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet & verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelyt -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Firewall-ikkunasta **Järjestelmäpalvelut**.
- 4 Valitse **Lisää**.
- 5 Määritä Järjestelmäpalvelut -ikkunan **Portit ja järjestelmäpalvelut** -kohdassa seuraavat asetukset:
 - ohjelman nimi
 - saapuvan liikenteen TCP/IP-portit

- lähtevän liikenteen TCP/IP-portit
 - saapuvan liikenteen UDP-portit
 - lähtevän liikenteen UDP-portit.
- 6 Jos haluat lähettää portin toimintaa koskevat tiedot toiseen verkossa olevaan ja saman Internet-yhteyden jakavaan Windows-tietokoneeseen, valitse **Ohjaa tämän portin verkkoliikenne verkon käyttäjille, jotka käyttävät Internet-yhteyden jakamista**.
- 7 Voit vaihtoehtoisesti myös kuvailla uuden kokoonpanon.
- 8 Valitse **OK**.

Huomautus: Jos tietokoneessa on sovellus, joka sallii sekä Web-että FTP-palvelinyhteydet, yhteyden jakavan tietokoneen on mahdollisesti avattava siihen liittyvä järjestelmäpalveluportti ja sallittava saapuvien yhteyksien siirtäminen kyseisiin portteihin. Jos käytät Internet Connection Sharing (ICS) -yhteyttä, sinun on myös lisättävä luotettava tietokoneyhteys luotettavien IP-osoitteiden luetteloon. Lisätietoja on kohdassa Lisää luotettava tietokoneyhteys.

Muokkaa järjestelmäpalveluporttia

Voit muokata olemassa olevan järjestelmäpalveluportin saapuvan ja lähtevän tietoliikenteen tietoja.

Huomautus: Jos portin tiedot annetaan virheellisesti, järjestelmäpalvelu ei toimi.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet & verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Firewall-ikkunasta **Järjestelmäpalvelut**.
- 4 Valitse järjestelmäpalvelu ja sitten **Muokkaa**.
- 5 Määritä Järjestelmäpalvelut -ikkunan **Portit ja järjestelmäpalvelut** -kohdassa seuraavat asetukset:
 - ohjelman nimi
 - saapuvan liikenteen TCP/IP-portit
 - lähtevän liikenteen TCP/IP-portit
 - saapuvan liikenteen UDP-portit
 - lähtevän liikenteen UDP-portit.

- 6 Jos haluat lähettää portin toimintaa koskevat tiedot toiseen verkossa olevaan ja saman Internet-yhteyden jakavaan Windows-tietokoneeseen, valitse **Ohjaa tämän portin verkkoliikenne verkon käyttäjille, jotka käyttävät Internet-yhteyden jakamista**.
- 7 Voit vaihtoehtoisesti myös kuvailla muokatun kokoonpanon.
- 8 Valitse **OK**.

Poista järjestelmäpalveluportti

Voit poistaa olemassa olevan järjestelmäpalveluportin tietokoneesta. Poistamisen jälkeen etätietokoneet eivät enää voi käyttää verkkopalvelua tietokoneessa.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet & verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Firewall-ikkunasta **Järjestelmäpalvelut**.
- 4 Valitse ensin järjestelmäpalvelu ja sitten **Poista**.
- 5 Vahvista valintasi kehotettaessa valitsemalla **Kyllä**.

L U K U 2 0

Tietokoneyhteyksien hallinta

Voit määrittää Firewallin hallitsemaan tietokoneen etäyhteyksiä luomalla etätietokoneiden IP-osoitteisiin perustuvia sääntöjä. Tietokoneille, joiden IP-osoitteet ovat luotettavia, voidaan myöntää lupa muodostaa yhteys käyttäjän tietokoneeseen, kun taas tietokoneita, joiden IP-osoitteet ovat tuntemattomia, epäilyttäviä tai epäluotettavia, voidaan estää muodostamasta yhteys käyttäjän tietokoneeseen.

Varmista yhteyttä sallittaessa, että luotettava tietokone on turvallinen. Jos luotettavassa tietokoneessa on mato tai se on saanut muun tartunnan, tietokoneesi saattaa olla altis tartunnoille. Tämän lisäksi McAfee suosittelee, että suojaat myös luotettavat tietokoneet palomuurilla ja ajan tasalla olevalla virustorjuntaohjelmalla. Firewall ei kirjaa tietoliikennettä eikä tapahtumahälytyksiä luotettavien IP-osoitteiden luettelossa oleville IP-osoitteille.

Tuntemattomiin, epäilyttäviin tai epäluotettaviin IP-osoitteisiin yhteydessä olevia tietokoneita voidaan estää muodostamasta yhteyttä tietokoneeseesi.

Palomuuuri estää kaiken ei-toivotun liikenteen, joten IP-osoitteita ei tavallisesti tarvitse estää erikseen. IP-osoitteet on estettävä erikseen vain silloin, kun olet varma siitä, että tietty Internet-yhteys on vaarallinen. Varmista, että et estä tärkeitä IP-osoitteita, kuten DNS- tai DHCP-palvelinta, tai muita Internet-palveluntarjoajan palvelimia. Suojausasetusten mukaan Firewall voi hälyttää, kun se huomaa estetyn tietokoneen yrittävän muodostaa yhteyttä.

Tässä luvussa

Tietokoneyhteyksiin luottaminen.....	104
Tietokoneyhteyksien estäminen	107

Tietokoneyhteyksiin luottaminen

Voit lisätä, muokata ja poistaa luotettavia IP-osoitteita Luotettavat ja estetyt IP-osoitteet -ikkunan **Luotettavat IP-osoitteet** -kohdassa.

Luotettavat ja estetyt IP-osoitteet -ikkunan **Luotettavat IP-osoitteet** -luettelosta voit sallia kaiken tietoliikenteen määrättyä tietokoneelta omalle tietokoneellesi. Firewall ei kirjaa lokiin tietoliikennettä eikä luo tapahtumahälytyksiä IP-osoitteista, jotka ovat **Luotettavat IP-osoitteet** -luettelossa.

Firewall luottaa kaikkiin luettelossa oleviin IP-osoitteisiin ja päästää luotettavista IP-osoitteista peräisin olevan tietoliikenteen aina palomuurin läpi kaikkiin portteihin. Firewall ei suodata eikä analysoi luotettavaa IP-osoitetta käyttävän tietokoneen ja käyttäjän tietokoneen välisiä tapahtumia. Oletusarvoisesti Luotettavat IP-osoitteet -kohdassa annetaan ensimmäinen yksityinen verkko, jonka Firewall löytää.

Varmista yhteyttä sallittaessa, että luotettava tietokone on turvallinen. Jos luotettavassa tietokoneessa on mato tai se on saanut muun tartunnan, tietokoneesi saattaa olla altis tartunnoille. Tämän lisäksi McAfee suosittelee, että suojaat myös luotettavat tietokoneet palomuurilla ja ajan tasalla olevalla virustorjuntaohjelmalla.

Lisää luotettava tietokoneyhteys

Voit lisätä luotettavan tietokoneyhteyden ja siihen liittyvän IP-osoitteen.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet & verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Firewall-ikkunasta **Luotettavat ja estetyt IP-osoitteet**.
- 4 Valitse Luotettavat ja estetyt IP-osoitteet -ikkunasta **Luotettavat IP-osoitteet** ja valitse **Lisää**.
- 5 Toimi **Lisää IP-osoitteen luotettavuussääntö** -kohdassa seuraavasti:
 - Valitse **Yksittäinen IP-osoite** ja anna IP-osoite.
 - Valitse **IP-osoitealue** ja kirjoita aloitus- ja lopetusosoitteet **IP-osoitteesta**- ja **IP-osoitteeseen**-kenttiin.

- 6 Jos järjestelmäpalvelu käyttää Internet Connection Sharing (ICS) -yhteyttä, voit lisätä IP-osoitealueeksi 192.168.0.1 - 192.168.0.255.
- 7 Valitse vaihtoehtoisesti **Säännön voimassaoloaika päättyy** ja anna päivien määrä, jonka haluat säännön olevan voimassa.
- 8 Kirjoita vaihtoehtoisesti kuvaus säännöstä.
- 9 Valitse **OK**.
- 10 Vahvista valintasi **Luotettavat ja estetyt IP-osoitteet** -ikkunassa valitsemalla **Kyllä**.

Huomautus: Lisätietoja Internet Connection Sharing (ICS) -yhteydestä on kohdassa Määritä uusi järjestelmäpalvelu.

Lisää luotettava tietokone saapuvien tapahtumien lokista

Voit lisätä luotettavan tietokoneyhteyden ja siihen liittyvän IP-osoitteen saapuvien tapahtumien lokista.

- 1 Valitse McAfee SecurityCenter -ikkunan Yleiset tehtävät -kohdasta **Lisävalikko**.
- 2 Valitse **Raportit ja lokit**.
- 3 Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
- 4 Valitse **Internet & verkko** ja valitse sitten **Saapuvat tapahtumat**.
- 5 Valitse IP-lähdeosoite ja napsauta **Haluan**-kohdassa **Luota tähän osoitteeseen**.
- 6 Vahvista valintasi valitsemalla **Kyllä**.

Luotettavan tietokoneyhteyden muokkaaminen

Voit muokata luotettavaa tietokoneyhteyttä ja siihen liittyvää IP-osoitetta.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet & verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Firewall-ikkunasta **Luotettavat ja estetyt IP-osoitteet**.
- 4 Valitse Luotettavat ja estetyt IP-osoitteet -ikkunasta **Luotettavat IP-osoitteet**.
- 5 Valitse ensin IP-osoite ja sitten **Muokkaa**.
- 6 Toimi **Muokkaa luotettavaa IP-osoitetta** -kohdassa seuraavasti:
 - Valitse **Yksittäinen IP-osoite** ja anna IP-osoite.

- Valitse **IP-osoitealue** ja kirjoita aloitus- ja lopetusosoitteet **IP-osoitteesta-** ja **IP-osoitteeseen-**kenttiin.
- 7 Valitse vaihtoehtoisesti **Säännön voimassaoloaika päättyy** ja anna päivien määrä, jonka haluat säännön olevan voimassa.
- 8 Kirjoita vaihtoehtoisesti kuvaus säännöstä.
- 9 Valitse **OK**.

Huomautus: Et voi muokata oletusarvoisia tietokoneyhteyksiä, jotka Firewall on automaattisesti lisännyt luotettavasta yksityisverkosta.

Poista luotettava tietokoneyhteys

Voit poistaa luotettavan tietokoneyhteyden ja siihen liittyvän IP-osoitteen.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet & verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Firewall-ikkunasta **Luotettavat ja estetyt IP-osoitteet**.
- 4 Valitse Luotettavat ja estetyt IP-osoitteet -ikkunasta **Luotettavat IP-osoitteet**.
- 5 Valitse ensin IP-osoite ja sitten **Poista**.
- 6 Vahvista valintasi **Luotettavat ja estetyt IP-osoitteet** -ikkunassa valitsemalla **Kyllä**.

Tietokoneyhteyksien estäminen

Voit lisätä, muokata ja poistaa estettyjä IP-osoitteita Luotettavat ja estetyt IP-osoitteet -ikkunan **Estetyt IP-osoitteet** -kohdassa.

Tuntemattomiin, epäilyttäviin tai epäluotettaviin IP-osoitteisiin yhteydessä olevia tietokoneita voidaan estää muodostamasta yhteyttä tietokoneeseesi.

Palomuuuri estää kaiken ei-toivotun liikenteen, joten IP-osoitteita ei tavallisesti tarvitse estää erikseen. IP-osoitteet on estettävä erikseen vain silloin, kun olet varma siitä, että tietty Internet-yhteys on vaarallinen. Varmista, että et estä tärkeitä IP-osoitteita, kuten DNS- tai DHCP-palvelinta, tai muita Internet-palveluntarjoajan palvelimia. Suojausasetusten mukaan Firewall voi hälyttää, kun se huomaa estetyn tietokoneen yrittävän muodostaa yhteyttä.

Lisää estetty tietokoneyhteys

Voit lisätä estetyn tietokoneyhteyden ja siihen liittyvän IP-osoitteen.

Huomautus: Varmista, että et estä tärkeitä IP-osoitteita, kuten DNS- tai DHCP-palvelinta, tai muita Internet-palveluntarjoajan palvelimia.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet & verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Firewall-ikkunasta **Luotettavat ja estetyt IP-osoitteet**.
- 4 Valitse Luotettavat ja estetyt IP-osoitteet -ikkunasta **Estetyt IP-osoitteet** ja valitse **Lisää**.
- 5 Toimi **Lisää IP-osoitteen estosääntö** -kohdassa seuraavasti:
 - Valitse **Yksittäinen IP-osoite** ja anna IP-osoite.
 - Valitse **IP-osoitealue** ja kirjoita aloitus- ja lopetusosoitteet **IP-osoitteesta**- ja **IP-osoitteeseen**-kenttiin.
- 6 Valitse vaihtoehtoisesti **Säännön voimassaoloaika päättyy** ja anna päivien määrä, jonka haluat säännön olevan voimassa.
- 7 Kirjoita vaihtoehtoisesti kuvaus säännöstä.
- 8 Valitse **OK**.
- 9 Vahvista valintasi **Luotettavat ja estetyt IP-osoitteet** -ikkunassa valitsemalla **Kyllä**.

Muokkaa estettyä tietokoneyhteyttä

Voit muokata estettyä tietokoneyhteyttä ja siihen liittyvää IP-osoitetta.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet & verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Firewall-ikkunasta **Luotettavat ja estetyt IP-osoitteet**.
- 4 Valitse Luotettavat ja estetyt IP-osoitteet -ikkunasta **Estetyt IP-osoitteet** ja valitse **Muokkaa**.
- 5 Toimi **Muokkaa estettyä IP-osoitetta** -kohdassa seuraavasti:
 - Valitse **Yksittäinen IP-osoite** ja anna IP-osoite.
 - Valitse **IP-osoitealue** ja kirjoita aloitus- ja lopetusosoitteet **IP-osoitteesta**- ja **IP-osoitteeseen**-kenttiin.
- 6 Valitse vaihtoehtoisesti **Säännön voimassaoloaika päättyy** ja anna päivien määrä, jonka haluat säännön olevan voimassa.
- 7 Kirjoita vaihtoehtoisesti kuvaus säännöstä.
- 8 Valitse **OK**.

Poista estetty tietokoneyhteys

Voit poistaa estetyn tietokoneyhteyden ja siihen liittyvän IP-osoitteen.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet & verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Firewall-ikkunasta **Luotettavat ja estetyt IP-osoitteet**.
- 4 Valitse Luotettavat ja estetyt IP-osoitteet -ikkunasta **Estetyt IP-osoitteet**.
- 5 Valitse ensin IP-osoite ja sitten **Poista**.
- 6 Vahvista valintasi **Luotettavat ja estetyt IP-osoitteet** -ikkunassa valitsemalla **Kyllä**.

Estä tietokone saapuvien tapahtumien lokista

Voit estää tietokoneyhteyden ja siihen liittyvän IP-osoitteen saapuvien tapahtumien lokista.

Saapuvien tapahtumien lokissa olevat IP-osoitteet estetään. Osoitteen estäminen ei siten lisää tietoturvaa, paitsi jos tietokone käyttää tarkoituksella avattuja portteja tai jos siinä on ohjelma, jolle on myönnetty oikeudet Internetin käyttöön.

Lisää IP-osoite **Estetyt IP-osoitteet** -luetteloon vain silloin, jos olet tarkoituksella avannut yhden tai useamman portin ja jos uskot, että kyseistä osoitetta on estettävä käyttämästä avattuja portteja.

Voit käyttää kaiken saapuvan Internet-tietoliikenteen IP-osoitteet sisältävää saapuvien tapahtumien sivua sellaisten IP-osoitteiden estämiseen, joiden uskot olevan epäilyttävien tai ei-toivottujen Internet-tapahtumien taustalla.

- 1 Valitse McAfee SecurityCenter -ikkunan **Yleiset tehtävät** -kohdasta **Lisävalikko**.
- 2 Valitse **Raportit ja lokit**.
- 3 Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
- 4 Valitse **Internet & verkko** ja valitse sitten **Saapuvat tapahtumat**.
- 5 Valitse IP-lähdeosoite ja napsauta **Haluan**-kohdassa **Estä tämä osoite**.
- 6 Vahvista valintasi valitsemalla **Lisää IP-osoitteen estosääntö** -valintaikkunassa **Kyllä**.

Estä tietokone tietomurtojen havainnoinnin tapahtumien lokista

Voit estää tietokoneyhteyden ja siihen liittyvän IP-osoitteen tietomurtojen havainnoinnin tapahtumien lokista.

- 1 Valitse McAfee SecurityCenter -ikkunan **Yleiset tehtävät** -kohdasta **Lisävalikko**.
- 2 Valitse **Raportit ja lokit**.
- 3 Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
- 4 Valitse ensin **Internet ja verkko** ja sitten **Tietomurtojen havainnoinnin tapahtumat**.
- 5 Valitse IP-lähdeosoite ja napsauta **Haluan**-kohdassa **Estä tämä osoite**.
- 6 Vahvista valintasi valitsemalla **Lisää IP-osoitteen estosääntö** -valintaikkunassa **Kyllä**.

LUKU 21

Kirjaus, valvonta ja analyysi

Firewall tarjoaa monipuolisia ja helppolukuisia menetelmiä Internet-tapahtumien ja tietoliikenteen kirjaukseen, valvontaan ja analysointiin. Internet-tietoliikenteen ja tapahtumien ymmärtäminen helpottaa Internet-yhteyksien hallintaa.

Tässä luvussa

Tapahtumien kirjaus.....	112
Tilastotietojen käsitteleminen	114
Internet-tietoliikenteen jäljittäminen	115
Internet-tietoliikenteen valvonta.....	118

Tapahtumien kirjaus

Firewallin avulla voit ottaa tapahtumien kirjauksen käyttöön tai poistaa sen käytöstä, ja jos olet ottanut sen käyttöön, voit valita, minkä tyyppisiä tapahtumia haluat kirjattavan. Tapahtumien kirjauksen avulla voit tarkastella äskettäisiä saapuvia ja lähteviä tapahtumia sekä tietomurtotapahtumia.

Määritä tapahtumalokin asetukset

Voit valita ja määrittää tapahtumatyypit, jotka Firewall kirjaa lokitiedostoon. Oletusarvoisesti tapahtumien kirjaus otetaan käyttöön kaikkien tapahtumien ja toimintojen kanssa.

- 1 Valitse Internet- ja verkkomäärittelykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 2 Valitse Firewall-ikkunasta **Tapahtumalokin asetukset**.
- 3 Jos tapahtumien kirjaus ei vielä ole käytössä, valitse **Ota tapahtumien kirjaus käyttöön**.
- 4 Valitse **Ota tapahtumien kirjaus käyttöön** -kohdasta tapahtumatyypit, jotka haluat kirjattavan, tai poista niiden valinnat. Tapahtumatyyppejä ovat muun muassa seuraavat:
 - estetyt ohjelmat
 - ICMP ping -pyynnöt
 - estetyistä IP-osoitteista saapuva liikenne
 - järjestelmäpalveluporttien tapahtumat
 - tuntemattomien porttien tapahtumat
 - tietomurtojen havainnointitapahtumat (IDS).
- 5 Jos haluat estää tiettyjen porttien kirjaamisen, valitse **Älä kirjaa tapahtumia seuraavista porteista** ja anna yksittäisten porttien numerot pilkuilla erotettuina tai porttialueet väliviivoilla yhdistettyinä, esimerkiksi 137-139, 445, 400-5000.
- 6 Valitse **OK**.

Tarkastele äskettäisiä tapahtumia

Jos kirjaus on otettu käyttöön, voit tarkastella äskettäisiä tapahtumia. Äskettäiset tapahtumat -ikkunassa näkyy tapahtuman päivämäärä ja kuvaus. Siinä näytetään vain niitä ohjelmia koskevat tapahtumat, jotka on estetty käyttämästä Internetiä.

- Valitse Yleiset tehtävät -ikkunan **Lisävalikko**-kohdasta **Raportit ja lokit** tai **Tarkastele äskettäisiä tapahtumia**. **Tarkastele äskettäisiä tapahtumia** -asetuksen voit vaihtoehtoisesti valita myös Perusvalikon Yleiset tehtävät -kohdasta.

Tarkastele saapuvia tapahtumia

Jos kirjaus on otettu käyttöön, voit tarkastella saapuvia tapahtumia. Saapuviin tapahtumiin kuuluvat muun muassa päivämäärä ja kellonaika, IP-lähdeosoite, isännän nimi, tiedot ja tapahtuman tyyppi.

- 1 Varmista, että Lisävalikko on otettu käyttöön. Valitse Yleiset tehtävät -ikkunasta **Raportit & Lokit**.
- 2 Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
- 3 Valitse **Internet & verkko** ja valitse sitten **Saapuvat tapahtumat**.

Huomautus: Saapuvien tapahtumien lokissa voit estää ja jäljittää IP-osoitteen sekä valita IP-osoitteen luotetuksi.

Tarkastele lähteviä tapahtumia

Jos kirjaus on otettu käyttöön, voit tarkastella lähteviä tapahtumia. Lähteviin tapahtumiin kuuluvat muun muassa lähtevän yhteyden muodostamista yrittävän ohjelman nimi, tapahtuman päivämäärä ja aika sekä ohjelman sijainti tietokoneessa.

- 1 Valitse Yleiset tehtävät -ikkunasta **Raportit & Lokit**.
- 2 Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
- 3 Valitse **Internet & verkko** ja valitse sitten **Lähtevät tapahtumat**.

Huomautus: Voit myöntää ohjelmalle täydet tai vain lähtevän tietoliikenteen käyttöoikeudet lähtevien tapahtumien lokista. Voit myös etsiä muita tietoja ohjelmasta.

Tarkastele tietomurtojen havainnoinnin tapahtumia

Jos kirjaus on otettu käyttöön, voit tarkastella saapuvia tietomurtotapahtumia. Tietomurtojen havainnoinnin tapahtumat näyttävät päivämäärän ja ajan, IP-lähdeosoitteen, tapahtuman isännän nimen ja tapahtuman tyyppin.

- 1 Valitse Yleiset tehtävät -ikkunasta **Raportit & Lokit**.
- 2 Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
- 3 Valitse ensin **Internet ja verkko** ja sitten **Tietomurtojen havainnoinnin tapahtumat**.

Huomautus: Tietomurtojen havainnoinnin tapahtumien lokissa voit estää ja jäljittää IP-osoitteen.

Tilastotietojen käsitleminen

Firewall hyödyntää McAfeen HackerWatch-tietoturvasivustoa ja tarjoaa tilastotietoja maailman Internet-tietoturva- ja -porttitapahtumista.

Tarkastele maailman tietoturvatapahtumien tilastotietoja

HackerWatch seuraa Internet-tietoturvatapahtumia maailmanlaajuisesti, ja voit tarkastella niitä SecurityCenterissä. Seurantatiedoissa ovat mukana tapahtumat, joista on ilmoitettu HackerWatchille viimeisen 24 tunnin, 7 päivän ja 30 päivän aikana.

- 1 Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
- 2 Valitse Työkalut-ikkunasta **HackerWatch**.
- 3 Tarkastele tietoturvatapahtumien tilastotietoja Tapahtumien seuranta -kohdassa.

Tarkastele maailman Internet-porttitapahtumia

HackerWatch seuraa Internet-tietoturvatapahtumia maailmanlaajuisesti, ja voit tarkastella niitä SecurityCenterissä. Siellä näytetään tietoja muun muassa tärkeimpien tapahtumien porteista, jotka on ilmoitettu HackerWatchille viimeisen seitsemän päivän aikana. Tavallisesti tietoja näytetään HTTP-, TCP- ja UDP-porteista.

- 1 Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
- 2 Valitse Työkalut-ikkunasta **HackerWatch**.
- 3 Tarkastele tärkeimpien tapahtumien porttitapahtumia **Äskettäiset porttitapahtumat** -kohdassa.

Internet-tietoliikenteen jäljittäminen

Firewall tarjoaa useita vaihtoehtoja Internet-tietoliikenteen jäljittämiseen. Näiden vaihtoehtojen avulla voit jäljittää verkkotietokoneen maantieteellisesti, hankkia toimialueeseen ja verkkoon liittyviä tietoja sekä jäljittää tietokoneita saapuvien tapahtumien ja tietomurtojen havainnoinnin tapahtumien lokeista.

Jäljitä verkkotietokone maantieteellisesti

Visuaalisen jäljityksen avulla voit etsiä tietokoneen, joka on muodostamassa tai yrittää muodostaa yhteyden tietokoneeseesi. Maantieteelliseen etsimiseen käytetään tietokoneen nimeä tai IP-osoitetta. Visuaalinen jäljitys mahdollistaa myös verkon ja rekisteröintitietojen käytön. Visuaalista jäljitystä käyttämällä saat näkyviin maailmankartan, joka näyttää tiedonsiirron todennäköisimmän reitin lähdetietokoneen ja sinun tietokoneesi välillä.

- 1 Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
- 2 Valitse Työkalut-ikkunasta **Visuaalinen jäljitys**.
- 3 Kirjoita tietokoneen IP-osoite ja valitse **Jäljitä**.
- 4 Valitse **Visuaalinen jäljitys** -kohdasta **Karttanäkymä**.

Huomautus: Silmukkaa käyttäviä, yksityisiä tai virheellisiä IP-osoitteita sisältäviä tapahtumia ei voi jäljittää.

Hanki tietokoneen rekisteröintitiedot

Voit hankkia tietokoneen rekisteröintitiedot SecurityCenteristä visuaalisen jäljityksen avulla. Tiedot sisältävät toimialueen nimen, rekisteröijän nimen ja osoitteen sekä hallinnoinnista vastaavan yhteyshenkilön tiedot.

- 1 Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
- 2 Valitse Työkalut-ikkunasta **Visuaalinen jäljitys**.
- 3 Kirjoita tietokoneen IP-osoite ja valitse **Jäljitä**.
- 4 Valitse **Visuaalinen jäljitys** -kohdasta **Rekisteröijänäkymä**.

Hanki tietokoneen verkkotiedot

Voit hankkia tietokoneen verkkotiedot SecurityCenteristä visuaalisen jäljityksen avulla. Verkkotiedot sisältävät yksityiskohtaisia tietoja verkosta, jossa toimialue sijaitsee.

- 1 Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
- 2 Valitse Työkalut-ikkunasta **Visuaalinen jäljitys**.
- 3 Kirjoita tietokoneen IP-osoite ja valitse **Jäljitä**.
- 4 Valitse **Visuaalinen jäljitys** -kohdasta **Verkkonäkymä**.

Jäljitä tietokone saapuvien tapahtumien lokista

Saapuvat tapahtumat -ikkunassa voit jäljittää IP-osoitteen, joka on saapuvien tapahtumien lokissa.

- 1 Varmista, että Lisävalikko on otettu käyttöön. Valitse Yleiset tehtävät -ikkunasta **Raportit & Lokit**.
- 2 Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
- 3 Valitse **Internet & verkko** ja valitse sitten **Saapuvat tapahtumat**.
- 4 Valitse ensin Saapuvat tapahtumat -ikkunasta IP-lähdeosoite ja sitten **Jäljitä tämä osoite**.
- 5 Valitse Visuaalinen jäljitys -ikkunassa yksi seuraavista:
 - **Karttanäkymä:** Etsi tietokone maantieteellisesti valitun IP-osoitteen perusteella.
 - **Rekisteröijänäkymä:** Etsi toimialuetiedot valitun IP-osoitteen perusteella.
 - **Verkkonäkymä:** Etsi verkkotiedot valitun IP-osoitteen perusteella.
- 6 Valitse **Valmis**.

Jäljitä tietokone tietomurtojen havainnoinnin tapahtumien lokista

Tietomurtojen havainnoinnin tapahtumat -ikkunassa voit jäljittää IP-osoitteen, joka on tietomurtojen havainnoinnin tapahtumien lokissa.

- 1 Valitse Yleiset tehtävät -ikkunasta **Raportit & Lokit**.
- 2 Valitse **Äskettäiset tapahtumat** -kohdasta **Tarkastele lokia**.
- 3 Valitse ensin **Internet ja verkko** ja sitten **Tietomurtojen havainnoinnin tapahtumat**. Valitse ensin Tietomurtojen havainnoinnin tapahtumat -ikkunasta IP-lähdeosoite ja sitten **Jäljitä tämä osoite**.
- 4 Valitse Visuaalinen jäljitys -ikkunassa yksi seuraavista:
 - **Karttanäkymä:** Etsi tietokone maantieteellisesti valitun IP-osoitteen perusteella.
 - **Rekisteröijänäkymä:** Etsi toimialuetiedot valitun IP-osoitteen perusteella.
 - **Verkkonäkymä:** Etsi verkkotiedot valitun IP-osoitteen perusteella.
- 5 Valitse **Valmis**.

Jäljitä valvottu IP-osoite

Jäljittämällä valvotun IP-osoitteen voit luoda maantieteellisen yleiskatsauksen, joka näyttää tiedonsiirron todennäköisimmän reitin lähdetietokoneen ja oman tietokoneesi välillä. Lisäksi voit hankkia IP-osoitteen rekisteröinti- ja verkkotiedot.

- 1 Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
- 2 Valitse Työkalut-ikkunasta **Tietoliikenteen valvonta**.
- 3 Valitse **Tietoliikenteen valvonta** -kohdasta **Aktiiviset ohjelmat**.
- 4 Valitse ohjelma ja sen jälkeen ohjelman nimen alla oleva IP-osoite.
- 5 Valitse **Ohjelmien tapahtumat** -kohdasta **Jäljitä tämä IP-osoite**.
- 6 **Visuaalinen jäljitys** -kohdassa voit tarkastella maailmankarttaa, joka näyttää tiedonsiirron todennäköisimmän reitin lähdetietokoneen ja oman tietokoneesi välillä. Lisäksi voit hankkia IP-osoitteen rekisteröinti- ja verkkotiedot.

Huomautus: Jos haluat tarkastella uusimpia tilastotietoja, valitse **Visuaalinen jäljitys** -kohdasta **Päivitä**.

Internet-tietoliikenteen valvonta

Palomuuuri tarjoaa useita tapoja Internet-tietoliikenteen valvontaan, muun muassa seuraavat:

- **Tietoliikenneanalyysin kaaviot:** Kuvaavat viimeisintä saapuvaa ja lähtevää Internet-tietoliikennettä.
- **Tietoliikenteen käytön kaaviot:** Näyttävät prosentteina, kuinka suuren osan kaistanleveydestä aktiivisimmat ohjelmat ovat käyttäneet viimeisen 24 tunnin aikana.
- **Aktiiviset ohjelmat:** Näyttää tietokoneen tällä hetkellä eniten verkkoyhteyksiä käyttävät ohjelmat ja niiden käyttämät IP-osoitteet.

Tietoja tietoliikenneanalyysin kaaviosta

Tietoliikenneanalyysin kaavio esittää saapuvan ja lähtevän Internet-tietoliikenteen numeerisessa ja graafisessa muodossa. Lisäksi Tietoliikenteen valvonta näyttää tietokoneen eniten verkkoyhteyksiä käyttävät ohjelmat ja niiden käyttämät IP-osoitteet.

Tietoliikenneanalyysi-ikkunassa voit tarkastella äskettäistä saapuvaa ja lähtevää Internet-tietoliikennettä sekä tiedonsiirron nykyistä, keskimääräistä ja suurinta mahdollista nopeutta. Voit tarkastella myös tietoliikenteen määrää, esimerkiksi Firewallin käynnistämisen jälkeistä tietoliikenteen määrää sekä tietoliikenteen kokonaismäärää kuluva kuukauden ja edellisten kuukausien aikana.

Tietoliikenneanalyysi-ikkuna näyttää tietokoneen reaaliaikaiset Internet-tapahtumat, kuten äskettäisen saapuvan ja lähtevän Internet-tietoliikenteen määrän ja tiedonsiirtonopeuden, yhteysnopeuden sekä Internetin kautta siirrettyjen tavujen yhteismäärän.

Yhtenäinen vihreä viiva osoittaa saapuvan liikenteen nykyisen tiedonsiirtonopeuden. Vihreä pisteviiva osoittaa saapuvan liikenteen keskimääräisen tiedonsiirtonopeuden. Jos nykyinen ja keskimääräinen tiedonsiirtonopeus ovat samat, kaaviossa ei ole pisteviivaa. Yhtenäinen viiva osoittaa sekä keskimääräisen että nykyisen tiedonsiirtonopeuden.

Yhtenäinen punainen viiva osoittaa lähtevän liikenteen nykyisen tiedonsiirtonopeuden. Punainen pisteviiva osoittaa lähtevän liikenteen keskimääräisen tiedonsiirtonopeuden. Jos nykyinen ja keskimääräinen tiedonsiirtonopeus ovat samat, kaaviossa ei ole pisteviivaa. Yhtenäinen viiva osoittaa sekä keskimääräisen että nykyisen tiedonsiirtonopeuden.

Analysoi saapuvaa ja lähtevää tietoliikennettä

Tietoliikenneanalyysin kaavio esittää saapuvan ja lähtevän Internet-tietoliikenteen numeerisessa ja graafisessa muodossa. Lisäksi Tietoliikenteen valvonta näyttää tietokoneen eniten verkkoyhteyksiä käyttävät ohjelmat ja niiden käyttämät IP-osoitteet.

- 1 Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
- 2 Valitse Työkalut-ikkunasta **Tietoliikenteen valvonta**.
- 3 Valitse **Tietoliikenteen valvonta** -kohdasta **Tietoliikenneanalyysi**.

Vihje: Jos haluat tarkastella uusimpia tilastotietoja, valitse **Tietoliikenneanalyysi**-kohdasta **Päivitä**.

Valvo ohjelman kaistanleveyttä

Voit tarkastella ympyräkaaviota, joka näyttää prosentteina, kuinka suuren osan kaistanleveydestä aktiivisimmat ohjelmat ovat käyttäneet viimeisen 24 tunnin aikana. Ympyräkaavio esittää visuaalisesti kunkin ohjelman käyttämän kaistanleveyden suhteellisen määrän.

- 1 Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
- 2 Valitse Työkalut-ikkunasta **Tietoliikenteen valvonta**.
- 3 Valitse **Tietoliikenteen valvonta** -kohdasta **Tietoliikenteen käyttö**.

Vihje: Jos haluat tarkastella uusimpia tilastotietoja, valitse **Tietoliikenteen käyttö** -kohdasta **Päivitä**.

Valvo ohjelmatapahtumia

Voit tarkastella saapuvia ja lähteviä ohjelmatapahtumia, kuten etätietokoneiden yhteyksiä ja portteja.

- 1 Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
- 2 Valitse Työkalut-ikkunasta **Tietoliikenteen valvonta**.
- 3 Valitse **Tietoliikenteen valvonta** -kohdasta **Aktiiviset ohjelmat**.
- 4 Voit tarkastella seuraavia tietoja:
 - Ohjelmatapahtumien kaavio: Valitse ohjelma, jonka tapahtumien kaaviota haluat tarkastella.
 - Kuunteluyhteys: Valitse kuunneltava kohde ohjelman nimen alta.
 - Tietokoneyhteys: Valitse IP-osoite ohjelman nimen, järjestelmäprosessin tai palvelun alta.

Huomautus: Jos haluat tarkastella uusimpia tilastotietoja, valitse **Aktiiviset ohjelmat** -kohdasta **Päivitä**.

LUKU 22

Perehtyminen Internet-tietoturvaan

Firewall hyödyntää McAfeen HackerWatch-tietoturvasivustoa ja tarjoaa ajan tasalla olevia tietoja ohjelmista ja maailman Internet-tapahtumista. Firewallista löydät myös HTML-muotoisen HackerWatch-opetusohjelman.

Tässä luvussa

Käynnistä HackerWatch-opetusohjelma 122

Käynnistä HackerWatch-opetusohjelma

Lisätietoja Firewallista saat SecurityCenterissä olevasta HackerWatch-opetusohjelmasta.

- 1 Varmista, että Lisävalikko on käytössä, ja valitse **Työkalut**.
- 2 Valitse Työkalut-ikkunasta **HackerWatch**.
- 3 Valitse **HackerWatch-resurssit**-kohdasta **Katso opetusohjelma**.

L U K U 23

McAfee Anti-Spam

Anti-Spam (aikaisemmalta nimeltään SpamKiller) estää ei-toivottujen sähköpostiviestien toimittamisen Saapuvat-kansioon tarkistamalla saapuvat sähköpostiviestit ja merkitsemällä ne roskapostiksi (sähköpostiviestit, jotka houkuttelevat sinua tekemään ostoksia) tai phishing-huijausviesteiksi (sähköpostiviestit, jotka houkuttelevat sinua antamaan henkilökohtaiset tietosi tunnetun tai mahdollisesti petollisen Web-sivuston käyttöön). Tämän jälkeen Anti-Spam suodattaa roskapostiviestit ja siirtää ne McAfee Anti-Spam -kansioon.

Jos ystäväsi lähettävät sinulle joskus roskapostilta näyttäviä asiallisia viestejä, voit estää niiden suodattamisen lisäämällä ystäväsi sähköpostiosoitteen Anti-Spamin ystäväluetteloon. Voit myös mukauttaa roskapostiviestien tunnistustapaa. Voit esimerkiksi suodattaa viestejä aggressiivisesti, määrittää viestistä haettavat asiat ja luoda omat suodattimesi.

Anti-Spam suojaa sinua myös silloin, jos yrität avata mahdollisesti petollisen Web-sivuston napsauttamalla sähköpostiviestissä olevaa linkkiä. Jos napsautat mahdollisesti petollisen Web-sivuston linkkiä, sinut uudelleenohjataan phishing-huijauksen suodatussivulle. Jos et halua suodattaa kaikkia Web-sivustoja, voit lisätä ne valkoiseen listaan (tässä listassa olevia Web-sivustoja ei suodateta).

Anti-Spam toimii useimpien sähköpostiohjelmien, kuten POP3-, POP3-Web-sähköposti-, Yahoo®-, MSN®/Hotmail®, Windows® Live™ Mail- ja MAPI (Microsoft Exchange Server) -tilien kanssa. Jos luet sähköpostiasi selaimen avulla, sinun on lisättävä Web-sähköpostitilisi Anti-Spamiin. Kaikki muut tilit määritetään automaattisesti, eikä sinun tarvitse lisätä niitä Anti-Spamiin.

Huomautus: SecurityCenter raportoi kriittiset ja ei-kriittiset suojausongelmat heti, kun se havaitsee ne. Jos tarvitset apua suojausongelmien selvittämisessä, voit käyttää McAfee Virtual Technician -palvelua.

Tässä luvussa

Anti-Spamin ominaisuudet	125
Web-sähköpostitilien määrittäminen	127
Ystävien määrittäminen	131
Roskapostiviestien tunnistustavan määrittäminen..	137
Sähköpostin suodatus.....	145
Suodatettujen sähköpostiviestien käsitteleminen....	149
Phishing-huijausten torjunnan asetusten määrittäminen	151

Anti-Spamin ominaisuudet

Anti-Spam tarjoaa seuraavat ominaisuudet.

Roskapostin suodatus

Anti-Spamin kehittyneet suodattimet estävät ei-toivottujen sähköpostiviestien toimittamisen Saapuvat-kansioon, ja ne päivitetään automaattisesti kaikkia sähköpostitilejäsi varten. Voit luoda myös mukautettuja suodattimia varmistaaksesi, että kaikki roskapostiviestit suodatetaan, ja lähettää roskapostiviestit McAfeeelle analysointia varten.

Phishing-suodatus

Phishing-huijaussuodattimen avulla voit tunnistaa mahdollisesti petolliset phishing-sivustot, joissa kerätään henkilökohtaisia tietoja.

Roskapostiviestien mukautettu käsittely

Merkitse ei-toivotut sähköpostiviestit roskapostiksi ja siirrä ne McAfee Anti-Spam -kansioon tai merkitse asialliset sähköpostiviestit ei-roskapostiksi ja siirrä ne Saapuneet-kansioon.

Ystävät

Tuo ystäväsi sähköpostiositteet ystäväluetteloon, jotta heidän lähettämiään sähköpostiviestejä ei suodateta.

Lajittele luettelokohteet tarkkuuden mukaan

Voit lajitella henkilökohtaiset suodattimet, ystävät, osoitekirjat ja Web-sähköpostitilit tarkkuuden mukaan (napsauta haluamasi sarakkeen nimeä).

Lisätuki

Anti-Spam tukee Mozilla® Thunderbird™ -sähköpostiohjelman versioiden 1.5 ja 2.0 käyttöä, ja siinä on Windows Vistan™ 64-bittinen tuki Windows Mailia varten. Uusi pelitilatoiminto tukee lisäksi Anti-Spamin taustaprosesseja, minkä ansiosta tietokoneesi ei hidastu, kun pelaat videopelejä tai katselet DVD-elokuvia. Anti-Spam suodattaa Microsoft® Outlook®-, Outlook Express- tai Windows Mail -tilit mitä tahansa porttia, myös SSL (Secure Socket Layer) -portteja käytettäessä.

LUKU 24

Web-sähköpostitilien määrittäminen

Jos luet sähköpostiasi selaimen avulla, sinun on määritettävä Anti-Spam muodostamaan yhteys tiliisi ja suodattamaan viestisi. Voit lisätä Web-sähköpostitilisi Anti-Spamiin lisäämällä siihen sähköpostipalvelun tarjoajalta saamasi tilin tiedot.

Kun olet lisännyt Web-sähköpostitilin, voit muokata tilisi tietoja ja perehtyä tarkemmin suodatettuun Web-sähköpostiin. Jos et enää käytä Web-sähköpostitiliä tai et halua suodattaa sitä, voit poistaa sen.

Anti-Spam toimii useimpien sähköpostiohjelmien, kuten POP3-, POP3-Web-sähköposti-, Yahoo®-, MSN/Hotmail-, Windows Live Mail- ja MAPI-tilien kanssa. POP3 on tavanomaisin tilityyppi, ja se on Internet-sähköpostistandardi. Kun sinulla on POP3-tili, Anti-Spam muodostaa yhteyden suoraan sähköpostipalvelimeen ja suodattaa viestit, ennen kuin sähköpostiohjelmasi ehtii vastaanottaa ne. POP3-Web-sähköposti-, Yahoo-, MSN/Hotmail- ja Windows Mail -tilit ovat Web-pohjaisia. POP3-Web-sähköpostitilien suodattaminen suoritetaan samalla tavoin kuin POP3-tilien suodattaminen. MAPI on Microsoftin suunnittelema järjestelmä, joka tukee monentyyppistä viestintää, kuten sähköpostin käyttöä, faksaamista ja Exchange-palvelinten välityksellä tapahtuvaa viestintää. Tällä hetkellä vain Microsoft Outlook on suoraan yhteensopiva MAPI-tilien kanssa.

Huomautus: Vaikka Anti-Spam pystyy avaamaan MAPI-tilit, se ei suodata sähköpostiviestejä, ennen kuin olet hakenut viestit Microsoft Outlookilla.

Tässä luvussa

Lisää Web-sähköpostitili	127
Muokkaa Web-sähköpostitiliä	128
Poista Web-sähköpostitili.....	129
Web-sähköpostitilin tietojen ymmärtäminen	129

Lisää Web-sähköpostitili

Lisää POP3- (esimerkiksi Yahoo), MSN/Hotmail- tai Windows Mail -Web-sähköpostitili (täydellinen tuki saatavana vain maksullisille versioille), jos haluat suodattaa kyseisellä tilillä olevat viestit roskapostin varalta.

1 Avaa Roskapostin torjunta -ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
2. Valitse Sähköposti ja pikaviesti -tietoaalueelta **Määritä**.
3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.
- 2 Valitse Roskapostin torjunta -ikkunasta **Web-sähköpostitilit**.
- 3 Valitse Web-sähköpostitilit -ikkunasta **Lisää**.
- 4 Määritä tilin tiedot (sivu 129) ja valitse **Seuraava**.
- 5 Määritä **Tarkistusasetukset**-kohdassa, milloin haluat Anti-Spamin tarkistavan tilisi roskapostin varalta (sivu 129).
- 6 Jos käytät puhelinverkkoyhteyttä, määritä, miten Anti-Spam muodostaa yhteyden Internetiin (sivu 129).
- 7 Valitse **Lopeta**.

Muokkaa Web-sähköpostitiliä

Sinun on muokattava Web-sähköpostitiliä, kun tilin tiedoissa tapahtuu muutoksia. Muokkaa Web-sähköpostitiliäsi esimerkiksi silloin, kun muutat salasanaasi tai haluat Anti-Spamin etsivän roskapostia useammin.

- 1 Avaa Roskapostin torjunta -ikkuna.
Miten?
 1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
 2. Valitse Sähköposti ja pikaviesti -tietoaalueelta **Määritä**.
 3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.
- 2 Valitse Roskapostin torjunta -ikkunasta **Web-sähköpostitilit**.
- 3 Valitse tili, jota haluat muokata, ja valitse sitten **Muokkaa**.
- 4 Määritä tilin tiedot (sivu 129) ja valitse **Seuraava**.
- 5 Määritä **Tarkistusasetukset**-kohdassa, milloin haluat Anti-Spamin tarkistavan tilisi roskapostin varalta (sivu 129).
- 6 Jos käytät puhelinverkkoyhteyttä, määritä, miten Anti-Spam muodostaa yhteyden Internetiin (sivu 129).
- 7 Valitse **Lopeta**.

Poista Web-sähköpostitili

Poista Web-sähköpostitili, jos et enää halua suodattaa sitä roskapostin varalta. Esimerkiksi jos tilisi ei ole enää aktiivinen tai sinulla on sen käytön kanssa ongelmia, voit poistaa sen ongelman ratkaisemisen yhteydessä.

1 Avaa Roskapostin torjunta -ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
2. Valitse Sähköposti ja pikaviesti -tietoaalueelta **Määritä**.
3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.

2 Valitse Roskapostin torjunta -ikkunasta **Web-sähköpostitilit**.

3 Valitse poistettava tili ja sitten **Poista**.

Web-sähköpostitilin tietojen ymmärtäminen

Seuraavissa taulukoissa kuvataan tietoja, jotka on määritettävä, kun lisäät tai muokkaat Web-sähköpostitilejä.

Tilitiedot

Tiedot	Kuvaus
Kuvaus	Kuvaile tili itseäsi varten. Voit kirjoittaa tähän ruutuun mitä tahansa tietoja.
Sähköpostiosoite	Määritä tähän sähköpostitiliin liittyvä sähköpostiosoite.
Tilin tyyppi	Määritä lisättävän sähköpostitilin tyyppi (esimerkiksi POP3-Web-sähköposti tai MSN/Hotmail).
Palvelin	Määritä tiliä hallinnoivan palvelimen nimi. Jos et tiedä palvelimen nimeä, tarkista se Internet-palveluntarjoajan antamista tiedoista.
Käyttäjänimi	Määritä tämän sähköpostitilin käyttäjänimi. Esimerkiksi jos sähköpostiosoitteesi on <i>käyttäjänimi@hotmail.com</i> , käyttäjänimesi on todennäköisesti <i>käyttäjänimi</i> .
Salasana	Määritä tämän sähköpostitilin salasana.
Vahvista salasana	Vahvista tämän sähköpostitilin salasana.

Tarkistusasetukset

Toiminto	Kuvaus
Tarkista	Anti-Spam tarkistaa tilin roskapostin varalta määrittelemäsi ajan (minuuteissa) välein. Aikavälin on oltava 5 - 3 600 minuuttia.
Tarkista käynnistettäessä	Anti-Spam tarkistaa tilin aina, kun tietokone käynnistetään uudelleen.

Yhteysasetukset

Toiminto	Kuvaus
Älä koskaan muodosta yhteyttä	Anti-Spam ei muodosta yhteyttä automaattisesti, vaan puhelinverkkoyhteys on muodostettava manuaalisesti.
Muodosta yhteys, kun yhteyttä ei ole	Kun Internet-yhteyttä ei ole, Anti-Spam yrittää muodostaa yhteyden käyttäen määrittämäsi puhelinverkkoyhteyttä.
Muodosta aina määritetty yhteys	Anti-Spam yrittää muodostaa yhteyden määrittämälläsi puhelinverkkoyhteydellä. Jos olet jo muodostanut toisen puhelinverkkoyhteyden, se katkaistaan.
Muodosta tämä yhteys	Määritä puhelinverkkoyhteys, jota käyttämällä Anti-Spam yrittää muodostaa yhteyden Internetiin.
Säilytä yhteys, kunnes suodattaminen on valmis	Tietokoneesi yhteys Internetiin säilyy, kun suodattaminen on päättynyt.

L U K U 2 5

Ystävien määrittäminen

Voit estää Anti-Spamia suodattamasta ystäväsi lähettämiä asiallisia sähköpostiviestejä lisäämällä ystäväsi osoitteet Anti-Spamin ystäväluetteloon.

Helpoin tapa päivittää ystäväluettelosi on lisätä osoitekirjasi Anti-Spamiin, jolloin kaikkien ystäväsi sähköpostiosoitteet tuodaan. Kun olet lisännyt osoitekirjan, sen sisältö tuodaan automaattisesti säännöllisin väliajoin (päivittäin, viikoittain tai kuukausittain). Tällä varmistetaan, että ystäväluettelosi pysyy ajan tasalla.

Voit päivittää Anti-Spamin ystäväluettelon myös manuaalisesti tai lisätä jopa kokonaisen toimialueen, jos haluat lisätä toimialueen jokaisen käyttäjän ystäväluetteloosi. Esimerkiksi jos lisäät toimialueen yritys.com, mitään kyseisen yrityksen lähettämää sähköpostiviestiä ei suodateta.

Tässä luvussa

Ystävien määrittäminen automaattisesti	132
Ystävien määrittäminen manuaalisesti	134

Ystävien määrittäminen automaattisesti

Voit päivittää ystäväluettelosi automaattisesti lisäämällä osoitekirjasi Anti-Spamiin. Kun lisäät osoitekirjan, Anti-Spam tuo siinä olevat sähköpostiosoitteet ja täyttää niillä ystäväluettelon.

Osoitekirjan lisäämisen jälkeen voit määrittää, kuinka usein sen sisältö tuodaan ystäväluetteloon. Voit myös poistaa osoitekirjan, kun et enää halua tuoda sen sisältöä.

Lisää osoitekirja

Lisää osoitekirjasi, jotta Anti-Spam voi automaattisesti tuoda kaikki sähköpostiosoitteesi ja päivittää ystäväluettelosi. Tällä voit varmistaa, että ystäväluettelosi on aina ajan tasalla.

- 1 Avaa Roskapostin torjunta -ikkuna.
Miten?
 1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
 2. Valitse Sähköposti ja pikaviesti -tietoaalueelta **Määritä**.
 3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.
- 2 Valitse Roskapostin torjunta -ikkunasta **Osoitekirjat**.
- 3 Valitse Osoitekirjat-ikkunasta **Lisää**.
- 4 Valitse tuotavan osoitekirjan tyyppi **Tyyppi**-luettelosta.
- 5 Jos **Lähde**-luettelo on täytetty, valitse osoitekirjan lähde. Esimerkiksi jos käytät Outlookin osoitekirjoja, sinun on valittava tästä luettelosta Outlook.
- 6 Valitse **Ajoita**-luettelosta **Päivittäin**, **Viikoittain** tai **Kuukausittain** ja määritä, milloin haluat Anti-Spamin tarkistavan osoitekirjasi uusien osoitteiden varalta.
- 7 Valitse **OK**.

Muokkaa osoitekirjaa

Osoitekirjojen lisäämisen jälkeen voit muuttaa niiden tärkeitä tietoja ja ajastusta. Muokkaa osoitekirjoja esimerkiksi silloin, jos haluat Anti-Spamin etsivän uusia osoitteita useammin.

- 1 Avaa Roskapostin torjunta -ikkuna.
Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
2. Valitse Sähköposti ja pikaviesti -tietoaalueelta **Määritä**.
3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.
- 2 Valitse Roskapostin torjunta -ikkunasta **Osoitekirjat**.
- 3 Valitse osoitekirja, jota haluat muokata, ja valitse sitten **Muokkaa**.
- 4 Valitse tuotavan osoitekirjan tyyppi **Tyyppi**-luettelosta.
- 5 Jos **Lähde**-luettelo on täytetty, valitse osoitekirjan lähde. Esimerkiksi jos käytät Outlookin osoitekirjoja, sinun on valittava tästä luettelosta Outlook.
- 6 Valitse **Ajoita**-luettelosta **Päivittäin**, **Viikoittain** tai **Kuukausittain** ja määritä, milloin haluat Anti-Spamin tarkistavan osoitekirjasi uusien osoitteiden varalta.
- 7 Valitse **OK**.

Poista osoitekirja

Poista osoitekirja, kun et enää halua Anti-Spamin tuovan siitä osoitteita automaattisesti (esimerkiksi jos osoitekirja ei ole enää ajan tasalla ja et enää halua käyttää sitä).

- 1 Avaa Roskapostin torjunta -ikkuna.
Miten?
 1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
 2. Valitse Sähköposti ja pikaviesti -tietoaalueelta **Määritä**.
 3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.
- 2 Valitse Roskapostin torjunta -ikkunasta **Osoitekirjat**.
- 3 Valitse poistettava osoitekirja ja sitten **Poista**.

Ystävien määrittäminen manuaalisesti

Voit päivittää ystäväluettelon manuaalisesti muokkaamalla jokaista merkintää erikseen. Esimerkiksi jos saat sähköpostiviestin ystävältä, jonka sähköpostiosoite ei ole osoitekirjassa, voit välittömästi lisätä sähköpostiosoitteen manuaalisesti. Helpoin tapa tehdä tämä on käyttää Anti-Spam-työkaluriviä. Jos et käytä Anti-Spam-työkaluriviä, sinun on määritettävä ystäväsi tiedot.

Lisää ystävä Anti-Spam-työkaluriviltä

Jos käytät Outlook-, Outlook Express-, Windows Mail-, Eudora™- tai Thunderbird-sähköpostiohjelmia, voit lisätä ystäviä Anti-Spam-työkaluriviltä.

Ystävän lisääminen ohjelmasta...	Valitse viesti ja sitten...
Outlook, Outlook Express, Windows Mail	Valitse Lisää ystävä .
Eudora, Thunderbird	Valitse Anti-Spam -valikosta Lisää ystävä .

Lisää ystävä manuaalisesti

Jos et halua lisätä ystävää suoraan työkaluriviltä tai unohdit tehdä niin, kun sait sähköpostiviestin, voit silti lisätä ystävän ystäväluettelosi ilman, että sinun tarvitsisi odottaa sitä, että Anti-Spam tuo osoitekirjasi automaattisesti.

- 1 Avaa Roskapostin torjunta -ikkuna.
Miten?
 1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
 2. Valitse Sähköposti ja pikaviesti -tietoaalueelta **Määritä**.
 3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.
- 2 Valitse Roskapostin torjunta -ikkunasta **Ystävät**.
- 3 Valitse Ystävät-ikkunasta **Lisää**.
- 4 Kirjoita ystäväsi nimi **Nimi**-ruutuun.
- 5 Valitse **Tyyppi**-luettelosta **Yksittäinen sähköpostiosoite**.
- 6 Kirjoita ystäväsi sähköpostiosoite **Sähköpostiosoite**-ruutuun.
- 7 Valitse **OK**.

Lisää toimialue

Lisää koko toimialue, jos haluat lisätä kaikki kyseisen toimialueen käyttäjät ystäväluettelosi. Esimerkiksi jos lisäät toimialueen yritys.com, mitään kyseisen yrityksen lähettämää sähköpostiviestiä ei suodateta.

1 Avaa Roskapostin torjunta -ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
2. Valitse Sähköposti ja pikaviesti -tietoaalueelta **Määritä**.
3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.

2 Valitse Roskapostin torjunta -ikkunasta **Ystävät**.

3 Valitse Ystävät-ikkunasta **Lisää**.

4 Kirjoita organisaation tai ryhmän nimi **Nimi**-ruutuun.

5 Valitse **Tyyppi**-luettelosta **Koko toimialue**.

6 Kirjoita toimialueen nimi **Sähköpostiosoite**-ruutuun.

7 Valitse **OK**.

Muokkaa ystävää

Jos ystäväsi tiedot muuttuvat, voit päivittää ystäväluettelosi ja varmistaa, että Anti-Spam ei merkitse heidän lähettämiään viestejä roskapostiksi.

1 Avaa Roskapostin torjunta -ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
2. Valitse Sähköposti ja pikaviesti -tietoaalueelta **Määritä**.
3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.

2 Valitse Roskapostin torjunta -ikkunasta **Ystävät**.

3 Valitse ystävä, jota haluat muokata, ja valitse sitten **Muokkaa**.

4 Muuta ystäväsi nimi **Nimi**-ruudussa.

5 Muuta ystäväsi sähköpostiosoite **Sähköpostiosoite**-ruudussa.

6 Valitse **OK**.

Muokkaa toimialuetta

Jos toimialueen tiedot muuttuvat, voit päivittää ystäväluettelosi ja varmistaa, että Anti-Spam ei merkitse kyseiseltä toimialueelta peräisin olevia viestejä roskapostiksi.

1 Avaa Roskapostin torjunta -ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
2. Valitse Sähköposti ja pikaviesti -tietoaalueelta **Määritä**.
3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.

2 Valitse Roskapostin torjunta -ikkunasta **Ystävät**.

3 Valitse Ystävät-ikkunasta **Lisää**.

4 Muuta organisaation tai ryhmän nimi **Nimi**-ruudussa.

5 Valitse **Tyyppi**-luettelosta **Koko toimialue**.

6 Muuta toimialueen nimi **Sähköpostiosoite**-ruudussa.

7 Valitse **OK**.

Poista ystävä

Jos ystäväluettelossasi oleva henkilö tai toimialue lähettää sinulle roskapostia, voit poistaa ne Anti-Spamin ystäväluettelosta, jolloin niiden sähköpostiviestit suodatetaan taas.

1 Avaa Roskapostin torjunta -ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
2. Valitse Sähköposti ja pikaviesti -tietoaalueelta **Määritä**.
3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.

2 Valitse Roskapostin torjunta -ikkunasta **Ystävät**.

3 Valitse poistettava ystävä ja valitse sitten **Poista**.

L U K U 2 6

Roskapostiviestien tunnistustavan määrittäminen

Anti-Spamin avulla voit mukauttaa roskapostiviestien tunnistustapaa. Voit suodattaa viestejä aggressiivisesti, määrittää viestistä haettavat asiat ja etsiä tiettyjä merkistöjä. Voit myös luoda henkilökohtaisia suodattimia, joiden avulla voit hienosäätää, mitkä viestit Anti-Spam katsoo roskapostiksi. Esimerkiksi jos laina-sanan sisältävää viestiä ei suodateta, voit lisätä laina-sanan sisältävän suodattimen.

Jos sinulla on ongelmia sähköpostin kanssa, voit poistaa roskapostisuojaus käytöstä osana vianmääritysstrategiaasi.

Tässä luvussa

Poista roskapostin torjunta käytöstä	137
Suodatusasetusten määrittäminen.....	138
Henkilökohtaisten suodattimien käyttäminen	142

Poista roskapostin torjunta käytöstä

Voit poistaa roskapostin torjunnan käytöstä, mikä estää Anti-Spamia suodattamasta sähköpostiviestejä.

- 1 Valitse Lisävalikosta **Määritä**.
- 2 Valitse Määritä-ikkunasta **Sähköposti ja pikaviesti**.
- 3 Valitse **Roskapostin torjunta** -kohdasta **Ei käytössä**.

Vihje: Muista valita **Roskapostin torjunta** -kohdasta **Käytössä**, jotta olet suojattu roskapostiviestejä vastaan.

Suodatusasetusten määrittäminen

Sääda Anti-Spamin suodatusasetuksia, jos haluat suodattaa viestejä aggressiivisesti, määrittää viestistä haettavat asiat ja etsiä tiettyjä merkistöjä.

Suodatustaso

Suodatustaso osoittaa, kuinka aggressiivisesti sähköpostiviestit suodatetaan. Esimerkiksi jos roskapostiviestejä ei suodateta ja suodatustasoksi on asetettu Normaali, voit muuttaa sen Korkeaksi. Jos suodatustasoksi on asetettu Korkea, vain ystäväluettelossa olevien lähettäjien sähköpostiviestit hyväksytään ja kaikki muut sähköpostiviestit suodatetaan.

Erikoissuodattimet

Suodatin määrittää, mitä Anti-Spam etsii sähköpostiviestistä. Erikoissuodattimet tunnistavat sähköpostiviestit, joissa on piilotekstiä, upotettuja kuvia, tahallisia HTML-muotoiluvirheitä ja muita roskapostittajien yleisesti käyttämiä tekniikoita. Koska nämä ominaisuudet sisältävät sähköpostiviestit ovat tavallisesti roskapostiviestejä, erikoissuodattimet otetaan oletusarvoisesti käyttöön. Esimerkiksi jos haluat vastaanottaa viestejä, joissa on upotettuja kuvia, sinun on mahdollisesti poistettava kuvien erikoissuodatin käytöstä.

Merkistöt

Anti-Spam voi etsiä tiettyjä merkistöjä roskapostiviestejä analysoidessaan. Merkistöjä käytetään kuvaamaan kieltä, mukaan lukien kielen kirjaimistoa, numeerisia lukuja ja muita symboleja. Jos saat kreikankielisiä roskapostiviestejä, voit suodattaa kaikki viestit, joissa käytetään kreikkalaista merkistöä.

Älä kuitenkaan suodata merkistöjä kielillä, joilla vastaanotat asiallisia sähköpostiviestejä. Esimerkiksi jos haluat suodattaa vain italiankieliset roskapostiviestit, sinun kannattaa ehkä valita länsi-eurooppalainen merkistö, sillä Italia on Länsi-Euroopassa. Huomaa kuitenkin, että jos saat asiallisia englanninkielisiä viestejä, länsi-eurooppalaisen merkistön valitseminen suodattaa myös englanniksi ja muilla länsi-eurooppalaista merkistöä käyttävillä kielillä kirjoitetut viestit. Tässä tapauksessa et voi suodattaa vain italiankielisiä viestejä.

Huomautus: Tietyn merkistön merkkejä sisältävien viestien suodatusta suositellaan vain kokeneille käyttäjille.

Muuta suodatustasoa

Voit muuttaa, kuinka aggressiivisesti haluat suodattaa sähköpostiviestejä. Jos esimerkiksi suodatat asiallisia sähköpostiviestejä, voit madaltaa suodatustasoa.

1 Avaa Roskapostin torjunta -ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
2. Valitse Sähköposti ja pikaviesti -tietoaalueelta **Määritä**.
3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.

2 Valitse Roskapostin torjunta -ikkunasta **Suodatusasetukset**.

3 Siirrä **Suodatusasetukset** -kohdassa liukusäädin haluamallesi tasolle ja valitse **OK**.

Taso	Kuvaus
Matala	Useimmat sähköpostiviestit hyväksytään.
Melko matala	Vain selvät roskapostiviestit suodatetaan.
Normaali	Sähköpostiviestit suodatetaan suositellun tason mukaisesti.
Melko korkea	Kaikki roskapostia muistuttavat sähköpostiviestit suodatetaan.
Korkea	Vain ystäväluettelossasi olevilta lähettäjiä saapuneet viestit hyväksytään.

Poista erikoissuodatin käytöstä

Erikoissuodattimet otetaan oletusarvoisesti käyttöön, sillä ne suodattavat roskapostittajien tyypillisesti lähettämiä viestejä. Esimerkiksi upotettuja kuvia sisältävät sähköpostiviestit ovat tavallisesti roskapostiviestejä. Jos kuitenkin saat usein asiallisia sähköpostiviestejä, joissa on upotettuja kuvia, poista kuvien erikoissuodatin käytöstä.

1 Avaa Roskapostin torjunta -ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
 2. Valitse Sähköposti ja pikaviesti -tietoaalueelta **Määritä**.
 3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.
- 2** Valitse Roskapostin torjunta -ikkunasta **Suodatusasetukset**.
- 3** Valitse **Erikoissuodattimet**-ikkunasta haluamasi valintaruudut tai poista niiden valinnat, ja valitse sen jälkeen **OK**.

Suodatin	Kuvaus
Suodata viestit, joissa on piilotekstiä.	Etsii piilotekstiä, sillä roskapostittajat käyttävät usein piilotekstiä sisältäviä viestejä tunnistamisen välttämiseksi.
Suodata viestit, joissa kuvat ja teksti ovat keskenään tietyssä suhteessa	Etsii upotettuja kuvia, sillä upotettuja kuvia sisältävät viestit ovat yleensä roskapostiviestejä.
Suodata viestit, joissa on tahallisia HTML-muotoiluvirheitä	Etsii viestejä, jotka sisältävät kelvotonta muotoilua, sillä kelvotonta muotoilua käytetään, jotta suodattimet eivät voisi suodattaa roskapostia.
Älä suodata viestejä, jotka ovat suurempia kuin	Ei etsi annettua kokoa suurempia viestejä, sillä suuret viestit eivät välttämättä ole roskapostiviestejä. Voit suurentaa tai pienentää viestin kokoa (välillä 0 - 250 kt).

Käytä merkistösuodattimia

Huomautus: Tietyn merkistön merkkejä sisältävien viestien suodatusta suositellaan vain kokeneille käyttäjille.

Voit suodattaa tiettyjä merkistöjä, mutta älä kuitenkaan suodata sellaisten kielten merkistöjä, joita käytetään sinulle lähetetyissä asiallisissa viesteissä.

- 1** Avaa Roskapostin torjunta -ikkuna.
Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
2. Valitse Sähköposti ja pikaviesti -tietoaalueelta **Määritä**.
3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.
- 2 Valitse Roskapostin torjunta -ikkunasta **Merkistöt**.
- 3 Valitse suodatettavien merkistöjen vieressä olevat valintaruudut.
- 4 Valitse **OK**.

Henkilökohtaisten suodattimien käyttäminen

Suodatin määrittää, mitä Anti-Spam etsii sähköpostiviestistä. Kun roskapostiviesti löydetään, se merkitään roskapostiksi ja jätetään Saapuneet-kansioon tai siirretään McAfee Anti-Spam -kansioon. Lisätietoja roskapostiviestien käsittelystä on kohdassa Muokkaa viestin käsittely- ja merkintätapaa (sivu 146).

Oletusarvoisesti Anti-Spam käyttää useita suodattimia, mutta lisäämällä suodattimia tai muokkaamalla olevassa olevia suodattimia voit edelleen hienosäätää sitä, mitkä viestit Anti-Spam tunnistaa roskapostiksi. Esimerkiksi jos lisäät laina-sanan sisältävän suodattimen, Anti-Spam suodattaa laina-sanan sisältävän viestit. Älä luo suodattimia asiallisissa sähköpostiviesteissä esiintyville tavallisille sanoille, sillä tällöin suodatetaan myös muut kuin roskapostiviestit. Kun olet luonut suodattimen, voit muokata sitä, jos se ei edelleenkään tunnista kaikkia roskapostiviestejä. Esimerkiksi jos olet luonut suodattimen, jonka avulla etsit sanaa viagra viestin otsikkoriviltä, mutta saat edelleen viestejä, jotka sisältävät sanan viagra viestin rungossa, muuta suodatinta siten, että sanaa viagra etsitään viestin rungosta otsikkorivin sijaan.

Säännönmukaiset lausekkeet (RegEx) ovat erikoismerkkejä ja -merkkisarjoja, joita voidaan käyttää myös henkilökohtaisissa suodattimissa. McAfee suosittelee säännönmukaisen lausekkeiden käyttöä kuitenkin vain kokeneille käyttäjille. Jos et ole perehtynyt säännönmukaisiin lausekkeisiin tai haluat tietää niiden käytöstä enemmän, löydät lisätietoja Internetistä (esimerkiksi sivustosta http://en.wikipedia.org/wiki/Regular_expression).

Lisää henkilökohtainen suodatin

Voit lisätä suodattimia, joiden avulla voit hienosäätää, mitkä viestit Anti-Spam katsoo roskapostiksi.

1 Avaa Roskapostin torjunta -ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
2. Valitse Sähköposti ja pikaviesti -tietoaalueelta **Määritä**.
3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.

2 Valitse Roskapostin torjunta -ikkunasta **Henkilökohtaiset suodattimet**.

3 Valitse **Lisää**.

4 Määritä, mitä haluat henkilökohtaisen suodattimen etsivän (sivu 143) sähköpostiviesteistä.

5 Valitse **OK**.

Muokkaa henkilökohtaista suodatinta

Muokkaa olemassa olevia suodattimia ja hienosäädä, mitkä viestit katsotaan roskapostiksi.

1 Avaa Roskapostin torjunta -ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
2. Valitse Sähköposti ja pikaviesti -tietoaalueelta **Määritä**.
3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.

2 Valitse Roskapostin torjunta -ikkunasta **Henkilökohtaiset suodattimet**.

3 Valitse muokattava suodatin ja sitten **Muokkaa**.

4 Määritä, mitä haluat henkilökohtaisen suodattimen etsivän (sivu 143) sähköpostiviesteistä.

5 Valitse **OK**.

Poista henkilökohtainen suodatin

Voit poistaa pysyvästi suodattimet, joita et enää halua käyttää.

1 Avaa Roskapostin torjunta -ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
2. Valitse Sähköposti ja pikaviesti -tietoaalueelta **Määritä**.
3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.

2 Valitse Roskapostin torjunta -ikkunasta **Henkilökohtaiset suodattimet**.

3 Valitse poistettava suodatin ja sitten **Poista**.

4 Valitse **OK**.

Henkilökohtaisen suodattimen määrittäminen

Seuraavassa taulukossa kuvataan, mitä henkilökohtainen suodatin etsii sähköpostiviesteistä.

Tiedot	Kuvaus
Kohde	Valitse merkintä ja tarkista, etsiikö suodatin sanoja tai fraaseja viestin aiheesta, tekstiosasta, otsikoista tai viestin lähettäjän tiedoista.

Ehto	Valitse merkintä ja tarkista, etsiikö suodatin sellaisia viestejä, joissa määrittämäsi sanat tai ilmaukset esiintyvät tai sellaisia, joissa ne eivät esiinny.
Sanat tai fraasit	Kirjoita, mitä haluat etsiä viestistä. Jos esimerkiksi määrität laina, kaikki kyseisen sanan sisältävät viestit suodatetaan.
Tämä suodatin käyttää säännönmukaisia lausekkeita (RegEx)	Määritä suodatusehdoissa käytettävät merkkisarjat. Voit testata merkkisarjan valitsemalla Testi .

LUKU 27

Sähköpostin suodatus

Anti-Spam tarkistaa saapuvat sähköpostiviestit ja luokittelee ne roskapostiksi (sähköpostiviestit, jotka houkuttelevat sinua tekemään ostoksia) tai phishing-huijausviesteiksi (sähköpostiviestit, jotka houkuttelevat sinua antamaan henkilökohtaiset tietosi tunnetun tai mahdollisesti petollisen Web-sivuston käyttöön). Oletusarvoisesti Anti-Spam merkitsee kaikki ei-toivotut sähköpostiviestit roskapostiksi tai phishing-huijausviesteiksi (viestin otsikkoriville lisätään tunniste [SPAM] tai [PHISH]) ja siirtää ne McAfee Anti-Spam -kansioon.

Voit mukauttaa tapaa, jolla Anti-Spam käsittelee sähköpostiviestejä, ja merkitä sähköpostiviestit roskapostiksi tai ei-roskapostiksi Anti-Spamin työkalurivillä, muuttaa sijaintia, jonne roskapostiviestit siirretään, tai muuttaa otsikkorivillä näkyvää tunnistetta.

Voit muuttaa roskapostiviestien käsittely- ja merkintätapaa mukauttamalla sijaintia, jonne roskaposti- ja phishing-huijausviestit siirretään, ja mukauttamalla otsikkorivillä näkyvän tunnisteen nimeä.

Voit myös poistaa Anti-Spamin työkalurivit käytöstä osana vianmääritysstrategiaasi, jos sinulla on ongelmia sähköpostiohjelmiasi kanssa.

Tässä luvussa

Merkitse viesti Anti-Spam-työkaluriviltä.....	145
Muokkaa viestin käsittely- ja merkintätapaa	146
Poista Anti-Spam-työkalurivi käytöstä	146

Merkitse viesti Anti-Spam-työkaluriviltä

Kun merkitset viestin roskapostiviestiksi, viestin otsikkoon lisätään [SPAM]-merkintä tai valitsemasi merkintä, ja viesti jää joko Saapuneet-kansioon, McAfee Anti-Spam -kansioon (Outlook, Outlook Express, Windows Mail, Thunderbird) tai roskapostikansioon (Eudora®). Kun merkitset viestin ei-roskapostiksi, tunniste poistetaan ja viesti siirretään Saapuneet-kansioon.

Viestin merkitseminen ohjelmasta...	Valitse viesti ja sitten...
Outlook, Outlook Express, Windows Mail	Valitse Merkitse roskapostiksi tai Merkitse ei roskapostiksi .

Eudora, Thunderbird	Valitse Anti-Spam -valikosta Merkitse roskapostiksi tai Merkitse ei roskapostiksi .
---------------------	--

Muokkaa viestin käsittely- ja merkintätapaa

Voit määrittää, miten roskaposti merkitään ja miten sitä käsitellään. Voit esimerkiksi päättää, haluatko jättää sähköpostiviestin Saapuneet-kansioon tai McAfee Anti-Spam -kansioon, ja muuttaa viestin otsikkorivillä näkyvää [SPAM]- tai [PHISH]-tunnistetta.

1 Avaa Roskapostin torjunta -ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
2. Valitse Sähköposti ja pikaviesti -tietoaalueelta **Määritä**.
3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.

2 Valitse Roskapostin torjunta -ikkunasta **Käsittely**.

3 Valitse haluamasi valintaruudut tai poista niiden valinnat, ja valitse sen jälkeen **OK**.

Toiminto	Kuvaus
Merkitse roskapostiksi ja siirrä McAfee Anti-Spam -kansioon	Tämä on oletusasetus. Roskapostiviestit siirretään McAfee Anti-Spam -kansioon.
Merkitse roskapostiksi ja jätä Saapuneet-kansioon	Roskapostiviestit jäävät Saapuneet-kansioon.
Liitä tämä mukautettava tunniste roskapostiviestien aiheeseen	Määrittämäsi tunniste lisätään roskapostiviestien aiheeriville.
Liitä tämä mukautettava tunniste phishing-huijausviestien aiheeseen	Määrittämäsi tunniste lisätään phishing-huijausviestien aiheeriville.

Poista Anti-Spam-työkalurivi käytöstä

Jos käytät Outlook-, Outlook Express -, Windows Mail -, Eudora- tai Thunderbird-sähköpostiohjelmaa, voit poistaa Anti-Spam-työkalurivin käytöstä.

1 Avaa Roskapostin torjunta -ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
2. Valitse Sähköposti ja pikaviesti -tietoalueelta **Määritä**.
3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.
- 2 Valitse Roskapostin torjunta -ikkunasta **Sähköpostityökalurivit**.
- 3 Poista valintaruudun valinta sen työkalurivin vierestä, jonka haluat poistaa käytöstä.
- 4 Valitse **OK**.

Vihje: Voit ottaa Anti-Spam-työkalurivit milloin tahansa uudelleen käyttöön valitsemalla niiden vieressä olevat valintaruudut.

LUKU 28

Suodatettujen sähköpostiviestien käsitteleminen

Kaikkia roskapostiviestejä ei aina välttämättä tunnisteta. Voit tällöin ilmoittaa roskapostiviesteistä McAfeelle, joka analysoi ne ja luo niiden perusteella suodatinpäivityksiä.

Jos käytät Web-sähköpostitiliä, voit kopioida ja poistaa suodatetut sähköpostiviestit sekä saada niistä lisätietoja. Tämä on käytännöllistä silloin, jos et ole varma, oletko suodattanut asiallisen viestin, tai kun haluat tietää, milloin viesti on suodatettu.

Tässä luvussa

Ilmoita roskapostista McAfeelle.....	149
Kopioi tai poista suodatettu Web-sähköpostiviesti..	150
Näytä suodatettujen Web-sähköpostiviestien tapahtumat	150

Ilmoita roskapostista McAfeelle

Voit ilmoittaa roskapostiviesteistä McAfeelle, joka analysoi ne ja luo niiden perusteella suodatinpäivityksiä.

- 1 Avaa Roskapostin torjunta -ikkuna.
Miten?
 1. Valitse SecurityCenterin Koti-ikkunasta **Sähköposti ja pikaviesti**.
 2. Valitse Sähköposti ja pikaviesti -tietoaalueelta **Määritä**.
 3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.
- 2 Valitse Roskapostin torjunta -ikkunasta **Raportointi McAfeelle**.
- 3 Valitse haluamasi valintaruudut ja valitse sen jälkeen **OK**.

Toiminto	Kuvaus
Ota raportointi käyttöön napsautettaessa Merkitse roskapostiksi	Ilmoittaa viestistä McAfeelle aina, kun merkitset sen roskapostiksi.
Ota raportointi käyttöön napsautettaessa Merkitse roskapostiksi	Ilmoittaa viestistä McAfeelle aina, kun merkitset sen ei roskapostiksi.

Lähetä koko viesti (ei vain otsikoita)	Lähetää koko viestin eikä vain otsikoita, kun ilmoitat viestistä McAfeeelle.
--	--

Kopioi tai poista suodatettu Web-sähköpostiviesti

Voit kopioida tai poistaa viestejä, jotka on suodatettu Web-sähköpostitililläsi.

- 1 Valitse **Yleiset tehtävät** -kohdasta **Tarkastele äskettäisiä tapahtumia**.
- 2 Valitse Äskettäiset tapahtumat -ruudusta **Näytä loki**.
- 3 Laajenna vasemmassa ikkunassa oleva **Sähköposti ja pikaviesti** -luettelo ja valitse **Web-sähköpostin suodatuksen tapahtumat**.
- 4 Valitse viesti.
- 5 Suorita jokin seuraavista toimenpiteistä **Haluan**-kohdassa:
 - Valitse **Kopioi**, jos haluat kopioida viestin leikepöydälle.
 - Valitse **Poista**, jos haluat poistaa viestin.

Näytä suodatettujen Web-sähköpostiviestien tapahtumat

Voit tarkistaa sähköpostiviestin suodatuksen päivämäärän ja kellonajan sekä tarkastella sen vastaanottanutta tiliä.

- 1 Valitse **Yleiset tehtävät** -kohdasta **Tarkastele äskettäisiä tapahtumia**.
- 2 Valitse Äskettäiset tapahtumat -ruudusta **Näytä loki**.
- 3 Laajenna vasemmassa ikkunassa oleva **Sähköposti ja pikaviesti** -luettelo ja valitse **Web-sähköpostin suodatuksen tapahtumat**.
- 4 Valitse loki, jota haluat tarkastella.

LUKU 29

Phishing-huijausten torjunnan asetusten määrittäminen

Anti-Spam luokittelee ei-toivotut sähköpostiviestit roskapostiksi (sähköpostiviestit, jotka houkuttelevat sinua tekemään ostoksia) tai phishing-huijausviesteiksi (sähköpostiviestit, jotka houkuttelevat sinua antamaan henkilökohtaiset tietosi tunnetun tai mahdollisesti petollisen Web-sivuston käyttöön). Phishing-suojaus suojaa sinua haitallisia Web-sivustoja vastaan. Jos napsautat sähköpostiviestissä olevaa linkkiä, joka johtaa tunnetusti tai mahdollisesti petolliseen Web-sivustoon, sinut uudelleenohjataan phishing-huijauksen suodatussivulle.

Jos et halua suodattaa kaikkia Web-sivustoja, lisää ne valkoiseen listaan. Voit myös muokata valkoisessa listassa olevia Web-sivustoja tai poistaa ne siitä. Sivustoja Google®, Yahoo tai McAfee ei tarvitse lisätä, sillä näitä sivustoja ei pidetä petollisina.

Huomautus: Jos olet asentanut SiteAdvisorin, sinulla ei ole käytössäsi Anti-Spamin phishing-suojausta, sillä SiteAdvisor käyttää Anti-Spamin kaltaista phishing-suojausta.

Tässä luvussa

Lisää Web-sivusto valkoiseen listaan	151
Muokkaa valkoisessa listassa olevia sivustoja.....	152
Poista Web-sivusto valkoisesta listasta.....	152
Poista phishing-huijausten torjunta käytöstä.....	153

Lisää Web-sivusto valkoiseen listaan

Jos et halua suodattaa kaikkia Web-sivustoja, lisää ne phishing-huijausten valkoiseen listaan.

- 1 Avaa Phishing-huijausten torjunta -ikkuna.
Miten?
 1. Valitse SecurityCenterin Koti-ikkunasta **Internet & verkko**.
 2. Valitse Internet & verkko -tietoaalueelta **Määritä**.
- 2 Valitse Phishing-huijausten torjunta -ikkunasta **Lisäasetukset**.
- 3 Valitse **Valkoinen lista** -kohdasta **Lisää**.
- 4 Kirjoita Web-sivuston osoite ja valitse **OK**.

Muokkaa valkoisessa listassa olevia sivustoja

Jos olet lisännyt valkoiseen listaan sivuston ja sen osoite muuttuu, voit aina päivittää sen.

- 1 Avaa Phishing-huijausten torjunta -ikkuna.
Miten?
 1. Valitse SecurityCenterin Koti-ikkunasta **Internet & verkko**.
 2. Valitse Internet & verkko -tietoaalueelta **Määritä**.
- 2 Valitse Phishing-huijausten torjunta -ikkunasta **Lisäasetukset**.
- 3 Valitse **Valkoinen lista** -kohdasta Web-sivusto, jonka haluat päivittää, ja valitse **Muokkaa**.
- 4 Muokkaa Web-sivuston osoitetta ja valitse **OK**.

Poista Web-sivusto valkoisesta listasta

Jos lisäsit Web-sivuston valkoiseen listaan, sillä halusit käydä siinä, mutta nyt haluat suodattaa sen, poista se valkoisesta listasta.

- 1 Avaa Phishing-huijausten torjunta -ikkuna.
Miten?
 1. Valitse SecurityCenterin Koti-ikkunasta **Internet & verkko**.
 2. Valitse Internet & verkko -tietoaalueelta **Määritä**.
- 2 Valitse Phishing-huijausten torjunta -ikkunasta **Lisäasetukset**.
- 3 Valitse **Valkoinen lista** -kohdasta Web-sivusto, jonka haluat poistaa, ja valitse **Poista**.

Poista phishing-huijausten torjunta käytöstä

Jos käytät jo muuta kuin McAfeen phishing-huijausten torjuntaohjelmistoa ja ohjelmistot eivät ole keskenään yhteensopivia, voit poistaa Anti-Spamin phishing-suojauksen käytöstä.

- 1 Valitse SecurityCenterin Koti-ikkunasta **Internet & verkko**.
- 2 Valitse Internet & verkko -tietoalueelta **Määritä**.
- 3 Valitse **Phishing-huijausten torjunta** -kohdasta **Ei käytössä**.

Vihje: Kun olet valmis, muista valita **Phishing-huijausten torjunta** -kohdasta **Käytössä**, jotta olet suojattu petollisia Web-sivustoja vastaan.

L U K U 3 0

McAfee-tietosuojapalvelu

Tietosuojapalvelu antaa lisäsuojaa sinulle, perheellesi, henkilökohtaisille tiedostoillesi ja tietokoneellesi. Sen avulla voit suojata henkilötietosi tietomurtojen varalta, estää henkilökohtaisten tietojen lähettämisen ja suodattaa mahdollisesti loukkaavaa sisältöä, kuten kuvia. Tietosuojapalvelusta saat myös suojatun säilytyspaikan salasanoille sekä edistyneitä käytönvalvontaominaisuuksia, joilla aikuiset voivat valvoa, säätää ja kirjata lokiin luvattomia Web-selaustapoja.

Voit tutustua Privacy Servicen suosituimpiin ominaisuuksiin ennen kuin alat käyttää sitä. Lisätietoja näiden ominaisuuksien määrittämisestä ja käyttämisestä on Privacy Servicen ohjeessa.

Huomautus: SecurityCenter raportoi kriittiset ja ei-kriittiset suojausongelmat heti, kun se havaitsee ne. Jos tarvitset apua suojausongelmien selvittämisessä, voit käyttää McAfee Virtual Technician -palvelua.

Tässä luvussa

Privacy Service -ohjelman ominaisuudet.....	156
Käytönvalvonnan määrittäminen.....	157
Tietojen suojaaminen Internetissä	173
Salasanojen suojaaminen.....	175

Privacy Service -ohjelman ominaisuudet

Privacy Service sisältää seuraavat ominaisuudet:

- Käytönvalvonta-asetukset
- Henkilökohtaisten tietojen suojaus
- Salasanasäilö

Käytönvalvonta-asetukset

Käytönvalvonta-asetusten avulla voit suodattaa SecurityCenter-käyttäjille mahdollisesti epäsovivat kuvat, määrittää sisältöluokitusryhmät (ikäryhmät, joiden mukaan rajoitetaan nähtävillä olevia Internet-sivuja ja sisältöjä) ja asettaa Web-selaukselle aikarajoitukset (kuinka kauan yksittäisellä käyttäjällä on Internet-yhteys käytössään). Käytönvalvonta-asetuksilla voit myös rajoittaa käyttäjien pääsyä Web-sivustoihin ja sallia tai estää käytön ikäryhmien käyttöoikeuksien tai avainsanojen perusteella.

Henkilökohtaisten tietojen suojaus

Henkilökohtaisten tietojen suojauksella voit estää arkaluonteisten ja luottamuksellisten tietojen (esimerkiksi luottokorttien numeroiden, pankkitilinumerojen, osoitteiden ja niin edelleen) lähettämisen Internetin kautta.

Salasanasäilö

Salasanasäilö on suojattu tallennusalue henkilökohtaisille salasanoillesi. Sen avulla voit tallentaa salasanasi luottaen siihen, ettei kukaan muu käyttäjä (ei edes järjestelmänvalvoja) saa niitä käyttöönsä.

LUKU 31

Käytönvalvonnan määrittäminen

Jos lapsesi käyttävät tietokonetta, voit määrittää heitä varten käytönvalvonta-asetukset. Käytönvalvonta-asetusten avulla voit määrittää, minkälaisilla sivuilla lapsesi voivat vierailla. Voit määrittää käytönvalvonnan ottamalla käyttöön kuvasuodatuksen tai poistamalla sen käytöstä, valitsemalla sisältöluokitusryhmän ja määrittämällä Web-selaukselle aikarajoitukset. Kuvasuodatus estää mahdollisesti sopimattomien kuvien näkymisen, kun lapsi selaa Web-sivustoja. Sisältöluokitusryhmät määrittävät lapsen ikäryhmän mukaan, minkälaisen sisällön ja Web-sivustojen käyttöoikeus lapsella on. Web-selauksen aikarajoitus määrittää, milloin lapsi voi selata Internetiä. Käytönvalvonnan avulla voit myös suodattaa (estää tai sallia) tiettyjä Web-sivustoja kaikilta lapsilta.

Huomautus: Käytönvalvonnan määrittämiseen vaaditaan järjestelmänvalvojan oikeudet.

Tässä luvussa

Käyttäjien määrittäminen	158
Mahdollisesti sopimattomien Web-kuvien suodattaminen	163
Sisältöluokitusryhmän määrittäminen	164
Web-selauksen aikarajoitusten määrittäminen.....	166
Web-sivustojen suodattaminen	167
Web-sivustojen suodattaminen avainsanojen avulla	170

Käyttäjien määrittäminen

Voit määrittää käytönvalvonnan määrittämällä SecurityCenter-käyttäjille käyttöoikeudet. Oletuksena SecurityCenter-käyttäjien käyttöoikeudet ovat samat kuin tietokoneen käyttäjille määritetyt Windowsin käyttöoikeudet. Jos olet kuitenkin päivittänyt SecurityCenterin aiemmasta versiosta, joka käytti McAfee-käyttäjiä, edellisen version käyttäjät ja heidän käyttöoikeutensa siirtyvät myös päivitettyyn versioon.

Huomautus: Sinun täytyy kirjautua SecurityCenteriin järjestelmänvalvojana, jotta voit määrittää käyttäjiä.

Windows-käyttäjien asetusten määrittäminen

Jotta voit määrittää käytönvalvonnan, käyttäjille on määritettävä käyttöoikeudet, jotka määrittävät, minkälaisia Web-sivuja kukin käyttäjä voi tarkastella. Oletuksena SecurityCenter-käyttäjien käyttöoikeudet ovat samat kuin tietokoneen käyttäjille määritetyt Windowsin käyttöoikeudet. Lisää käyttäjä, muokkaa käyttäjän tilitietoja tai poista käyttäjä Windowsin Tietokoneen hallinnassa. Tämän jälkeen voit määrittää käyttäjille käytönvalvonta-asetukset SecurityCenterissä.

Jos olet päivittänyt SecurityCenterin aiemmasta versiosta, joka käytti McAfee-käyttäjiä, saat lisätietoja kohdasta McAfee-käyttäjien asetusten määrittäminen (sivu 160).

McAfee-käyttäjien asetusten määrittäminen

Jos olet päivittänyt SecurityCenterin aiemmasta versiosta, joka käytti McAfee-käyttäjiä, edellisen version käyttäjät ja heidän käyttöoikeutensa siirtyvät automaattisesti myös päivitettyyn versioon. Voit jatkaa McAfee-käyttäjien määrittämistä ja hallintaa. On kuitenkin suositeltavaa vaihtaa Windows-käyttäjiin, koska Windows-käyttäjien hallinta on McAfee-käyttäjien hallintaa helpompaa. Kun olet vaihtanut Windows-käyttäjiin, et voi enää vaihtaa takaisin McAfee-käyttäjiin.

Jos jatkat McAfee-käyttäjien käyttämistä, voit lisätä, muokata ja poistaa käyttäjiä sekä vaihtaa tai palauttaa McAfee-valvojan salasanan.

Windows-käyttäjiin vaihtaminen

On suositeltavaa vaihtaa Windows-käyttäjiin, koska Windows-käyttäjien ylläpito on McAfee-käyttäjien ylläpitoa helpompaa. Kun olet vaihtanut Windows-käyttäjiin, et voi enää vaihtaa takaisin McAfee-käyttäjiin.

1 Avaa Käyttäjäasetukset-ikkuna.

Miten?

1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
2. Valitse SecurityCenterin Koti-ikkunasta **Käytönvalvonta-asetukset**.
3. Valitse käytönvalvontatieto-osasta **Määritä**.
4. Valitse Käytönvalvonta-asetukset-asetusikkunasta **Lisäasetukset**.

2 Valitse Käyttäjäasetukset-ikkunassa **Vaihda**.

3 Vahvista toiminto.

Lisää McAfee-käyttäjä

Kun McAfee-käyttäjä on luotu, voit määrittää käyttäjän käytönvalvonta-asetukset. Lisätietoja on Tietosuojapalvelu-ohjeessa.

1 Kirjaudu SecurityCenteriin järjestelmänvalvojana.

2 Avaa Käyttäjäasetukset-ikkuna.

Miten?

1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
2. Valitse SecurityCenterin Koti-ikkunasta **Käytönvalvonta-asetukset**.
3. Valitse käytönvalvontatieto-osasta **Määritä**.
4. Valitse Käytönvalvonta-asetukset-asetusikkunasta **Lisäasetukset**.
- 3 Valitse Käyttäjäasetukset-ikkunasta **Lisää**.
- 4 Määritä käyttäjänimi, salasana, tilityyppi ja käytönvalvonta-asetukset toimimalla näytön ohjeiden mukaan.
- 5 Valitse **Luo**.

Muokkaa McAfee-käyttäjän tilitietoja

Voit muuttaa McAfee-käyttäjän salasanan, tilityypin tai automaattisen kirjausasetuksen.

- 1 Kirjaudu SecurityCenteriin järjestelmänvalvojana.
- 2 Avaa Käyttäjäasetukset-ikkuna.

Miten?

1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
2. Valitse SecurityCenterin Koti-ikkunasta **Käytönvalvonta-asetukset**.
3. Valitse käytönvalvontatieto-osasta **Määritä**.
4. Valitse Käytönvalvonta-asetukset-asetusikkunasta **Lisäasetukset**.
- 3 Valitse Käyttäjäasetukset-ikkunasta käyttäjänimi ja valitse sitten **Muokkaa**.
- 4 Muokkaa käyttäjän salasanaa, tilityyppiä ja käytönvalvonta-asetuksia toimimalla näytön ohjeiden mukaan.
- 5 Valitse **OK**.

Poista McAfee-käyttäjä

Voit poistaa McAfee-käyttäjän milloin tahansa.

Poista McAfee-käyttäjä seuraavasti:

- 1 Kirjaudu SecurityCenteriin järjestelmänvalvojana.
- 2 Avaa Käyttäjäasetukset-ikkuna.

Miten?

1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
 2. Valitse SecurityCenterin Koti-ikkunasta **Käytönvalvonta-asetukset**.
 3. Valitse käytönvalvontatieto-osasta **Määritä**.
 4. Valitse Käytönvalvonta-asetukset-asetusikkunasta **Lisäasetukset**.
- 3** Valitse Käyttäjäasetukset-ikkunan **McAfee-käyttäjätilit** -kohdasta käyttäjänimi ja valitse sitten **Poista**.

[Vaihda McAfee-järjestelmänvalvojan salasana](#)

Jos sinun on vaikeata muistaa McAfee-järjestelmänvalvojan salasanaa tai epäilet sen joutuneen väärin käsiin, voit vaihtaa sen.

- 1** Kirjaudu SecurityCenteriin järjestelmänvalvojana.
- 2** Avaa Käyttäjäasetukset-ikkuna.

Miten?

1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
 2. Valitse SecurityCenterin Koti-ikkunasta **Käytönvalvonta-asetukset**.
 3. Valitse käytönvalvontatieto-osasta **Määritä**.
 4. Valitse Käytönvalvonta-asetukset-asetusikkunasta **Lisäasetukset**.
- 3** Valitse Käyttäjäasetukset-ikkunan **McAfee-käyttäjätilit** -kohdasta **Järjestelmänvalvoja** ja valitse sitten **Muokkaa**.
- 4** Kirjoita uusi salasana Muokkaa käyttäjätilit -valintaikkunan **Uusi salasana** -ruutuun ja kirjoita se sitten uudelleen **Anna salasana uudelleen** -ruutuun.
- 5** Valitse **OK**.

[Nouda McAfee-järjestelmänvalvojan salasana](#)

Jos unohdat järjestelmänvalvojan salasanan, voit palauttaa sen.

- 1** Napsauta SecurityCenter-kuvaketta  hiiren kakkospainikkeella ja valitse **Vaihda käyttäjää**.
- 2** Valitse **Käyttäjänimi**-luettelosta **Järjestelmänvalvoja** ja valitse sitten **Unohditko salasanasasi?**
- 3** Kirjoita vastaus salaiseen kysymykseen **Vastaus**-ruutuun.
- 4** Valitse **Lähetä**.

Mahdollisesti sopimattomien Web-kuvien suodattaminen

Käyttäjän ikä- tai kypsyystason mukaan voit suodattaa (estää tai sallia) mahdollisesti sopimattomat kuvat, kun käyttäjä selaa Web-sivustoja. Voit esimerkiksi estää mahdollisesti sopimattomien kuvien näkymisen, kun nuori lapsesi selaa Web-sivustoja, mutta sallia kuvien näkemisen kotona oleville teini-ikäisille ja aikuisille. Oletuksena kuvasuodatus on poistettu käytöstä Aikuinen-ryhmän kaikilta jäseniltä, joten mahdollisesti sopimattomat kuvat ovat kyseisten käyttäjien nähtävissä Web-sivustoja selattaessa. Lisätietoja käyttäjän ikäryhmistä on kohdassa Sisältöluokitusryhmän määrittäminen (sivu 164).

Suodata mahdollisesti sopimattomat Web-kuvat

Oletuksena uudet käyttäjät lisätään Aikuinen-ryhmään ja kuvasuodatus on poistettu käytöstä. Jos haluat estää mahdollisesti sopimattomien kuvien esittämisen, kun tietty käyttäjä selaa Web-sivustoja, voit ottaa kuvasuodatuksen käyttöön. Kukin mahdollisesti sopimaton Web-kuva korvataan automaattisesti staattisella McAfee-kuvalla.

1 Avaa Käyttäjäasetukset-ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Käytönvalvonta-asetukset**.
2. Valitse käytönvalvontatieto-osasta **Määritä**.
3. Valitse Käytönvalvonta-asetukset-asetusikkunasta **Lisäasetukset**.
4. Valitse Käytönvalvonta-asetukset-ikkunasta **Käyttäjäasetukset**.

2 Valitse Käyttäjäasetukset-ikkunasta käyttäjänimi ja valitse sitten **Muokkaa**.

3 Valitse Muokkaa käyttäjätiliä -ikkunan **Kuvasuodatus**-kohdasta **Käytössä**.

4 Valitse **OK**.

Sisältöluokitusryhmän määrittäminen

Käyttäjä voi kuulua johonkin seuraavista sisältöluokitusryhmistä:

- pieni lapsi
- lapsi
- nuorempi teini-ikäinen
- vanhempi teini-ikäinen
- aikuinen.

Tietosuojapalvelu arvioi (estää tai sallii) Web-sisällön sen ryhmän perusteella, johon käyttäjä kuuluu. Tällöin voit estää tai sallia tiettyjen Web-sivustojen näkymisen käyttäjäkohtaisesti kotonasi. Voit esimerkiksi estää Web-sivuston näkymisen käyttäjille, jotka kuuluvat Nuori lapsi -ryhmään, mutta sallia sen näkymisen Nuorempi teini-ikäinen -ryhmän jäsenille. Jos haluat rajoittaa käyttäjän käytettävissä olevia sisältöjä tarkemmin, voit sallia käyttäjän käyttää vain **Suodatetut Web-sivustot** -luettelossa mainittuja sivustoja. Lisätietoja on kohdassa Web-sivustojen suodattaminen (sivu 167).

Oletuksena uusi käyttäjä lisätään Aikuinen-ryhmään. Tällöin kaikki Web-sivustot ovat käytettävissä.

Määritä käyttäjän sisältöluokitusryhmä

Oletuksena uusi käyttäjä lisätään Aikuinen-ryhmään. Tällöin kaikki Web-sivustot ovat käytettävissä. Tarvittaessa voit muuttaa käyttäjän sisältöluokitusryhmää käyttäjän ikä- ja kypsyystason mukaan.

1 Avaa Käyttäjäasetukset-ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Käytönvalvonta-asetukset**.
 2. Valitse käytönvalvontatieto-osasta **Määritä**.
 3. Valitse Käytönvalvonta-asetukset-asetusikkunasta **Lisäasetukset**.
 4. Valitse Käytönvalvonta-asetukset-ikkunasta **Käyttäjäasetukset**.
- 2** Valitse Käyttäjäasetukset-ikkunasta käyttäjänimi ja valitse sitten **Muokkaa**.
- 3** Valitse Muokkaa käyttäjätiliä -ikkunasta **Sisältöluokitus** ja napsauta ikäryhmää, jonka haluat määrittää käyttäjälle.
- Voit estää käyttäjää näkemästä Web-sivustoja, joiden käyttö on estetty **Suodatetut Web-sivustot** -luettelossa, valitsemalla **Tämä käyttäjä voi käyttää vain Suodatetut Web-sivustot -luettelossa mainittuja sivustoja** -valintaruudun.
- 4** Valitse **OK**.

Web-selauksen aikarajoitusten määrittäminen

Jos olet huolestunut vastuuttomasta tai liiallisesta Internetin käytöstä, voit määrittää lapsille Web-selauksen aikarajoitukset. Kun rajoitat lasten Web-selauksen tiettyihin aikoihin, SecurityCenter huolehtii rajoituksista, vaikka olisit poissa kotoa.

Lapset voivat oletuksena selata Internetiä milloin tahansa, mutta voit rajoittaa Internetin käytön tiettyihin päiviin tai kellonaikoihin tai estää Internetin käytön kokonaan. Jos lapsi yrittää käyttää Internetiä estettynä aikana, McAfee ilmoittaa käyttäjälle estosta. Jos estät Internetin käytön kokonaan, lapsi voi käyttää tietokonetta ja muita Internet-ohjelmia, kuten sähköpostia, pikaviestiohjelmia, ftp-ohjelmia, pelejä ym., lukuun ottamatta Web-sivustoja.

Web-selauksen aikarajoitusten määrittäminen

Web-selauksen aikarajaruudun avulla voit määrittää tietyt päivät ja kellonajat, jolloin lapsi voi selata Web-sivuja.

- 1 Avaa Käyttäjäasetukset-ikkuna.
Miten?
 1. Valitse SecurityCenterin Koti-ikkunasta **Käytönvalvonta-asetukset**.
 2. Valitse käytönvalvontatieto-osasta **Määritä**.
 3. Valitse Käytönvalvonta-asetukset-asetusikkunasta **Lisäasetukset**.
 4. Valitse Käytönvalvonta-asetukset-ikkunasta **Käyttäjäasetukset**.
- 2 Valitse Käyttäjäasetukset-ikkunasta käyttäjänimi ja valitse sitten **Muokkaa**.
- 3 Valitse Muokkaa käyttäjätiliä -ikkunan **Internet-aikarajat**-kohdasta hiiren osoittimella päivät ja ajat, jolloin tietty käyttäjä ei voi selata Web-sivuja.
- 4 Valitse **OK**.

Web-sivustojen suodattaminen

Voit suodattaa (estää tai sallia) Web-sivustoja kaikilta paitsi Aikuinen-ryhmään kuuluvilta käyttäjiltä. Voit estää Web-sivuston, jotta lapsi ei pääse kyseiseen sivustoon selatessaan Internetiä. Kun lapsi yrittää käyttää estettyä Web-sivustoa, näyttöön tulee viesti siitä, että McAfee estää sivuston käytön.

Voit sallia Web-sivuston, jos McAfee on torjunut sen oletuksena, mutta haluat antaa lastesi käyttää sivustoa. Lisätietoja Web-sivustoista, jotka McAfee estää oletusarvoisesti, on kohdassa Web-sivustojen suodattaminen avainsanojen avulla (sivu 170). Voit myös päivittää tai poistaa suodatetun Web-sivuston milloin tahansa.

Huomautus: Käyttäjät (mukaan lukien järjestelmänvalvojat), jotka kuuluvat Aikuinen-ryhmään, voivat käyttää myös estettyjä Web-sivustoja. Kirjaudu sisään muuna kuin Aikuinen-ryhmään kuuluvana käyttäjänä, jos haluat testata Web-sivustojen estoa.

Web-sivuston estäminen

Voit estää Web-sivuston, jotta lapsi ei pääse kyseiseen sivustoon selatessaan Internetiä. Kun lapsi yrittää käyttää estettyä Web-sivustoa, näyttöön tulee viesti siitä, että McAfee estää sivuston käytön.

1 Avaa Käytönvalvonta-asetukset-ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Käytönvalvonta-asetukset**.
2. Valitse käytönvalvontatieto-osasta **Määritä**.
3. Varmista Käytönvalvonta-asetukset-asetusikkunasta, että käytönvalvonta on käytössä, ja valitse **Lisäasetukset**.

2 Valitse Käytönvalvonta-asetukset -ikkunasta **Suodatetut Web-sivustot**.

3 Kirjoita Web-sivuston osoite Suodatetut Web-sivustot -ikkunan **http://**-ruutuun ja napsauta **Estä**-painiketta.

4 Valitse **OK**.

Vihje: Voit estää aiemmin sallitun Web-sivuston napsauttamalla Web-sivuston osoitetta **Suodatetut Web-sivustot** -luettelossa ja valitsemalla sitten **Estä**.

Web-sivuston salliminen

Voit sallia Web-sivuston, jotta se on varmasti kaikkien käyttäjien käytettävissä. Jos sallit Web-sivuston, jonka McAfee on estänyt oletusarvoisesti, ohitat oletusasetuksen.

1 Avaa Käytönvalvonta-asetukset-ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Käytönvalvonta-asetukset**.
2. Valitse käytönvalvontatieto-osasta **Määritä**.
3. Varmista Käytönvalvonta-asetukset-asetusikkunasta, että käytönvalvonta on käytössä, ja valitse **Lisäasetukset**.

2 Valitse Käytönvalvonta-asetukset -ikkunasta **Suodatetut Web-sivustot**.

3 Kirjoita Web-sivuston osoite Suodatetut Web-sivustot -ikkunan **http://**-ruutuun ja napsauta **Salli**-painiketta.

4 Valitse **OK**.

Vihje: Voit sallia aiemmin estetyn Web-sivuston napsauttamalla Web-sivuston osoitetta **Suodatetut Web-sivustot** -luettelossa ja valitsemalla sitten **Salli**.

Suodatetun Web-sivuston päivittäminen

Jos Web-sivuston osoite muuttuu tai jos kirjoitit väärän osoitteen, kun estät tai sallit sivuston, voit päivittää osoitteen.

1 Avaa Käytönvalvonta-asetukset-ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Käytönvalvonta-asetukset**.
2. Valitse käytönvalvontatieto-osasta **Määritä**.
3. Varmista Käytönvalvonta-asetukset-asetusikkunasta, että käytönvalvonta on käytössä, ja valitse **Lisäasetukset**.

2 Valitse Käytönvalvonta-asetukset -ikkunasta **Suodatetut Web-sivustot**.

3 Valitse kohde Suodatetut Web-sivustot -ikkunan **Suodatetut Web-sivustot** -luettelosta, muokkaa Web-sivuston osoitetta **http://**-ruudussa ja napsauta sitten **Päivitä**-painiketta.

4 Valitse **OK**.

Suodatetun Web-sivuston poistaminen

Voit poistaa suodatetun Web-sivuston, jos et enää halua estää tai sallia sivustoa.

1 Avaa Käytönvalvonta-asetukset-ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Käytönvalvonta-asetukset**.
2. Valitse käytönvalvontatieto-osasta **Määritä**.
3. Varmista Käytönvalvonta-asetukset-asetusikkunasta, että käytönvalvonta on käytössä, ja valitse **Lisäasetukset**.

2 Valitse Käytönvalvonta-asetukset-ikkunasta **Suodatetut Web-sivustot**.

3 Valitse kohde Suodatetut Web-sivustot -ikkunan **Suodatetut Web-sivustot** -luettelosta ja napsauta sitten **Poista**-painiketta.

4 Valitse **OK**.

Web-sivustojen suodattaminen avainsanojen avulla

Avainsanasuodatuksen avulla voit estää alaikäisiä käyttäjiä vieraillemasta Web-sivuistoissa, jotka sisältävät mahdollisesti sopimattomia sanoja. Kun avainsanojen suodatus on käytössä, sisältö luokitellaan käyttäjille avainsanojen oletusluettelon ja niitä vastaavien sääntöjen avulla käyttäjien sisältöluokitusryhmän mukaan. Vain tiettyyn ryhmään kuuluvat käyttäjät voivat selailla tiettyjä avainsanoja sisältäviä sivustoja. Vain Aikuinen-ryhmään kuuluvat käyttäjät voivat selata Web-sivustoja, jotka sisältävät sanan *porno* ja vain Lapsi-ryhmän jäsenet tai vanhemmat käyttäjät voivat selata sivustoja, jotka sisältävät sanan *huumeet*.

Voit myös lisätä omia avainsanoja oletusarvoiseen luetteloon ja yhdistää ne sisältöluokitusryhmiin. Lisäämäsi avainsanasäännöt ohittavat oletusarvoisen avainsanojen luettelon mahdollisesti vastaavat avainsanat.

Avainsanojen suodatuksen poistaminen käytöstä

Avainsanojen suodatus on käytössä oletuksena, mikä tarkoittaa, että sisältö luokitellaan käyttäjille avainsanojen oletusluettelon ja niitä vastaavien sääntöjen avulla käyttäjien sisältöluokitusryhmän mukaan. Voit poistaa avainsanojen suodatuksen käytöstä milloin tahansa, vaikkakaan McAfee ei suosittele sitä.

1 Avaa Käytönvalvonta-asetukset-ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Käytönvalvonta-asetukset**.
2. Valitse käytönvalvontatieto-osasta **Määritä**.
3. Varmista Käytönvalvonta-asetukset-asetusikkunasta, että käytönvalvonta on käytössä, ja valitse **Lisäasetukset**.

2 Valitse Käytönvalvonta-asetukset-ikkunasta **Avainsanat**.

3 Valitse Avainsanat-ikkunasta **Ei käytössä**.

4 Valitse **OK**.

Estä Web-sivustot avainsanojen perusteella

Jos haluat estää Web-sivustoja sisällön perusteella, mutta et tiedä sivustojen tarkkoja osoitteita, voit estää sivustoja avainsanojen perusteella. Kirjoita vain avainsana ja määritä, mitkä sisältöluokitusryhmät voivat käyttää Web-sivustoja, joilla avainsana esiintyy.

1 Avaa Käytönvalvonta-asetukset-ikkuna.

Miten?

1. Valitse SecurityCenterin Koti-ikkunasta **Käytönvalvonta-asetukset**.
2. Valitse käytönvalvontatieto-osasta **Määritä**.
3. Varmista Käytönvalvonta-asetukset-asetusikkunasta, että käytönvalvonta on käytössä, ja valitse **Lisäasetukset**.
- 2 Valitse Käytönvalvonta-asetukset-ikkunasta **Avainsanat** ja varmista, että avainsanasuodatus on käytössä.
- 3 Kirjoita avainsana **Avainsanaluettelo**-kohdan **Etsi**-ruutuun.
- 4 Määritä vähimmäisikäryhmä **Vähimmäisikä**-liukusäätimen avulla.
Kyseiseen tai vanhempaan ikäryhmään kuuluvat käyttäjät voivat käyttää sivustoja, joilla kyseinen avainsana esiintyy.
- 5 Valitse **OK**.

L U K U 3 2

Tietojen suojaaminen Internetissä

Voit suojata henkilökohtaisia tietojasi ja tiedostojasi estämällä tietojen lähettämisen, kun selaat Web-sivustoja. Voit esimerkiksi estää henkilökohtaisten tietojen (kuten nimien, osoitteiden, luottokorttien ja pankkitilien numeroiden) lähettämisen Internetiin lisäämällä ne estotieto-alueelle.

Huomautus: Privacy Service ei estä henkilökohtaisten tietojen lähettämistä suojattuihin verkkosivustoihin (siis sivustoihin, jotka käyttävät https://-protokollaa), kuten pankkien sivustoihin.

Tässä luvussa

Henkilökohtaisten tietojen suojaaminen 174

Henkilökohtaisten tietojen suojaaminen

Voit estää henkilökohtaisten tietojen (kuten nimien, osoitteiden, luottokorttien ja pankkitilien numeroiden) lähettämisen Internetiin. Jos McAfee havaitsee henkilökohtaisia tietoja esimerkiksi tiedostossa tai lomakkeen kentässä, jota ollaan lähettämässä Internetiin, se toimii seuraavasti.

- Jos olet järjestelmänvalvoja, järjestelmä kehottaa vahvistamaan tietojen lähettämisen.
- Jos et ole järjestelmänvalvoja, estetyt tiedot korvataan tähtimerkeillä (*). Jos esimerkiksi haitallinen Web-sivusto yrittää lähettää luottokorttisi numeroa toiseen tietokoneeseen, numero korvataan tähtimerkeillä.

Suojaa henkilökohtaisia tietoja

Voit estää seuraavantyyppisten henkilökohtaisten tietojen lähettämisen: nimi, osoite, postinumero, sosiaaliturvatunnus, puhelinnumero, luottokorttien numerot, pankkitilien numerot, arvopaperitilit ja puhelinkortit. Jos haluat estää muuntyyppisten henkilökohtaisten tietojen lähettämisen, voit asettaa tyyppiä **muut**.

- 1 Avaa Suojatut tiedot (Protected Information) -ikkuna.
Miten?
 1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
 2. Valitse SecurityCenterin Koti-ikkunasta **Internet & verkko**.
 3. Valitse Internet & verkko -osasta **Määritä**.
 4. Varmista Internet- & verkko-määrittelyt -ikkunasta, että henkilökohtaisten tietojen suojaus on käytössä, ja napsauta **Lisäasetukset**-painiketta.
- 2 Valitse Suojatut tiedot (Protected Information) -ikkunasta **Lisää**.
- 3 Valitse luettelosta estettävän tiedon tyyppi.
- 4 Kirjoita henkilökohtainen tieto ja valitse **OK**.

L U K U 3 3

Salasanojen suojaaminen

Salasanasäiliö on suojattu tallennusalue henkilökohtaisille salasanoillesi. Sen avulla voit tallentaa salasanasasi luottaen siihen, ettei kukaan muu käyttäjä (ei edes järjestelmänvalvoja) saa niitä käyttöönsä.

Tässä luvussa

Salasanasäilön asentaminen 176

Salanasäilön asentaminen

Ennen kuin alat käyttää Salanasäilöä, sinun täytyy asettaa Salanasäilön salasana. Vain käyttäjät, jotka tietävät salanasasi, voivat käyttää Salanasäilöäsi. Jos unohdat Salanasäilön salasanan, voit nollata sen. Kaikki aiemmin tallennetut salasanat kuitenkin poistetaan.

Kun olet asettanut Salanasäilön salasanan, voit lisätä, muokata ja poistaa säilön salasanoja. Voit myös vaihtaa Salanasäilön salasanan milloin tahansa.

Lisää salasana

Jos salasanojen muistaminen tuottaa ongelmia, voit lisätä salasanat Salanasäilöön. Salanasäilö on suojattu tallennusalue, jota voivat käyttää vain salasanan tietävät käyttäjät.

- 1 Avaa Salanasäilö-ikkuna.
Miten?
 1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
 2. Valitse SecurityCenterin Koti-ikkunasta **Internet & verkko**.
 3. Valitse Internet & verkko -osasta **Määritä**.
 4. Valitse Internet- & Verkko-määrittelyt -ikkunan **Salanasäilö** -kohdasta **Lisäasetukset**.
- 2 Kirjoita Salanasäilön salanasasi **Salasana**-tekstiruutuun ja kirjoita se uudelleen **Vahvista salasana** -tekstiruutuun.
- 3 Valitse **Avaa**.
- 4 Valitse Salanasäilö-ikkunasta **Lisää**.
- 5 Kirjoita salasanan kuvaus (esimerkiksi mihin salasana on) **Kuvaus**-tekstiruutuun ja kirjoita salasana **Salasana**-tekstiruutuun.
- 6 Valitse **OK**.

Muokkaa salasanaa

Varmista, että Salanasäilöön tallennetut salanasasi ovat täsmällisiä ja luotettavia päivittämällä ne aina, kun muutat salasanaa.

- 1 Avaa Salanasäilö-ikkuna.
Miten?

1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
2. Valitse SecurityCenterin Koti-ikkunasta **Internet & verkko**.
3. Valitse Internet & verkko -osasta **Määritä**.
4. Valitse Internet- & Verkko-määritykset -ikkunan **Salanasäilö** -kohdasta **Lisäasetukset**.
- 2 Kirjoita Salanasäilön salasana **Salasana**-tekstiruutuun.
- 3 Valitse **Avaa**.
- 4 Valitse salasana Salanasäilö-ikkunasta ja valitse sitten **Muokkaa**.
- 5 Muokkaa salasanan kuvausta (esimerkiksi mihin salasana on) **Kuvaus**-tekstiruudussa tai muokkaa salasanaa **Salasana**-tekstiruudussa.
- 6 Valitse **OK**.

Poista salasana

Voit poistaa salasanoja Salanasäilöstä milloin tahansa. Säilöstä poistettuja salasanoja ei voi palauttaa.

- 1 Avaa Salanasäilö-ikkuna.
Miten?
 1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
 2. Valitse SecurityCenterin Koti-ikkunasta **Internet & verkko**.
 3. Valitse Internet & verkko -osasta **Määritä**.
 4. Valitse Internet- & Verkko-määritykset -ikkunan **Salanasäilö** -kohdasta **Lisäasetukset**.
- 2 Kirjoita Salanasäilön salasana **Salasana**-tekstiruutuun.
- 3 Valitse **Avaa**.
- 4 Valitse salasana Salanasäilö-ikkunasta ja valitse sitten **Poista**.
- 5 Valitse Poiston vahvistus -valintaikkunasta **Kyllä**.

Vaihda Salanasäilön salasana

Voit vaihtaa Salanasäilön salasanan milloin tahansa.

- 1 Avaa Salanasäilö-ikkuna.
Miten?

1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
2. Valitse SecurityCenterin Koti-ikkunasta **Internet & verkko**.
3. Valitse Internet & verkko -osasta **Määritä**.
4. Valitse Internet- & Verkko-määritykset -ikkunan **Salanasäilö** -kohdasta **Lisäasetukset**.
- 2 Kirjoita Salanasäilö-ikkunan **Salasana**-ruutuun nykyinen salanasasi ja valitse sitten **Avaa**.
- 3 Valitse Salanasäilö-ikkunasta **Vaihda salasana**.
- 4 Kirjoita uusi salasana **Valitse salasana** -ruutuun ja kirjoita se uudelleen **Anna salasana uudelleen** -ruutuun.
- 5 Valitse **OK**.
- 6 Valitse Salanasäilön salasana vaihdettu -valintaikkunasta **OK**.

Nollaa salanasäilön salasana

Jos unohdat Salanasäilön salasanan, voit nollata sen. Kaikki aiemmin tallennetut salasanat kuitenkin poistetaan.

- 1 Avaa Salanasäilö-ikkuna.
Miten?
 1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
 2. Valitse SecurityCenterin Koti-ikkunasta **Internet & verkko**.
 3. Valitse Internet & verkko -osasta **Määritä**.
 4. Valitse Internet- & Verkko-määritykset -ikkunan **Salanasäilö** -kohdasta **Lisäasetukset**.
- 2 Kirjoita uusi salasana **Palauta salanasäilö** -ikkunan **Salasana**-ruutuun ja kirjoita se uudelleen **Anna salasana uudelleen** -tekstiruutuun.
- 3 Valitse **Palauta**.
- 4 Valitse Salasan nollauksen vahvistus -valintaikkunasta **Kyllä**.

L U K U 3 4

McAfee Data Backup

Data Backup -ohjelman avulla voit estää tietojen tahattoman menettämisen arkistoimalla tiedostosi CD- tai DVD-levylle, USB-asetalle, ulkoiselle kiintolevylle tai verkkoasemalle. Paikallisen arkistoinnin ansiosta voit arkistoida (varmuuskopioida) tiedot CD- tai DVD-levylle, USB-asetalle, ulkoiselle kiintolevylle tai verkkoasemalle. Tällöin sinulla on paikallinen kopio tiedoista, asiakirjoista ja muista henkilökohtaisista materiaaleista niiden tahattoman menettämisen varalta.

Voit tutustua Data Backupin suosituimpiin ominaisuuksiin, ennen kuin alat käyttää sitä. Lisätietoja näiden ominaisuuksien määrittämisestä ja käyttämisestä on Data Backupin ohjeessa. Kun olet perehtynyt ohjelman ominaisuuksiin, varmista, että sinulla on riittävästi arkistointimediaa paikallisten arkistojen luomista varten.

Tässä luvussa

Ominaisuudet.....	180
Tiedostojen arkistointi.....	181
Arkistoitujen tiedostojen käsitteleminen	189

Ominaisuudet

Data Backup tarjoaa seuraavat valokuvien, musiikin ja muiden tärkeiden tiedostojen tallennus- ja palautusominaisuudet.

Ajoitettu paikallinen arkistointi

Suojaa tietojasi arkistoimalla tiedostoja ja kansioita CD- tai DVD-levyille, USB-asemalle, ulkoiselle kiintolevyllä tai verkkoasemalle. Kun olet muodostanut ensimmäisen arkiston, lisääarkistointi suoritetaan puolestasi automaattisesti.

Yhden napsautuksen palautustoiminto

Jos tiedostoja ja kansiota poistetaan vahingossa tai ne vioittuvat tietokoneellasi, voit palauttaa viimeisimmän arkistoidun version käytetyltä arkistointimedialta.

Pakkaus ja sala

Oletusarvoisesti arkistoidut tiedostot pakataan, mikä säästää tilaa arkistointimedialla. Lisäsuojaustoimenpiteenä arkistosi salataan oletusarvoisesti.

LUKU 35

Tiedostojen arkistointi

McAfee Data Backupin avulla voit arkistoida tietokoneella olevista tiedostoista kopion CD- tai DVD-levylle, USB-asemalle, ulkoiselle kiintolevylle tai verkkoasemalle. Käyttämällä tätä tiedostojen arkistointitapaa voit varmistaa, että tahattomasti menetetyt tai vahingoittuneet tiedot ovat helposti noudettavissa.

Ennen kuin aloitat tiedostojen arkistoinnin, sinun on valittava oletusarkistointisijainti (CD- tai DVD-levy, USB-asema, ulkoinen kiintolevy tai verkkoasema). Osan asetuksista, kuten kansiot ja arkistoitavat tiedostotyytit, McAfee on määrittänyt jo valmiiksi. Voit kuitenkin muuttaa näitä asetuksia.

Kun olet määrittänyt paikallisen arkiston asetukset, voit muokata oletusasetuksia ja määrittää, kuinka usein haluat Data Backupin suorittavan täydellisen arkistoinnin ja pika-arkistoinnin. Voit suorittaa manuaalisen arkistoinnin milloin tahansa.

Tässä luvussa

Arkiston asetusten määrittäminen	182
Täydellisen arkistoinnin ja pika-arkistoinnin suorittaminen.....	187

Arkiston asetusten määrittäminen

Ennen kuin aloitat tietojen arkistoinnin, sinun on määritettävä tietyt paikallisen arkiston asetukset. Sinun on esimerkiksi määritettävä tarkkailukohteet ja tarkkailtavat tiedostotyyppit. Tarkkailukohteet ovat tietokoneessa olevia kansioita, joita Data Backup valvoo uusien tiedostojen ja tiedostojen muutosten varalta. Tarkkailtavat tiedostotyyppit ovat tiedostotyyppijä (esimerkiksi .doc ja .xls), jotka Data Backup arkistoi tarkkailukohteissa. Oletusarvoisesti Data Backup tarkkailee kaikkia tarkkailukohteisiin tallennettuja tiedostotyyppijä.

Voit määrittää kahdentyyppisiä tarkkailukohteita: tärkeitä tarkkailukohteita ja melko tärkeitä tarkkailukohteita. Jos määrität tärkeän tarkkailukohteen, Data Backup arkistoi kaikki kyseisen kansion ja sen alihakemistojen tarkkailtavien tiedostotyyppien mukaiset tiedostot. Jos määrität melko tärkeän tarkkailukohteen, Data Backup arkistoi ainoastaan kyseisen kansion tarkkailtavien tiedostotyyppien mukaiset tiedostot (ei alihakemistoja). Oletusarvoisesti Windowsin työpöytä ja Omat tiedostot määritetään tärkeiksi tarkkailukohteiksi.

Kun olet määrittänyt tarkkailtavat tiedostotyyppit ja tarkkailukohteet, sinun on määritettävä arkistointisijainti (CD- tai DVD-levy, USB-asema, ulkoinen kiintolevy tai verkkoasema, jolle arkistoitavat tiedot tallennetaan). Voit muuttaa arkistointisijaintia milloin tahansa.

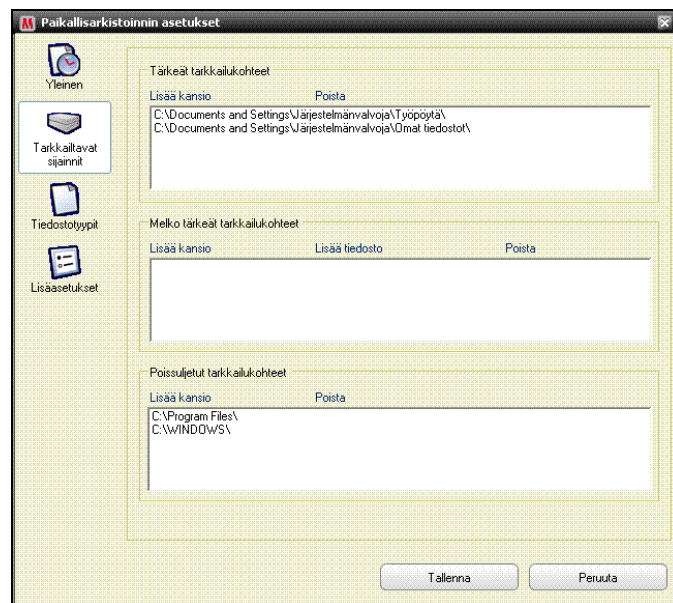
Turvallisuussyistä tai koon rajoittamiseksi salaus tai pakkaus otetaan arkistoiduissa tiedostoissa oletusarvoisesti käyttöön. Salattujen tiedostojen sisältö muunnetaan tekstistä koodiksi siten, että henkilöt, jotka eivät osaa purkaa salausta, eivät voi lukea tietoja. Pakatut tiedostot pakataan muotoon, joka minimoi niiden tallentamiseen tai siirtämiseen vaadittavan levytilan määrän. Voit poistaa salauksen tai pakkauksen käytöstä milloin tahansa, vaikkakaan McAfee ei suosittele sitä.

Lisää kohde arkistoon

Voit määrittää arkistointia varten kahdentyyppisiä tarkkailukohteita: tärkeitä ja melko tärkeitä. Jos määrität tärkeän tarkkailukohteen, Data Backup valvoo kyseisen kansion ja sen alihakemistojen sisältöä muutosten varalta. Jos määrität melko tärkeän tarkkailukohteen, Data Backup valvoo ainoastaan kyseisen kansion sisältöä (ei alihakemistoja).

Tarkkailukohteen lisääminen arkistoon:

- 1 Valitse **Paikallinen arkisto** -välilehti.
- 2 Valitse vasemmasta ruudusta **Asetukset**.
- 3 Valitse Paikallisarkistoinnin asetukset -valintaikkunasta **Tarkkailukohteet**.



- 4 Valitse jokin seuraavista:
 - Jos haluat arkistoida kansion ja sen alikansioiden sisällön, valitse **Tärkeät tarkkailukohteet** -kohdasta **Lisää kansio**.
 - Jos haluat arkistoida kansion sisällön, mutta et sen alikansioiden sisältöä, valitse **Melko tärkeitä tarkkailukohteet** -kohdasta **Lisää kansio**.
- 5 Siirry Etsi kansio -valintaikkunassa tarkkailtavan kansion kohdalle ja napsauta **OK**.
- 6 Valitse **Tallenna**.

Vihje: Jos haluat Data Backupin tarkkailevan kansiota, jota et ole vielä luonut, lisää kansio valitsemalla Etsi kansio -valintaikkunasta **Tee uusi kansio** ja määritä se samalla tarkkailukohteeksi.

Määritä arkistotiedostojen tyypit

Voit määrittää, mitkä tärkeiden tai melko tärkeiden tarkkailukohteiden tiedostotyytit arkistoidaan. Voit valita olemassa olevasta tiedostotyyppien luettelosta tai lisätä luetteloon uuden tyytin.

Arkistoitavien tiedostotyyppien määrittäminen:

- 1 Valitse **Paikallinen arkisto** -välilehti.
- 2 Valitse vasemmasta ruudusta **Asetukset**.
- 3 Valitse Paikallisarkistoinnin asetukset -valintaikkunasta **Tiedostotyytit**.
- 4 Laajenna tiedostotyyppien luettelot ja valitse arkistoitavien tiedostotyyppien vieressä olevat valintaruudut.
- 5 Valitse **Tallenna**.

Vihje: Jos haluat lisätä uuden tiedostotyytin **Valitut tiedostotyytit** -luetteloon, kirjoita tiedostotunniste **Lisää mukautettu tiedostotyyppi kohtaan 'Muut'** -ruutuun ja valitse **Lisää**. Uusi tiedostotyyppi muuttuu automaattisesti tarkkailtavaksi tiedostotyyppiksi.

Sulje kohde arkistosta pois

Voit sulkea kohteen arkistosta pois, jos haluat estää kyseisen kohteen (kansion) ja sisällön arkistoinnin.

Kohteen sulkeminen arkistosta pois:

- 1 Valitse **Paikallinen arkisto** -välilehti.
- 2 Valitse vasemmasta ruudusta **Asetukset**.
- 3 Valitse Paikallisarkistoinnin asetukset -valintaikkunasta **Tarkkailtavat kansiot**.
- 4 Valitse **Poissuljetut tarkkailukohteet** -kohdasta **Lisää kansio**.
- 5 Siirry Etsi kansio -valintaikkunassa poissuljettavan kohteen kohdalle, valitse se ja napsauta **OK**.
- 6 Valitse **Tallenna**.

Vihje: Jos haluat Data Backupin sulkevan kansion pois, jota et ole vielä luonut, lisää kansio valitsemalla Etsi kansio -valintaikkunasta **Tee uusi kansio** ja sulje se samalla pois.

Muuta arkiston sijaintia

Kun muutat arkiston sijaintia, aikaisemmin eri kohteeseen arkistoidut tiedostot merkitään *Ei koskaan arkistoitu*.

Arkiston sijainnin muuttaminen:

- 1 Valitse **Paikallinen arkisto** -välilehti.
- 2 Valitse vasemmasta ruudusta **Asetukset**.
- 3 Valitse **Muuta arkiston sijaintia**.
- 4 Valitse Arkiston sijainti -valintaikkunassa yksi seuraavista vaihtoehtoista:
 - Valitse **Valitse tallentava CD/DVD-asema**, valitse tietokoneen CD- tai DVD-asema tietokoneen **Tallentava asema** -luettelosta ja valitse **Tallenna**.
 - Valitse **Valitse kohdeasema**, siirry USB-aseman, paikallisen aseman tai ulkoisen kiintolevyaseman kohdalle, valitse se ja valitse sitten **OK**.
 - Valitse **Valitse verkkosijainti**, siirry verkkokansion kohdalle ja valitse **OK**.
- 5 Vahvista uusi arkistointisijainti **Valittu arkistointisijainti** -kohdasta ja valitse **OK**.
- 6 Valitse vahvistusvalintaikkunasta **OK**.
- 7 Valitse **Tallenna**.

Poista arkiston salaus ja pakkaus käytöstä

Arkistoitujen tiedostojen salaaminen suojaa tietojesi luottamuksellisuutta muuttamalla tiedostojen sisältöä siten, että tietoja ei voi lukea. Arkistoitujen tiedostojen pakkaaminen pienentää tiedostojen kokoa. Oletusarvoisesti sekä salaus että pakkaus ovat käytössä, mutta voit poistaa nämä asetukset käytöstä milloin tahansa.

Arkiston salauksen ja pakkauksen poistaminen käytöstä

- 1 Valitse **Paikallinen arkisto** -välilehti.
- 2 Valitse vasemmasta ruudusta **Asetukset**.
- 3 Valitse Paikallisarkistoinnin asetukset -valintaikkunasta **Lisäasetukset**.
- 4 Poista **Paranna suojausta ottamalla salaus käyttöön** -valintaruudun valinta.
- 5 Poista **Vähennä käytettävän levytilan määrää ottamalla pakkaus käyttöön** -valintaruudun valinta.
- 6 Valitse **Tallenna**.

Huomaa: McAfee suosittelee, että et poista salausta ja pakkausta käytöstä tiedostoja arkistoidessa.

Täydellisen arkistoinnin ja pika-arkistoinnin suorittaminen

Voit suorittaa kahdentyyppisen arkistoinnin: täydellisen arkistoinnin tai pika-arkistoinnin. Kun suoritat täydellisen arkistoinnin, arkistoit kaikki tarkkailtavien tiedostotyyppien ja tarkkailukohteiden tiedot, jotka olet määrittänyt. Kun suoritat pika-arkistoinnin, arkistoit vain ne tarkkailtavat tiedostot, jotka ovat muuttuneet edellisen täydellisen arkistoinnin tai pika-arkistoinnin jälkeen.

Oletusarvoisesti Data Backup on ajoitettu suorittamaan tarkkailukohteissa olevien tarkkailtavien tiedostotyyppien täydellinen arkistointi maanantaisin klo 9.00 ja pika-arkistointi 48 tuntia edellisen täydellisen arkistoinnin tai pika-arkistoinnin jälkeen. Ajoittamalla voidaan varmistaa, että tiedostoista on aina olemassa ajan tasalla oleva arkisto. Jos et halua arkistoida 48 tunnin välein, voit mukauttaa aikataulun omiin tarpeisiisi.

Jos haluat arkistoida tarkkailukohteiden sisällön tarvittaessa, voit tehdä tämän milloin tahansa. Jos esimerkiksi muutat tiedostoa ja haluat arkistoida sen, mutta Data Backupia ei ole ajoitettu suorittamaan täydellistä arkistointia tai pika-arkistointia vielä muutamaan tuntiin, voit arkistoida tiedostot manuaalisesti. Kun arkistoit tiedostot manuaalisesti, automaattiselle arkistoinnille asetettu aikaväli nollataan.

Voit myös keskeyttää automaattisen tai manuaalisen arkistoinnin, jos se tapahtuu sopimattomaan aikaan. Jos esimerkiksi olet suorittamassa resursseja vaativaa tehtävää ja automaattinen arkistointi käynnistyy, voit keskeyttää sen. Kun keskeytät automaattisen arkistoinnin, automaattiselle arkistoinnille asetettu aikaväli nollataan.

Ajoita automaattinen arkistointi

Määrittämällä täydellisen arkistoinnin ja pika-arkistoinnin toistumistiheyden voit varmistaa tietojesi jatkuvan suojauksen.

Automaattisen arkistoinnin ajoittaminen:

- 1 Valitse **Paikallinen arkisto** -välilehti.
- 2 Valitse vasemmasta ruudusta **Asetukset**.
- 3 Valitse Paikallisarkistoinnin asetukset -valintaikkunasta **Yleinen**.
- 4 Jos haluat suorittaa täydellisen arkistoinnin päivittäin, viikoittain tai kuukausittain, valitse **Täydellinen arkistointi joka** -kohdasta yksi seuraavista:
 - **Päivä**
 - **Viikko**

- **Kuukausi**

5 Valitse sen päivän vieressä oleva valintaruutu, jolloin haluat suorittaa täydellisen arkistoinnin.

6 Valitse arvo **Klo**-luettelosta ja määritä ajankohta, jolloin haluat suorittaa täydellisen arkistoinnin.

7 Jos haluat suorittaa pika-arkistoinnin päivittäin tai tunneittain, valitse **Pika-arkistointi**-kohdasta yksi seuraavista:

- **Tunti**

- **Päivä**

8 Kirjoita toistumistiheyttä ilmaiseva arvo **Pika-arkistointi joka** -ruutuun.

9 Valitse **Tallenna**.

[Keskeytä automaattinen arkistointi](#)

Data Backup arkistoi tarkkailukohteissa olevat tiedostot automaattisesti määrittämäsi aikataulun mukaan. Jos automaattinen arkistointi on käynnissä ja haluat kuitenkin keskeyttää sen, voit tehdä tämän milloin tahansa.

Automaattisen arkistoinnin keskeyttäminen:

1 Valitse vasemmasta ruudusta **Keskeytä arkistointi**.

2 Valitse vahvistusvalintaikkunasta **Kyllä**.

Huomaa: **Keskeytä arkistointi** -linkki tulee näkyviin vain silloin, kun arkistointi on käynnissä.

[Suorita manuaalinen arkistointi](#)

Vaikka automaattinen arkistointi suoritetaan ennalta määrätyn aikataulun mukaan, voit suorittaa pika-arkistoinnin tai täydellisen arkistoinnin milloin tahansa. Pika-arkistoinnissa arkistoidaan ainoastaan ne tiedostot, jotka ovat muuttuneet viimeisimmän täydellisen arkistoinnin tai pika-arkistoinnin jälkeen. Täydellisessä arkistoinnissa arkistoidaan kaikkien tarkkailukohteiden kaikki tiedostotyytit.

Pika-arkistoinnin tai täydellisen arkistoinnin suorittaminen manuaalisesti:

1 Valitse **Paikallinen arkisto** -välilehti.

2 Jos haluat suorittaa pika-arkistoinnin, valitse vasemmasta ruudusta **Pika-arkistointi**.

3 Jos haluat suorittaa täydellisen arkistoinnin, valitse vasemmasta ruudusta **Täydellinen arkistointi**.

4 Vahvista levytilasi ja asetukset Valmis aloittamaan arkistoinnin -valintaikkunasta ja valitse sitten **Jatka**.

LUKU 36

Arkistoitujen tiedostojen käsitleminen

Kun olet arkistoinut tiedostot, voit käsitellä niitä Data Backupilla. Arkistoidut tiedostot esitetään perinteisessä resurssienhallintanäytössä, mikä helpottaa niiden hakua. Kun arkistosi kasvaa, voit haluta lajitella tiedostoja tai etsiä niitä. Voit myös avata tiedostoja resurssienhallintanäytössä ja tarkastella niiden sisältöä tiedostoja noutamatta.

Voit noutaa tiedostoja arkistosta, jos tiedoston paikallinen kopio vanhentuu, puuttuu tai vioittuu. Data Backup tarjoaa myös tietoja, jotka ovat välttämättömiä paikallisten arkistojen ja tallennusvälineiden hallintaan.

Tässä luvussa

Paikallisen arkiston hallintaohjelman käyttäminen ..	190
Arkistoitujen tiedostojen palauttaminen	192
Arkistojen hallinta	194

Paikallisen arkiston hallintaohjelman käyttäminen

Paikallisen arkiston hallintaohjelman avulla voit tarkastella ja käsitellä paikallisesti arkistoituja tiedostoja. Voit tarkastella kunkin tiedoston nimeä, tyyppiä, sijaintia, kokoa, tilaa (arkistoitu, arkistoimaton, arkistointi käynnissä) ja viimeisimmän arkistoinnin ajankohtaa. Voit myös luokitella tiedostot näiden ehtojen mukaan.

Jos arkisto on suuri, voit löytää tiedoston nopeasti etsimällä. Voit etsiä antamalla tiedoston nimen tai polun kokonaan tai osittain, minkä jälkeen voit tarkentaa hakua määrittelemällä tiedoston likimääräisen koon ja viimeisimmän arkistoinnin ajankohdan.

Kun löydät tiedoston, voit avata sen paikallisen arkiston hallintaohjelman avulla. Data Backup avaa tiedoston omalla ohjelmallaan, jolloin voit muokata sitä paikallisen arkiston hallintaohjelmasta poistumatta. Tiedosto tallennetaan tietokoneella alkuperäiseen tarkkailukohteeseen, ja se arkistoidaan automaattisesti määrittämäsi arkistointiaikataulun mukaan.

Lajittele arkistoidut tiedostot

Voit lajitella arkistoidut tiedostot ja kansiot seuraavien ehtojen mukaan: nimi, tiedostotyyppi, koko, tila (arkistoitu, arkistoimaton, arkistointi käynnissä), viimeisimmän arkistoinnin ajankohta tai tiedostojen sijainti tietokoneella (polku).

Arkistoitujen tiedostojen lajitteleminen:

- 1 Valitse **Paikallinen arkisto** -välilehti.
- 2 Valitse oikeasta ruudusta sarakkeen nimi.

Etsi arkistoitua tiedostoa

Jos arkistoitujen tiedostojen varasto on suuri, voit löytää tiedoston nopeasti etsimällä. Voit etsiä antamalla tiedoston nimen tai polun kokonaan tai osittain, minkä jälkeen voit tarkentaa hakua määrittelemällä tiedoston likimääräisen koon ja viimeisimmän arkistoinnin ajankohdan.

Arkistoidun tiedoston etsiminen:

- 1 Kirjoita tiedoston nimi kokonaan tai osittain näytön yläreunassa olevaan **Etsi**-ruutuun ja paina ENTER.
- 2 Kirjoita polku kokonaan tai osittain **Osa polusta tai koko polku** -ruutuun.
- 3 Määritä etsittävän tiedoston likimääräinen koko seuraavasti:
 - Valitse **<100 kt, <1 Mt tai >1 Mt**.
 - Valitse **Koko kilotavuina** ja määritä sopivat arvot ruutuihin.

- 4 Määritä tiedoston viimeisimmän online-varmuuskopioinnin likimääräinen ajankohta seuraavasti:
- Valitse **Tällä viikolla, Tässä kuussa** tai **Tänä vuonna**.
 - Valitse **Määritä päivämäärät**, valitse luettelosta **Arkistoitu** ja valitse likimääräisen päivämäärän arvot päivämääräluetteloista.
- 5 Valitse **Etsi**.

Huomaa: Jos et tiedä viimeisimmän arkistoinnin likimääräistä kokoa tai ajankohtaa, valitse **Tuntematon**.

[Avaa arkistoitu tiedosto](#)

Voit tarkastella arkistoidun tiedoston sisältöä avaamalla sen paikallisen arkiston hallintaohjelman avulla.

Arkistoitujen tiedostojen avaaminen:

- 1 Valitse **Paikallinen arkisto** -välilehti.
- 2 Valitse oikeasta ruudusta tiedostonimi ja sitten **Avaa**.

Vihje: Voit avata arkistoidun tiedoston kaksoisnapsauttamalla sen nimeä.

Arkistoitujen tiedostojen palauttaminen

Jos tarkkailtava tiedosto vioittuu, katoaa tai poistetaan vahingossa, voit palauttaa siitä tehdyn kopion paikallisesta arkistosta. Tästä syystä on tärkeää varmistaa, että arkistoit tiedostosi säännöllisesti. Paikallisesta arkistosta voit palauttaa myös vanhempia tiedostoversioita. Jos esimerkiksi arkistoit tiedoston säännöllisesti, mutta haluat palata sen aikaisempaan versioon, voit etsiä tiedoston sen arkistosijainnista. Jos arkistointisijainti on paikallinen asema tai verkkoasema, voit etsiä tiedoston selaamalla. Jos arkistointisijainti on ulkoinen kiintolevyasema tai USB-asema, sinun on liitettävä asema tietokoneeseen ja sen jälkeen etsittävä tiedostoa selaamalla. Jos arkistointisijainti on CD- tai DVD-levy, sinun on asetettava levy tietokoneeseen ja sen jälkeen etsittävä tiedostoa selaamalla.

Voit myös palauttaa yhdeltä tietokoneelta arkistoimasi tiedostot toisella tietokoneella. Jos olet esimerkiksi arkistoinut tiedostoja tietokoneeseen A liitetylle ulkoiselle kiintolevyasemalle, voit palauttaa kyseiset tiedostot tietokoneella B. Tällöin sinun on asennettava McAfee Data Backup tietokoneelle B ja liitettävä ulkoinen kiintolevyasema siihen. Sen jälkeen voit etsiä tiedostot Data Backupista selaamalla, ja ne lisätään **Puuttuvat tiedostot** -luetteloon palauttamista varten.

Lisätietoja tiedostojen arkistoinnista on kohdassa Tiedostojen arkistointi. Jos poistat tarkkailtavan tiedoston arkistosta tahallisesti, voit poistaa merkinnän myös **Puuttuvat tiedostot** -luettelosta.

Palauta puuttuvia tiedostoja paikallisesta arkistosta

Data Backupin paikallisen arkiston avulla voit noutaa paikallisen tietokoneesi tarkkailtavasta kansista puuttuvat tiedot. Jos esimerkiksi tiedosto siirretään tarkkailtavasta kansista tai se poistetaan, mutta se on jo arkistoitu, voit palauttaa sen paikallisesta arkistosta.

Puuttuvan tiedoston palauttaminen paikallisesta arkistosta:

- 1 Valitse **Paikallinen arkisto** -välilehti.
- 2 Valitse näytön alareunasta **Puuttuvat tiedostot** -välilehti ja valitse palautettavan tiedoston nimen vieressä oleva valintaruutu.
- 3 Valitse **Palauta**.

Vihje: Voit palauttaa kaikki **Puuttuvat tiedostot** -luettelossa olevat tiedostot valitsemalla **Palauta kaikki**.

Palauta tiedoston aikaisempi versio paikallisesta arkistosta

Jos haluat palauttaa arkistoidun tiedoston aikaisemman version, voit etsiä sen ja lisätä sen **Puuttuvat tiedostot** -luetteloon. Sen jälkeen voit palauttaa tiedoston kuin minkä tahansa muun **Puuttuvat tiedostot** -luettelossa olevan tiedoston.

Tiedoston aikaisemman version palauttaminen paikallisesta arkistosta:

- 1 Valitse **Paikallinen arkisto** -välilehti.
- 2 Valitse näytön alareunassa olevasta **Puuttuvat tiedostot** -välilehdestä **Selaa** ja siirry sijaintiin, jonne arkisto on tallennettu.

Arkistoitujen kansioiden nimet ovat seuraavassa muodossa: `cre ddmmyy_hh-mm-ss_***`, jossa `ddmmyy` on tiedostojen arkistointipäivämäärä, `hh-mm-ss` on tiedostojen arkistointiaika ja `***` on joko `Full` tai `Inc`, sen mukaan, suoritettiin täydellinen arkistointi vai pika-arkistointi.

- 3 Valitse sijainti ja sitten **OK**.

Valitussa sijainnissa olevat tiedostot ilmestyvät **Puuttuvat tiedostot** -luetteloon, ja ne voidaan palauttaa. Lisätietoja on kohdassa **Palauta puuttuvia tiedostoja paikallisesta arkistosta**.

Poista tiedostoja Puuttuvat tiedostot -luettelosta

Kun arkistoitu tiedosto siirretään tarkkailtavasta kansioista tai se poistetaan, se ilmestyy automaattisesti **Puuttuvat tiedostot** -luetteloon. Tämä varoittaa arkistoitujen tiedostojen ja tarkkailtavissa kansioissa olevien tiedostojen välisestä ristiriidasta. Jos tiedosto poistettiin tai siirrettiin pois tarkkailtavasta kansioista tahallisesti, voit poistaa tiedoston **Puuttuvat tiedostot** -luettelosta.

Tiedoston poistaminen Puuttuvat tiedostot -luettelosta:

- 1 Valitse **Paikallinen arkisto** -välilehti.
- 2 Valitse näytön alareunasta **Puuttuvat tiedostot** -välilehti ja valitse poistettavan tiedoston nimen vieressä oleva valintaruutu.
- 3 Valitse **Poista**.

Vihje: Voit poistaa kaikki **Puuttuvat tiedostot** -luettelossa olevat tiedostot valitsemalla **Poista kaikki**.

Arkistojen hallinta

Voit tarkastella täydellisten arkistojen ja pika-arkistojen tietojen yhteenvetoa milloin tahansa. Voit esimerkiksi tarkastella tietoja tarkkailtavien tietojen määrästä, arkistoitujen tietojen määrästä ja tarkkailtavien, mutta vielä arkistoimattomien tietojen määrästä. Voit tarkastella myös arkistointiaikatauluun liittyviä tietoja, kuten edellisen ja seuraavan arkistoinnin päivämäärää.

Näytä arkistointitoimintojen yhteenveto

Voit tarkastella arkistointitoimintoihin liittyviä tietoja milloin tahansa. Voit esimerkiksi tarkastella arkistoitujen tiedostojen prosentuaalista määrää, tarkkailtavien tietojen kokoa, arkistoitujen tietojen kokoa ja tarkkailtavien, mutta vielä arkistoimattomien tietojen kokoa. Voit tarkastella myös edellisen ja seuraavan arkistoinnin päivämäärää.

Varmuuskopiointitoimintojen yhteenvedon näyttäminen:

- 1 Valitse **Paikallinen arkisto** -välilehti.
- 2 Valitse näytön yläreunasta **Tilin yhteenveto**.

L U K U 3 7

McAfee QuickClean

QuickClean parantaa tietokoneen suorituskykyä poistamalla tiedostot, jotka voivat vain viedä turhaan tilaa tietokoneessa. Ohjelmisto tyhjentää roskakorin ja poistaa väliaikaiset tiedostot, pikakuvakkeet, kadonneet tiedostopirstaleet, rekisteritiedostot, välimuistiin tallennetut tiedostot, evästeet, selaimen historiatiedostot, lähetetyt ja poistetut sähköpostiviestit, viimeksi käytetyt tiedostot, ActiveX-tiedostot ja järjestelmän palautuspistetiedostot. QuickClean suojaa yksityisyyttäsi myös käyttämällä McAfee Shredderiä sellaisten kohteiden turvalliseen ja pysyvään poistamiseen, jotka voivat sisältää arkaluonteisia ja henkilökohtaisia tietoja, kuten nimesi ja osoitteesi. Lisätietoja tiedostojen tuhoamisesta on McAfee Shredderin ohjeessa.

Levyn eheytyys järjestää tietokoneessa olevat tiedostot ja kansiot siten, että ne eivät hajoa osiin (pirstoudu), kun ne tallennetaan tietokoneen kiintolevylle. Eheyttämällä kiintolevyä säännöllisin väliajoin voit varmistaa, että pirstoutuneet tiedostot ja kansiot yhdistetään, minkä ansiosta voit käyttää niitä myöhemmin nopeammin.

Jos et halua suorittaa tietokoneen ylläpitoa manuaalisesti, voit ajoittaa sekä QuickCleanin että Levyn eheytyksen käynnistymään automaattisesti ja itsenäisesti niin usein kuin haluat.

Huomautus: SecurityCenter raportoi kriittiset ja ei-kriittiset suojausongelmat heti, kun se havaitsee ne. Jos tarvitset apua suojausongelmien selvittämisessä, voit käyttää McAfee Virtual Technician -palvelua.

Tässä luvussa

QuickCleanin toiminnot.....	196
Tietokoneen puhdistaminen.....	197
Tietokoneen eheyttäminen	200
Tehtävän ajoittaminen	201

QuickCleanin toiminnot

QuickCleanissä on erilaisia tyhjennysohjelmia, joiden avulla voit poistaa tarpeettomat tiedostot nopeasti ja turvallisesti. Poistamalla nämä tiedostot voit lisätä tietokoneesi kiintolevyllä olevaa tilaa ja parantaa sen suorituskykyä.

Tietokoneen puhdistaminen

QuickClean poistaa tiedostot, jotka voivat turhaan viedä tilaa tietokoneessa. Ohjelmisto tyhjentää Roskakorin ja poistaa väliaikaiset tiedostot, pikakuvakkeet, kadonneet tiedostopirstaleet, rekisteritiedostot, välimuistiin tallennetut tiedostot, evästeet, selaimen historiatiedostot, lähetetyt ja poistetut sähköpostiviestit, viimeksi käytetyt tiedostot, ActiveX-tiedostot ja järjestelmän palautuspistetiedostot. QuickClean poistaa nämä kohteet muihin tärkeisiin tietoihin vaikuttamatta.

Voit poistaa tietokoneessa olevat tarpeettomat tiedostot QuickCleanin tyhjennysohjelmien avulla. Seuraavassa taulukossa kuvataan QuickCleanin tyhjennysohjelmat:

Nimi	Toiminto
Roskakorin tyhjennysohjelma	Poistaa Roskakorissa olevat tiedostot.
Väliaikaisten tiedostojen tyhjennysohjelma	Poistaa väliaikaisten tiedostojen kansioihin tallennetut tiedostot.
Pikakuvakkeiden tyhjennysohjelma	Poistaa rikkinäiset pikakuvakkeet ja pikakuvakkeet, joihin ei liity mitään ohjelmaa.
Hävinneiden tiedostopirstaleiden tyhjennysohjelma	Poistaa kadonneet tiedostopirstaleet tietokoneesta.
Rekisterin tyhjennysohjelma	Poistaa Windows®-rekisteritiedot ohjelmista, jotka on poistettu tietokoneesta. Rekisteri on tietokanta, johon Windows tallentaa kokoonpanoon liittyvät tiedot. Rekisteri sisältää jokaisen tietokoneen käyttäjän profiilin ja tietoja järjestelmän laitteista, asennetuista ohjelmista ja ominaisuuksien asetuksista. Windows käyttää näitä tietoja koko ajan toimiessaan.
Välimuistin tyhjennysohjelma	Poistaa välimuistiin tallennetut tiedostot, joita kertyy Web-sivuja selattaessa. Nämä tiedostot tallennetaan tavallisesti väliaikaisina tiedostoina välimuistissa olevaan kansioon. Välimuisti on tietokoneessa oleva tilapäinen säilytysalue. Web-sivujen selaamisen nopeuttamiseksi ja tehokkuuden parantamiseksi selain voi hakea Web-sivun etäpalvelimen sijaan välimuistista, kun haluat tarkastella sitä seuraavan kerran.

Evästeiden tyhjennysohjelma	Poistaa evästeet. Nämä tiedostot tallennetaan tavallisesti väliaikaisina tiedostoina. Eväste on Web-sivuja selaavan henkilön tietokoneeseen tallennettu pieni tiedosto, joka sisältää erilaisia tietoja, kuten käyttäjänimen sekä nykyisen päivämäärän ja kellonajan. Web-sivustot käyttävät evästeitä lähinnä aikaisemmin sivustoon rekisteröityneiden tai siellä käyneiden henkilöiden tunnistamiseen, mutta myös hakkerit voivat käyttää niitä hyväkseen.
Selainhistorian tyhjennysohjelma	Poistaa Web-selaimen historiatiedot.
Outlook Express- ja Outlook-ohjelmien sähköpostien tyhjennysohjelma (lähetetyt ja poistetut kohteet)	Poistaa Outlook®- ja Outlook Express-ohjelmista lähetetyt ja poistetut sähköpostiviestit.
Viimeksi käytettyjen kohteiden tyhjennysohjelma	Poistaa viimeksi käytetyt tiedostot, jotka on luotu seuraavilla ohjelmilla: ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
ActiveX-objektien tyhjennysohjelma	Poistaa ActiveX-ohjausobjektit. ActiveX-objektit ovat ohjelmien tai Web-sivustojen toiminnallisuutta parantavia ohjelmistokomponentteja, jotka sulautuvat ohjelmiin tai Web-sivustoihin ja toimivat niiden osana. Useimmat ActiveX-ohjausobjektit ovat harmittomia, mutta jotkin niistä voivat kaapata tietokoneesta tietoja.
Järjestelmän palautuspisteiden tyhjennysohjelma	Poistaa vanhat järjestelmän palautuspisteet tietokoneesta (viimeisintä palautuspistettä lukuun ottamatta). Windows luo järjestelmän palautuspisteitä tallentaakseen tietokoneeseen tehdyt muutokset, jotta ongelmatilanteessa järjestelmä voidaan palauttaa aikaisempaan tilaan.

Puhdista tietokone

Voit poistaa tietokoneessa olevat tarpeettomat tiedostot QuickCleanin tyhjennysohjelmien avulla. Kun tehtävä on suoritettu, **Pikatyhjennyksen yhteenveto** -kohdassa voit tarkastella tyhjennyksen avulla vapautettua levytilaa, poistettujen tiedostojen määrää sekä QuickCleanin viimeisen käyttökerran päivämäärää ja kellonaikaa.

- 1 Valitse McAfee SecurityCenter -ruudun **Yleiset tehtävät** -kohdasta **Ylläpidä tietokonetta**.
- 2 Valitse **McAfee QuickClean**-kohdasta **Käynnistä**.
- 3 Valitse jokin seuraavista:
 - Hyväksy luettelon oletustyhjennysohjelmat valitsemalla **Seuraava**.
 - Valitse tai poista haluamasi tyhjennysohjelmat ja valitse sitten **Seuraava**. Jos valitset Viimeksi käytettyjen kohteiden tyhjennysohjelma -vaihtoehdon, voit valita tai poistaa luettelossa olevilla ohjelmilla viimeksi luodut tiedostot valitsemalla **Ominaisuudet**. Valitse sen jälkeen **OK**.
 - Palauta oletustyhjennysohjelmat valitsemalla **Palauta oletusasetukset** ja valitse sitten **Seuraava**.
- 4 Kun analyysi on suoritettu, valitse **Seuraava**.
- 5 Vahvista tiedoston poistaminen valitsemalla **Seuraava**.
- 6 Valitse jokin seuraavista:
 - Hyväksy oletusasetus **Ei, haluan poistaa tiedostot perinteisellä Windowsin poistomenetelmällä** valitsemalla **Seuraava**.
 - Valitse **Kyllä, haluan poistaa tiedostot turvallisesti käyttämällä Shredder-ohjelmaa**, määritä poistokertojen määrä (enintään kymmenen) ja valitse **Seuraava**. Tiedostojen tuhoaminen voi kestää pitkään, jos poistettavia tietoja on paljon.
- 7 Jos tiedostoja tai muita kohteita lukitaan tyhjennyksen aikana, näyttöön voi tulla kehote käynnistää tietokone uudelleen. Sulje kehote valitsemalla **OK**.
- 8 Valitse **Lopeta**.

Huomautus: Shredder-ohjelmalla poistettuja tiedostoja ei voi palauttaa. Lisätietoja tiedostojen tuhoamisesta on McAfee Shredderin ohjeessa.

Tietokoneen eheyttäminen

Levyn eheytyks järjestää tietokoneessa olevat tiedostot ja kansiot siten, että ne eivät hajoa osiin (pirstoudu), kun ne tallennetaan tietokoneen kiintolevyille. Eheyttämällä kiintolevyä säännöllisin väliajoin voit varmistaa, että pirstoutuneet tiedostot ja kansiot yhdistetään, jolloin voit käyttää niitä myöhemmin nopeammin.

Eheytä tietokoneesi

Eheyttämällä tietokoneesi voit parantaa tiedostojen ja kansioden käyttöä ja hakua.

- 1 Valitse McAfee SecurityCenter -ruudun **Yleiset tehtävät** -kohdasta **Ylläpidä tietokonetta**.
- 2 Valitse **Levyn eheytyks** -kohdasta **Analysoi**.
- 3 Toimi näytön ohjeiden mukaan.

Huomautus: Lisätietoja Levyn eheytyksestä on Windowsin Ohjeessa.

Tehtävän ajoittaminen

Tehtävien ajoitus määrittää automaattisesti QuickCleanin tai Levyn eheytyksen suoritustiheyden. Voit esimerkiksi ajoittaa QuickClean-tehtävän tyhjentämään Roskakorin sunnuntaisin klo 9.00 tai Levyn eheytyksen tehtävän eheyttämään tietokoneen kiintolevyn aina kuukauden viimeisenä päivänä. Voit luoda, muokata tai poistaa tehtäviä milloin tahansa. Sinun on kirjauduttava tietokoneeseen, jotta ajoitettu tehtävä voidaan suorittaa. Jos tehtävää ei jostakin syystä voida suorittaa, se ajoitetaan suoritettavaksi viisi minuuttia sisäänkirjautumisen jälkeen.

Ajoita QuickClean-tehtävä

Voit ajoittaa QuickClean-tehtävän puhdistamaan tietokoneen automaattisesti yhdellä tai useammalla tyhjennysohjelmalla. Kun tehtävä on suoritettu, **Pikatyhjennyksen yhteenveto** -kohdassa voit tarkistaa päivämäärän ja kellonajan, jolloin tehtävä on ajoitettu suoritettavaksi seuraavan kerran.

1 Avaa Tehtävien ajoitus -ruutu.

Miten?

1. Valitse McAfee SecurityCenter -ruudun **Yleiset tehtävät** -kohdasta **Ylläpidä tietokonetta**.

2. Valitse **Tehtävien ajoitus** -kohdasta **Käynnistä**.

2 Valitse **Valitse ajoitettava toiminto** -luettelosta **McAfee QuickClean**.

3 Kirjoita tehtävän nimi **Tehtävän nimi** -tekstiruutuun ja valitse **Luo**.

4 Valitse jokin seuraavista:

- Hyväksy luettelon tyhjennysohjelmat valitsemalla **Seuraava**.
- Valitse tai poista haluamasi tyhjennysohjelmat ja valitse sitten **Seuraava**. Jos valitset Viimeksi käytettyjen kohteiden tyhjennysohjelma -vaihtoehdon, voit valita tai poistaa luettelossa olevilla ohjelmilla viimeksi luodut tiedostot valitsemalla **Ominaisuudet**. Valitse sen jälkeen **OK**.
- Palauta oletustyhjennysohjelmat valitsemalla **Palauta oletusasetukset** ja valitse sitten **Seuraava**.

5 Valitse jokin seuraavista:

- Hyväksy oletusasetus **Ei, haluan poistaa tiedostot perinteisellä Windowsin poistomenetelmällä** valitsemalla **Ajoita**.

- Valitse **Kyllä, haluan poistaa tiedostot turvallisesti käyttämällä Shredder-ohjelmaa**, määritä poistokertojen määrä (enintään kymmenen) ja valitse **Ajoita**.
- 6 Määritä **Ajoita**-valintaikkunassa tehtävän suoritustiheys ja valitse **OK**.
 - 7 Jos muutit Viimeksi käytettyjen kohteiden tyhjennysohjelma -vaihtoehdon asetuksia, näyttöön voi tulla kehote käynnistää tietokone uudelleen. Sulje kehote valitsemalla **OK**.
 - 8 Valitse **Lopeta**.

Huomautus: Shredder-ohjelmalla poistettuja tiedostoja ei voi palauttaa. Lisätietoja tiedostojen tuhoamisesta on McAfee Shredderin ohjeessa.

Muokkaa QuickClean-tehtävää

Voit muokata ajoitettua QuickClean-tehtävää, jos haluat muuttaa käytettyjä tyhjennysohjelmia tai tehtävän automaattista suoritustiheyttä. Kun tehtävä on suoritettu, **Pikatyhjennyksen yhteenveto** -kohdassa voit tarkistaa päivämäärän ja kellonajan, jolloin tehtävä on ajoitettu suoritettavaksi seuraavan kerran.

- 1 Avaa Tehtävien ajoitus -ruutu.
Miten?
 1. Valitse McAfee SecurityCenter -ruudun **Yleiset tehtävät** -kohdasta **Ylläpidä tietokonetta**.
 2. Valitse **Tehtävien ajoitus** -kohdasta **Käynnistä**.
- 2 Valitse **Valitse ajoitettava toiminto** -luettelosta **McAfee QuickClean**.
- 3 Valitse tehtävä **Valitse olemassa oleva tehtävä** -luettelosta ja valitse **Muokkaa**.
- 4 Valitse jokin seuraavista:
 - Hyväksy tehtävää varten valitut tyhjennysohjelmat valitsemalla **Seuraava**.
 - Valitse tai poista haluamasi tyhjennysohjelmat ja valitse sitten **Seuraava**. Jos valitset Viimeksi käytettyjen kohteiden tyhjennysohjelma -vaihtoehdon, voit valita tai poistaa luettelossa olevilla ohjelmilla viimeksi luodut tiedostot valitsemalla **Ominaisuudet**. Valitse sen jälkeen **OK**.
 - Palauta oletustyhjennysohjelmat valitsemalla **Palauta oletusasetukset** ja valitse sitten **Seuraava**.
- 5 Valitse jokin seuraavista:
 - Hyväksy oletusasetus **Ei, haluan poistaa tiedostot perinteisellä Windowsin poistomenetelmällä** valitsemalla **Ajoita**.

- Valitse **Kyllä, haluan poistaa tiedostot turvallisesti käyttämällä Shredder-ohjelmaa**, määritä poistokertojen määrä (enintään kymmenen) ja valitse **Ajoita**.
- 6 Määritä **Ajoita**-valintaikkunassa tehtävän suoritustiheys ja valitse **OK**.
 - 7 Jos muutit Viimeksi käytettyjen kohteiden tyhjennysohjelma -vaihtoehdon asetuksia, näyttöön voi tulla kehote käynnistää tietokone uudelleen. Sulje kehote valitsemalla **OK**.
 - 8 Valitse **Lopeta**.

Huomautus: Shredder-ohjelmalla poistettuja tiedostoja ei voi palauttaa. Lisätietoja tiedostojen tuhoamisesta on McAfee Shredderin ohjeessa.

Poista QuickClean-tehtävä

Voit poistaa ajoitetun QuickClean-tehtävän, jos et enää halua suorittaa sitä automaattisesti.

- 1 Avaa Tehtävien ajoitus -ruutu.
Miten?
 1. Valitse McAfee SecurityCenter -ruudun **Yleiset tehtävät** -kohdasta **Ylläpidä tietokonetta**.
 2. Valitse **Tehtävien ajoitus** -kohdasta **Käynnistä**.
- 2 Valitse **Valitse ajoitettava toiminto** -luettelosta **McAfee QuickClean**.
- 3 Valitse tehtävä **Valitse olemassa oleva tehtävä** -luettelosta.
- 4 Napsauta **Poista** ja hyväksy sen jälkeen poistaminen valitsemalla **Kyllä**.
- 5 Valitse **Lopeta**.

Ajoita Levyn eheytyksen tehtävä

Voit ajoittaa Levyn eheytyksen tehtävän ja määrittää, kuinka usein tietokoneen kiintolevy ehytetään automaattisesti. Kun tehtävä on suoritettu, **Levyn eheytyksen** -kohdassa voit tarkistaa päivämäärän ja kellonajan, jolloin tehtävä on ajoitettu suoritettavaksi seuraavan kerran.

- 1 Avaa Tehtävien ajoitus -ruutu.
Miten?

1. Valitse McAfee SecurityCenter -ruudun **Yleiset tehtävät** -kohdasta **Ylläpidä tietokonetta**.
2. Valitse **Tehtävien ajoitus** -kohdasta **Käynnistä**.
- 2 Valitse **Valitse ajoitettava toiminto** -luettelosta **Levyn eheyty**s.
- 3 Kirjoita tehtävän nimi **Tehtävän nimi** -tekstiruutuun ja valitse **Luo**.
- 4 Valitse jokin seuraavista:
 - Valitse **Ajoita**, jos haluat hyväksyä oletusarvoisen **Suorita levyn eheyty**s, **vaikka vapaa levytila olisi vähissä** -asetuksen.
 - Poista **Suorita levyn eheyty**s, **vaikka vapaa levytila olisi vähissä** -asetuksen valinta ja valitse **Ajoita**.
- 5 Määritä **Ajoita**-valintaikkunassa tehtävän suoritustiheys ja valitse **OK**.
- 6 Valitse **Lopeta**.

Muokkaa Levyn eheyty -tehtävää

Voit muokata ajoitettua Levyn eheyty -tehtävää, jos haluat muuttaa tehtävän automaattista suoritustiheyttä. Kun tehtävä on suoritettu, **Levyn eheyty**s -kohdassa voit tarkistaa päivämäärän ja kellonajan, jolloin tehtävä on ajoitettu suoritettavaksi seuraavan kerran.

- 1 Avaa Tehtävien ajoitus -ruutu.
Miten?
 1. Valitse McAfee SecurityCenter -ruudun **Yleiset tehtävät** -kohdasta **Ylläpidä tietokonetta**.
 2. Valitse **Tehtävien ajoitus** -kohdasta **Käynnistä**.
- 2 Valitse **Valitse ajoitettava toiminto** -luettelosta **Levyn eheyty**s.
- 3 Valitse tehtävä **Valitse olemassa oleva tehtävä** -luettelosta ja valitse **Muokkaa**.
- 4 Valitse jokin seuraavista:
 - Valitse **Ajoita**, jos haluat hyväksyä oletusarvoisen **Suorita levyn eheyty**s, **vaikka vapaa levytila olisi vähissä** -asetuksen.
 - Poista **Suorita levyn eheyty**s, **vaikka vapaa levytila olisi vähissä** -asetuksen valinta ja valitse **Ajoita**.
- 5 Määritä **Ajoita**-valintaikkunassa tehtävän suoritustiheys ja valitse **OK**.
- 6 Valitse **Lopeta**.

Poista Levyn eheytyksen tehtävä

Voit poistaa ajoitetun Levyn eheytyksen tehtävän, jos et enää halua suorittaa sitä automaattisesti.

- 1 Avaa Tehtävien ajoitus -ruutu.
Miten?
 1. Valitse McAfee SecurityCenter -ruudun **Yleiset tehtävät** -kohdasta **Ylläpidä tietokonetta**.
 2. Valitse **Tehtävien ajoitus** -kohdasta **Käynnistä**.
- 2 Valitse **Valitse ajoitettava toiminto** -luettelosta **Levyn eheytyksen**.
- 3 Valitse tehtävä **Valitse olemassa oleva tehtävä** -luettelosta.
- 4 Napsauta **Poista** ja hyväksy sen jälkeen poistaminen valitsemalla **Kyllä**.
- 5 Valitse **Lopeta**.

L U K U 3 8

McAfee Shredder

McAfee Shredder poistaa pysyvästi (tuhooa) tietokoneen kiintolevyllä olevat kohteet. Vaikka poistat tiedostot ja kansiot manuaalisesti, tyhjennät Roskakorin tai poistat Väliaikaiset Internet-tiedostot -kansion, tiedot voi silti palauttaa tietokoneen jäljitystyökalujen avulla. Poistetut tiedostot voidaan palauttaa usein myös siksi, että jotkin ohjelmat tekevät avatuista tiedostoista väliaikaisia piilotiedostoja. Shredder parantaa tietosuojasi poistamalla ei-toivotut tiedostot turvallisesti ja pysyvästi. On tärkeää muistaa, että tuhottuja tiedostoja ei voi palauttaa.

Huomautus: SecurityCenter raportoi kriittiset ja ei-kriittiset suojausongelmat heti, kun se havaitsee ne. Jos tarvitset apua suojausongelmien selvittämisessä, voit käyttää McAfee Virtual Technician -palvelua.

Tässä luvussa

Shredderin toiminnot	208
Tiedostojen, kansioden ja levyjen tuhoaminen	209

Shredderin toiminnot

Shredder poistaa tietokoneen kiintolevyllä olevat kohteet siten, että niihin liittyviä tietoja ei voi palauttaa. Se parantaa tietosuojaa poistamalla tiedostot ja kansiot, Roskakoriassa ja Väliaikaiset Internet-tiedostot -kansiossa olevat kohteet sekä muun muassa uudelleenkirjoitettavien CD-levyjen, ulkoisten kiintolevyjen ja levykkeiden sisällön turvallisesti ja pysyvästi.

Tiedostojen, kansioden ja levyjen tuhoaminen

Shredder varmistaa, että Roskakorissa ja Väliaikaiset Internet-tiedostot -kansiossa olevia poistettuja tiedostoja ja kansioita ei voi palauttaa erikoistyoäkaluillakaan. Shredderissä voit määrittää, kuinka monta kertaa (enintään 10 kertaa) haluat poistaa kohteen. Mitä suurempi poistomäärä, sitä parempi tiedostojen poiston tietosuoja on.

Tuhoa tiedostoja ja kansioita

Voit tuhota tietokoneen kiintolevyllä olevia tiedostoja ja kansioita, muun muassa Roskakorissa ja Väliaikaiset Internet-tiedostot -kansiossa olevia kohteita.

1 Avaa **Shredder**.

Miten?

1. Valitse McAfee SecurityCenter -ikkunan **Yleiset tehtävät** -kohdasta **Lisävalikko**.
2. Valitse vasemmasta ruudusta **Työkalut**.
3. Valitse **Shredder**.

2 Valitse Tuhoa tiedostoja ja kansioita -ruudun **Haluan**-kohdasta **Poistaa tiedostoja ja kansioita**.

3 Valitse **Tuhoamistaso**-kohdasta jokin seuraavista tuhoamistasoista:

- **Nopea**: Poistaa valitut kohteet yhden kerran.
- **Perusteellinen**: Poistaa valitut kohteet seitsemän kertaa.
- **Mukautettu**: Poistaa valitut kohteet jopa kymmenen kertaa.

4 Valitse **Seuraava**.

5 Valitse jokin seuraavista:

- Valitse **Valitse tuhottava(t) tiedosto(t)** -luettelosta **Roskakorin sisältö** tai **Väliaikaiset Internet-tiedostot**.
- Valitse **Selaa**, siirry poistettavien tiedostojen kohdalle, valitse ne ja valitse **Avaa**.

6 Valitse **Seuraava**.

7 Valitse **Käynnistä**.

8 Kun Shredder on suorittanut tehtävän loppuun, valitse **Valmis**.

Huomautus: Älä ryhdy muihin toimiin, ennen kuin Shredder on suorittanut tehtävän loppuun.

Tuhoa koko levy

Voit tuhota levyn koko sisällön kerralla. Voit tuhota vain siirrettävien asemien (esimerkiksi ulkoisten kiintolevyjen, kirjoitettavien CD-levyjen ja levykkeiden) sisällön.

1 Avaa **Shredder**.

Miten?

1. Valitse McAfee SecurityCenter -ikkunan **Yleiset tehtävät** -kohdasta **Lisävalikko**.
2. Valitse vasemmasta ruudusta **Työkalut**.
3. Valitse **Shredder**.

2 Valitse Tuhoa tiedostoja ja kansioita -ruudun **Haluan**-kohdasta **Tyhjentää koko levyn**.

3 Valitse **Tuhoamistaso**-kohdasta jokin seuraavista tuhoamistasoista:

- **Nopea:** Tyhjentää valitun aseman yhden kerran.
- **Perusteellinen:** Tyhjentää valitun aseman seitsemän kertaa.
- **Mukautettu:** Tyhjentää valitun aseman jopa 10 kertaa.

4 Valitse **Seuraava**.

5 Valitse **Valitse levy** -luettelosta levy, jonka haluat tyhjentää.

6 Valitse **Seuraava** ja vahvista valintasi painamalla **Kyllä**.

7 Valitse **Käynnistä**.

8 Kun Shredder on suorittanut tehtävän loppuun, valitse **Valmis**.

Huomautus: Älä ryhdy muihin toimiin, ennen kuin Shredder on suorittanut tehtävän loppuun.

L U K U 3 9

McAfee Network Manager

McAfee Network Manager esittää graafisen näkymän kotiverkon tietokoneista ja osista. Network Managerin avulla voi valvoa kunkin verkkosi hallitun tietokoneen suojauksen tilaa ja korjata raportoituja tietoturvan puutteita.

Voit tutustua Networkin Managerin ominaisuuksiin, ennen kuin alat käyttää sitä. Lisätietoja näiden ominaisuuksien määrittämisestä ja käyttämisestä on Network Managerin ohjeessa.

Huomautus: SecurityCenter raportoi kriittiset ja ei-kriittiset suojausongelmat heti, kun se havaitsee ne. Jos tarvitset apua suojausongelmien selvittämisessä, voit käyttää McAfee Virtual Technician -palvelua.

Tässä luvussa

Network Managerin ominaisuudet.....	212
Network Managerin kuvakkeiden toiminta	213
Hallitun verkon määrittäminen	215
Verkon etähallinta	221

Network Managerin ominaisuudet

Network Manager tarjoaa seuraavat ominaisuudet.

Graafinen verkkokartta

Network Managerin verkkokartta tarjoaa graafisen näkymän muiden tietokoneiden ja kotiverkon osien suojaustilasta. Kun teet muutoksia verkkoosi (esimerkiksi lisäät siihen tietokoneen), verkkokartta tunnistaa muutokset. Voit päivittää verkkokarttaa, nimetä sen uudelleen ja mukauttaa näkymää näyttämällä tai piilottamalla verkkokartan osia. Voit myös tarkastella verkkokartassa näkyviin osiin liittyviä tietoja.

Etähallinta

Voit hallita kotiverkkosi tietokoneiden suojaustilaa Network Managerin verkkokartan avulla. Voit kutsua tietokoneen hallittuun verkkoon, valvoa hallitun tietokoneen suojaustilaa ja korjata tunnettuja tietoturvan puutteita verkkosi etätietokoneelta.

Network Managerin kuvakkeiden toiminta

Seuraavassa taulukossa kuvataan Network Managerin verkkokartassa yleisesti käytettyjä kuvakkeita.

Kuvake	Kuvaus
	Kuvaa verkossa olevaa hallittua tietokonetta
	Kuvaa hallittua tietokonetta, joka ei ole verkossa
	Kuvaa hallinnan piiriin kuulumatonta tietokonetta, johon on asennettu SecurityCenter
	Kuvaa hallinnan piiriin kuulumatonta tietokonetta, joka ei ole verkossa
	Kuvaa verkossa olevaa tietokonetta, johon ei ole asennettu SecurityCenteriä, tai tuntematonta verkkolaitetta
	Kuvaa tietokonetta, joka ei ole verkossa ja johon ei ole asennettu SecurityCenteriä, tai tuntematonta verkkolaitetta, joka ei ole verkossa
	Osoittaa, että vastaava kohde on suojattu ja kytketty
	Osoittaa, että vastaava kohde voi vaatia huomiota
	Osoittaa, että vastaava kohde vaatii välitöntä huomiota
	Kuvaa langatonta kotireititintä
	Kuvaa tavallista kotireititintä
	Kuvaa Internetiä, kun yhteys on muodostettu
	Kuvaa Internetiä, kun yhteys on katkaistu

L U K U 4 0

Hallitun verkon määrittäminen

Voit määrittää hallitun verkon käyttämällä verkkokartan kohteita ja lisäämällä jäseniä (tietokoneita) verkkoon. Tietokoneen täytyy olla verkon luotettu jäsen, ennen kuin sitä voidaan etähallita tai sille voidaan myöntää oikeus etähallita toisia verkon tietokoneita. Verkon jäsenyyden uusille tietokoneille myöntää verkossa jo oleva jäsen, jolla on järjestelmänvalvojan käyttöoikeudet.

Voit tarkastella verkkokartassa näkyviin osiin liittyviä tietoja, vaikka teet muutoksia verkkoon (esimerkiksi lisäät siihen tietokoneen).

Tässä luvussa

Verkkokartan käyttäminen	216
Hallittuun verkkoon liittyminen	218

Verkkokartan käyttäminen

Kun kytket tietokoneen verkkoon, Network Manager analysoi verkon ja tarkistaa, onko verkossa hallittuja tai hallinnan piiriin kuulumattomia jäseniä, sekä määrittää reitittimen asetukset ja Internet-tilan. Ellei jäseniä löydy, Network Manager olettaa, että nyt kytkettävä tietokone on verkon ensimmäinen tietokone ja tekee tietokoneesta järjestelmänvalvojan oikeuksin varustetun jäsenen. Oletusarvoisesti verkon nimeen sisältyy ensimmäisen sellaisen tietokoneen työryhmän tai toimialueen nimi, joka on liitetty verkkoon ja johon on asennettu SecurityCenter.

Kun teet muutoksia verkkoosi (esimerkiksi lisäät siihen tietokoneen), voit mukauttaa verkkokarttaa. Voit esimerkiksi päivittää verkkokarttaa, nimetä sen uudelleen ja mukauttaa näkymää näyttämällä tai piilottamalla verkkokartan osia. Voit myös tarkastella verkkokartassa näkyviin osiin liittyviä tietoja.

Käytä verkkokarttaa

Verkkokartta on graafinen esitys kotiverkon tietokoneista ja osista.

- Valitse Perus- tai Lisävalikon kohta **Verkonhallinta**.

Huomautus: Ensimmäisellä kerralla, kun käytät verkkokarttaa, sinua pyydetään luottamaan muihin verkon tietokoneisiin.

Päivitä verkkokartta

Voit päivittää verkkokartan milloin tahansa, esimerkiksi kun toinen tietokone liittyy hallittuun verkkoon.

- 1 Valitse Perus- tai Lisävalikon kohta **Verkonhallinta**.
- 2 Valitse **Haluan**-kohdasta **Päivitä verkkokartta**.

Huomautus: Päivitä verkkokartta -linkki on käytettävissä vain, jos verkkokartalta ei ole valittu kohteita. Voit poistaa kohteen valinnan napsauttamalla valittua kohdetta tai napsauttamalla verkkokartan valkoista kohtaa.

Nimeä verkko uudelleen

Oletusarvoisesti verkon nimeen sisältyy ensimmäisen sellaisen tietokoneen työryhmän tai toimialueen nimi, joka on liitetty verkkoon ja johon on asennettu SecurityCenter. Jos haluat käyttää toista nimeä, voit muuttaa sen.

- 1 Valitse Perus- tai Lisävalikon kohta **Verkonhallinta**.
- 2 Valitse **Haluan**-kohdasta **Verkon nimeäminen uudelleen**.
- 3 Kirjoita verkon nimi **Verkon nimi** -ruutuun.
- 4 Valitse **OK**.

Huomautus: Nimeä verkko uudelleen -linkki on käytettävissä vain, jos verkkokartalta ei ole valittu kohteita. Voit poistaa kohteen valinnan napsauttamalla valittua kohdetta tai napsauttamalla verkkokartan valkoista kohtaa.

Näytä tai piilota kohde verkkokartalla

Oletusarvoisesti kaikki kotiverkkosi tietokoneet ja osat näkyvät verkkokartalla. Jos sinulla on piilotettuja kohteita, saat ne näkyviin milloin tahansa. Vain hallinnan piiriin kuulumattomat kohteet voidaan piilottaa, hallittuja tietokoneita ei voi piilottaa.

Toiminto	Valitse Perus- tai Lisävalikosta Verkonhallinta ja tee näin...
Kohteen piilottaminen verkkokartalla	Napsauta verkkokartalla näkyvää kohdetta ja valitse Haluan -kohdasta Piilota tämä . Valitse vahvistusvalintaikkunasta Kyllä .
Piilotettujen kohteiden näyttäminen verkkokartalla	Valitse Haluan -kohdasta Näytä piilotetut kohteet .

Näytä kohteen tiedot

Voit tarkastella yksityiskohtaisia tietoja mistä tahansa verkkosi osasta valitsemalla sen verkkokartalta. Näitä tietoja ovat muun muassa osan nimi, sen suojauksen tila ja muut osan hallintaan tarvittavat tiedot.

- 1 Napsauta verkkokartalla näkyvää kohteen kuvaketta.
- 2 **Tiedot**-kohdassa voit tarkastella kohteen tietoja.

Hallittuun verkkoon liittyminen

Tietokoneen täytyy olla verkon luotettu jäsen, ennen kuin sitä voidaan etähallita tai sille voidaan myöntää oikeus etähallita toisia verkon tietokoneita. Verkon jäsenyyden uusille tietokoneille myöntää verkossa jo oleva jäsen, jolla on järjestelmänvalvojan käyttöoikeudet. Jotta varmistetaan, että vain luotetut tietokoneet voivat liittyä verkkoon, täytyy sekä myöntävän että liittyvän tietokoneen todentaa toisensa.

Kun tietokone liittyy verkkoon, järjestelmä pyytää sitä paljastamaan McAfee-suojauksensa muille verkon tietokoneille. Jos tietokone suostuu paljastamaan suojauksensa, siitä tulee verkon hallittu jäsen. Jos tietokone ei suostu paljastamaan suojauksensa, siitä tulee hallinnan piiriin kuulumaton verkon jäsen. Hallinnan piiriin kuulumattomat verkon jäsenet ovat tavallisesti vierailevia tietokoneita, jotka haluavat käyttää muita verkon ominaisuuksia (esimerkiksi lähettää tiedostoja tai jakaa tulostimia).

Huomautus: Jos tietokoneeseen on asennettu muita McAfee-verkko-ohjelmia, kuten EasyNetwork, tietokone tunnistetaan hallittavaksi tietokoneeksi myös näiden ohjelmien osalta. Network Managerissa määritetty oikeustaso koskee kaikkia McAfee-verkko-ohjelmia. Lisätietoja vieraan käyttöoikeuksista, täysistä käyttöoikeuksista ja järjestelmänvalvojan käyttöoikeuksista McAfee-verkko-ohjelmissa on ohjelmien mukana toimitetuissa käyttöohjeissa.

Liity hallittuun verkkoon

Kun saat kutsun liittyä verkkoon, voit joko hyväksyä tai hylätä sen. Voit määrittää myös, haluatko tämän ja muiden tietokoneiden valvovan toistensa suojausasetuksia (esimerkiksi ovatko tietokoneen virustorjuntapalvelut ajan tasalla).

- 1 Varmista, että Hallittu verkko -valintaikkunan **Salli jokaisen tässä verkossa olevan tietokoneen valvoa suojausasetuksia** -valintaruutu on valittuna.
- 2 Valitse **Liity**.
Kun hyväksyt kutsun, kaksi pelikorttia tulee näkyviin.
- 3 Vahvista, että kortit ovat samat kuin sinut hallittuun verkkoon kutsuneella tietokoneella näkyvät kortit.
- 4 Valitse **OK**.

Huomautus: Jos sinut hallittuun verkkoon kutsuneen tietokoneen näytössä näkyvät kortit eivät ole samat kuin suojausvarmistuksen valintaikkunassa näkyvät kortit, hallitun verkon turvallisuus on uhattuna. Verkkoon liittyminen saattaa altistaa tietokoneesi turvallisuusriskeille, joten valitse Hallittu verkko -valintaikkunasta **Peruuta**.

Kutsu tietokone hallittuun verkkoon

Jos hallittuun verkkoon lisätään tietokone tai verkossa on hallinnan piiriin kuulumaton tietokone, voit kutsua ne liittymään hallittuun verkkoon. Vain tietokoneet, joilla on järjestelmänvalvojan oikeudet verkossa, voivat kutsua toisia tietokoneita liittymään verkkoon. Kun lähetät pyynnön, määrität samalla liittyvälle tietokoneelle myönnettävän oikeustason.

- 1 Napsauta verkkokartalla näkyvää hallinnan piiriin kuulumattoman tietokoneen kuvaketta.
- 2 Valitse **Haluan**-kohdasta **Valvo tätä tietokonetta**.
- 3 Valitse Kutsu tietokone liittymään hallittuun verkkoon - valintaikkunasta jokin seuraavista:
 - Valitse **Myönnä vieraan oikeudet hallitun verkon ohjelmien käyttöön**, jos haluat myöntää tietokoneelle oikeudet verkon käyttöön (voit käyttää tätä asetusta, jos kodissasi on tilapäisiä tietokoneen käyttäjiä).
 - Valitse **Myönnä täydet oikeudet hallitun verkon ohjelmien käyttöön**, jos haluat myöntää tietokoneelle oikeudet verkon käyttöön.
 - Valitse **Myönnä järjestelmänvalvojan oikeudet hallitun verkon ohjelmien käyttöön**, jos haluat myöntää tietokoneelle järjestelmänvalvojan oikeudet verkon käyttöön. Niillä varustettu tietokone voi myös myöntää käyttöoikeuden muille tietokoneille, jotka haluavat liittyä hallittuun verkkoon.
- 4 Valitse **OK**.
Kutsu liittyä hallittuun verkkoon lähetään tietokoneelle. Kun tietokone hyväksyy kutsun, kaksi pelikorttia tulee näkyviin.
- 5 Vahvista, että kortit ovat samat kuin hallittuun verkkoon kutsutussa tietokoneessa näkyvät kortit.
- 6 Valitse **Myönnä käyttöoikeudet**.

Huomautus: Jos hallittuun verkkoon kutsumasi tietokoneen näytössä näkyvät kortit eivät ole samat kuin suojausvarmistuksen valintaikkunassa näkyvät kortit, hallitun verkon turvallisuus on uhattuna. Käyttöoikeuden myöntäminen tälle tietokoneelle saattaa altistaa toiset tietokoneet vaaroille, joten valitse suojausvarmistuksen valintaikkunasta **Hylkää käyttöoikeudet**.

Lakkaa luottamasta verkon tietokoneisiin

Jos luotit verkon tietokoneisiin vahingossa, voit lakata luottamasta niihin.

- Valitse **Haluan**-kohdasta **Lopeta tämän verkon tietokoneisiin luottaminen**.

Huomautus: Lopeta tämän verkon tietokoneisiin luottaminen -linkki ei ole käytettävissä, jos sinulla on järjestelmänvalvojan oikeudet ja verkossa on muita hallittuja tietokoneita.

LUKU 41

Verkon etähallinta

Kun olet asentanut hallitun verkon, voit etähallita verkon tietokoneita ja osia. Voit valvoa tietokoneiden ja osien tilaa ja oikeustasoja sekä korjata useimmat tietoturvan puutteet etäältä.

Tässä luvussa

Tilan ja oikeuksien valvonta	222
Tietoturvan puutteiden korjaaminen	224

Tilan ja oikeuksien valvonta

Hallitussa verkossa on hallittuja ja hallinnan piiriin kuulumattomia jäseniä. Hallitut jäsenet sallivat muiden verkon tietokoneiden valvoa McAfee-suojaustasoaan, hallinnan piiriin kuulumattomat eivät. Hallinnan piiriin kuulumattomat verkon jäsenet ovat tavallisesti vierailevia tietokoneita, jotka haluavat käyttää muita verkon ominaisuuksia (esimerkiksi lähettää tiedostoja tai jakaa tulostimia). Toinen hallitun verkon tietokone voi kutsua hallinnan piiriin kuulumattoman tietokoneen hallituksi tietokoneeksi. Samoin hallitusta tietokoneesta voidaan tehdä hallinnan piiriin kuulumaton milloin tahansa.

Hallituilla tietokoneilla on joko järjestelmänvalvojan, täydet tai vieraan käyttöoikeudet. Järjestelmänvalvojan oikeuksilla hallitut tietokoneet voivat hallita toisten hallittujen tietokoneiden suojaustilaa verkossa ja myöntää toisille tietokoneille verkon jäsenyyksiä. Täysillä käyttöoikeuksilla ja vieraan käyttöoikeuksilla tietokoneet voivat vain käyttää verkkoa. Voit muokata tietokoneen oikeustasoa milloin tahansa.

Hallittuun verkkoon voi kuulua myös laitteita (esimerkiksi reitittimiä), joita voit myös hallita Network Managerin avulla. Voit myös määrittää ja muokata laitteen näytön ominaisuuksia verkkokartalla.

Valvo tietokoneen suojauksen tilaa

Jos tietokoneen suojauksen tilaa ei valvota verkossa (tietokone ei ole verkon jäsen tai se on hallinnan piiriin kuulumaton verkon jäsen), sen valvontaa voi pyytää.

- 1 Napsauta verkkokartalla näkyvää hallinnan piiriin kuulumattoman tietokoneen kuvaketta.
- 2 Valitse **Haluan**-kohdasta **Valvo tätä tietokonetta**.

Lopeta tietokoneen suojauksen tilan valvominen

Voit lopettaa verkossa olevan hallitun tietokoneen valvomisen, mutta tällöin tietokoneesta tulee hallinnan piiriin kuulumaton, jolloin et voi valvoa sen suojauksen tilaa etäyhteyden kautta.

- 1 Napsauta verkkokartalla näkyvää hallitun tietokoneen kuvaketta.
- 2 Valitse **Haluan**-kohdasta **Lopeta tämän tietokoneen valvonta**.
- 3 Valitse vahvistusvalintaikkunasta **Kyllä**.

Muokkaa hallitun tietokoneen oikeuksia

Voit muuttaa hallitun tietokoneen oikeuksia milloin tahansa. Oikeuksien avulla voit määrittää, mitkä tietokoneet valvovat toisten verkon tietokoneiden suojauksen tilaa.

- 1 Napsauta verkkokartalla näkyvää hallitun tietokoneen kuvaketta.
- 2 Valitse **Haluan**-kohdasta **Muuta tämän tietokoneen käyttöoikeuksia**.
- 3 Määritä, voivatko hallitun verkon tietokoneet valvoa toistensa suojauksen tilaa valitsemalla tai poistamalla valinta käyttöoikeuksien muuttamisen valintaikkunan valintaruudusta.
- 4 Valitse **OK**.

Hallitse laitetta

Voit hallita laitetta käyttämällä sen hallinnan Web-sivua Network Managerista käsin.

- 1 Napsauta verkkokartalla näkyvää laitteen kuvaketta.
- 2 Valitse **Haluan**-kohdasta **Ota tämä laite hallintaan**. Laitteen hallinnan Web-sivu aukeaa selaimen.
- 3 Kirjoita kirjautumistietosi selaimen ja määritä laitteen suojausasetukset.

Huomautus: Jos laite on Wireless Network Securityn suojaama langaton reititin tai yhteyspiste, sen suojausasetusten määrittämiseen on käytettävä Wireless Network Securityä.

Muokkaa laitteen näytön ominaisuuksia

Kun muokkaat laitteen näytön ominaisuuksia, voit muuttaa laitteen näyttönimeä verkossa ja määrittää, onko laite langaton reititin.

- 1 Napsauta verkkokartalla näkyvää laitteen kuvaketta.
- 2 Valitse **Haluan**-kohdasta **Muokkaa laitteen ominaisuuksia**.
- 3 Voit määrittää laitteen näyttönimen kirjoittamalla nimen **Nimi**-ruutuun.
- 4 Määritä laitteen tyyppi valitsemalla **Tavallinen reititin**, jos kyseessä ei ole langaton reititin, tai **Langaton reititin**, jos kyseessä on langaton reititin.
- 5 Valitse **OK**.

Tietoturvan puutteiden korjaaminen

Järjestelmänvalvojan oikeuksilla varustetut tietokoneet voivat valvoa verkossa olevien toisten hallittujen tietokoneiden McAfee-suojaustasoja ja korjata raportoituja tietoturvan puutteita. Jos esimerkiksi hallitun tietokoneen McAfee-suojaustaso ilmaisee, ettei virustorjunta ole käytössä, toinen järjestelmävalvojan oikeuksin varustettu hallittu tietokone voi ottaa VirusScanin käyttöön etäyhteyden kautta.

Kun korjaat tietoturvan puutteita etäyhteyden kautta, Network Manager korjaa useimmat raportoidut ongelmat. Tietty tietoturvan puutteet saattavat kuitenkin vaatia manuaalisia toimia paikalliselta tietokoneelta. Tässä tapauksessa Network Manager korjaa ne ongelmat, jotka se pystyy korjaamaan etäyhteyden kautta ja pyytää korjaamaan loput ongelmat kirjautumalla kyseisessä tietokoneessa SecurityCenteriin ja noudattamalla tarjottuja suosituksia. Joissakin tapauksissa suositeltava korjaustapa on SecurityCenterin uusimman version asentaminen etätietokoneeseen tai verkon tietokoneisiin.

Korjaa tietoturvan puutteet

Network Managerin avulla voit korjata useimmat hallittujen tietokoneiden tietoturvan puutteet etäyhteyttä käyttäen. Jos esimerkiksi VirusScan on poistettu käytöstä etätietokoneesta, voit ottaa sen käyttöön.

- 1 Napsauta verkkokartalla näkyvää kohteen kuvaketta.
- 2 Kohteen suojauksen tila näkyy **Lisätiedot**-kohdassa.
- 3 Valitse **Haluan**-kohdasta **Tietoturvan puutteiden korjaaminen**.
- 4 Kun tietoturvan puutteet on korjattu, napsauta **OK**-painiketta.

Huomautus: Vaikka Network Manager korjaa automaattisesti useimmat tietoturvan puutteet, joidenkin puutteiden korjaus edellyttää SecurityCenterin avaamista kyseisessä tietokoneessa ja tarjottujen suositusten noudattamista.

Asenna McAfee-tietoturvaohjelmisto etätietokoneisiin

Jos yksi tai useampi verkkosi tietokone ei käytä SecurityCenterin uusinta versiota, niiden suojauksen tilaa ei voida valvoa etäyhteyden kautta. Jos haluat valvoa kyseisiä tietokoneita etäyhteydettä käyttäen, niihin täytyy asentaa SecurityCenterin uusin versio.

- 1** Avaa SecurityCenter tietokoneella, johon haluat asentaa tietoturvaohjelmiston.
- 2** Valitse **Yleiset tehtävät** -kohdasta **Oma tili**.
- 3** Kirjaudu sisään käyttämällä sähköpostiosoitetta ja salasanaa, joita käytit, kun rekisteröit tietoturvaohjelmiston asennuksen yhteydessä.
- 4** Valitse oikea tuote, napsauta **Lataa/Asenna**-kuvaketta ja noudata sitten näytön ohjeita.

L U K U 4 2

McAfee EasyNetwork

EasyNetwork antaa mahdollisuuden tiedostojen suojattuun jakamiseen, tiedostonsiirron yksinkertaistamiseen ja tulostimien jakamiseen kotiverkkosi tietokoneiden kesken. EasyNetwork on kuitenkin asennettava verkossa oleviin tietokoneisiin, ennen kuin sen ominaisuuksia voidaan käyttää.

Voit tutustua Easy Networkin ominaisuuksiin, ennen kuin alat käyttää sitä. Lisätietoja näiden ominaisuuksien määrittämisestä ja käyttämisestä on EasyNetworkin ohjeessa.

Huomautus: SecurityCenter raportoi kriittiset ja ei-kriittiset suojausongelmat heti, kun se havaitsee ne. Jos tarvitset apua suojausongelmien selvittämisessä, voit käyttää McAfee Virtual Technician -palvelua.

Tässä luvussa

EasyNetworkin ominaisuudet.....	228
EasyNetworkin asentaminen	229
Tiedostojen jakaminen ja lähettäminen.....	235
Tulostinten jakaminen.....	241

EasyNetworkin ominaisuudet

EasyNetwork tarjoaa seuraavat ominaisuudet.

Tiedostojen jakaminen

EasyNetworkin avulla voit jakaa tiedostoja helposti toisten verkossa olevien tietokoneiden kanssa. Kun jaat tiedostoja, myönnät toisille tietokoneille lukuoikeuden kyseisiin tiedostoihin. Vain hallitun verkon täysillä oikeuksilla tai järjestelmänvalvojan oikeuksilla varustetut tietokoneet (jäsenet) voivat jakaa tiedostoja ja lukea toisten jäsentietokoneiden jakamia tiedostoja.

Tiedostonsiirto

Voit lähettää tiedostoja muihin hallitun verkon täysillä tai järjestelmänvalvojan oikeuksilla varustettuihin tietokoneisiin (jäsenille). Kun vastaanotat tiedoston, se näkyy EasyNetworkin Saapuneet-kansiossa. Saapuneet-kansio on väliaikainen tallennuspaikka kaikille verkon muista tietokoneista sinulle lähetetyille tiedostoille.

Automaattinen tulostimen jakaminen

Kun olet liittynyt hallittuun verkkoon, voit jakaa tietokoneeseesi liitetyt paikalliset tulostimet muiden jäsenten kanssa ja käyttää jaetun tulostimen nimenä tulostimen nykyistä nimeä. Lisäksi tulostin havaitsee muiden verkon tietokoneiden tulostimet ja sallii kyseisten tulostimien määrittämisen ja käyttämisen.

L U K U 4 3

EasyNetworkin asentaminen

EasyNetwork on avattava ja liitettävä hallittuun verkkoon ennen käyttöä. Kun olet liittynyt hallittuun verkkoon, voit jakaa, etsiä ja lähettää tiedostoja muihin verkossa oleviin tietokoneisiin. Voit myös jakaa tulostimia. Jos päätät poistua verkosta, voit tehdä niin milloin tahansa.

Tässä luvussa

Avaa EasyNetwork.....	229
Hallittuun verkkoon liittyminen	230
Hallitusta verkosta poistuminen.....	234

Avaa EasyNetwork

Oletusarvoisesti järjestelmä kehottaa avaamaan EasyNetworkin asennuksen jälkeen, mutta voit kuitenkin avata EasyNetworkin myöhemminkin.

- Valitse **Käynnistä**-valikosta **Ohjelmat, McAfee** ja valitse **McAfee EasyNetwork**.

Vihje: Jos olet luonut asennuksen yhteydessä työpöytä- ja pikakäynnistyskuvakkeet, voit avata EasyNetworkin myös kaksoisnapsauttamalla työpöydällä tai tehtäväpalkin oikeassa reunassa sijaitsevalla ilmaisinalueella olevaa McAfee EasyNetwork -kuvaketta.

Hallittuun verkkoon liittyminen

Jos yhtäkään verkossa olevaa tietokonetta ei ole liitetty SecurityCenteriin, järjestelmä tekee sinusta verkon jäsenen ja kehottaa sinua määrittämään, onko verkko luotettava. Ensimmäisenä verkkoon liittyvänä tietokoneena tietokoneesi nimi sisällytetään verkon nimeen. Voit kuitenkin muuttaa verkon nimeä milloin tahansa.

Kun tietokone liittyy verkkoon, se lähettää muille verkon tietokoneille erillisen liittymispyynnön. Pyyntö voidaan hyväksyä miltä tahansa tietokoneelta, jolla on verkonvalvojan oikeudet. Myöntäjä voi myös määrittää verkkoon liittyvien tietokoneiden oikeuksien tason, esimerkiksi vieraan käyttöoikeudet (vain tiedostonsiirto) tai täydet tai järjestelmänvalvojan käyttöoikeudet (tiedostonsiirto ja tiedostonjako). Järjestelmänvalvojaoikeuksin varustetut tietokoneet voivat myöntää EasyNetworkissa käyttöoikeudet muille tietokoneille ja hallita oikeuksia (ylentää tai alentaa tietokoneita). Täysillä käyttöoikeuksilla varustetut tietokoneet eivät voi suorittaa kyseisiä järjestelmänvalvojan tehtäviä.

Huomautus: Jos tietokoneeseen on asennettu muita McAfeen verkko-ohjelmia, kuten Network Manager, tietokone tunnistetaan hallittavaksi tietokoneeksi myös näiden ohjelmien osalta. Tietokoneelle EasyNetworkissa määritetty oikeuksien taso koskee kaikkia McAfeen verkko-ohjelmia. Lisätietoja vieraan käyttöoikeuksista, täysistä käyttöoikeuksista ja järjestelmänvalvojan käyttöoikeuksista McAfeen verkko-ohjelmissa on ohjelmien mukana toimitetuissa käyttöohjeissa.

Liity verkkoon

Kun tietokone liittyy luotettavaan verkkoon ensimmäistä kertaa EasyNetworkin asentamisen jälkeen, näyttöön tulee viesti, jossa kysytään, haluatko liittyä hallittuun verkkoon. Jos tietokone hyväksyy liittymiskutsun, lähetetään pyyntö kaikille verkon tietokoneille, joilla on järjestelmänvalvojan oikeudet. Pyyntöön tarvitaan hyväksyntä, ennen kuin tietokone voi jakaa tulostimia ja tiedostoja tai lähettää ja kopioida tiedostoja verkossa. Verkon ensimmäiselle tietokoneelle myönnetään automaattisesti järjestelmänvalvojan oikeudet.

- 1 Valitse Jaetut tiedostot -ikkunasta **Liity verkkoon**. Kun verkon järjestelmänvalvoja-tietokone hyväksyy pyyntösi, näyttöön tulee viesti, jossa kysytään, sallitaanko tämän ja muiden verkon tietokoneiden hallita toistensa suojausasetuksia.
- 2 Jos haluat sallia tietokoneen ja muiden verkon tietokoneiden keskinäisen suojausasetusten hallitsemisen, valitse **OK**, muussa tapauksessa valitse **Peruuta**.
- 3 Varmista, että myöntävän tietokoneen näytössä näkyvät samat pelikortit kuin suojausvarmistuksen valintaikkunassa, ja valitse **OK**.

Huomautus: Jos sinut hallittuun verkkoon kutsuneen tietokoneen näytössä näkyvät kortit eivät ole samat kuin suojausvarmistuksen valintaikkunassa näkyvät kortit, hallitun verkon turvallisuus on uhattuna. Verkkoon liittyminen saattaa altistaa tietokoneesi turvallisuusriskeille, joten valitse suojausvarmistuksen valintaikkunasta **Peruuta**.

Myönnä verkon käyttöoikeudet

Kun tietokone pyytää oikeutta liittyä hallittuun verkkoon, muille verkon järjestelmänvalvojatietokoneille lähetetään viesti. Ensimmäisenä vastaavasta tietokoneesta tulee myöntäjä. Myöntäjä päättää tietokoneelle myönnettävän käyttöoikeustyyppin: vieras, täydet oikeudet tai järjestelmänvalvoja.

- 1 Napsauta ilmoituksessa oikeata käyttöoikeustasoa.
- 2 Valitse Kutsu tietokone liittymään hallittuun verkkoon - valintaikkunasta jokin seuraavista:
 - Valitse **Myönnä vieraan oikeudet hallitun verkon ohjelmien käyttöön**, jos haluat myöntää tietokoneelle oikeudet verkon käyttöön (voit käyttää tätä asetusta, jos kodissasi on tilapäisiä tietokoneen käyttäjiä).
 - Valitse **Myönnä täydet oikeudet hallitun verkon ohjelmien käyttöön**, jos haluat myöntää tietokoneelle oikeudet verkon käyttöön.

- Valitse **Myönnä järjestelmänvalvojan oikeudet hallitun verkon ohjelmien käyttöön**, jos haluat myöntää tietokoneelle järjestelmänvalvojan oikeudet verkon käyttöön. Niillä varustettu tietokone voi myös myöntää käyttöoikeuden muille tietokoneille, jotka haluavat liittyä hallittuun verkkoon.

3 Valitse **OK**.

4 Varmista, että tietokoneen näytössä näkyvät samat pelikortit kuin suojausvarmistuksen valintaikkunassa, ja valitse **Myönnä käyttöoikeudet**.

Huomautus: Jos tietokoneen näytössä näkyvät kortit eivät vastaa suojausvarmistuksen valintaikkunassa näkyviä kortteja, hallitun verkon turvallisuus on uhattuna. Käyttöoikeuden myöntäminen kyseiselle tietokoneelle saattaa altistaa tietokoneesi tietoturvariskeille, joten valitse suojausvarmistuksen valintaikkunasta **Hylkää käyttöoikeudet**.

Nimeä verkko uudelleen

Oletusarvoisesti verkon nimi sisältää ensimmäisen siihen liittyneen tietokoneen nimen, mutta voit kuitenkin muuttaa verkon nimeä milloin tahansa. Kun nimeät verkon uudelleen, EasyNetworkissa näkyvä verkon kuvaus muuttuu.

- 1 Valitse **Valinnat**-valikosta **Määritä**.
- 2 Kirjoita verkon nimi Määritä-valintaikkunan **Verkon nimi** -ruutuun.
- 3 Valitse **OK**.

Hallitusta verkosta poistuminen

Jos liittyt hallittuun verkkoon ja päätät, ettet enää halua kuulua verkkoon, voit poistua verkosta. Kun poistut hallitusta verkosta, voit aina liittyä siihen uudelleen, mutta sinulle on myönnettävä siihen uudelleen oikeudet. Lisätietoja verkkoon liittymisestä on kohdassa Hallittuun verkkoon liittyminen (sivu 230).

Poistu hallitusta verkosta

Voit poistua hallitusta verkosta, johon olet aiemmin liittynyt.

- 1 Valitse **Työkalut**-valikosta **Poistu Verkosta**.
- 2 Valitse Poistu verkosta -valintaikkunasta sen verkon nimi, josta haluat poistua.
- 3 Valitse **Poistu verkosta**.

LUKU 44

Tiedostojen jakaminen ja lähettäminen

EasyNetworkin avulla voit helposti jakaa tiedostoja ja lähettää tiedostoja verkon muihin tietokoneisiin. Kun jaat tiedostoja, myönnät toisille tietokoneille lukuoikeuden niihin. Vain hallitun verkon jäsentietokoneet (täysillä oikeuksilla tai järjestelmänvalvojan oikeuksilla varustetut tietokoneet) voivat jakaa tiedostoja tai lukea toisten jäsentietokoneiden jakamia tiedostoja.

Huomautus: Suuren tiedostomäärän jakaminen voi vaikuttaa tietokoneen resursseihin.

Tässä luvussa

Tiedostojen jakaminen	236
Tiedostojen lähettäminen toisiin tietokoneisiin.....	239

Tiedostojen jakaminen

Vain hallitun verkon jäsentietokoneet (täysillä oikeuksilla tai järjestelmänvalvojan oikeuksilla varustetut tietokoneet) voivat jakaa tiedostoja tai lukea toisten jäsentietokoneiden jakamia tiedostoja. Jos jaat kansion, järjestelmä jakaa automaattisesti kaikki kansion sisältämät tiedostot ja alikansiot. Kansioon myöhemmin lisättäviä tiedostoja ei kuitenkaan jaeta. Jos jaettu tiedosto tai kansio poistetaan, se poistetaan Jaetut tiedostot -ikkunasta. Voit lopettaa tiedoston jakamisen milloin tahansa.

Voit avata jaetun tiedoston avaamalla sen suoraan EasyNetworkissa tai kopioimalla sen tietokoneeseen ja avaamalla sen siellä. Jos jaettujen tiedostojen luettelo on pitkä ja tiedostoa on vaikeata löytää, voit hakea sen.

Huomautus: EasyNetworkilla jaettuja tiedostoja ei voi käyttää toisesta tietokoneesta käsin Windowsin Resurssienhallinnan avulla, sillä tiedostoja EasyNetworkilla jaettaessa on käytettävä suojattuja yhteyksiä.

Jaa tiedosto

Kun jaat tiedoston, se on kaikkien niiden hallitun verkon jäsentietokoneiden saatavilla, joilla on täydet tai järjestelmänvalvojan oikeudet.

- 1 Etsi Windowsin Resurssienhallinnassa tiedosto, jonka haluat jakaa.
- 2 Vedä tiedosto Windowsin Resurssienhallinnasta EasyNetworkin Jaetut tiedostot -kansioon.

Vihje: Voit jakaa tiedoston myös valitsemalla **Työkalut**-valikosta **Jaa tiedostot**. Siirry Jakaminen-valintaikkunassa kansioon, jossa jaettava tiedosto sijaitsee, valitse se ja valitse sitten **Jaa**.

Lopeta tiedoston jakaminen

Jos jaat tiedostoa hallitussa verkossa, voit lopettaa jakamisen milloin tahansa. Kun lopetat tiedoston jakamisen, muut hallitun verkon tietokoneet eivät voi käyttää sitä.

- 1 Valitse **Työkalut**-valikosta **Lopeta tiedostojen jakaminen**.
- 2 Valitse Lopeta jakaminen -valintaikkunasta tiedosto, jonka jakamisen haluat lopettaa.
- 3 Valitse **OK**.

Kopioi jaettu tiedosto

Kopioi jaettu tiedosto, jotta voit käyttää sitä myös silloin, kun sitä ei enää jaeta. Voit kopioida jaetun tiedoston mistä tahansa hallitun verkon tietokoneesta.

- Vedä tiedosto EasyNetworkin Jaetut tiedostot -ikkunasta Windowsin Resurssienhallintaan tai Windowsin työpöydälle.

Vihje: Voit kopioida jaetun tiedoston myös valitsemalla sen EasyNetworkissa ja valitsemalla sitten **Työkalut**-valikosta **Kopioi kohteeseen**. Siirry Kopioi kohteeseen -valintaikkunassa kansioon, johon haluat kopioida tiedoston, valitse se ja napsauta **Tallenna**-painiketta.

Hae jaettu tiedosto

Voit hakea tiedostoa, joka on ollut jaettuna joko omassa tietokoneessasi tai jossakin toisessa verkon jäsentietokoneessa. Kun kirjoitat hakuetoja, EasyNetwork näyttää hakuasi vastaavat tulokset Jaetut tiedostot -ikkunassa.

- 1 Valitse Jaetut tiedostot -ikkunasta **Haku**.
- 2 Valitse **Sisältää**-luettelosta haluamasi vaihtoehto (sivu 237).
- 3 Kirjoita tiedoston tai tiedostopolun nimi osittain tai kokonaan **Tiedoston tai tiedostopolun nimi** -luetteloon.
- 4 Valitse **Tyyppi**-luettelosta haluamasi tiedostotyyppi (sivu 237).
- 5 Valitse **Mistä**- ja **Mihin**-luetteloiden avulla aikaväli, jonka aikana tiedosto on luotu.

Hakuehdot

Seuraavissa taulukoissa kuvataan hakuehtoja, jotka voit määrittää, kun haet jaettuja tiedostoja.

Tiedoston tai polun nimi

Sisältää	Kuvaus
Sisältää sanat	Hae tiedoston tai tiedostopolun nimi, joka sisältää kaikki Tiedoston tai tiedostopolun nimi -luettelossa määrittämäsi sanat missä tahansa järjestyksessä.
Sisältää minkä tahansa sanoista	Hae tiedoston tai tiedostopolun nimi, joka sisältää Tiedoston tai tiedostopolun nimi -luettelossa määrittämiäsi sanat.
Sisältää merkkijonon	Hae tiedoston tai tiedostopolun nimi, joka sisältää Tiedoston tai tiedostopolun nimi -luettelossa määrittämäsi koko lauseen.

Tiedoston tyyppi

Tyyppi	Kuvaus
Mikä tahansa	Hae kaikkia jaettuja tiedostotyypppejä.
Asiakirja	Hae kaikkia jaettuja asiakirjoja.
Kuvatiedosto	Hae kaikkia jaettuja kuvatiedostoja.
Videoleike	Hae kaikkia jaettuja videotiedostoja.
Äänitiedosto	Hae kaikkia jaettuja äänitiedostoja.
Pakattu	Hae kaikkia pakattuja tiedostoja (esimerkiksi .zip-tiedostoja).

Tiedostojen lähettäminen toisiin tietokoneisiin

Voit lähettää tiedostoja muihin hallitun verkon jäsentietokoneisiin. Ennen tiedoston lähettämistä EasyNetwork tarkistaa, että vastaanottavassa tietokoneessa on riittävästi vapaata levytilaa.

Kun vastaanotat tiedoston, se näkyy EasyNetworkin Saapuneet-kansiossa. Saapuneet-kansio on väliaikainen tallennuspaikka muista verkon tietokoneista sinulle lähetetyille tiedostoille. Jos EasyNetwork on auki, kun vastaanotat tiedoston, tiedosto näkyy heti Saapuneet-kansiossa. Muussa tapauksessa viesti näkyy tehtäväpalkin oikeassa reunassa sijaitsevalla ilmaisinalueella. Jos et halua nähdä vastaanoton ilmoitusviestejä (esimerkiksi jos ne häiritsevät sitä, mitä olet juuri tekemässä), voit poistaa tämän toiminnon käytöstä. Jos Saapuneet-kansiossa on jo samanniminen tiedosto, uuden tiedoston nimen perään lisätään numeroliite. Tiedostot säilyvät Saapuneet-kansiossa, kunnes hyväksyt ne (kopioit ne tietokoneeseen).

Lähetä tiedosto toiseen tietokoneeseen

Voit lähettää tiedoston toiseen hallitun verkon tietokoneeseen jakamatta sitä. Ennen kuin vastaanottavan tietokoneen käyttäjä voi katsella tiedostoa, se täytyy tallentaa paikalliseen sijaintiin. Lisätietoja on kohdassa Hyväksy tiedosto toisesta tietokoneesta (sivu 240).

- 1 Etsi Windowsin Resurssienhallinnassa tiedosto, jonka haluat lähettää.
- 2 Vedä tiedosto Windowsin Resurssienhallinnasta EasyNetworkissa aktiivisena olevan tietokoneen kuvakkeen päälle.

Vihje: Voit lähettää tietokoneeseen useita tiedostoja painamalla CTRL-näppäintä tiedostoja valitessasi. Voit lähettää tiedostoja myös valitsemalla **Työkalut**-valikosta **Lähetä**, valitsemalla tiedostot ja napsauttamalla sitten **Lähetä**-painiketta.

Hyväksy tiedosto toisesta tietokoneesta

Jos toinen hallitun verkon tietokone lähettää sinulle tiedoston, sinun täytyy hyväksyä se tallentamalla se tietokoneeseen. Jos EasyNetwork ei ole käynnissä, kun tietokoneeseen lähetetään tiedosto, saat ilmoitusviestin, joka näkyy tehtäväpalkin oikeassa reunassa sijaitsevalla ilmaisinalueella. Avaa EasyNetwork napsauttamalla ilmoitusviestiä, niin pääset käyttämään tiedostoa.

- Napsauta **Vastaanotettu**-painiketta ja vedä tiedosto EasyNetworkin Saapuneet-kansiosta Windowsin Resurssienhallinnan kansioon.

Vihje: Voit vastaanottaa tiedoston toisesta tietokoneesta myös valitsemalla tiedoston EasyNetworkin Saapuneet-kansiosta ja valitsemalla sitten **Työkalut**-valikosta **Hyväksy**. Siirry Hyväksy kansioon -valintaikkunassa siihen kansioon, johon haluat tallentaa vastaanottamasi tiedostot, valitse se ja napsauta **Tallenna**-painiketta.

Ilmoituksen saaminen tiedoston lähettämisestä

Voit saada ilmoitusviestin, kun toinen hallitun verkon tietokone lähettää sinulle tiedoston. Jos EasyNetwork ei ole käynnissä, ilmoitusviesti tulee tehtäväpalkin oikeassa reunassa olevalle ilmaisinalueelle.

- 1 Valitse **Valinnat**-valikosta **Määritä**.
- 2 Valitse Määritä-valintaruudusta **Ilmoita, kun toinen tietokone lähettää tiedostoja** -valintaruutu.
- 3 Valitse **OK**.

LUKU 45

Tulostinten jakaminen

Kun olet liittynyt hallittuun verkkoon, EasyNetwork jakaa tietokoneeseen liitetyt paikalliset tulostimet ja käyttää jaetun tulostimen nimenä tulostimen nykyistä nimeä. EasyNetwork havaitsee myös verkon muiden tietokoneiden tulostimet ja sallii kyseisten tulostimien määrittämisen ja käyttämisen.

Jos olet määrittänyt tulostinohjaimen tulostamaan verkon tulostuspalvelimen kautta (esimerkiksi langaton USB-tulostuspalvelin), EasyNetwork tulkitsee tulostimen paikalliseksi tulostimeksi ja jakaa sen verkossa. Voit lopettaa tulostimen jakamisen milloin tahansa.

Tässä luvussa

Jaettujen tulostinten käyttäminen242

Jaettujen tulostinten käyttäminen

EasyNetwork havaitsee verkon tietokoneiden jakamat tulostimet. Jos EasyNetwork havaitsee etätulostimen, jota ei ole kytketty tietokoneeseen, Jaetut tiedostot -ikkunassa näkyy **Saatavilla olevat verkkotulostimet** -linkki, kun avaat EasyNetworkin ensimmäisen kerran. Voit sen jälkeen asentaa saatavilla olevia tulostimia tai poistaa tietokoneeseen jo kytkettyjen tulostimien asennuksia. Voit myös päivittää tulostimien luettelon ja siten varmistaa, että näkemäsi tiedot ovat ajan tasalla.

Jos et ole liittynyt hallittuun verkkoon, mutta olet kytkeytynyt siihen, voit käyttää jaettuja tulostimia Windowsin tulostimien ohjauspaneelin kautta.

Lopeta tulostimen jakaminen

Kun lopetat tulostimen jakamisen, jäsenet eivät enää voi käyttää sitä.

- 1 Valitse **Työkalut**-valikosta **Tulostimet**.
- 2 Valitse Hallitse tulostimia -valintaikkunasta sen tulostimen nimi, jonka jakamisen haluat lopettaa.
- 3 Napsauta **Älä jaa** -painiketta.

Asenna käytettävissä oleva verkkotulostin

Jos olet hallitun verkon jäsen, voit käyttää jaettuja tulostimia, mutta sitä varten sinun on asennettava tulostimen käyttämä tulostinohjain. Jos tulostimen omistaja lopettaa sen jakamisen, et voi käyttää sitä.

- 1 Valitse **Työkalut**-valikosta **Tulostimet**.
- 2 Valitse tulostimen nimi Saatavilla olevat verkkotulostimet -valintaikkunasta.
- 3 Napsauta **Asenna**-painiketta.

Opas

Termisanasto luettelee ja määrittää McAfee-tuotteissa useimmin käytetyt tietoturvatерmit.

Sanasto

8

802.11

Kokoelma IEEE-standardeja, joiden avulla lähetetään tietoja langattomassa verkossa. 802.11 tunnetaan yleisesti nimellä Wi-Fi.

802.11a

802.11-standardin laajennus, jonka avulla tietoa voidaan siirtää jopa 54 Mbps:n nopeudella 5 Ghz:n kaistassa. Vaikka tiedonsiirron nopeus on suurempi kuin 802.11b-standardissa, laajennuksen kantoalue on paljon pienempi.

802.11b

802.11-standardin laajennus, jonka avulla tietoa voidaan siirtää jopa 11 Mbps:n nopeudella 2,4 Ghz:n kaistassa. Vaikka tiedonsiirron nopeus on pienempi kuin 802.11a-standardissa, laajennuksen kantoalue on paljon suurempi.

802.1x

Tavallisten ja langattomien verkkojen IEEE-todennusstandardi. 802.1x-standardia käytetään yleensä langattoman 802.11-verkon kanssa.

A

ActiveX-komponentti

ActiveX-objektit ovat ohjelmien tai Web-sivustojen toiminnallisuutta parantavia ohjelmistokomponentteja, jotka sulautuvat ohjelmiin tai Web-sivustoihin ja toimivat niiden osana. Useimmat ActiveX-ohjausobjektit ovat harmittomia, mutta jotkin niistä voivat kaapata tietokoneesta tietoja.

arkistointi

Tärkeiden tiedostojen kopiointi CD- tai DVD-levylle, USB-asemalle, ulkoiselle kiintolevyasemalle tai verkkoasemalle.

asiakas

Sovellus, joka toimii henkilökohtaisessa tietokoneessa tai työasemassa ja käyttää palvelinta tiettyjen toimintojen suorittamiseen. Esimerkiksi sähköpostiasiakas on sovellus, jonka avulla voit lähettää ja vastaanottaa sähköpostia.

avain

Kirjaimista ja numeroista muodostuva sarja, jota kaksi laitetta käyttää niiden välisen viestinnän todentamiseen. Molemmilla laitteilla täytyy olla sama avain. Katso myös WEP, WPA, WPA2, WPA-PSK ja WPA2-PSK.

avainsana

Sana, jonka avulla voidaan määrittää varmuuskopioidun tiedoston suhde tai yhteys muihin tiedostoihin, joille on määritetty sama avainsana. Kun tiedostoille on määritetty avainsanoja, Internetissä julkaistuja tiedostoja on helpompi hakea.

D

DAT

(Virusmäärittystiedostot) Tiedostot sisältävät määrittäykset, joita käytetään viruksien, troijalaisten, vakoiluohjelmien, mainosohjelmien ja muiden mahdollisten haittaohjelmien tunnistamiseen tietokoneessa tai USB-asemassa.

DNS

(Toimialueen nimijärjestelmä) Järjestelmä, joka muuntaa isäntä- tai toimialuenimet IP-osoitteiksi. Internetissä DNS-järjestelmää käytetään muuntamaan helposti luettavissa oleva Web-osoite (esimerkiksi www.myhostname.com) IP-osoitteeksi (esimerkiksi 111.2.3.44) Web-sivuston hakua varten. Ilman DNS-järjestelmää käyttäjän olisi itse kirjoitettava IP-osoite Web-selaimen osoitekenttään.

DNS-palvelin

(Toimialueen nimijärjestelmäpalvelin) Tietokone, joka palauttaa isännän tai toimialueen nimeen liittyvän IP-osoitteen. Katso myös DNS.

E

eristäminen

Esimerkiksi VirusScan-ohjelmassa epäilyttävät tiedostot tunnistetaan ja eristetään, jotta ne eivät voi aiheuttaa vahinkoa tietokoneelle tai tiedostoille.

ESS

(Laajennettu palvelukokoelma) Vähintään kahden verkon kokoelma, joka muodostaa yhtenäisen aliverkon.

eväste

Web-sivuja selaavan henkilön tietokoneeseen tallennettu pieni tiedosto, joka sisältää erilaisia tietoja, kuten käyttäjänimen sekä nykyisen päivämäärän ja kellonajan. Web-sivustot käyttävät evästeitä lähinnä aikaisemmin sivustoon rekisteröityneiden tai siellä käyneiden henkilöiden tunnistamiseen, mutta myös hakkerit voivat käyttää niitä hyväkseen.

H

hallittu verkko

Kotiverkko, jossa on kahdentyyppisiä jäseniä: hallittuja jäseniä ja hallinnan piiriin kuulumattomia jäseniä. Hallitut jäsenet sallivat muiden verkon tietokoneiden valvoa suojaustasoaan, hallinnan piiriin kuulumattomat eivät.

I

Internet

Internet sisältää valtavan määrän toisiinsa liitettyjä verkkoja, jotka käyttävät TCP/IP-protokollaa tiedonsiirtoon ja etsimiseen. Internet perustuu Yhdysvaltojen puolustusministeriön 1960-luvun lopulla ja 1970-luvun alussa rahoittamaan yliopistojen ja korkeakoulujen tietokoneiden muodostamaan verkkoon, jota kutsuttiin ARPANETiksi. Tänä päivänä Internet on maailmanlaajuinen verkko, joka sisältää lähes 100 000 itsenäistä verkkoa.

intranet

Yleensä organisaation sisäinen yksityinen tietokoneverkko, joka on vain hyväksyttyjen käyttäjien käytettävissä.

IP-huijausyritys

IP-paketin IP-osoitteiden väärentäminen. Tätä huijauskeinoa käytetään useissa erilaisissa hyökkäyksissä, kuten istunnon kaappauksissa. Sitä käytetään usein myös roskapostiviestien otsikoiden väärentämiseen, jotta viestejä ei voida jäljittää.

IP-osoite

TCP/IP-verkkoon liitetyn tietokoneen tai laitteen tunniste. Verkot, jotka käyttävät TCP/IP-protokollaa, reitittävät viestejä kohteen IP-osoitteen perusteella. IP-osoitteet ovat 32-bittisessä numeerisessa osoitemuodossa, jossa neljä numerosarjaa erotellaan pisteillä. Jokainen numerosarja voi olla 0–255 (esimerkiksi 192.168.1.100).

J

jaettu salaisuus

Merkkijono tai avain (yleensä salasana), joka on sovittu kahden keskustelevan osapuolen välillä ennen kommunikoinnin aloittamista. Jaettua salaisuutta käytetään RADIUS-viestien arkaluonteisten osien suojaamiseen.

jakaminen

Toiminto, jonka avulla sähköpostiviestin vastaanottajat voivat ladata varmuuskopioituja tiedostoja rajoitetun ajanjakson aikana. Kun tiedosto jaetaan, tiedoston varmuuskopioitu versio lähetetään sähköpostiviestin vastaanottajille. Viestin vastaanottajat saavat McAfee Data Backup -ohjelman lähettämän sähköpostiviestin, jossa heille kerrotaan jaettavista tiedostoista. Sähköpostiviesti sisältää linkin, josta jaettavat tiedostot voidaan ladata.

julkaiseminen

Varmuuskopioidun tiedoston julkaiseminen Internetissä. Voit etsiä julkaistuja tiedostoja Data Backup -kirjastosta.

järjestelmän palautuspiste

Tietokoneen muistin tai tietokannan sisällön tilannevedos. Windows luo palautuspisteitä säännöllisin väliajoin sekä merkittävien järjestelmätapahtumien yhteydessä (esimerkiksi kun ohjelma tai ohjain asennetaan). Voit myös itse luoda palautuspisteitä ja nimetä niitä milloin haluat.

K

kaistanleveys

Tiedon määrä, joka voidaan siirtää tietyssä ajassa.

kieltoluettelo

Phishing-huijaussuojauksessa haitallisina pidettyjen Web-sivustojen luettelo.

kirjasto

Varmuuskopioitujen ja julkaistujen tiedostojen online-tallennusalue. Data Backup -kirjasto on Internetin Web-sivusto, jota voi käyttää kuka tahansa Internet-käyttäjä.

komentosarja

Komentoluettelo, joka voidaan suorittaa automaattisesti (ilman käyttäjän toimintaa). Toisin kuin ohjelmat, komentosarjat tallennetaan yleensä tekstimuotoisena ja käännetään suorituksen yhteydessä. Makroja ja erätiedostoja kutsutaan myös komentosarjoiksi.

kotiverkko

Vähintään kaksi kotitietokonetta, jotka on liitetty toisiinsa siten, että tiedostojen yhteiskäyttö ja Internet-käyttö on mahdollista. Katso myös lähiverkko.

kuvasuodatus

Käytönvalvonta-asetus, joka estää mahdollisesti sopimattomien Web-kuvien esittämisen.

Käyttöpiste

Verkkolaite (yleisesti langaton reititin), joka voidaan kytkeä Ethernet-keskittimeen tai -kytkimeen, jotta langattoman verkon käyttöalue laajenee. Kun langattomat käyttäjät liikkuvat langattomien laitteiden kanssa, lähetykset siirtyvät käyttöpisteestä toiseen eikä yhteys katkea.

käytönvalvonta-asetukset

Asetukset, joiden avulla voit määrittää, millaisilla Web-sivuilla lapsesi voivat vierailla. Voit määrittää käytönvalvonnan ottamalla käyttöön kuvasuodatuksen tai poistamalla sen käytöstä, valitsemalla sisältöluokitusryhmän ja määrittämällä Web-selaukselle aikarajoitukset.

L

langaton USB-verkkosovitinkortti

Langaton sovitinkortti, joka asetetaan tietokoneen USB-korttipaikkaan.

langaton verkkopiste

Wi-Fi (802.11) -käyttöpisteen kattama maantieteellinen alue. Langattomaan verkkopisteeseen tulevat käyttäjät, joilla on langaton kannettava tietokone, voivat muodostaa Internet-yhteyden. Tämä edellyttää, että verkkopisteestä on ilmoitettu ja että käyttöoikeuden todentamista ei vaadita. Langattomat verkkopisteet sijaitsevat usein paikoissa, joissa on suuria ihmismääriä (esimerkiksi lentokentillä).

langaton verkkosovitin

Laite, jonka avulla tietokone tai PDA voi käyttää langatonta tietoliikenneyhteyttä. Sovitin liitetään USB-porttiin, PC-korttipaikkaan (CardBus), muistikorttipaikkaan tai sisäiseen PCI-väylään.

langattomat PCI-verkkosovitinkortit

(PCI eli Peripheral Component Interconnect) Langaton sovitinkortti, joka asetetaan tietokoneen PCI-korttipaikkaan.

laukaisualusta

U3-liittymän komponentti, joka toimii U3 USB -ohjelmien käynnistämisen ja hallinnan aloituspisteenä.

luotettujen luettelo

Sisältää kohteet, joihin luotat ja joihin ei suoriteta tunnistusta. Jos merkitset kohteen (esimerkiksi mahdollisen haittaohjelman tai rekisterimuutoksen) luotettavaksi vahingossa tai haluat, että kohde tunnistetaan uudelleen, kohde on poistettava tästä luettelosta.

luvaton käyttöpiste

Luvattomat käyttäjät voivat asentaa luvattomia käyttöpisteitä suojattuun yritysverkkoon saadakseen verkon käyttöoikeudet. Hyökkääjät voivat luoda niitä myös MITM-hyökkäyksen toteuttamista varten.

lähiverkko

(LAN, Local Area Network) Tietokoneverkko, joka kattaa suhteellisen pienen alueen (esimerkiksi yksittäisen rakennuksen). Lähiverkossa olevat tietokoneet voivat olla yhteydessä toisiinsa ja käyttää samoja resursseja, esimerkiksi samaa tulostinta tai samoja tiedostoja.

M

MAC-osoite

Yksilöivä sarjanumero, joka on määritetty verkkoa käyttävälle fyysiselle laitteelle.

mahdollinen haittaohjelma (PUP)

Ohjelma, joka kerää ja lähettää henkilökohtaisia tietoja ilman käyttäjän myöntämää lupaa (esimerkiksi vakoilu- tai mainosohjelma).

MAPI

Microsoftin liittymämäärittäjä, jonka avulla eri viestintä- ja työryhmäsovellukset (kuten sähköposti, ääniviestit ja faksi) toimivat yhden asiakkaan, esimerkiksi Exchange-asiakkaan, kautta.

mato

Mato on itseään kopioiva virus, joka piileskelee tietokoneen aktiivisessa muistissa ja voi lähettää itsensä kopioita sähköpostiviesteissä. Madot kopioituvat ja kuluttavat järjestelmäresursseja, mikä heikentää tietokoneen suorituskykyä tai keskeyttää tehtäviä.

melko tärkeät tarkkailukohteet

Tietokoneellasi sijaitseva kansio, jonka muutoksia McAfee Data Backup tarkkailee. Jos määrität melko tärkeän tarkkailukohteen, McAfee Data Backup varmuuskopioi ainoastaan kyseisen kansion tarkkailtavien tiedostotyyppien mukaiset tiedostot ilman alihakemistoja.

MITM-hyökkäys

Kahden osapuolen välisten viestien sieppaaminen ja mahdollinen muokkaaminen niin, ettei kumpikaan osapuoli huomaa tietoliikennelinkkiin murtautumista.

MSN

(Microsoft Network) Microsoft Corporationin Web-pohjaisten palvelujen kokonaisuus, johon kuuluvat esimerkiksi hakukone, sähköposti, pikaviestit ja portaali.

N

NIC

(Network Interface Card) Kortti, joka liitetään kannettavaan tietokoneeseen tai muuhun laitteeseen ja jonka avulla laite voidaan liittää lähiverkkoon.

O

online-varmuuskopiovarasto

Online-palvelimen sijainti, johon tiedostot tallentuvat varmuuskopioinnin jälkeen.

P

pakkaus

Toiminto, jonka avulla tiedostoja pakataan muotoon, joka minimoi niiden tallentamiseen tai siirtämiseen vaadittavan levytilan määrän.

palauttaminen

Tiedoston kopion noutaminen online-varmuuskopiovarastosta tai arkistosta.

palomuuuri

Järjestelmä (laitteisto, ohjelmisto tai molemmat), joka on kehitetty estämään luvattomia saapuvia ja lähteviä yhteyksiä yksityisessä verkossa. Palomuuureja käytetään usein luvattomien Internet-käyttäjien estämiseen, jotta he eivät pysty muodostamaan yhteyttä Internetiin liitettyihin yksityisiin verkkoihin, kuten intranet-verkkoihin. Kaikki intranetin saapuvat ja lähtevät viestit kulkevat palomuurin läpi. Palomuuuri tutkii jokaisen viestin ja estää ne viestit, jotka eivät vastaa määritettyjä suojausheitoja.

palvelin

Tietokone tai ohjelma, joka hyväksyy yhteydet muista tietokoneista tai ohjelmista ja palauttaa sopivat vastaukset. Esimerkiksi sähköpostiohjelma muodostaa yhteyden sähköpostipalvelimeen joka kerta, kun lähetät tai vastaanotat sähköpostiviestejä.

palvelun esto

Hyökkäystyyppi, joka hidastaa verkkoliikennettä tai keskeyttää sen kokonaan. Palvelunestohyökkäyksessä verkkoon tulvii liikaa ylimääräisiä pyyntöjä, minkä vuoksi tavanomainen liikenne hidastuu tai keskeytyy täysin. Palvelunestohyökkäys ei yleensä aiheuta tietovarkauksia tai muita tietoturvan puutteita.

perusteksti

Teksti, jota ei ole salattu. Katso myös salaus.

phishing-huijaus

Internet-huijausyritys, jossa tuntemattomat henkilöt yrittävät varastaa tärkeitä tietoja (kuten luottokorttinumeroita ja sosiaaliturvatunnuksia, käyttäjätunnuksia ja salasanoja) käytettäväksi petostarkoituksessa.

piilojäljitteet

Pienet grafiikkatiedostot, jotka voivat upottaa itsensä HTML-sivuihisi ja sallia luvattoman lähteen asettaa evästeitä tietokoneeseesi. Nämä evästeet voivat sitten lähettää tietoja luvattomalle lähteelle. Piilojäljitteitä kutsutaan myös pikselitunnisteiksi, läpinäkyviksi GIF-tiedostoiksi tai näkymättömiksi GIF-tiedostoiksi.

pika-arkistointi

Ainoastaan niiden tiedostojen arkistointi, jotka ovat muuttuneet viimeisimmän täydellisen tai pika-arkistoinnin jälkeen. Katso myös täydellinen arkistointi.

pikakuvake

Tiedosto, joka sisältää vain tietokoneessasi olevan toisen tiedoston sijaintitiedot.

plug-in

Pieni ohjelmisto, joka toimii suuremman ohjelman kanssa ja joka lisää siihen toimintoja. Esimerkiksi plug-in-laajennukset antavat Web-selaimen käyttää ja suorittaa HTML-asiakirjoihin upotettuja tiedostoja, jotka ovat selaimen tunnistamattomassa muodossa (esimerkiksi animaatio-, video- ja äänitiedostot).

ponnahdusikkunat

Pieniä ikkunoita, jotka tulevat näyttöön muiden ikkunoiden päälle. Ponnahdusikkunoita käytetään useimmiten mainosten näyttämiseen Web-selaimissa.

POP3

(Lyhenne sanoista Post Office Protocol 3.) Sähköpostiasiakasohjelman ja sähköpostipalvelimen välinen liittymä. Useimmilla kotikäyttäjillä on POP3-sähköpostitili. POP3-tili tunnetaan myös tavanomaisena sähköpostitilinä.

portti

Paikka, johon tieto kulkee tietokoneelle tai tietokoneelta. Esimerkiksi perinteinen analoginen modeemi liitetään sarjaporttiin.

PPPoE

(Lyhenne sanoista Point-to-Point Protocol Over Ethernet.) Point-to-Point Protocol (PPP) -soittoprotokollan käyttötapa Ethernet-yhteyden kautta.

protokolla

Muoto (laitteisto tai ohjelmisto), jonka avulla tietoja siirretään kahden laitteen välillä. Tietokoneen tai laitteen on tuettava oikeaa protokollaa, jos sen halutaan kommunikoida muiden tietokoneiden kanssa.

puskurin ylivuoto

Tilanne, joka esiintyy, kun epäilyttävät ohjelmat tai prosessit yrittävät tallentaa tietokoneen puskuriin (tietojen väliaikaiseen tallennusalueeseen) enemmän tietoja kuin siihen mahtuu. Puskurin ylivuoto vioittaa vierekkäisissä puskureissa olevia tietoja tai korvaa ne.

R

RADIUS

(Lyhenne sanoista Remote Access Dial-In User Service.) Protokolla, jonka avulla käyttäjät voidaan todentaa. Protokollaa käytetään useimmiten etäyhteyksien yhteydessä. Protokolla kehitettiin alun perin etäkäyttöpalvelimia varten, mutta nykyään sitä käytetään useissa erilaisissa todennusympäristöissä, esimerkiksi langattoman verkon käyttäjän jaetun salaisuuden todentamisessa 802.1x-standardin yhteydessä.

reaaliaikainen tarkistus

Tiedostojen ja kansioden tarkistus virusten ja muiden haitallisten mekanismien varalta, kun käyttäjä tai tietokone käyttää niitä.

reititin

Verkkolaite, joka edelleenlähettää datapaketteja verkosta toiseen. Reitittimet perustuvat sisäisiin reititystaulukoihin. Ne lukevat jokaisen saapuvan paketin ja päättävät sitten, miten paketti lähetetään eteenpäin. Lähetystapa määräytyy paketin lähde- ja kohdeosoitteen sekä verkkoliikenteen tilatietojen, kuten verkon käytön, kustannusten ja heikkojen yhteyksien perusteella. Reititintä kutsutaan joskus käyttöpisteeksi.

rekisteri

Tietokanta, johon Windows tallentaa kokoonpanoon liittyvät tiedot. Rekisteri sisältää jokaisen tietokoneen käyttäjän profiilin ja tietoja järjestelmän laitteista, asennetuista ohjelmista ja ominaisuuksien asetuksista. Windows käyttää näitä tietoja koko ajan toimiessaan.

roaming

Toiminto, jonka avulla voidaan siirtyä yhden käyttöpisteen käyttöalueelta toiselle ilman palvelukatkoja ja yhteyden menetyksiä.

roskakori

Simuloitu roskakori poistettuja tiedostoja ja kansioita varten Windowsissa.

S

salasana

Useimmiten kirjaimista ja numeroista koostuva koodi, jonka avulla voit käyttää tietokonetta, tiettyä ohjelmaa tai Web-sivustoa.

salasanasäilö

Salasanasäilö on henkilökohtaisten salasanojesi suojattu tallennesäilö. Sen avulla voit tallentaa salasanasasi luottaen siihen, ettei kukaan muu käyttäjä (ei edes järjestelmänvalvoja) saa niitä käyttöönsä.

salattu teksti

Salattu teksti. Salattu teksti ei ole lukukelpoista, ennen kuin se on muunnettu perustekstiksi (eli salaamattomaksi).

salaus

Toiminto, jossa tietoa muunnetaan tekstistä koodiksi muuttaen tietoa siten, että henkilöt, jotka eivät tiedä, kuinka salaus puretaan, eivät voi lukea sitä.

sallittujen sivustojen luettelo

Luettelo Web-sivustoista, jotka eivät sisällä haitallisia toimintoja ja joiden käyttö on siksi sallittu.

sanakirjahyökkäys

Väsytyksen menetelmähyökkäystyyppi, jossa tavallisia sanoja kokeilemalla yritetään keksiä käytössä oleva salasana.

selain

Internetin Web-sivujen selailussa käytettävä ohjelma. Suosittuja Web-selaimia ovat Microsoft Internet Explorer ja Mozilla Firefox.

sisältöluokitus-ryhmä

Käytönvalvonta-asetuksissa määritettävä ikäryhmä, johon käyttäjä kuuluu. Sisältö otetaan käyttöön tai poistetaan käytöstä käyttäjän sisältöluokitusryhmän perusteella. Sisältöluokitusryhmiä ovat pieni lapsi, lapsi, nuorempi teini-ikäinen, vanhempi teini-ikäinen ja aikuinen.

SMTP

(Simple Mail Transfer Protocol) TCP/IP-protokolla, jonka avulla viestejä voidaan lähettää verkon tietokoneesta toiseen. Tätä protokollaa käytetään Internetissä sähköpostin reitittämiseen.

solmu

Verkkoon liitetty yksittäinen tietokone.

SSID

(Service Set Identifier) Tunnus (salainen avain), jonka avulla tunnistetaan Wi-Fi (802.11) -verkko. SSID-tunnuksen määrittää verkon järjestelmänvalvoja. Jos käyttäjä haluaa liittyä verkkoon, hänen on annettava tämä tunnus.

SSL

(Secure Sockets Layer) Netscapen kehittämä protokolla henkilökohtaisten asiakirjojen lähettämiseen Internetissä. SSL-protokolla salaa SSL-yhteyden välityksellä lähetettävät tiedot julkisen avaimen avulla. SSL-yhteyden vaativa URL-osoite alkaa tekstillä https (ei http).

synkronointi

Voit yhtenäistää varmuuskopioitujen tiedostoversioiden ja paikalliseen tietokoneeseen tallennettujen tiedostoversioiden tiedot synkronoinnin avulla. Tiedostot kannattaa synkronoida silloin, kun online-varmuuskopiovarastossa oleva tiedostoversio on uudempi kuin muissa tietokoneissa olevat tiedostoversiot.

SystemGuard-toiminto

McAfee-hälytykset, jotka tunnistavat tietokoneeseen tehdyt luvattomat muutokset ja varoittavat niistä.

sähköposti

Tietokoneverkon kautta sähköisesti lähetetyt ja vastaanotetut viestit. Katso myös Webmail.

sähköpostiasiakas

Tietokoneessa suoritettava ohjelma sähköpostiviestien lähettämistä ja vastaanottamista varten (esimerkiksi Microsoft Outlook).

T

tapautuma

Käyttäjän, laitteen tai tietokoneen itsensä alulle panema toiminto, joka käynnistää vastauksen. McAfee rekisteröi tapahtumat tapahtumalokiin.

tarkistus tarvittaessa

Tarkistus, joka käynnistetään tarvittaessa (eli toiminto käynnistetään). Toisin kuin reaaliaikainen tarkistus, tarkistus tarvittaessa ei käynnisty automaattisesti.

tarkkailtavat tiedostotyypit

Tiedostotyypit (esimerkiksi .doc ja .xls), jotka McAfee Data Backup varmuuskopioi tai arkistoi tarkkailukohteissa.

tarkkailukohteet

Tietokoneen kansiot, joita McAfee Data Backup tarkkailee.

tavallinen sähköpostitili

Katso POP3.

tiedostopirstaleet

Levyille tallennettujen tiedostojen jäänteitä. Tiedostot pirstoutuvat, kun tiedostoja lisätään ja poistetaan. Levyn pirstoutuminen voi hidastaa tietokoneen suorituskykyä.

tietomurto-ohjelmisto

Työkalukokoelma (tai ohjelmakokoelma), joka takaa käyttäjälle järjestelmänvalvojaoikeudet tietokoneeseen tai tietokoneverkkoon. Tietomurto-ohjelmistot voivat olla vakoiluohjelmia ja muita mahdollisia haittaohjelmia, jotka voivat aiheuttaa suojaus- ja tietoturvariskejä tietokoneelle ja sen tiedoille.

TKIP

(Temporal Key Integrity Protocol) Protokolla, joka puuttuu WEP-suojauksen tietoturva-aukkoihin, erityisesti salausavainten uudelleenkäyttöön liittyviin ongelmiin. TKIP-protokolla vaihtaa väliaikaisia avaimia 10 000 paketin välein. Dynaamisen jakelukeinon ansiosta verkon suojausta voidaan parantaa huomattavasti. TKIP-suojaus aloitetaan 128-bittisellä väliaikaisella avaimella, jota jaetaan verkon asiakkaiden ja käyttöpisteiden välillä. TKIP-protokolla yhdistää väliaikaisen avaimen asiakkaan MAC-osoitteeseen ja luo sitten avaimen, jolla tiedot salataan, lisäämällä huomattavan suuren 16 oktetin alustusvektorin. Näin varmistetaan, että jokainen asema käyttää eri avainvirtaa tietojen salaamiseen. TKIP-protokolla käyttää RC4:ää salauksen suorittamiseen.

todennus

Henkilön tunnistusmenetelmä, joka useimmiten perustuu yksilöivään nimeen ja salasanaan.

toimialue

Paikallinen aliverkko tai kuvaus Internet-sivustoja varten.

Lähiverkossa (LAN) toimialue on asiakas- ja palvelintietokoneista koostuva aliverkko, jota valvoo yksi suojaustietokanta. Tässä kontekstissa toimialueet voivat parantaa suorituskkyä. Internetissä toimialue on osa jokaista Web-osoitetta (esimerkiksi osoitteessa www.abc.com toimialue on abc).

troijalainen

Ohjelma, joka näyttää luvalliselta, mutta joka voi vahingoittaa arvokkaita tiedostoja, häiritä tietokoneen toimintaa ja sallia tietokoneen luvattoman käytön.

tärkeä tarkkailukohde

Tietokoneellasi sijaitseva kansio, jonka muutoksia McAfee Data Backup tarkkailee. Jos määrität tärkeän tarkkailukohteen, McAfee Data Backup varmuuskopioi kaikki kyseisen kansion ja sen alihakemistojen tarkkailtavien tiedostotyyppien mukaiset tiedostot.

täydellinen arkistointi

Käyttäjän määrittämien tiedostotyyppien ja sijaintien tietojen täydellinen arkistointi. Katso myös pika-arkistointi.

U

U3

Käyttöympäristö, jossa Windows 2000- tai Windows XP -ohjelmia voi käyttää suoraan USB-asemasta. U3 on M-Systemsin ja SanDiskin vuonna 2004 julkaisema hanke, joka mahdollistaa U3-ohjelmien suorittamisen Windows-tietokoneessa, vaikka tietoja ja asetuksia ei ole asennettu eikä tallennettu koneeseen.

ulkoinen kiintolevyasema

Kiintolevyasema, joka sijaitsee tietokoneen ulkopuolella.

URL

Internet-osoitteiden standardimuoto.

USB

(Universal Serial Bus) Standardoitu sarjakäyttöliittymä, jonka avulla voit liittää tietokoneeseen oheislaitteita (esimerkiksi näppäimistön, peliohjaimen tai tulostimen).

USB-asema

Pienikokoinen muistiasema, joka liitetään tietokoneen USB-porttiin. USB-asema toimii kuten pienikokoinen levyasema. Sen avulla tiedostoja on helppo siirtää tietokoneesta toiseen.

W

wardriver-verkkovaras

Henkilö, joka etsii Wi-Fi (802.11) -verkkoja. Hän ajlee ympäri kaupunkia mukanaan Wi-Fi-tietokone sekä erityisohjelmistoja ja -laitteita.

V

varmuuskopiointi

Kopioiden luominen tärkeistä tiedostoista suojattuun online-palvelimeen.

W

Webmail

Internetin kautta sähköisesti lähetetyt ja vastaanotetut viestit. Katso myös sähköposti.

WEP

(Wired Equivalent Privacy) Salaus- ja todennusprotokolla, joka kehitettiin osana Wi-Fi (802.11) -standardia. Protokollan ensimmäiset versiot perustuivat RC4-salaustekstiin ja sisälsivät merkittäviä tietoturva-aukkoja. WEP yrittää suojata tiedot salaamalla radioaaltojen välityksellä siirrettäviä tietoja siten, että ne ovat suojattuja, kun niitä siirretään verkon yhdestä päätepisteestä toiseen. Viime aikoina on kuitenkin huomattu, että WEP-salaus ei ole aivan niin turvallinen kuin aiemmin on uskottu.

V

verkko

Yhteyspisteiden ja niihin liittyvien käyttäjien joukko, vastaavanlainen kuin ESS.

verkkoasema

Levy- tai nauha-asema, joka on liitetty useiden käyttäjien jakaman verkon palvelimeen. Verkkoasemia kutsutaan joskus etäasemiksi.

verkkokartta

Graafinen esitys kotiverkon tietokoneista ja osista.

W

Wi-Fi

(Wireless Fidelity) Wi-Fi Alliance -yhteistyöjärjestön käyttämä termi, jolla viitataan kaikkiin 802.11-verkkoihin.

Wi-Fi Alliance

Organisaatio, jonka muodostavat johtavat langattomien laitteistojen ja ohjelmistojen tarjoajat. Wi-Fi Alliancen tavoitteena on varmistaa kaikkien 802.11-standardiin perustuvien tuotteiden yhteentoimivuus sekä tehdä Wi-Fi-termi tunnetuksi kaikkien 802.11-standardiin perustuvien langattomien lähiverkkotuotteiden kansainvälisenä brändinimenä kaikilla markkinoilla. Organisaatio toimii yhteistyöjärjestönä, testauslaboratoriona ja selvitystoimistona toimittajille, jotka haluavat edistää toimialan kasvua.

Wi-Fi Certified (Wi-Fi-varmennettu)

Wi-Fi Alliancen testattavat ja hyväksyttävät tuotteet. Wi-Fi Certified -tuotteita pidetään yhteensopivina, vaikka ne olisivat eri valmistajien valmistamia. Wi-Fi Certified -tuotteen käyttäjä voi käyttää minkä tahansa valmistajan käyttöpistettä minkä tahansa valmistajan asiakasohjelmistolla edellyttäen, että myös asiakasohjelmisto on Wi-Fi Certified -tuote.

V

viestin todennuskoodi (MAC)

Tietokoneiden välillä lähetettävien viestien salaamiseen käytetty turvakoodi. Viesti hyväksytään, jos tietokone tunnistaa koodin kelvolliseksi salauksen purkamisen jälkeen.

virus

Itseään kopioiva ohjelma, joka voi tehdä muutoksia tiedostoihin tai tietoihin. Usein se näyttää tulevan luotetulta lähettäjältä tai sisältävän jotakin kiinnostavaa.

W

WLAN

(Wireless Local Area Network) Langaton lähiverkko (LAN). WLAN käyttää korkeataajuuksisia radioaaltoja johtojen sijaan tietokoneiden väliseen viestintään.

WPA

(Wi-Fi Protected Access) Määritysstandardi, joka lisää nykyisten ja tulevien langattomien lähiverkkojärjestelmien tietosuojaa ja käyttöoikeuksien hallintaa erittäin paljon. Standardi on suunniteltu toimimaan olemassa olevissa laitteistoissa ohjelmistopäivityksenä, koska WPA on kehitetty IEEE 802.11i-standardin pohjalta ja on yhteensopiva sen kanssa. Kun WPA on asennettu oikein, se tarjoaa langattomien lähiverkkojen käyttäjille korkeatasoisen suojauksen ja varmistuksen siitä, että vain luvalliset verkkokäyttäjät voivat muodostaa yhteyden verkkoon.

WPA-PSK

Erikoislaatuinen WPA-tila, joka on suunniteltu kotikäyttäjille, jotka eivät vaadi vahvaa yritystason tietosuojaa ja eivät käytä todennuspalvelimia. Tässä tilassa kotikäyttäjä antaa aloitussalasanana manuaalisesti aktivoidakseen suojatun langattoman verkkoyhteyden esijaetun avaintilan, ja vaihtaa sitten verkon jokaisen langattoman tietokoneen ja käyttöpiirteen salasanaa säännöllisesti. Katso myös kohdat WPA2-PSK ja TKIP.

WPA2

WPA-tietosuojastandardin päivitys, joka perustuu 802.11i IEEE -standardiin.

WPA2-PSK

Erityinen WPA-tila, joka on samankaltainen WPA-PSK:n kanssa ja perustuu WPA2-standardiin. WPA2-PSK:n yleinen ominaisuus on se, että laitteet tukevat usein monia erilaisia salaustoimintoja (kuten AES, TKIP) samanaikaisesti, kun vanhemmat laitteet useimmiten tukivat vain yhtä salaustoimintoa kerralla (eli kaikkien laitteiden täytyi käyttää samaa salaustoimintoa).

V

VPN

(Virtual Private Network) Yksityinen verkko, joka on konfiguroitu julkiseen verkkoon niin, että se voi hyödyntää julkisen verkon hallintaominaisuuksia. VPN-verkkojen avulla yritykset muodostavat maantieteellisesti laajoja suuralueverkkoja (WAN-verkkoja), joilla yhdistetään sivukonttorit toisiinsa tai mahdollistetaan mobiilikäyttäjien yhteys yrityksen lähiverkkoon.

väliaikainen tiedosto

Käyttöjärjestelmän tai jonkin muun ohjelman muistiin tai levyille luoma tiedosto, jota käytetään istunnon aikana ja joka sen jälkeen poistetaan.

välimuisti

Tietokoneessa oleva tietojen väliaikainen tallennusalue. Esimerkiksi Web-sivujen selaamisen nopeuttamiseksi ja tehokkuuden parantamiseksi selain voi hakea Web-sivun (etäpalvelimen sijaan) välimuistista, kun haluat tarkastella sitä seuraavan kerran.

välimuistipalvelin

Palomuurin osa, joka hallitsee lähiverkon saapuvaa ja lähtevää Internet-tietoliikennettä. Välimuistipalvelin voi parantaa verkon suorituskykyä toimittamalla usein pyydettyjä tietoja, kuten suosittuja Web-sivuja, ja suodattamalla ja hylkäämällä pyyntöjä, joita verkon omistaja ei pidä asianmukaisina, kuten yksityistiedostojen luvaton käyttöä koskevia pyyntöjä.

välityspalvelin

Tietokone tai tietokoneessa suoritettava ohjelmisto, joka toimii verkon ja Internetin välisenä suojamuurina ja näyttää ainoastaan yhden verkko-osoitteen ulkopuolisille sivustoille. Koska välityspalvelin edustaa kaikkia sisäisiä tietokoneita, se suojaa käyttäjien verkkoidentiteettiä mahdollistaen kuitenkin Internet-yhteyksien muodostamisen. Katso myös välimuistipalvelin.

väsytyksen menetelmähyökkäys

Menetelmä, jonka avulla yritetään purkaa salattua tietoa (esimerkiksi salasanoja) sinnikkäällä yrittämisellä (väsytyksen menetelmällä) älykkään strategian sijaan. Väsytyksen menetelmää pidetään erehtymättömänä, joskin aikaa vievänä murtautumiskeinona. Väsytyksen menetelmähyökkäystä kutsutaan myös väsytyksen menetelmämurtautumiseksi.

Y

yhdistetty yhdyskäytävä

Laite, joka yhdistää langattoman käyttöpiirteen, reitittimen ja palomuurin toiminnot. Jotkut laitteet saattavat sisältää myös suojausparannuksia ja siltausominaisuuksia.

yhteyden muodostaja

Internet-yhteyden muodostamisessa käytettävä ohjelmisto. Yhteyden muodostajia voidaan käyttää haitallisesti ohjaamalla Internet-yhteydet edelleen muualle kuin oletusarvoisen Internet-palveluntuottajan (ISP) osoitteeseen ilmoittamatta käyttäjälle aiheutuvista lisäkustannuksista.

Ä

älykäs asema

Katso USB-asema.

Tietoja McAfeesta

McAfee, Inc.:n pääkonttori sijaitsee Santa Clarassa, Kaliforniassa. McAfee on maailman johtavia tietomurtojen esto- ja tietoturvariskien hallintasoventusten valmistajia. McAfee toimittaa luotettavia ratkaisuja ja palveluita, jotka suojaavat järjestelmiä ja verkkoja ympäri maailman. McAfeen kokemus tietoturvakysymyksissä ja sen tehokas tuotekehitys tuottavat sovelluksia, joiden avulla kotikäyttäjät, yritykset, julkisen sektorin laitokset ja palveluntarjoajat pystyvät torjumaan hyökkäyksiä, estämään haittayrityksiä ja kehittämään ja parantamaan tietoturvaansa jatkuvasti.

Copyright

Copyright © 2007–2008 McAfee, Inc., Kaikki oikeudet pidätetään. Mitään tämän julkaisun osaa ei saa jäljentää, lähettää, kopioida, tallentaa tallennusjärjestelmään eikä kääntää millekään kielelle missään muodossa tai millään tavalla ilman McAfee, Inc.:n myöntämää kirjallista lupaa. McAfee ja muut tässä julkaisussa mainitut tavaramerkit ovat McAfee, Inc.:n ja/tai sen yhteistyökumppaneiden rekisteröityjä tavaramerkkejä Yhdysvalloissa ja/tai muissa maissa. McAfee käyttää mainonnassaan tuotteilleen ominaista punaista väriä, jonka avulla McAfee-tuotteet voidaan erottaa muista tietoturvatuotteista. Kaikki muut tässä julkaisussa mainitut rekisteröidyt ja rekisteröimättömät tavaramerkit ja tekijänoikeuden suojaamat materiaalit ovat yksinomaan omistajiensa omaisuutta.

TAVARAMERKIT

AVERT, EPO, EPOLICY ORCHESTRATOR, FLASHBOX, FOUNDSTONE, GROUPSHIELD, HERCULES, INTRUSHIELD, INTRUSION INTELLIGENCE, LINUXSHIELD, MANAGED MAIL PROTECTION, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, MCAFEE.COM, NETSHIELD, PORTALSHIELD, PREVENTSYS, PROTECTION-IN-DEPTH STRATEGY, PROTECTIONPILOT, SECURE MESSAGING SERVICE, SECURITYALLIANCE, SITEADVISOR, THREATSCAN, TOTAL PROTECTION, VIREX, VIRUSSCAN.

Käyttöoikeus

HUOMAUTUS KAIKILLE KÄYTTÄJILLE: LUE HUOLELLISESTI OSTAMAASI KÄYTTÖOIKEUTTA VASTAAVA LAILLINEN SOPIMUS, JOSSA MÄÄRITETÄÄN LISENSSINALAISET OHJELMISTON YLEISET KÄYTTÖEHDOT. ELLET TIEDÄ HANKKIMASI KÄYTTÖOIKEUDEN TYYPPIÄ, TUTKI OHJELMISTON MUKANA TULLEITA MYYNTEI-, MYYNITILAUS- JA MUITA KÄYTTÖOIKEUDEN MYÖNTÄMISEEN LIITTYVIÄ ASIAKIRJOJA TAI ASIAKIRJOJA, JOITA OLET SAANUT ERILLÄÄN OSTON YHTEYDESSÄ (VIHKONA, TIEDOSTONA TUOTTEEN CD-LEVYLLÄ TAI TIEDOSTONA INTERNET-SIVUSTOSTA, JOSTA OLET LADANNUT OHJELMISTOPAKETIN). JOS ET HYVÄKSY KAIKKIA TÄMÄN SOPIMUKSEN EHTOJA, ÄLÄ ASENNA OHJELMISTOA. TIETYISSÄ TAPAUKSISSA VOIT PALAUTTAA TUOTTEEN MCAFEE-YHTIÖLLE TAI OSTOPAIKKAAN JA SAADA TÄYDEN HYVITYKSEN MAKSUSTASI.

L U K U 4 6

Asiakaspalvelu ja tekninen tuki

SecurityCenter raportoi kriittiset ja ei-kriittiset suojausongelmat heti, kun se havaitsee ne. Kriittiset suojausongelmat vaativat välittömiä toimenpiteitä ja vaarantavat suojauksen tilan (väri muuttuu punaiseksi). Ei-kriittiset ongelmat eivät vaadi välittömiä toimenpiteitä, mutta ne voivat vaarantaa suojauksen tilan (ongelmatyypin mukaan). Jotta saat suojauksen tilan vihreäksi, sinun täytyy ratkaista kaikki kriittiset ongelmat ja joko ratkaista tai ohittaa kaikki ei-kriittiset ongelmat. Jos tarvitset apua suojausongelmien selvittämisessä, voit käyttää McAfee Virtual Technician -palvelua. Lisätietoja McAfee Virtual Technician -palvelusta löydät McAfee Virtual Technician -ohjeesta.

Jos ostit ohjelmiston McAfeen kumppanilta tai muulta toimittajalta kuin McAfee, avaa Web-selain ja siirry osoitteeseen www.mcafeehelp.com. Siirry sitten McAfee Virtual Technician -palveluun valitsemalla kohdasta Partner Links käyttämäsi kumppani tai palveluntarjoaja.

Huomautus: Sinun on kirjauduttava Windowsiin järjestelmänvalvojana, jotta voit asentaa McAfee Virtual Technicianin. Jos et tee näin, MVT ei ehkä voi ratkaista ongelmia. Tietoja Windowsiin kirjautumisesta järjestelmänvalvojana on Windowsin ohjeessa. Windows Vista™ näyttää ilmoituksen, kun käynnistät MVT:n. Kun näyttöön tulee ilmoitus, valitse **Hyväksy**. Virtual Technician -palvelu ei toimi Mozilla® Firefoxilla.

Tässä luvussa

McAfee Virtual Technician -palvelun käyttö.....	262
Tuki ja lataukset	263

McAfee Virtual Technician -palvelun käyttö

Virtual Technician -palvelu on kuin oma tukihenkilösi. Se kerää tietoja tietokoneeseesi asennetuista SecurityCenter-ohjelmista ja auttaa sinua ratkaisemaan tietokoneesi turvallisuusongelmat. Kun käynnistät Virtual Technician -palvelun, se tarkistaa, että tietokoneesi SecurityCenter-ohjelmat toimivat oikein. Jos ongelmia löytyy, Virtual Technician tarjoutuu ratkaisemaan ne, tai se antaa sinulle tarkempia tietoja niistä. Lopuksi Virtual Technician näyttää analyysinsä tulokset ja antaa mahdollisuuden hakea lisää teknistä tukea McAfeelta tarvittaessa.

Jotta tietokoneesi ja tiedostojesi tietoturva ja eheys säilyvät, Virtual Technician ei kerää henkilö- eikä tunnistetietoja.

Huomautus: Saat lisätietoja Virtual Technician -palvelusta napsauttamalla **Help**-kuvaketta.

Virtual Technician -palvelun käynnistäminen

Virtual Technician kerää tietoja tietokoneeseesi asennetuista SecurityCenter-ohjelmista ja auttaa sinua ratkaisemaan tietokoneesi suojausongelmat. Yksityisyytesi turvaamiseksi näihin tietoihin ei sisälly henkilö- eikä tunnistetietoja.

- 1 Valitse **Yleiset tehtävät** -kohdasta **McAfee Virtual Technician**.
- 2 Lataa Virtual Technician toimimalla näytön ohjeiden mukaan.

Tuki ja lataukset

Lisätietoja oman maasi McAfeen tuki- ja lataussivustoista sekä käyttöoppaiden lataussivustoista on seuraavissa taulukoissa.

Tuki ja lataukset

Maa	McAfee-tuki	McAfee-lataussivustot
Australia	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brasilia	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Kanada (englanti)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Kanada (ranska)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Kiina (Kiina)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
Kiina (Taiwan)	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Tšekki	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Tanska	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Suomi	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
Ranska	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Saksa	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Iso-Britannia	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
Italia	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Japani	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
Korea	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Meksiko	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Norja	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
Puola	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp

Portugali	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
Espanja	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Ruotsi	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Turkki	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
Yhdysvallat	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

McAfee Total Protection -käyttöoppaat

Maa	McAfee-käyttöoppaat
Australia	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brasilia	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Kanada (englanti)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Kanada (ranska)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
Kiina (Kiina)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
Kiina (Taiwan)	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Tšekki	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Tanska	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Suomi	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
Ranska	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Saksa	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Iso-Britannia	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Alankomaat	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
Japani	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf

Korea	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Meksiko	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Norja	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Puola	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
Portugali	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Espanja	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Ruotsi	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Turkki	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Yhdysvallat	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

McAfee Internet Security -käyttöoppaat

Maa	McAfee-käyttöoppaat
Australia	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brasilia	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Kanada (englanti)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Kanada (ranska)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
Kiina (Kiina)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
Kiina (Taiwan)	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Tšekki	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Tanska	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Suomi	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
Ranska	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Saksa	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf

Iso-Britannia	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Alankomaat	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Japani	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Meksiko	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Norja	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Puola	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portugali	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
Espanja	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Ruotsi	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Turkki	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Yhdysvallat	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

McAfee VirusScan Plus -käyttöoppaat

Maa	McAfee-käyttöoppaat
Australia	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brasilia	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Kanada (englanti)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Kanada (ranska)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
Kiina (Kiina)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
Kiina (Taiwan)	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Tšekki	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf

Tanska	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Suomi	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
Ranska	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Saksa	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Iso-Britannia	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Alankomaat	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japani	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Meksiko	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Norja	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Puola	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Portugali	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
Espanja	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Ruotsi	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Turkki	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
Yhdysvallat	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

McAfee VirusScan -käyttöoppaat

Maa	McAfee-käyttöoppaat
Australia	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brasilia	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Kanada (englanti)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf

Kanada (ranska)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
Kiina (Kiina)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
Kiina (Taiwan)	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Tšekki	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Tanska	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Suomi	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
Ranska	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Saksa	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Iso-Britannia	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Alankomaat	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japani	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Meksiko	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Norja	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
Puola	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portugali	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
Espanja	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Ruotsi	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Turkki	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Yhdysvallat	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

Lisätietoja oman maasi McAfee Threat Centeristä ja virustietoja sisältävistä sivustoista on seuraavassa taulukossa.

Maa	Tietoturvasivustot	Virustietoja
Australia	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brasilia	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Kanada (englanti)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Kanada (ranska)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Kiina (Kiina)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
Kiina (Taiwan)	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Tšekki	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Tanska	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Suomi	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
Ranska	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Saksa	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Iso-Britannia	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Alankomaat	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Italia	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japani	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Korea	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Meksiko	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Norja	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
Puola	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
Portugali	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo

Espanja	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Ruotsi	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Turkki	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Yhdysvallat	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

Lisätietoja oman maasi HackerWatch-sivustoista on seuraavassa taulukossa.

Maa	HackerWatch
Australia	www.hackerwatch.org
Brasilia	www.hackerwatch.org/?lang=pt-br
Kanada (englanti)	www.hackerwatch.org
Kanada (ranska)	www.hackerwatch.org/?lang=fr-ca
Kiina (Kiina)	www.hackerwatch.org/?lang=zh-cn
Kiina (Taiwan)	www.hackerwatch.org/?lang=zh-tw
Tšekki	www.hackerwatch.org/?lang=cs
Tanska	www.hackerwatch.org/?lang=da
Suomi	www.hackerwatch.org/?lang=fi
Ranska	www.hackerwatch.org/?lang=fr
Saksa	www.hackerwatch.org/?lang=de
Iso-Britannia	www.hackerwatch.org
Alankomaat	www.hackerwatch.org/?lang=nl
Italia	www.hackerwatch.org/?lang=it
Japani	www.hackerwatch.org/?lang=jp
Korea	www.hackerwatch.org/?lang=ko
Meksiko	www.hackerwatch.org/?lang=es-mx
Norja	www.hackerwatch.org/?lang=no
Puola	www.hackerwatch.org/?lang=pl
Portugali	www.hackerwatch.org/?lang=pt-pt
Espanja	www.hackerwatch.org/?lang=es
Ruotsi	www.hackerwatch.org/?lang=sv
Turkki	www.hackerwatch.org/?lang=tr

Yhdysvallat www.hackerwatch.org

Hakemisto

8

802.11	244
802.11a.....	244
802.11b	244
802.1x.....	244

A

ActiveX-komponentti	244
Ajoita automaattinen arkistointi	187
Ajoita Levyn eheytytys -tehtävä	203
Ajoita QuickClean-tehtävä.....	201
Analysoi saapuvaa ja lähtevää tietoliikennettä	119
Anti-Spamin ominaisuudet	125
arkistointi	244
Arkistoitujen tiedostojen käsittelyminen	189
Arkistoitujen tiedostojen palauttaminen	192
Arkistojen hallinta	194
Arkiston asetusten määrittäminen.....	182
Asenna käytettävissä oleva verkkotulostin	242
Asenna McAfee-tietoturvaohjelmisto etätietokoneisiin.....	225
Aseta tietoturvasoksi Lukitus.....	77
asiakas	244
Asiakaspalvelu ja tekninen tuki	261
Avaa arkistoitu tiedosto.....	191
Avaa EasyNetwork	229
avain	244
avainsana	245
Avainsanojen suodatuksen poistaminen käytöstä.....	170

C

Copyright	259
-----------------	-----

D

DAT	245
DNS.....	245
DNS-palvelin.....	245

E

EasyNetworkin asentaminen.....	229
EasyNetworkin ominaisuudet	228

Eheytä tietokoneesi	200
Eristettyjen ohjelmien ja evästeiden käsittelyminen.....	61
Eristettyjen tiedostojen käsittelyminen.....	60
eristäminen.....	245
ESS	245
Estä käyttöoikeudet äskettäisten tapahtumien lokista.....	94
Estä ohjelman käyttöoikeudet.....	93
Estä olemassa olevan järjestelmäpalveluportin käyttö.....	99
Estä tietokone saapuvien tapahtumien lokista.....	109
Estä tietokone tietomurtojen havainnoinnin tapahtumien lokista.....	109
Estä uuden ohjelman käyttöoikeudet.....	93
Estä Web-sivustot avainsanojen perusteella	170
Etsi arkistoitua tiedostoa	190
eväste.....	245

F

Firewallin lukitseminen ja palauttaminen	85
--	----

H

Hae jaettu tiedosto	237
Hae ohjelmatietoja lähtevien tapahtumien lokista.....	96
Hakuehdot	237
Hallitse laitetta	223
Hallitse McAfee-tiliä.....	11
hallittu verkko	245
Hallittuun verkkoon liittyminen . 218, 230, 234	
Hallitun verkon määrittäminen	215
Hallitusta verkosta poistuminen	234
Hanki ohjelmatietoja	96
Hanki tietokoneen rekisteröintitiedot . 115	
Hanki tietokoneen verkkotiedot	115
Henkilökohtaisen suodattimen määrittäminen	142, 143
Henkilökohtaisten suodattimien käyttäminen	142
Henkilökohtaisten tietojen suojaaminen	174

Hyväksy tiedosto toisesta tietokoneesta	239, 240
Hälytyksiin liittyvien suositusten asetusten määrittäminen	80
Hälytysasetusten määrittäminen	24
Hälytysten käsitteleminen	14, 21, 69

I

Ilmoita roskapostista McAfeelle	149
Ilmoituksen saaminen tiedoston lähettämisestä	240
Internet.....	246
Internet-tietoliikenteen jäljittäminen ..	115
Internet-tietoliikenteen valvonta	118
intranet.....	246
IP-huijausyritys.....	246
IP-osoite	246

J

Jaa tiedosto.....	236
jaettu salaisuus	246
Jaettujen tulostinten käyttäminen	242
jakaminen	246
julkaiseminen	246
Jäljitä tietokone saapuvien tapahtumien lokista	116
Jäljitä tietokone tietomurtojen havainnoinnin tapahtumien lokista ..	116
Jäljitä valvottu IP-osoite	117
Jäljitä verkkotietokone maantieteellisesti	115
järjestelmän palautuspiste.....	246
Järjestelmäpalveluiden hallinta.....	97
Järjestelmäpalveluporttien asetusten määrittäminen	98

K

kaistanleveys	247
Keskeytä automaattinen arkistointi	188
kieltoluettelo	247
kirjasto	247
Kirjaus, valvonta ja analyysi.....	111
komentosarja	247
Kopioi jaettu tiedosto	237
Kopioi tai poista suodatettu Web- sähköpostiviesti.....	150
Korjaa suojausongelmat automaattisesti	18
Korjaa suojausongelmat manuaalisesti ..	19
Korjaa tietoturvan puutteet	224
kotiverkko.....	247
Kutsu tietokone hallittuun verkkoon ...	219
kuvasuodatus	247

Käynnistä HackerWatch-opetusohjelma	122
Käynnistä komentosarjatarkistussuojaus	34
Käynnistä pikaviestisuojaus	35
Käynnistä reaaliaikainen virustorjunta ..	31
Käynnistä sähköpostisuojaus	34
Käynnistä vakoiluohjelmassuojaus	34
Käyttäjien määrittäminen.....	158
Käyttöoikeus	260
Käyttöpiste	247
Käytä merkistösuodattimia	140
Käytä verkkokarttaa.....	216
Käytönvalvonnan määrittäminen	157
käytönvalvonta-asetukset.....	247

L

Laadi tarkistusaikataulu.....	43
Lajittele arkistoidut tiedostot	190
Lakkaa luottamasta verkon tietokoneisiin	220
langaton USB-verkkosovitinkortti	247
langaton verkkopiste.....	247
langaton verkkosovitin	248
langattomat PCI-verkkosovitinkortit ...	248
laukaisualusta.....	248
Liity hallittuun verkkoon	218
Liity verkkoon	231
Lisäsuojauksen ottaminen käyttöön.....	33
Lisää estetty tietokoneyhteys	107
Lisää henkilökohtainen suodatin.....	142
Lisää kohde arkistoon	183
Lisää luotettava tietokone saapuvien tapahtumien lokista.....	105
Lisää luotettava tietokoneyhteys.....	104
Lisää McAfee-käyttäjä	160
Lisää osoitekirja.....	132
Lisää salasana	176
Lisää toimialue	135
Lisää Web-sivusto valkoiseen listaan...	151
Lisää Web-sähköpostitili	127
Lisää ystävä Anti-Spam-työkaluriviltä ..	134
Lisää ystävä manuaalisesti	134
Lopeta reaaliaikainen virustorjunta.....	31
Lopeta tiedoston jakaminen.....	236
Lopeta tietokoneen suojauksen tilan valvominen.....	222
Lopeta tulostimen jakaminen	242
Lukitse Firewall välittömästi	85
Luotettavan tietokoneyhteyden muokkaaminen	105
luotettujen luettelo.....	248
Luotettujen luetteloiden hallinta	51
Luotettujen luetteloiden käyttäminen...	51

luvaton käyttö piste	248
Lähetä tiedosto toiseen tietokoneeseen	239
lähiverkko	248

M

MAC-osoite	248
mahdollinen haittaohjelma (PUP)	248
Mahdollisesti sopimattomien Web-kuvien suodattaminen	163
Mahdollisten haittaohjelmien käsittely	60
Manuaalisen tarkistuksen asetusten määrittäminen	40
MAPI	248
mato	248
McAfee Anti-Spam	123
McAfee Data Backup	179
McAfee EasyNetwork	227
McAfee Internet Security	3
McAfee Network Manager	211
McAfee Personal Firewall	63
McAfee QuickClean	195
McAfee SecurityCenter	5
McAfee Shredder	207
McAfee Virtual Technician -palvelun käyttö	262
McAfee VirusScan	29
McAfee-käyttäjien asetusten määrittäminen	159, 160
McAfee-tietosuojapalvelu	155
McAfee-tilin hallinta	11
melko tärkeät tarkailukohteet	249
Merkitse viesti Anti-Spam-työkaluriviltä	145
MITM-hyökkäys	249
MSN	249
Muokkaa estettyä tietokoneyhteyttä	108
Muokkaa hallitun tietokoneen oikeuksia	223
Muokkaa henkilökohtaista suodatinta	143
Muokkaa järjestelmäpalveluporttia	100
Muokkaa laitteen näytön ominaisuuksia	223
Muokkaa Levyn eheytyksen tehtävää	204
Muokkaa McAfee-käyttäjän tilitietoja	161
Muokkaa osoitekirjaa	132
Muokkaa QuickClean-tehtävää	202
Muokkaa salasanaa	176
Muokkaa toimialuetta	136
Muokkaa valkoisessa listassa olevia sivustoja	152
Muokkaa Web-sähköpostitiliä	128

Muokkaa viestin käsittely- ja merkintätapaa	142, 146
Muokkaa ystävää	135
Muuta arkiston sijaintia	185
Muuta suodatustasoa	139
Myönnä ohjelmalle täydet käyttöoikeudet	88
Myönnä ohjelmalle vain lähtevän tietoliikenteen käyttöoikeudet	91
Myönnä täydet käyttöoikeudet lähtevien tapahtumien lokista	90
Myönnä täydet käyttöoikeudet äskettäisten tapahtumien lokista	89
Myönnä uudelle ohjelmalle täydet käyttöoikeudet	89
Myönnä vain lähtevän tietoliikenteen käyttöoikeudet lähtevien tapahtumien lokista	92
Myönnä vain lähtevän tietoliikenteen oikeudet äskettäisten tapahtumien lokista	91
Myönnä verkon käyttöoikeudet	231
Määritä arkistotiedostojen tyypit	184
Määritä automaattiset päivitykset	14
Määritä käyttäjän sisältöluokitusryhmä	164
Määritä manuaalisen tarkistuksen asetukset	40
Määritä manuaalisen tarkistuksen kohteen sijainti	42
Määritä palomuurin suojauksen tilan asetukset	84
Määritä ping-pyyntöjen asetukset	83
Määritä reaaliaikaisen tarkistuksen asetukset	38
Määritä SystemGuards-asetukset	45
Määritä tapahtumalokin asetukset	112
Määritä tietomurtojen havainnoinnin asetukset	83
Määritä uuden järjestelmäpalveluportin asetukset	99

N

Network Managerin kuvakkeiden toiminta	213
Network Managerin ominaisuudet	212
NIC	249
Nimeä verkko uudelleen	217, 233
Nollaa salasanasäilön salasana	178
Nouda McAfee-järjestelmänvalvojan salasana	162
Näytä arkistointitoimintojen yhteenveto	194
Näytä hälytykset pelaamisen aikana	73

Näytä kohteen tiedot	217
Näytä suodatettujen Web- sähköpostiviestien tapahtumat	150
Näytä tai piilota kohde verkkokartalla	217
Näytä tai piilota tiedottavat hälytykset	22
Näytä tai piilota tiedottavat hälytykset pelejä pelattaessa	23
Näytä tarkistuksen tulokset	56
Näytä vain suositukset	81

O

Ohita suojausongelma	20
Ohitettujen ongelmien näyttäminen tai piilottaminen	20
Ohjelmien Internet-käyttöoikeuden estäminen	93
Ohjelmien Internet-käyttöoikeuden salliminen	88
Ohjelmien ja käyttöoikeuksien hallinta	87
Ohjelmien käyttöoikeuksien poistaminen	95
Ominaisuudet	180
online-varmuuskopiovarasto	249
Opas	243
Ota SystemGuards-suojaus käyttöön	45

P

Paikallisen arkiston hallintaohjelman käyttäminen	190
pakkaus	249
Palauta Firewallin asetukset	86
Palauta puuttuvia tiedostoja paikallisesta arkistosta	192
Palauta tiedoston aikaisempi versio paikallisesta arkistosta	193
palauttaminen	249
palomuuuri	249
Palomuurin käynnistäminen	67
Palomuurin suojauksen optimointi	82
Palomuurin tietoturvasojen hallinta	76
Palomuurisuojauksen asetusten määrittäminen	75
Palomuurisuojauksen käynnistäminen	67
Palomuurisuojauksen pysäyttäminen	68
palvelin	249
palvelun esto	249
Perehtyminen Internet-tietoturvaan	121
Perehtyminen ohjelmiin	96
Personal Firewall -ohjelman ominaisuudet	64
perusteksti	250
phishing-huijaus	250
Phishing-huijausten torjunnan asetusten määrittäminen	151

piilojäljitteet	250
Piilota aloitusnäyttö käynnistyksessä	24
Piilota tiedottavat hälytykset	74
Piilota virusesiintymähälytykset	25
pika-arkistointi	250
pikakuvake	250
plug-in	250
Poista Anti-Spam-työkalurivi käytöstä	146
Poista arkiston salaus ja pakkaus käytöstä	186
Poista automaattiset päivitykset käytöstä	14
Poista erikoissuodatin käytöstä	139
Poista estetty tietokoneysteys	108
Poista Firewallin lukitus välittömästi	85
Poista henkilökohtainen suodatin	143
Poista järjestelmäpalveluportti	101
Poista Levyn eheytytys -tehtävä	205
Poista luotettava tietokoneysteys	106
Poista McAfee-käyttäjä	161
Poista ohjelman käyttöoikeudet	95
Poista osoitekirja	133
Poista phishing-huijausten torjunta käytöstä	153
Poista QuickClean-tehtävä	203
Poista roskapostin torjunta käytöstä	137
Poista salasana	177
Poista suositukset käytöstä	81
Poista tiedostoja Puuttuvat tiedostot - luettelosta	193
Poista Web-sivusto valkoisesta listasta	152
Poista Web-sähköpostitili	129
Poista ystävä	136
Poistu hallitusta verkosta	234
ponnahdusikkunat	250
POP3	250
portti	250
PPPoE	250
Privacy Service -ohjelman ominaisuudet	156
protokolla	250
Puhdista tietokone	199
puskurin ylivuoto	251
Päivitä verkkokartta	216

Q

QuickCleanin toiminnot	196
------------------------------	-----

R

RADIUS	251
reaaliaikainen tarkistus	251
Reaaliaikaisen tarkistuksen asetusten määrittäminen	38

Reaaliaikaisen virustorjunnan	
käynnistäminen.....	31
reititin	251
rekisteri.....	251
roaming	251
roskakori.....	251
Roskapostiviestien tunnistustavan	
määrittäminen	137

S

salasana	251
salasanasäilö	251
Salasanasäilön asentaminen	176
Salasanojen suojaaminen	175
salattu teksti	252
salaus	252
Salli olemassa olevan	
järjestelmäpalveluportin käyttö	99
sallittujen sivustojen luettelo	252
sanakirjahyökkäys	252
SecurityCenterin käyttäminen	7
SecurityCenterin ominaisuudet	6
SecurityCenterin päivittäminen	13
selain	252
Shredderin toiminnot	208
sisältöluokitus-ryhmä	252
Sisältöluokitusryhmän määrittäminen	
.....	163, 164
SMTP	252
Soita ääni hälytyksen esiintyessä	24
solmu	252
SSID	252
SSL	252
Sulje kohde arkistosta pois	184
Suodata mahdollisesti sopimattomat	
Web-kuvat.....	163
Suodatettujen sähköpostiviestien	
käsitleminen.....	149
Suodatetun Web-sivuston poistaminen	
.....	169
Suodatetun Web-sivuston päivittäminen	
.....	168
Suodatusasetusten määrittäminen	138
Suojaa henkilökohtaisia tietoja	174
Suojaa tietokonetta käynnistyksen aikana	
.....	82
Suojauksen tilan toiminta.....	7, 8, 9
Suojausluokkien toiminta.....	7, 9, 27
Suojausongelmien korjaaminen	8, 18
Suojausongelmien korjaaminen ja	
ohittaminen	8, 17
Suojausongelmien ohittaminen	20
Suojauspalveluiden toiminta.....	10

Suojaustason määrittäminen Avoin-	
tasolle.....	79
Suojaustason määrittäminen Luottava-	
tasolle.....	78
Suojaustason määrittäminen Normaali-	
tasolle.....	78
Suojaustason määrittäminen Tiukka-	
tasolle.....	78
Suojaustason määrittäminen Vaikeasti	
havaittava -tasolle	77
Suorita manuaalinen arkistointi	188
Suosittelun käyttöönotto	80
synkronointi	253
SystemGuards-toimintojen asetukset ..	44
SystemGuard-toiminto	253
sähköposti.....	253
sähköpostiasiakas.....	253
Sähköpostin suodatus.....	145

T

tapahtuma	253
Tapahtumien kirjaus.....	112
Tapahtumien näyttäminen	18, 27
Tarkastele kaikkia tapahtumia	27
Tarkastele lähteviä tapahtumia.....	89, 113
Tarkastele maailman Internet-	
porttitapahtumia	114
Tarkastele maailman	
tietoturvatapahtumien tilastotietoja	114
Tarkastele saapuvia tapahtumia	113
Tarkastele tietomurtojen havainnoinnin	
tapahtumia.....	113
Tarkastele äskettäisiä tapahtumia .	27, 112
Tarkista päivitykset	13, 14
Tarkistuksen tulosten käyttäminen	59
tarkistus tarvittaessa	253
tarkkailtavat tiedostotyypit.....	253
tarkkailukohteet	253
tavallinen sähköpostitili.....	253
Tehtävän ajoittaminen	201
Tiedostojen arkistointi.....	181
Tiedostojen jakaminen	236
Tiedostojen jakaminen ja lähettäminen	
.....	235
Tiedostojen lähettäminen toisiin	
tietokoneisiin	239
Tiedostojen, kansiodien ja levyjen	
tuhoaminen.....	209
tiedostopirstaleet	253
Tiedottavien hälytysten hallinta.....	73
Tiedottavien hälytysten näyttäminen ja	
piilottaminen	22
Tietoja hälytyksistä.....	70

Tietoja luotettujen luetteloiden tyypeistä	52
Tietoja McAfeesta	259
Tietoja SystemGuards-tyypeistä.....	46, 47
Tietoja tietoliikenneanalyysin kaaviosta	118
Tietojen suojaaminen Internetissä	173
Tietokoneen eheyttäminen.....	200
Tietokoneen puhdistaminen	197
Tietokoneen tarkistaminen	31, 55, 56
Tietokoneyhteyksien estäminen	107
Tietokoneyhteyksien hallinta	103
Tietokoneyhteyksiin luottaminen	104
tietomurto-ohjelmisto	253
Tietoturvan puutteiden korjaaminen	224
Tilan ja oikeuksien valvonta	222
Tilastotietojen käsitteleminen	114
TKIP	254
todennus	254
toimialue	254
troijalainen.....	254
Tuhoa koko levy.....	210
Tuhoa tiedostoja ja kansioita.....	209
Tuki ja lataukset.....	263
Tulostinten jakaminen	241
tärkeä tarkkailukohde	254
täydellinen arkistointi	254
Täydellisen arkistoinnin ja pika- arkistoinnin suorittaminen	187

U

U3	254
ulkoinen kiintolevyasema.....	254
URL.....	254
USB	255
USB-asema.....	255

V,W

Vahvista tilaus.....	11
Vaihda McAfee-järjestelmänvalvojan salasana.....	162
Vaihda Salanasäilön salasana	177
Vain lähtevän tietoliikenteen käyttöoikeuksien myöntäminen	91
Valvo ohjelman kaistanleveyttä.....	119
Valvo ohjelmatapahtumia	119
Valvo tietokoneen suojauksen tilaa.....	222
wardriver-verkkovaras	255
varmuuskopiointi	255
Webmail	255
Web-selauksen aikarajoitusten määrittäminen	166
Web-sivustojen suodattaminen ..	164, 167

Web-sivustojen suodattaminen avainsanojen avulla	167, 170
Web-sivuston estäminen	167
Web-sivuston salliminen	168
Web-sähköpostitilien määrittäminen ..	127
Web-sähköpostitilin tietojen ymmärtäminen	128, 129
WEP	255
verkko	255
verkkoasema.....	255
Verkkokartan käyttäminen	216
verkkokartta.....	255
Verkon etähallinta	221
viestin todennuskoodi (MAC)	256
Wi-Fi.....	255
Wi-Fi Alliance	256
Wi-Fi Certified (Wi-Fi-varmennettu) ..	256
Windows-käyttäjien asetusten määrittäminen	159
Windows-käyttäjiin vaihtaminen.....	160
Virtual Technician -palvelun käynnistäminen	262
virus.....	256
VirusScan-ohjelman ominaisuudet	30
Virusten ja troijalaisten käsitteleminen ..	59
Virustorjunnan määrittäminen	37, 55
WLAN	256
WPA	256
WPA2	256
WPA2-PSK.....	257
WPA-PSK.....	256
VPN.....	257
väliaikainen tiedosto	257
välimuisti	257
välimuistipalvelin.....	257
välityspalvelin.....	257
väsytyksen menetelmähyökkäys	257

Y

yhdistetty yhdyskäytävä.....	257
yhteyden muodostaja	258
Ystävien määrittäminen	131
Ystävien määrittäminen automaattisesti	132
Ystävien määrittäminen manuaalisesti	134

Ä

älykäs asema.....	258
-------------------	-----