

McAfee® **Total Protection**

Käyttöopas

Sisältö

McAfee Total Protection	3
McAfee SecurityCenter	5
SecurityCenterin ominaisuudet	6
SecurityCenterin käyttäminen	7
Suojausongelmien korjaaminen ja ohittaminen	17
Hälytysten käsitteleminen	21
Tapahtumien näyttäminen	27
McAfee VirusScan	29
VirusScan-ohjelman ominaisuudet	30
Tietokoneen tarkistaminen	31
Tarkistuksen tulosten käyttäminen	37
Tarkistustavat	40
Lisäsuojauksen käyttäminen	43
Virustorjunnan määrittäminen	47
McAfee Personal Firewall	65
Personal Firewallin ominaisuudet	66
Palomuurin käynnistäminen	67
Hälytysten käsitteleminen	69
Tiedottavien hälytysten hallinta	71
Palomuurisuojauksen asetusten määrittäminen	73
Ohjelmien ja käyttöoikeuksien hallinta	85
Tietokoneyhteyksien hallinta	93
Järjestelmäpalveluiden hallinta	101
Kirjaus, valvonta ja analyysi	107
Perehtyminen Internet-tietoturvaan	117
McAfee Anti-Spam	119
Anti-Spamin ominaisuudet	121
Roskapostiviestien tunnistustavan määrittäminen	123
Sähköpostin suodatus	131
Ystävien määrittäminen	133
Web-sähköpostitilien määrittäminen	137
Suodatettujen sähköpostiviestien käsitteleminen	141
Phishing-huijausten torjunnan asetusten määrittäminen	143
McAfee Parental Controls	145
Parental Controlsin ominaisuudet	146
Lasten suojaaminen	147
Tietojen suojaaminen Internetissä	161
Salasanojen suojaaminen	163
McAfee Backup and Restore	167
Backup and Restoren ominaisuudet	168
Tiedostojen arkistointi	169
Arkistoitujen tiedostojen käsitteleminen	179
McAfee QuickClean	185
QuickCleanin toiminnot	186
Tietokoneen puhdistaminen	187
Tietokoneen eheyttäminen	191
Tehtävän ajoittaminen	193

McAfee Shredder	199
Shredderin toiminnot	200
Tiedostojen, kansioden ja levyjen tuhoaminen	200
McAfee Network Manager	203
Network Managerin ominaisuudet.....	204
Network Managerin kuvakkeiden toiminta	205
Hallitun verkon määrittäminen	207
Verkon etähallinta	213
Verkkojen valvonta	219
McAfee EasyNetwork	223
EasyNetworkin ominaisuudet.....	224
EasyNetworkin asentaminen	225
Tiedostojen jakaminen ja lähettäminen	229
Tulostinten jakaminen.....	235
Opas	237
Sanasto	238
<hr/>	
Tietoja McAfeesta	253
<hr/>	
Käyttöoikeus.....	253
Copyright.....	254
Asiakaspalvelu ja tekninen tuki.....	255
McAfee Virtual Technician -palvelun käyttö	256
Hakemisto	266
<hr/>	

LUKU 1

McAfee Total Protection

Total Protection on enemmän kuin pelkkä tietoturvaohjelmisto – se on täydellinen puolustusjärjestelmä, joka suojaa sinua ja perhettäsi, kun työskentelet tai pelaat verkossa. Total Protectionin avulla voit suojata tietokoneesi viruksia, hakkereita ja vakoiluohjelmia vastaan, valvoa Internetin tietoliikennettä epäilyttävien tapahtumien varalta, suojata perheesi yksityisyyttä, estää vaarallisia Web-sivustoja ja tehdä paljon muuta.

Tässä luvussa

McAfee SecurityCenter	5
McAfee VirusScan	29
McAfee Personal Firewall	65
McAfee Anti-Spam	119
McAfee Parental Controls	145
McAfee Backup and Restore	167
McAfee QuickClean	185
McAfee Shredder	199
McAfee Network Manager.....	203
McAfee EasyNetwork.....	223
Opas.....	237
Tietoja McAfeesta.....	253
Asiakaspalvelu ja tekninen tuki	255

LUKU 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 alkumäärytykset 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
Suojausongelmien korjaaminen ja ohittaminen	17
Hälytysten käsitteleminen	21
Tapahtumien näyttäminen	27

SecurityCenterin ominaisuudet

Yksinkertaistettu suojaustila

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

Automaattiset päivitykset ja uudet tuoteversiot

SecurityCenter lataa ja asentaa ohjelmien päivitykset automaattisesti. Kun uusi McAfee-ohjelmistoversio on saatavilla, se toimitetaan automaattisesti tietokoneeseen tilauksesi voimassaolon ajan, jotta suojauksesi on aina ajan tasalla.

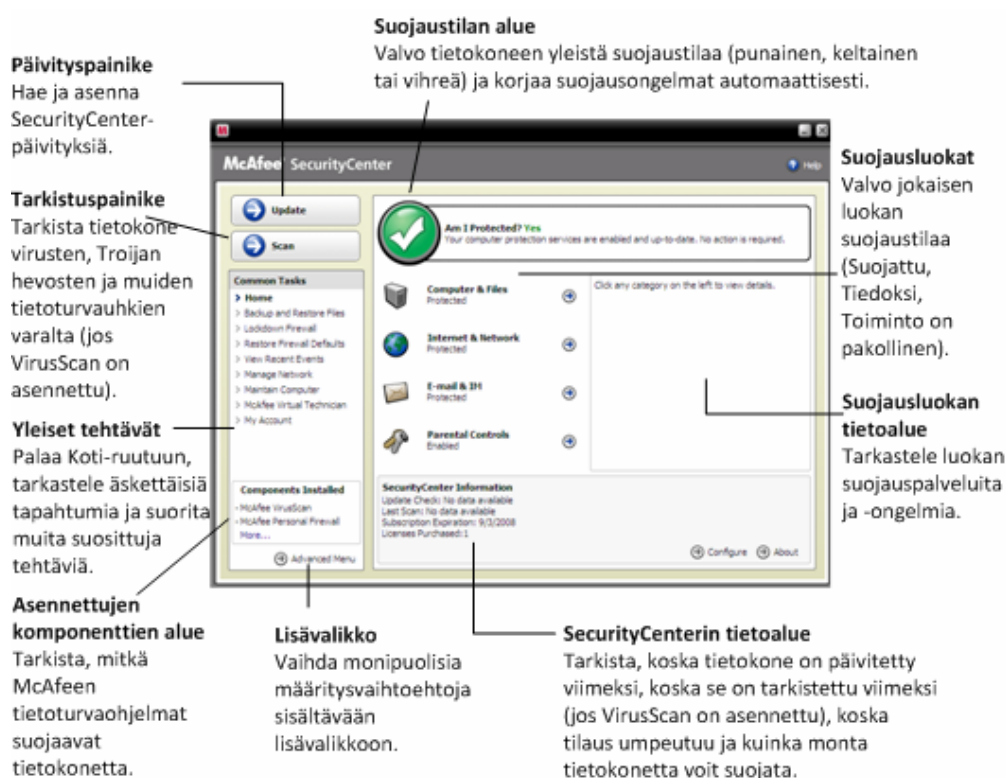
Reaaliaikaiset hälytykset

Suojaushälytykset ilmoittavat merkittävistä virusesiintymistä ja tietoturvauhista.

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
Tilausten hallinta	10
SecurityCenterin päivittäminen	13

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 tietoturvaohjelmien, muiden tietoturvaohjelmien ja Internet-yhteyttä käyttävien ohjelmien vaikutuksesta.

Tietokoneesi suojauksen tila voi olla punainen, keltainen tai vihreä.

Suojauksen tila	Kuvaus
Punainen	<p>Tietokonetta ei ole suojattu. SecurityCenter Koti-ikkunan suojauksen tila -kohdan punainen väri tarkoittaa, että tietokonettasi ei ole suojattu. SecurityCenter ilmoittaa ainakin yhdestä kriittisestä tietoturvaongelmasta.</p> <p>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).</p>
Keltainen	<p>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.</p> <p>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).</p>
Vihreä	<p>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.</p> <p>Jokaisessa suojausluokassa on luettelo tietokonettasi suojaavista palveluista.</p>

Suojausluokkien toiminta

SecurityCenterin suojauspalvelut voidaan jakaa neljään luokkaan: tietokone ja tiedostot, Internet ja verkko, sähköposti ja 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 ja tiedostot	Tietokone ja tiedostot -luokassa voit määrittää seuraavien suojauspalveluiden asetuksia: <ul style="list-style-type: none"> ▪ Virustentorjunta ▪ Vakoiluohjelmien torjunta ▪ SystemGuards ▪ Windows-suojaus ▪ Tietokoneen kunto
Internet ja verkko	Internet ja verkko -luokassa voit määrittää seuraavien suojauspalveluiden asetuksia: <ul style="list-style-type: none"> ▪ Palomuurin suojaus ▪ Phishing-huijausten torjunta ▪ Henkilöllisyyden suojaus
Sähköposti ja pikaviestit	Sähköposti ja pikaviestit -luokassa voit määrittää seuraavien suojauspalveluiden asetuksia: <ul style="list-style-type: none"> ▪ Sähköpostin virussuojaus ▪ Pikaviestiohjelmien virustorjunta ▪ Sähköpostin vakoiluohjelmien suojaus ▪ Pikaviestiohjelmien vakoiluohjelmien suojaus ▪ Roskapostin torjunta
Käytönvalvonta-asetukset	Käytönvalvonta-asetukset-luokassa voit määrittää seuraavien suojauspalveluiden asetuksia: <ul style="list-style-type: none"> ▪ Sisällön estäminen

Suojauspalveluiden toiminta

Suojauspalvelut ovat erilaisia suojauskomponentteja. Voit suojata tietokoneesi ja tiedostosi määrittämällä niiden asetuksia. Suojauspalvelut vastaavat McAfeen ohjelmistoja. Esimerkiksi kun asennat VirusScan-ohjelman, seuraavat suojauspalvelut tulevat käyttöön: virustentorjunta, vakoiluohjelmien torjunta ja komentosarjatarkistukset. Tarkempia tietoja suojauspalveluista löytyy VirusScan-ohjeesta.

Oletusarvoisesti kaikki asennettuun ohjelmaan liittyvät suojauspalvelut ovat käytössä. Suojauspalveluita voi kuitenkin poistaa käytöstä milloin tahansa. Esimerkiksi kun asennat käytönvalvonta-asetukset, 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.

Tilausten hallinta

Jokaisen hankitun McAfee-tietoturvatuotteen mukana toimitetaan tilaus, joka oikeuttaa sinut tuotteen käyttöön tietyssä määrässä tietokoneita tietyn ajan. Tilauksen pituus vaihtelee hankitun tuotteen mukaan, mutta se alkaa tavallisesti tuotteen aktivointihetkellä. Aktivointi on helppoa ja maksutonta, tarvitset siihen vain Internet-yhteyden. Sen suorittaminen on kuitenkin tärkeätä, sillä se oikeuttaa sinut säännöllisiin ja automaattisiin tuotepäivityksiin, jotka suojaavat tietokonettasi uusimmilta uhilta.

Aktivointi suoritetaan tavallisesti tuotteen asennuksen yhteydessä, mutta jos päätät odottaa (esimerkiksi jos sinulla ei ole Internet-yhteyttä), sinulla on aktivointiin 15 päivää aikaa. Jos et aktivoi tuotteitasi 15 päivän kuluessa, niihin ei enää toimiteta tärkeitä päivityksiä, eivätkä ne enää pysty suorittamaan tarkistuksia. Ilmoitamme sinulle myös säännöllisesti (näyttöön tulevien ilmoitusten muodossa), ennen kuin tilauksesi voimassaoloaika on päättymässä. Näin voit välttää suojauksesi keskeytymisen ja uudistaa tilauksesi aikaisemmin tai ottaa automaattisen uudistamisen sivustossamme käyttöön.

Jos näyttöön tulee linkki, jossa SecurityCenter kehottaa sinua aktivoimaan tilauksesi, sitä ei ole aktivoitu. Voit tarkistaa tilauksesi viimeisen voimassaolopäivän tilisivultasi.

McAfee-tilisi käyttäminen

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

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

Aktivoi tuotteesi


Aktivointi suoritetaan tavallisesti tuotteen asennuksen yhteydessä. Jos näin ei kuitenkaan ole, näyttöön tulee SecurityCenterin linkki, jossa sinua kehoitetaan aktivoimaan tuotteesi. Ilmoitamme sinulle tästä myös säännöllisesti.

- Valitse SecurityCenterin Koti-ikkunan **SecurityCenterin tiedot** -kohdasta **Aktivoi tilauksesi**.

Vihje: Voit suorittaa aktivoinnin myös napsauttamalla säännöllisesti näyttöön tulevaa ilmoitusta.

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.

Uudista tilauksesi

Hieman ennen tilauksesi viimeistä voimassaolopäivää näyttöön tulee SecurityCenterin linkki, jossa sinua kehoitetaan uudistamaan tuotteesi. Ilmoitamme sinulle viimeisen voimassaolopäivän lähestymisestä myös säännöllisesti näyttöön tulevilla ilmoituksilla.

- Valitse SecurityCenterin Koti-ikkunan **SecurityCenterin tiedot** -kohdasta **Uudista**.

Vihje: Voit uudistaa tuotteesi tilauksen myös napsauttamalla säännöllisesti näyttöön tulevaa ilmoitusta. Tilisivullasi voit myös uudistaa tilauksesi tai ottaa automaattisen uudistamisen käyttöön.

LUKU 4

SecurityCenterin päivittäminen

SecurityCenter varmistaa, että rekisteröimäsi McAfee-ohjelmistot ovat ajan tasalla, tarkistamalla ja asentamalla uusimmat Internet-päivitykset neljän tunnin välein. Asennettujen ja aktivoitujen 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 asensit McAfee-tuotteesi CD-levyltä, ne on aktivoitava 15 päivän kuluessa. Muussa tapauksessa niihin ei enää toimiteta tärkeitä päivityksiä, eivätkä ne enää pysty suorittamaan tarkistuksia.

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 liitettynä 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 käsitteleminen (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 Avaa SecurityCenter-asetusikkuna.
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**.
- 3** Valitse vahvistusvalintaikkunasta **Kyllä**.

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

LUKU 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 (ongelmatyyppin 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.....	19

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 aktivoitu, eikä se tarjoa täydellistä suojaa.	Aktivoi ohjelma McAfee-verkkosivuilla.
Tilauksesi voimassaoloaika on päättynyt.	Tarkista tilisi tilanne McAfee-verkkosivuilta. Lisätietoja on kohdassa Tilausten hallinta (sivu 10).

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 käytönvalvonta-asetuspalvelua ei ole asennettu) ohitetaan automaattisesti. Ohitetut ongelmat eivät näy SecurityCenterin Koti-ikkunan suojausluokan tietoaalueessa, ellei tietokoneesi suojauksen tila ole vihreä. Jos ohitat ongelman, saat sen halutessasi myöhemmin näkyviin suojausluokan tietoaalueeseen, 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 tietoaalueesta.

- 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 tietoaalueessa poistamalla kyseisen valintaruudun valinnan.

4 Valitse **OK**.

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

LUKU 6

Hälytysten käsitteleminen

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 kolme 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**.

Piilota tietoturvailmoitukset

Voit piilottaa tietoturvailmoitukset, jotka liittyvät muiden kotiverkossasi olevien tietokoneiden suojaamiseen. Näissä ilmoituksissa on tietoja tilauksestasi, sen avulla suojattavissa olevien tietokoneiden määrästä ja tilauksen laajentamisesta muihin tietokoneisiin.

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 **Näytä virustiedotteet tai muut turvavaroitukset**.

Vihje: Saat nämä tietoturvailmoitukset takaisin näkyviin valitsemalla **Näytä virustiedotteet tai muut turvavaroitukset**.

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 järjestelee 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 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.

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 käynnistyksen 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
Tietokoneen tarkistaminen.....	31
Tarkistuksen tulosten käyttäminen.....	37
Tarkistustavat	40
Lisäsuojauksen käyttäminen	43
Virustorjunnan määrittäminen	47

VirusScan-ohjelman ominaisuudet

Perusteellinen virussuoja

Suojaa itseäsi ja tietokoneettasi uusimmilta tietoturvauhilta, kuten troijalaisilta, seurantaevästeiltä, vakoilu- ja mainosohjelmilta sekä muilta mahdollisesti ei-toivotuilta ohjelmilta. VirusScan suojaa pöytäkonetta tai kannettavaa tietokonetta tiedostojen ja kansiodien lisäksi myös muiden tulokohtien, kuten sähköpostin, pikaviestien ja Web-sivustojen, kautta tulevilta uhilta. Hankalaa valvontaa ei tarvita.

Resurssitietoiset tarkistusasetukset

Mukauta tarkistusasetuksia mieleesi mukaan. Jos et kuitenkaan halua tehdä muutoksia, tietokoneesi pysyy suojattuna. Jos tarkistusnopeus on hidas, voit kytkeä mahdollisimman vähäisen resurssien kulutuksen pois käytöstä. Huomaa kuitenkin, että tällöin virussuojaukseen käytetään enemmän resursseja kuin muihin tehtäviin.

Automaattinen korjaus

Jos VirusScan havaitsee turvallisuusuhan 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 manuaalisen tarkistuksen.

L U K U 9

Tietokoneen tarkistaminen

VirusScanin reaaliaikainen virustorjunta alkaa suojella tietokonetta mahdollisesti haitallisilta viruksilta, troijalaisilta ja muilta tietoturvahilta jo ennen kuin SecurityCenter käynnistetään ensimmäisen kerran. 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 tarkistuksen määrittämisestä on kohdassa Virustorjunnan määrittäminen (sivu 47).

VirusScanissa on tavallista kattavammat tarkistusasetukset, joiden avulla voit ajoittain tarkistaa tietokoneen tavallista tarkemmin. SecurityCenterissä voit suorittaa täydellisen, nopean, mukautetun tai ajoitetun tarkistuksen. Voit myös käynnistää manuaalisen tarkistuksen Windowsin Resurssienhallinnasta työskennellessäsi. Kun suoritat tarkistuksen SecurityCenterissä, voit muuttaa tarkistusasetuksia käytön aikana. Windowsin Resurssienhallinnassa sen sijaan on kätevät tietoturvatoinnot.

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

Tarkista tietokone	32
Näytä tarkistuksen tulokset.....	35

Tarkista tietokone

VirusScan tarjoaa virustorjuntaan monipuolisia tarkistusasetuksia, joita ovat muun muassa reaaliaikainen tarkistus (joka valvoo tietokonetta jatkuvasti uhkien varalta), Resurssienhallinnan manuaalinen tarkistus sekä SecurityCenterin täydellinen, nopea, mukautettu ja ajoitettu tarkistus.

Toiminto	Toimenpide
Reaaliaikaisen tarkistuksen käynnistäminen, jos haluat valvoa tietokonetta jatkuvasti virusten varalta ja tarkistaa tiedostot aina, kun niitä avataan.	<p>1. Avaa Tietokone ja tiedostot -asetusikkuna.</p> <p>Miten?</p> <ol style="list-style-type: none"> 1. Valitse vasemmanpuoleisesta ruudusta Lisävalikko. 2. Valitse Määritä. 3. Valitse Määritä-ruudusta Tietokone ja tiedostot. <p>2. Valitse Virustorjunta-kohdassa Käytössä.</p> <p>Huomaa: Reaaliaikainen tarkistus otetaan oletusarvoisesti käyttöön.</p>
Pikatarkistuksen käynnistäminen ja tietokoneen tarkistaminen nopeasti uhkien varalta	<ol style="list-style-type: none"> 1. Valitse Perusvalikosta Tarkista. 2. Valitse Pikatarkistus-kohdassa olevasta Tarkistusasetukset-ruudusta Käynnistä.
Täydellisen tarkistuksen käynnistäminen ja tietokoneen tarkistaminen perusteellisesti uhkien varalta	<ol style="list-style-type: none"> 1. Valitse Perusvalikosta Tarkista. 2. Valitse Täydellinen tarkistus -kohdassa olevasta Tarkistusasetukset-ruudusta Käynnistä.

Toiminto	Toimenpide
Omiin asetuksiin perustuvan mukautetun tarkistuksen käynnistäminen	<ol style="list-style-type: none">1. Valitse Perusvalikosta Tarkista.2. Valitse Anna minun valita -kohdassa olevasta Tarkistusasetukset-ruudusta Käynnistä.3. Mukauta tarkistusta valitsemalla seuraavat asetukset tai poistamalla niiden valinnat: Kaikki uhat kaikissa tiedostoissa Tuntemattomat virukset Arkistotiedostot Vakoiluohjelmat ja mahdolliset uhat Seurantaevästeet Vaikeasti havaittavat ohjelmat4. Valitse Käynnistä.
Manuaalisen tarkistuksen käynnistäminen tiedostoissa, kansioissa tai asemissa olevien uhkien tarkistamiseksi	<ol style="list-style-type: none">1. Avaa Windowsin Resurssienhallinta.2. Napsauta tiedostoa, kansiota tai asemaa hiiren kakkospainikkeella ja valitse sitten Tarkista.

Toiminto	Toimenpide
<p>Käynnistä ajoitettu tarkistus, joka tarkistaa tietokoneesi säännöllisesti uhkien varalta</p>	<p>1. Avaa Ajoitettu tarkistus -ikkuna. Miten?</p> <ol style="list-style-type: none"> 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 -määrittelyikkunasta, että virustorjunta on käytössä, ja napsauta Lisäasetukset -painiketta. 5. Napsauta Virustorjunta-ikkunan kohtaa Ajoitettu tarkistus. <p>2. Valitse Ota käyttöön ajoitettu tarkistus.</p> <p>3. Voit vähentää tarkistukseen käytettävää prosessoritehoa valitsemalla Tarkista minimiresursseilla.</p> <p>4. Valitse vähintään yksi päivä.</p> <p>5. Määritä aloitusaika.</p> <p>6. Valitse OK.</p>

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**.

Huomautus: Lisätietoja tarkistusasetuksista on kohdassa Tarkistustavat (sivu 40).

Näytä tarkistuksen tulokset

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

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

Toiminto	Toimenpide
Tarkistuksen tulosten tarkasteleminen hälytysikkunassa	Tarkastele tuloksia Tarkistus on päättynyt -ikkunassa.
Tarkistuksen tuloksia koskevien lisätietojen näyttäminen	Valitse Tarkistus on päättynyt -ikkunassa Näytä tarkistuksen lisätiedot .
Tarkistuksen tulosten yhteenvedon tarkasteleminen	Napsauta tehtäväpalkin ilmaisinalueen Tarkistus on päättynyt -kuvaketta.
Tarkistus- ja tunnistustilastojen tarkasteleminen	Kaksoisnapsauta ilmaisinalueen Tarkistus on päättynyt -kuvaketta.
Havaittujen kohteiden, tartunnan tilan ja tartunnan tyyppin tietojen tarkasteleminen	1. Kaksoisnapsauta ilmaisinalueen Tarkistus on päättynyt -kuvaketta. 2. Valitse Täydellinen tarkistus-, Pikatarkistus-, Mukautettu tarkistus- tai Manuaalinen tarkistus -ruudusta Tiedot .
Viimeisimmän tarkistuksen tietojen tarkasteleminen	Kaksoisnapsauta ilmaisinalueen Tarkistus on suoritettu -kuvaketta ja tarkastele viimeisimmän tarkistuksen tuloksia Täydellinen tarkistus-, Pikatarkistus-, Mukautettu tarkistus- tai Manuaalinen tarkistus -ruudun Tarkistuksesi-kohdassa.

LUKU 10

Tarkistuksen tulosten käyttäminen

Jos VirusScan havaitsee turvallisuusuhan tarkistuksen aikana, se yrittää käsitellä uhan automaattisesti uhkatyypin mukaan. Jos VirusScan esimerkiksi havaitsee viruksen, troijalaisen tai seurantaevästeen, VirusScan yrittää puhdistaa saastuneen tiedoston. VirusScan eristää tiedoston aina, ennen kuin se yrittää puhdistaa sen. Jos tiedosto ei ole puhdas, se eristetään.

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	37
Mahdollisten haittaohjelmien käsitleminen.....	38
Eristettyjen tiedostojen käsitleminen	38
Eristettyjen ohjelmien ja evästeiden käsitleminen	39

Virusten ja troijalaisten käsitleminen

Jos VirusScan havaitsee tietokoneessa olevassa tiedostossa viruksen tai troijalaisen, se 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 **Virukset ja troijalaiset**.

Huomautus: Lisätietoja VirusScanin eristämien tiedostojen käsittelemisestä on kohdassa Eristettyjen tiedostojen käsitteleminen (sivu 38).

Mahdollisten haittaohjelmien käsitteleminen

Jos VirusScan havaitsee tietokoneessa mahdollisen haittaohjelman, voit joko poistaa ohjelman tai määrittää sen luotettavaksi. Jos et tunne ohjelmaa, suosittelemme sen poistamista. 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 käsittelyminen

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.

Tarkistustavat

VirusScan tarjoaa virustorjuntaan monipuolisia tarkistusasetuksia, joita ovat muun muassa reaaliaikainen tarkistus (joka valvoo tietokonetta jatkuvasti uhkien varalta), Resurssienhallinnan manuaalinen tarkistus, mahdollisuus suorittaa täydellinen, nopea tai mukautettu tarkistus SecurityCenterissä ja ajoitettujen tarkistusten suoritusajkojen mukauttaminen. Kun suoritat tarkistuksen SecurityCenterissä, voit muuttaa tarkistusasetuksia käytön aikana.

Reaaliaikainen tarkistus:

Reaaliaikainen virustorjunta valvoo virustoimintaa tietokoneessasi jatkuvasti. Se tarkistaa tiedostot aina, kun niitä avataan. Jos haluat varmistaa, että tietokoneesi pysyy suojattuna uusimmilta turvallisuushilta, pidä reaaliaikainen virustorjunta käytössä ja laadi säännöllinen aikataulu perusteellisempia manuaalisia tarkistuksia varten.

Voit määrittää reaaliaikaisen tarkistuksen oletusasetukset, joihin kuuluvat muun muassa tarkistukset tuntemattomien virusten varalta sekä seurantaevästeissä ja verkkoasemissa olevien uhkien tunnistaminen. Voit hyödyntää myös puskurin ylivuotosuojausta, joka otetaan oletusarvoisesti käyttöön (paitsi jos käytät 64-bittistä Windows Vista -käyttöjärjestelmää). Lisätietoja on kohdassa Reaaliaikaisen tarkistuksen asetusten määrittäminen (sivu 48).

Pikatarkistus

Pikatarkistuksen avulla voit tarkistaa käynnissä olevat prosessit, tärkeät Windowsin tiedostot ja muut tietokoneen haavoittuvat alueet uhkien varalta.

Täydellinen tarkistus

Täydellisen tarkistuksen avulla voit tarkistaa koko tietokoneen perusteellisesti virusten, vakoiluohjelmien ja muiden tietoturvaohjelmien varalta.

Mukautettu tarkistus

Mukautettua tarkistusta käytettäessä voit valita omat tarkistusasetuksesi tietokoneessa olevien uhkien etsimistä varten. Mukautettuihin tarkistusasetuksiin kuuluvat muun muassa uhkien etsiminen kaikista tiedostoista, arkistotiedostoista ja evästeistä, mutta tarkistuksen piiriin kuuluvat myös tuntemattomat virukset, vakoiluohjelmat ja vaikeasti havaittavat ohjelmat.

Voit määrittää mukautetun tarkistuksen oletusasetukset, joihin kuuluvat muun muassa tarkistukset tuntemattomien virusten, arkistotiedostojen, vakoiluohjelmien ja mahdollisten uhkien, seurantaevästeiden ja vaikeasti havaittavien ohjelmien varalta. Voit suorittaa tarkistuksen myös käyttämällä mahdollisimman vähän tietokoneen resursseja. Lisätietoja on kohdassa Mukautetun tarkistuksen asetusten määrittäminen (sivu 50).

Manuaalinen tarkistus

Manuaalisen tarkistuksen avulla voit tarkistaa tiedostot, kansiot ja asemat Resurssienhallinnasta nopeasti uhkien varalta.

Tarkistuksen ajoittaminen

Ajoitettujen tarkistusten avulla voit tarkistaa tietokoneesi virusten ja uhkien varalta perusteellisesti 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. Lisätietoja on kohdassa Tarkistuksen ajoittaminen (sivu 53)

Huomaa: Valitse itsellesi sopivin tarkistusasetus perehtymällä kohtaan Tarkista tietokone (sivu 32)

LUKU 11

Lisäsuojauksen käyttäminen

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 tai selaimessa. 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 sähköpostiviestien ja liitetiedostojen epäilyttävää toimintaa.

Pikaviestisuojaus

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

Tässä luvussa

Käynnistä komentosarjatarkistussuojaus.....	44
Käynnistä vakoiluohjelmasuojaus.....	44
Käynnistä sähköpostisuojaus	44
Käynnistä pikaviestisuojaus.....	45

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 vakoiluohjelmasuojaus

Kun otat vakoiluohjelmasuojauksen 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 vakoiluohjelmasuojauksen 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 sähköpostisuojauksen käytöstä milloin tahansa. Tämä ei kuitenkaan ole suotavaa, sillä tällöin tietokone altistuu sähköpostiuhille.

Käynnistä pikaviestisuojaus

Kun otat pikaviestisuojauksen käyttöön, virustorjuntaohjelmisto havaitsee saapuvien pikaviestien liitetiedostoihin liittyvät tietoturvaohauhat.

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 pikaviestisuojauksen käytöstä milloin tahansa. Tämä ei kuitenkaan ole suotavaa, sillä tällöin tietokone altistuu haitallisille pikaviestien liitetiedostoille.

LUKU 12

Virustorjunnan määrittäminen

Voit määrittää ajoitetulle, mukautetulle ja reaaliaikaiselle tarkistukselle erilaiset asetukset. Esimerkki: Koska reaaliaikainen suojaus valvoo tietokonetta jatkuvasti, voit valita sille tietyt perustarkistusasetukset. Voit määrittää kattavammat tarkistusasetukset manuaaliselle, tarvittaessa suoritettavalle suojaukselle.

Voit määrittää myös sen, miten haluat VirusScanin valvovan ja hallitsevan mahdollisesti luvattomia tai ei-toivottuja muutoksia tietokoneessa SystemGuards- ja Luotetut luettelot -toimintojen avulla. 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. Luotetut luettelot -toiminnon avulla voit määrittää, haluatko luottaa tiedostoihin tai rekisteriin tehtyjä muutoksia (SystemGuard), ohjelmia tai puskurin ylivuotoja havaitseviin sääntöihin tai poistaa ne. Jos luotat kohteeseen etkä halua, että siitä ilmoitetaan jatkossa, kohde lisätään luotettujen kohteiden luetteloon eikä VirusScan enää havaitse sitä tai ilmoita sen toiminnasta.

Tässä luvussa

Reaaliaikaisen tarkistuksen asetusten määrittäminen	48
Mukautettujen tarkistusasetusten määrittäminen.....	50
Tarkistuksen ajoittaminen	53
SystemGuards-toimintojen asetukset.....	54
Luotettujen luetteloiden käyttäminen.....	60

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 tiedostotyyppisiä 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 tiedostotyyppisiä 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 -määrittysikkunasta, että virustorjunta on käytössä, ja napsauta **Lisäasetukset**-painiketta.

2 Määritä reaaliaikaisen tarkistuksen asetukset ja napsauta **OK**.

Toiminto	Toimenpide
Tuntemattomien virusten ja tunnettujen virusten uusien muunnelmien havaitseminen	Valitse Tarkista tuntemattomat virukset .
Evästeiden havaitseminen	Valitse Tarkista ja poista seurantaevästeet .
Virusten ja mahdollisten uhkien havaitseminen verkkoasemilta	Valitse Tarkista verkkoasemat .
Tietokoneen suojaaminen puskurin ylivuodoilta	Valitse Ota käyttöön puskurin ylivuotosuojaus .
Tarkistettavien tiedostotyyppien määrittäminen	Valitse joko Kaikki tiedostot (suositus) tai Vain ohjelmatiedostot ja asiakirjat .

Lopeta reaaliaikainen virustorjunta

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.

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**.

Mukautettujen tarkistusasetusten määrittäminen

Mukautetulla virustorjunnalla voit tarkistaa tiedostoja halutessasi. Kun aloitat mukautetun tarkistuksen, VirusScan etsii tietokoneestasi viruksia ja muita mahdollisesti haitallisia kohteita käyttäen kattavia tarkistusasetuksia. Kun muutat mukautetun tarkistuksen asetuksia, sinun täytyy päättää, mitä tarkistuksia VirusScan tekee. Voit esimerkiksi määrittää, etsiikö VirusScan tuntemattomia viruksia, mahdollisesti ei-toivottuja ohjelmia, kuten vakoilu- ja mainosohjelmia, vaikeasti havaittavia ohjelmia ja tietomurto-ohjelmistoja, jotka mahdollistavat tietokoneen luvattoman käytön, tai seurantaevästeitä, joiden avulla sivustot voivat seurata toimintaasi. 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 sekä kaikki verkkoasemat jokaisen mukautetun tarkistuksen yhteydessä. Voit kuitenkin muuttaa tarkistuskohteita tarpeittesi mukaan. Voit esimerkiksi tarkistaa vain tietokoneen tärkeimmät tiedostot, työpöydällä olevat tiedostot tai Program Files -kansiossa olevat tiedostot. Jos et halua olla itse vastuussa jokaisen mukautetun tarkistuksen aloittamisesta, voit myös laatia säännöllisen tarkistusaikataulun. 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.

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

Määritä mukautetun tarkistuksen asetukset

Voit määrittää, mitä VirusScan etsii mukautetun tarkistuksen aikana. Lisäksi voit määrittää tarkistettavat tiedostojen sijaintipaikat ja tiedostotyypit. Asetuksiin kuuluu esimerkiksi tuntemattomien virusten, arkistotiedostojen, vakoiluohjelmien, ei-toivottujen ohjelmien, seurantaevästeiden, tietomurto-ohjelmistojen ja vaikeasti havaittavien ohjelmien tarkistus. Voit myös määrittää paikan, mistä VirusScan etsii viruksia ja muita vahingollisia kohteita mukautetun tarkistuksen aikana. Voit tarkistaa kaikki tietokoneesi tiedostot, kansiot ja asemat tai voit rajoittaa tarkistuksen tiettyihin kansioihin ja asemiin.

1 Avaa Mukautettu 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 -määrittämissivustalta, että virustorjunta on käytössä, ja napsauta **Lisäasetukset**-painiketta.
5. Napsauta Virustorjunta-ikkunan kohtaa **Manuaalinen tarkistus**.

2 Määritä mukautetun tarkistuksen asetukset ja napsauta **OK**.

Toiminto	Toimenpide
Tuntemattomien virusten ja tunnettujen virusten uusien muunnelmien havaitseminen	Valitse Tarkista tuntemattomat virukset .
Virusten tunnistaminen ja poistaminen .zip-tiedostoista ja muista pakatuista tiedostoista	Valitse Tarkista arkistotiedostot .
Vakoilu- ja mainosohjelmien sekä muiden mahdollisten ei-toivottujen ohjelmien havaitseminen	Valitse Tarkista vakoiluohjelmat ja mahdolliset uhat .
Evästeiden havaitseminen	Valitse Tarkista ja poista seurantaevästeet .

Toiminto	Toimenpide
Windowsin järjestelmätiedostoja mahdollisesti muuttavien ja hyödyntävien tietoturva-ohjelmistojen ja vaikeasti havaittavien ohjelmien havaitseminen	Valitse Tarkista piilo-ohjelmat.
Tarkistuksiin käytettävän prosessoritehon vähentäminen ja muiden tehtävien priorisointi (esimerkiksi Web-selaus ja asiakirjojen avaaminen)	Valitse Tarkista käyttämällä mahdollisimman vähän tietokoneen resursseja.
Tarkistettavien tiedostotyyppien määrittäminen	Valitse joko Kaikki tiedostot (suositus) tai Vain ohjelmatiedostot ja asiakirjat.

3. Valitse **Oletustarkistussijainti**, valitse tarkistettavat tai ohitettavat sijainnit tai poista niiden valinnat, ja valitse **OK**.

Toiminto	Toimenpide
Kaikkien tietokoneesi tiedostojen ja kansioden tarkistaminen	Valitse (Oma)Tietokone.
Tiettyjen tiedostojen, kansioden ja asemien tarkistaminen	Poista (Oma)Tietokone -valintaruudun valinta ja valitse vähintään yksi kansio tai asema.
Tärkeimpien järjestelmätiedostojen tarkistaminen	Poista (Oma)Tietokone -valintaruudun valinta ja valitse Tärkeät järjestelmätiedostot -valintaruutu.

Tarkistuksen ajoittaminen

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.

Ajoita tarkistuksia, jotka tarkistavat koko tietokoneen perusteellisesti virusten ja muiden uhkien varalta käyttäen oletusasetuksia. Oletusasetuksena VirusScan suorittaa ajoitetun tarkistuksen kerran viikossa.

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 -määritysikkunasta, 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 kolme 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 luvatonta toimintaa, kuten käyttäjän ohjaamista epäilyttäviin Web-sivustoihin, selaimen asetusten ja määritysten luvatonta 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-suojaus 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 57).

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 tietokoneesi 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 -rekisteriavaimen, mikä mahdollistaa vahingollisten ohjelmien suorittamisen tietokoneen käynnistyksen yhteydessä.

SystemGuard-toiminto	Kohde
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-tekniologia auttaa estämään selaimen luvatonta toimintaa, kuten käyttäjän ohjaamista epäilyttäviin Web-sivustoihin, selaimen asetusten ja määrittysten luvatonta 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.

SystemGuard-toiminto	Havaitsee...
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 -määrittelyikkunasta, 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 62).

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	<p>Luotetut luettelot -ikkunan ohjelmien SystemGuards-toiminnot ilmaisevat VirusScan-ohjelman aiemmin havaitsemia luvattomia rekisteri- ja tiedostomuutoksia, jotka olet hyväksynyt hälytyksessä tai Tarkistuksen tulokset -ikkunassa.</p> <p>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.</p>
Windows SystemGuards-suojaukset	<p>Luotetut luettelot -ikkunan Windows SystemGuards-toiminnot ilmaisevat VirusScan-ohjelman aiemmin havaitsemia luvattomia rekisteri- ja tiedostomuutoksia, jotka olet hyväksynyt hälytyksessä tai Tarkistuksen tulokset -ikkunassa.</p> <p>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.</p>

Toiminto	Kuvaus
Selaimen SystemGuards-toiminnot	<p>Luotetut luettelot -ikkunan selaimen SystemGuards-toiminnot ilmaisevat VirusScan-ohjelman aiemmin havaitsemissa luvattomia rekisteri- ja tiedostomuutoksia, jotka olet hyväksynyt hälytysikkunassa tai Tarkistuksen tulokset -ikkunassa.</p> <p>Selaimen SystemGuards-toiminnot havaitsevat selainpuohjelmien 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.</p>
Luotetut ohjelmat	Luotetut ohjelmat ovat VirusScan-ohjelman aiemmin havaitsemissa mahdollisesti ei-toivottuja ohjelmia, jotka olet hyväksynyt hälytysikkunassa tai Tarkistuksen tulokset -ikkunassa.
Luotetut puskurin ylivuodot	<p>Luotetut puskurin ylivuodot ovat VirusScan-ohjelman aiemmin havaitsemissa luvattomia toimenpiteitä, jotka olet hyväksynyt hälytysikkunassa tai Tarkistuksen tulokset -ikkunassa.</p> <p>Puskurin ylivuodot voivat vahingoittaa tietokonetta ja tiedostoja. Puskurin ylivuoto tapahtuu, jos ohjelmien tai prosessien käyttämä puskurin määrä ylittää puskurin kapasiteetin.</p>

LUKU 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 Firewallin ominaisuudet	66
Palomuurin käynnistäminen	67
Hälytysten käsitteleminen	69
Tiedottavien hälytysten hallinta	71
Palomuurisuojausten asetusten määrittäminen	73
Ohjelmien ja käyttöoikeuksien hallinta	85
Tietokoneyhteyksien hallinta	93
Järjestelmäpalveluiden hallinta	101
Kirjaus, valvonta ja analyysi	107
Perehtyminen Internet-tietoturvaan	117

Personal Firewallin ominaisuudet

Vakio ja mukautettu tietoturvaso	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	Hallitse ohjelmien Internet-käyttöä hälytyksien ja tapahtumalokien avulla ja määritä käyttöoikeudet haluamillesi ohjelmille.
Pelaamisen suojaus	Pelaamisen suojaus estää tietomurtoyrityksiä ja epäilyttäviä tapahtumia koskevia hälytyksiä häiritsemästä sinua pelatessasi koko näytön tilassa.
Tietokoneen käynnistysuojau	Suojaa tietokoneitasi tietomurtoyrityksiltä, ei-toivotuilta ohjelmilta ja tietoliikenteeltä jo Windowsin® käynnistymisen yhteydessä.
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	Estä kaikki tietokoneesi ja Internetin välinen saapuva ja lähtevä tietoliikenne välittömästi.
Palomuurin palauttaminen	Palauta Firewallin alkuperäiset suojausasetukset välittömästi.
Trojajalaisten tehokas tunnistaminen	Havaitse ja estä mahdollisesti haitallisia sovelluksia, kuten troijalaisia, lähettämstä henkilökohtaisia tietojasi Internetiin.
Tapahtumien kirjaus	Seuraa äskettäistä tulevaa ja lähtevää tietoliikennettä sekä tietomurtotapahtumia.
Internet-tietoliikenteen valvonta	Voit tarkastella maailmanlaajuisia karttoja, 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. Tarjoamme kolmannen suojauskerroksen käyttämällä heuristista menetelmää, joka estää hyökkäyksiä tai tietomurtoyrityksiä muistuttavat kohteet.
Kehittynyt tietoliikenneanalyysi	Tarkastele saapuvaa ja lähtevää Internet-tietoliikennettä sekä ohjelmien muodostamia yhteyksiä, myös niitä, jotka kuuntelevat aktiivisesti avoimia yhteyksiä. Näin voit tunnistaa tietomurroille 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 Automaattinen-suojaustaso (jossa ohjelmille on sallittu vain lähtevä Internet-liikenne) ovat automaattisesti käytössä.

Voit poistaa palomuurin 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 ottaa palomuurin käyttöön myös Internet- ja verkkomäärittelyt -ikkunasta.

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

Huomaa: Määritä palomuuuri avaamalla Internet ja verkko -asetusikkuna.

Tässä luvussa

Palomuurisuojaus käynnistäminen.....	67
Palomuurisuojaus pysäyttäminen	68

Palomuurisuojaus 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 palomuuari havaitsee ja estää tietokoneessa olevan troijalaisen ja suosittelee tietokoneen tarkistamista uusien uhkien välttämiseksi. Troijalainen näyttää luvalliselta ohjelmalta, mutta se voi aiheuttaa tietokoneelle vahinkoa tai sallia tietokoneen luvattoman käytön. Hälytys esiintyy kaikilla tietoturvasoilla.

Keltaiset hälytykset

Keltainen hälytys on yleisin hälytystyyppi. Se ilmoittaa palomuurin havaitsemista ohjelmatoiminnoista ja verkkotapahtumista. Keltainen hälytys kuvaa ohjelmatoiminnon tai verkkotapahtuman, ja se voi ehdottaa eri menettelytapoja. Näyttöön tulee esimerkiksi **Uusi verkkoyhteys** -hälytys, kun tietokone, johon palomuuari on asennettu, kytketään uuteen verkkoon. Voit määrittää uuden verkon luotettavuuden tason, minkä jälkeen verkko tulee näkyviin Verkot-luettelo. Jos suositukset on otettu käyttöön, tunnetut ohjelmat lisätään automaattisesti Ohjelmien käyttöoikeudet -ikkunaan.

Vihreät hälytykset

Useimmissa tapauksissa vihreä hälytys antaa perustietoja tapahtumasta eikä vaadi käyttäjän vastausta. Vihreät hälytykset poistetaan oletusarvoisesti käytöstä.

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 palomuuari on havainnut tietokoneessa.
- **Kerro McAfeelle tästä ohjelmasta:** Lähetä McAfeelle tietoja tuntemattomasta tiedostosta, jonka palomuuari on havainnut tietokoneessa.
- **McAfee suosittelee:** Hälytysten käsittelyyn liittyviä neuvoja. Hälytys voi esimerkiksi suositella, että myönnet 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.....	71
Piilota tiedottavat hälytykset.....	72

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**.

LUKU 17

Palomuurisuojausten 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 Automaattinen 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	74
Hälytyksiin liittyvien suositusten asetusten määrittäminen.....	77
Palomuurin suojausten optimointi	79
Palomuurin lukitseminen ja palauttaminen	82

Palomuurin tietoturvasojen hallinta

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

Kun Automaattinen-tietoturvaso on asetettu ja suositukset on otettu käyttöön, keltaiset hälytykset antavat mahdollisuuden sallia käyttöoikeudet tuntemattomille, saapuvaa yhteyttä tarvitseville ohjelmille tai estää ne. Vaikka vihreät hälytykset poistetaan oletusarvoisesti käytöstä, ne tulevat näyttöön tunnettujen ohjelmien havaitsemisen yhteydessä, 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 Normaali) kohdalla käytetään enemmän asetuksia ja näytetään enemmän hälytyksiä, joihin käyttäjän on vastattava.

Seuraavassa taulukossa kuvataan palomuurin kolme suojaustasoa erittäin rajoittavasta vähiten rajoittavaan:

Taso	Kuvaus
Vaikeasti havaittava	Estää kaikki saapuvat Internet-yhteydet (paitsi avoimet portit) ja estää muita näkemästä tietokonettasi Internetissä. Palomuuuri hälyttää, kun uudet ohjelmat yrittävät muodostaa yhteyden Internetiin tai vastaanottavat saapuvia yhteyspyyntöjä. Estetyt ja lisätyt ohjelmat näkyvät Ohjelmien käyttöoikeudet -ikkunassa.
Normaali	Palomuuuri valvoo saapuvia ja lähteviä verkkoyhteyksiä ja ilmoittaa käyttäjälle, kun uudet ohjelmat yrittävät muodostaa yhteyden Internetiin. Estetyt ja lisätyt ohjelmat näkyvät Ohjelmien käyttöoikeudet -ikkunassa.
Automaattinen	Palomuuuri sallii joko saapuvat ja lähtevät tai vain lähtevät Internet-yhteydet. Oletussuojaustaso on Automaattinen 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.

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

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 -ikkunasta **Internet ja verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomäärittäykset -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 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 verkkomäärittäykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Siirrä Tietoturvaso-ikkunan liukusäädintä siten, että sen nykyisenä tasona on **Normaali**.
- 4 Valitse **OK**.

Suojaustason määrittäminen Automaattinen-tasolle

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

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet ja verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Siirrä Tietoturvaso-ikkunan liukusäädintä siten, että sen nykyisenä tasona on **Automaattinen**.
- 4 Valitse jokin seuraavista:
 - Voit sallia saapuvan ja lähtevän liikenteen valitsemalla **Salli kaikki käyttö**.
 - Voit sallia pelkästään lähtevän liikenteen valitsemalla **Salli vain lähtevä käyttö**.
- 5 Valitse **OK**.

Huomautus: **Salli vain lähtevä käyttö** on oletusasetus.

Hälytyksiin liittyvien suositusten asetusten määrittäminen

Voit määrittää, miten haluat palomuurin hälyttävän ohjelmista, jotka yrittävät muodostaa Internet-yhteyden. Palomuuuri 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 Automaattinen ja vain lähtevät yhteydet on sallittu), palomuuuri sallii tunnetut ohjelmat ja estää mahdollisesti vaaralliset ohjelmat automaattisesti.

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

Kun suositusten arvoksi on asetettu Näytä, palomuuuri kehottaa sallimaan tai estämään yhteyksiä ja antaa suosituksia.

Ota suositukset käyttöön

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

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet ja verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelyt -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Tietoturvaso-ikkunan **Suosituksien**-kohdasta **Käytä suosituksia**.
- 4 Valitse **OK**.

Poista suositukset käytöstä

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

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet ja verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Tietoturvaso-ikkunan **Suosituks**-kohdasta **Älä käytä suosituksia**.
- 4 Valitse **OK**.

Näytä suositukset

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

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet ja verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Tietoturvaso-ikkunan **Suosituks**-kohdasta **Näytä suositukset**.
- 4 Valitse **OK**.

Palomuurin suojauksen optimointi

Tietokoneen suojaus voi pettää monesta syystä. Jotkin ohjelmat voivat esimerkiksi yrittää muodostaa Internet-yhteyden Windowsin® käynnistyessä. Kokeneet tietokoneen käyttäjät voivat määrittää, onko tietokoneesi verkossa, lähettämällä ping-pyyntöä tietokoneeseesi. He voivat myös lähettää tietokoneellesi tietoja UDP-protokollan avulla viestiyksiköiden (datagrammien) muodossa. Palomuuuri suojaa tietokoneitasi tällaisilta tietomurroilta antamalla sinulle mahdollisuuden estää ohjelmia muodostamasta Internet-yhteyttä Windowsin käynnistyessä, estää ping-pyyntöt, joiden avulla muut käyttäjät voivat havaita tietokoneesi verkossa ja estää muita käyttäjiä lähettämästä tietoja tietokoneellesi viestiyksiköiden (datagrammien) muodossa.

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. Palomuuuri näyttää niitä ohjelmia koskevat hälytykset, jotka pysyvät Internetin käyttöoikeuksia. Voit päättää, myönnätkö vai estätkö oikeudet.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet ja verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelyt -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Tietoturvasuojaus-ikkunan **Suojausasetukset**-kohdasta **Ota suojaus käyttöön Windowsin käynnistyessä**.
- 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 verkkomäärittelyt -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 UDP-asetukset

Voit antaa muille verkossa olevien tietokoneiden käyttäjille luvan lähettää viestiyksiköitä (datagrammeja) tietokoneellesi UDP-protokollan avulla. Tämä on kuitenkin mahdollista vain silloin, jos olet sulkenut järjestelmäpalveluportin tämän protokollan estämiseksi.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet ja verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelyt -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Tietoturvasuojaus-ikkunan **Suojausasetukset**-kohdasta jompikumpi seuraavista:
 - Voit antaa muille verkossa olevien tietokoneiden käyttäjille luvan lähettää viestiyksiköitä (datagrammeja) tietokoneellesi valitsemalla **Ota UDP-seuranta käyttöön**.
 - Poista **Ota UDP-seuranta käyttöön** -valintaruudun valinta, jos haluat estää muita verkossa olevien tietokoneiden käyttäjiä lähettämästä viestiyksiköitä (datagrammeja) tietokoneellesi.
- 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 verkkomäärittelyt -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 suojausten 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 **Suojausten tila** -kohdasta **Lisäasetukset**.
- 3 Valitse Ohitetut ongelmat -ikkunasta vähintään yksi seuraavista vaihtoehdoista:
 - **Palomuurisuojaus ei ole käytössä.**
 - **Palomuuripalvelu ei ole käytössä.**
 - **Palomuurisuojausta ei ole asennettu tietokoneeseen.**
 - **Windowsin palomuri on poistettu käytöstä.**
 - **Lähtevää palomuuria ei ole asennettu tietokoneeseen.**
- 4 Valitse **OK**.


Palomuurin lukitseminen ja palauttaminen

Lukitus estää kaikki lähtevät ja saapuvat verkkoyhteydet, mukaan lukien yhteydet Web-sivustoihin, sähköpostiin ja tietoturvapäivityksiin. Lukituksella on sama vaikutus kuin tietokoneen verkkokaapeleiden irrottamisella. Tällä asetuksella voit estää Järjestelmäpalvelut-ikkunassa avoinna olevat portit sekä eristää ja määrittää tietokoneessa ilmenevät viat.

Lukitse palomuuuri välittömästi

Palomuurin lukitseminen estää välittömästi kaiken tietokoneen ja verkkojen välisen tietoliikenteen, Internet mukaan lukien.

- 1 Valitse McAfee SecurityCenter -ikkunan **Yleiset tehtävät** -kohdasta **Lukitse palomuuuri**.
- 2 Valitse Lukitse palomuuuri -ikkunasta **Ota palomuurin lukitus käyttöön**.
- 3 Vahvista valintasi valitsemalla **Kyllä**.

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

Poista palomuurin lukitus välittömästi

Palomuurin lukituksen poistaminen sallii kaiken tietokoneen ja verkkojen välisen tietoliikenteen, Internet mukaan lukien.

- 1 Valitse McAfee SecurityCenter -ikkunan **Yleiset tehtävät** -kohdasta **Lukitse palomuuuri**.
- 2 Valitse Lukitus käytössä -ikkunasta **Poista palomuurin lukitus käytöstä**.
- 3 Vahvista valintasi valitsemalla **Kyllä**.

Palauta palomuurin asetukset

Voit palauttaa palomuurin alkuperäiset suojausasetukset nopeasti. Tämä muuttaa suojaustason takaisin Automaattiseksi 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 palomuurin oletusasetukset**.
- 2 Valitse Palauta palomuurin oletusasetukset -ikkunasta **Palauta oletusasetukset**.
- 3 Vahvista valintasi valitsemalla **Kyllä**.
- 4 Valitse **OK**.

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.....	86
Vain lähtevän tietoliikenteen käyttöoikeuksien myöntäminen	88
Ohjelmien Internet-käyttöoikeuden estäminen.....	90
Ohjelmien käyttöoikeuksien poistaminen	91
Perehtyminen ohjelmiin	92

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 verkkomäärittelyt -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 estetylle 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 109)

Myönnä täydet käyttöoikeudet lähtevien tapahtumien lokista

Voit myöntää lähtevien tapahtumien lokissa olevalle estetylle 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 verkkomäärittelykset -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 estetylle 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 verkkomäärittelykset -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 verkkomäärittelykset -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 verkkomäärittelykset -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 tietoturvauhkista.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet & verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelykset -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 tietoturvauhista.

- 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

Tietokoneyhteyksien hallinta

Voit määrittää palomuurin 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 luotettavan tietokoneen myös palomuurilla ja ajan tasalla olevalla virustorjuntaohjelmalla. Palomuuuri ei kirjaa tietoliikennettä tai luo tapahtumahälytyksiä **Verkot**-luettelossa oleville luotettaville IP-osoitteille.

Voit estää tuntemattomiin, epäilyttäviin tai epäluotettaviin IP-osoitteisiin yhteydessä olevia tietokoneita 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.

Tässä luvussa

Tietoja tietokoneyhteyksistä	94
Tietokoneyhteyksien estäminen	98

Tietoja tietokoneyhteyksistä

Tietokoneyhteydet ovat yhteyksiä, jotka luot verkossa olevien tietokoneiden ja oman tietokoneesi välille. Voit lisätä, muokata ja poistaa IP-osoitteita **Verkot**-luettelossa. Nämä IP-osoitteet liittyvät verkkoihin, joiden luotettavuuden tason haluat määrittää, kun niiden ja oman tietokoneesi välille muodostetaan yhteys: Luotettu, Vakio ja Julkinen.

Taso	Kuvaus
Luotettu	Palomuuuri sallii IP-osoitteesta peräisin olevan liikenteen kaikkien porttien kautta. Palomuuuri ei suodata eikä analysoi luotettavaa IP-osoitetta käyttävän tietokoneen ja käyttäjän tietokoneen välisiä tapahtumia. Oletusarvoisesti ensimmäinen palomuurin löytämä yksityinen verkko merkitään Verkot -luettelossa luotettavaksi. Esimerkki luotettavasta verkosta on paikallis- tai kotiverkossa oleva tietokone.
Vakio	Palomuuuri valvoo IP-osoitteesta peräisin olevaa tietoliikennettä (mutta ei muista verkossa olevista tietokoneista peräisin olevaa tietoliikennettä), kun verkosta muodostetaan yhteys tietokoneeseen. Palomuuuri sallii tai estää tietoliikenteen Järjestelmäpalvelut -luettelossa olevien sääntöjen perusteella. Palomuuuri kirjaa tietoliikenteen lokiin ja luo tapahtumahälytyksiä tavallisista IP-osoitteista peräisin oleville tapahtumille. Esimerkki tavallisesta verkosta on yritysverkossa oleva tietokone.
Julkinen	Palomuuuri valvoo julkisen verkon tietoliikennettä Järjestelmäpalvelut -luettelossa olevien sääntöjen perusteella. Esimerkki julkisesta verkosta on kahvilan, hotellin tai lentokentän Internet-verkko.

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 luotettavan tietokoneen myös palomuurilla ja ajan tasalla olevalla virustorjuntaohjelmalla.

Lisää tietokoneyhteys

Voit lisätä luotettavan, vakion tai julkisen tietokoneyhteyden ja siihen liittyvän IP-osoitteen.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet ja verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Palomuuuri-ikkunasta **Verkot**.
- 4 Valitse Verkot-ikkunasta **Lisää**.
- 5 Jos tietokoneyhteys on IPv6-verkossa, valitse **IPv6**-valintaruutu.
- 6 Toimi **Lisää sääntö** -kohdassa seuraavasti:
 - Valitse **Yksi** ja kirjoita IP-osoite **IP-osoite**-ruutuun.
 - Valitse **Alue** ja kirjoita aloitus- ja lopetusosoitteet **IP-osoitteesta**- ja **IP-osoitteeseen**-kenttiin. Jos tietokoneyhteys on IPv6-verkossa, kirjoita IP-aloitusosoite ja etuliitteen pituus **IP-osoitteesta**- ja **Etuliitteen pituus**-ruutuihin.
- 7 Toimi **Tyyppi**-kohdassa seuraavasti:
 - Valitse **Luotettu**, jos haluat osoittaa, että tämä tietokoneyhteys (esimerkiksi kotiverkossa oleva tietokone) on luotettava.
 - Valitse **Vakio**, jos haluat osoittaa, että tämä tietokoneyhteys (esimerkiksi yritysverkossa oleva tietokone, mutta eivät muut samassa verkossa olevat tietokoneet) on luotettava.
 - Valitse **Julkinen**, jos haluat osoittaa, että tämä tietokoneyhteys (esimerkiksi Internet-kahvilassa, hotellissa tai lentokentällä oleva tietokone) on julkinen.
- 8 Jos järjestelmäpalvelu käyttää Internet Connection Sharing (ICS) -yhteyttä, voit lisätä IP-osoitealueeksi 192.168.0.1 - 192.168.0.255.
- 9 Valitse vaihtoehtoisesti **Säännön voimassaoloaika päättyy** ja anna päivien määrä, jonka haluat säännön olevan voimassa.
- 10 Voit kirjoittaa myös kuvauksen säännöstä.
- 11 Valitse **OK**.

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

Lisää tietokone saapuvien tapahtumien lokista

Voit lisätä luotettavan tai tavallisen 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 ja verkko** ja valitse sitten **Saapuvat tapahtumat**.
- 5 Valitse IP-lähdeosoite ja toimi **Haluan**-kohdassa seuraavasti:
 - Valitse **Lisää tämä IP-osoite määrittämällä sen tyyppiä Luotettu**, jos haluat lisätä tämän tietokoneen **Verkot**-luetteloon merkinnällä Luotettu.
 - Valitse **Lisää tämä IP-osoite määrittämällä sen tyyppiä Vakio**, jos haluat lisätä tämän tietokoneen **Verkot**-luetteloon merkinnällä Vakio.
- 6 Vahvista valintasi valitsemalla **Kyllä**.

Muokkaa tietokoneyhteyttä

Voit muokata luotettavaa, vakiota tai julkista tietokoneyhteyttä ja siihen liittyvää IP-osoitetta.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet ja verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelyt -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Palomuuuri-ikkunasta **Verkot**.
- 4 Valitse Verkot-ikkunasta ensin IP-osoite ja sitten **Muokkaa**.
- 5 Jos tietokoneyhteys on IPv6-verkossa, valitse **IPv6**-valintaruutu.
- 6 Toimi **Muokkaa sääntöä** -kohdassa seuraavasti:
 - Valitse **Yksi** ja kirjoita IP-osoite **IP-osoite**-ruutuun.
 - Valitse **Alue** ja kirjoita aloitus- ja lopetusosoitteet **IP-osoitteesta**- ja **IP-osoitteeseen**-kenttiin. Jos tietokoneyhteys on IPv6-verkossa, kirjoita IP-aloitusosoite ja etuliitteen pituus **IP-osoitteesta**- ja **Etuliitteen pituus**-ruutuihin.
- 7 Toimi **Tyyppi**-kohdassa seuraavasti:
 - Valitse **Luotettu**, jos haluat osoittaa, että tämä tietokoneyhteys (esimerkiksi kotiverkossa oleva tietokone) on luotettava.

- Valitse **Vakio**, jos haluat osoittaa, että tämä tietokoneyhteys (esimerkiksi yritysverkossa oleva tietokone, mutta eivät muut samassa verkossa olevat tietokoneet) on luotettava.
 - Valitse **Julkinen**, jos haluat osoittaa, että tämä tietokoneyhteys (esimerkiksi Internet-kahvilassa, hotellissa tai lentokentällä oleva tietokone) on julkinen.
- 8** Valitse vaihtoehtoisesti **Säännön voimassaoloaika päättyy** ja anna päivien määrä, jonka haluat säännön olevan voimassa.
- 9** Voit kirjoittaa myös kuvauksen säännöstä.
- 10** Valitse **OK**.

Huomautus: Et voi muokata oletusarvoista tietokoneyhteyttä, jonka palomuuuri on automaattisesti lisännyt luotettavasta yksityisverkosta.

Poista tietokoneyhteys

Voit poistaa luotettavan, vakion tai julkisen tietokoneyhteyden ja siihen liittyvän IP-osoitteen.

- 1** Valitse McAfee SecurityCenter -ikkunasta **Internet ja verkko** ja valitse **Määritä**.
- 2** Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3** Valitse Palomuuuri-ikkunasta **Verkot**.
- 4** Valitse Verkot-ikkunasta ensin IP-osoite ja sitten **Poista**.
- 5** Vahvista valintasi valitsemalla **Kyllä**.

Tietokoneyhteyksien estäminen

Voit lisätä, muokata ja poistaa estettyjä IP-osoitteita Estetyt IP-osoitteet -ikkunassa.

Voit estää tuntemattomiin, epäilyttäviin tai epäluotettaviin IP-osoitteisiin yhteydessä olevia tietokoneita 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.

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 ja verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Palomuuuri-ikkunasta **Estetyt IP-osoitteet**.
- 4 Valitse Estetyt IP-osoitteet -ikkunasta **Lisää**.
- 5 Jos tietokoneyhteys on IPv6-verkossa, valitse **IPv6**-valintaruutu.
- 6 Toimi **Lisää sääntö** -kohdassa seuraavasti:
 - Valitse **Yksi** ja kirjoita IP-osoite **IP-osoite**-ruutuun.
 - Valitse **Alue** ja kirjoita aloitus- ja lopetusosoitteet **IP-osoitteesta**- ja **IP-osoitteeseen**-kenttiin. Jos tietokoneyhteys on IPv6-verkossa, kirjoita IP-aloitusosoite ja etuliitteen pituus **IP-osoitteesta**- ja **Etuliitteen pituus**-ruutuihin.
- 7 Valitse vaihtoehtoisesti **Säännön voimassaoloaika päättyy** ja anna päivien määrä, jonka haluat säännön olevan voimassa.
- 8 Voit kirjoittaa myös kuvauksen säännöstä.
- 9 Valitse **OK**.
- 10 Vahvista valintasi valitsemalla **Kyllä**.

Muokkaa estettyä tietokoneyhteyttä

Voit muokata estettyä tietokoneyhteyttä ja siihen liittyvää IP-osoitetta.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet ja verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Palomuuuri-ikkunasta **Estetyt IP-osoitteet**.
- 4 Valitse Estetyt IP-osoitteet -ikkunasta **Muokkaa**.
- 5 Jos tietokoneyhteys on IPv6-verkossa, valitse **IPv6**-valintaruutu.
- 6 Toimi **Muokkaa sääntöä** -kohdassa seuraavasti:
 - Valitse **Yksi** ja kirjoita IP-osoite **IP-osoite**-ruutuun.
 - Valitse **Alue** ja kirjoita aloitus- ja lopetusosoitteet **IP-osoitteesta**- ja **IP-osoitteeseen**-kenttiin. Jos tietokoneyhteys on IPv6-verkossa, kirjoita IP-aloitusosoite ja etuliitteen pituus **IP-osoitteesta**- ja **Etuliitteen pituus**-ruutuihin.
- 7 Valitse vaihtoehtoisesti **Säännön voimassaoloaika päättyy** ja anna päivien määrä, jonka haluat säännön olevan voimassa.
- 8 Voit kirjoittaa myös kuvauksen säännöstä.
- 9 Valitse **OK**.

Poista estetty tietokoneyhteys

Voit poistaa estetyn tietokoneyhteyden ja siihen liittyvän IP-osoitteen.

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

Estä tietokone saapuvien tapahtumien lokista

Voit estää tietokoneyhteyden ja siihen liittyvän IP-osoitteen saapuvien tapahtumien lokista. Voit käyttää kaiken saapuvan Internet-tietoliikenteen IP-osoitteet sisältävää lokia sellaisten IP-osoitteiden estämiseen, joiden uskot olevan epäilyttävien tai ei-toivottujen Internet-tapahtumien taustalla.

Lisää IP-osoite **Estetyt IP-osoitteet** -luetteloon, jos haluat estää kaiken kyseisestä IP-osoitteesta saapuvan Internet-tietoliikenteen siihen katsomatta, ovatko järjestelmän palveluportit auki vai kiinni.

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

LUKU 20

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 palomuuuri sulkee nämä järjestelmäpalveluportit, sillä järjestelmän haavoittuvuus johtuu useimmiten juuri niistä. Etätietokoneyhteydet edellyttävät kuitenkin, että nämä järjestelmäpalveluportit ovat auki.

Tässä luvussa

Järjestelmäpalveluporttien asetusten määrittäminen 102

Järjestelmäpalveluporttien asetusten määrittäminen

Järjestelmäpalveluportit voidaan määrittää tietokoneen verkkopalvelun etäkäytön sallimiseksi tai estämiseksi. Nämä järjestelmäpalveluportit voidaan avata tai sulkea tietokoneissa, joiden tilana on **Verkot**-luettelossa Luotettu, Vakio tai Julkinen.

Alla oleva luettelo sisältää yleisimmät järjestelmäpalvelut ja niiden portit:

- Käyttöjärjestelmän yleinen portti 5327
- Tiedonsiirto-protokolla (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-yhdyskävänä, 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 järjestelmäpalvelun 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 ja verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelyt -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Palomuuuri-ikkunasta **Järjestelmäpalvelut**.
- 4 Avaa portti valitsemalla **Avaa järjestelmäpalveluportti** -kohdasta järjestelmäpalvelu.
- 5 Valitse **Muokkaa**.
- 6 Valitse jokin seuraavista:
 - Jos haluat avata portin johonkin tietokoneeseen luotetussa, vakiossa tai julkisessa verkossa (esimerkiksi kotiverkossa, yrityksen verkossa tai Internet-verkossa), valitse **Luotettu, Vakio tai Julkinen**.
 - Jos haluat avata portin johonkin tietokoneeseen vakioverkossa (esimerkiksi yrityksen verkossa), valitse **Vakio (sisältää Luotetun)**.
- 7 Valitse **OK**.

Estä olemassa olevan järjestelmäpalveluportin käyttö

Voit sulkea olemassa olevan portin ja estää tietokoneen järjestelmäpalvelun etäkäytön.

- 1 Valitse McAfee SecurityCenter -ikkunasta **Internet ja verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelyt -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Palomuuuri-ikkunasta **Järjestelmäpalvelut**.
- 4 Poista suljettavan järjestelmäpalveluportin vieressä olevan **Avaa järjestelmäpalveluportti** -valintaruudun valinta.
- 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 ja verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomääritykset -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Palomuuuri-ikkunasta **Järjestelmäpalvelut**.
- 4 Valitse **Lisää**.
- 5 Määritä Järjestelmäpalvelut-ikkunan **Lisää järjestelmäpalvelusääntö** -kohdassa seuraavat asetukset:
 - Järjestelmäpalvelun nimi
 - Järjestelmäpalvelun luokka
 - Paikalliset TCP/IP-portit
 - Paikalliset UDP-portit
- 6 Valitse jokin seuraavista:
 - Jos haluat avata portin johonkin tietokoneeseen luotetussa, vakiossa tai julkisessa verkossa (esimerkiksi kotiverkossa, yrityksen verkossa tai Internet-verkossa), valitse **Luotettu, Vakio tai Julkinen**.
 - Jos haluat avata portin johonkin tietokoneeseen vakioverkossa (esimerkiksi yrityksen verkossa), valitse **Vakio (sisältää Luotetun)**.
- 7 Jos haluat lähettää portin toimintaa koskevat tiedot toiseen verkossa olevaan ja saman Internet-yhteydet jakavaan Windows-tietokoneeseen, valitse **Ohjaa tämän portin verkkoliikenne verkon tietokoneisiin, jotka käyttävät Internet-yhteyden jakamista**.
- 8 Voit myös antaa uuden kokoonpanon kuvauksen.
- 9 Valitse **OK**.

Huomaa: Jos tietokoneessa on ohjelma, 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 **Verkot**-luetteloon. Lisätietoja on kohdassa Lisää 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 ja verkko** ja valitse **Määritä**.
- 2 Valitse Internet- ja verkkomäärittelyt -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 3 Valitse Palomuuuri-ikkunasta **Järjestelmäpalvelut**.
- 4 Valitse järjestelmäpalvelun vieressä oleva valintaruutu ja sitten **Muokkaa**.
- 5 Muokkaa Järjestelmäpalvelut-ikkunan **Lisää järjestelmäpalvelusääntö** -kohdassa seuraavia asetuksia:
 - Järjestelmäpalvelun nimi
 - Paikalliset TCP/IP-portit
 - Paikalliset UDP-portit
- 6 Valitse jokin seuraavista:
 - Jos haluat avata portin johonkin tietokoneeseen luotetussa, vakiossa tai julkisessa verkossa (esimerkiksi kotiverkossa, yrityksen verkossa tai Internet-verkossa), valitse **Luotettu, Vakio tai Julkinen**.
 - Jos haluat avata portin johonkin tietokoneeseen vakioverkossa (esimerkiksi yrityksen verkossa), valitse **Vakio (sisältää Luotetun)**.
- 7 Jos haluat lähettää portin toimintaa koskevat tiedot toiseen verkossa olevaan ja saman Internet-yhteydet jakavaan Windows-tietokoneeseen, valitse **Ohjaa tämän portin verkkoliikenne verkon tietokoneisiin, jotka käyttävät Internet-yhteyden jakamista**.
- 8 Voit myös antaa muokatun kokoonpanon kuvauksen.
- 9 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**.

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.....	108
Tilastotietojen käsitteleminen.....	110
Internet-tietoliikenteen jäljittäminen.....	110
Internet-tietoliikenteen valvonta	113

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 verkkomäärittelyt -ikkunan **Palomuurisuojaus on käytössä** -kohdasta **Lisäasetukset**.
- 2 Valitse Firewall-ikkunasta **Tapahumalokin 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 käsitteleminen

Palomuuuri 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 käytettäviä, 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 IP-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 IP-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.

Huomaa: 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. Tietoliikenteen valvonta näyttää myös 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 kuluvan 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 pisteiviivaa. 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 pisteiviivaa. 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. Tietoliikenteen valvonta näyttää myös 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

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

Tässä luvussa

Käynnistä HackerWatch-opetusohjelma..... 118

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**.

LUKU 23

McAfee Anti-Spam

Anti-Spam (aikaisemmalta nimeltään SpamKiller) estää ei-toivottujen sähköpostiviestien toimittamisen Saapuneet-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 muun muassa Yahoo®-, MSN®/Hotmail®-, Windows® Mail- ja Live™ Mail-, Microsoft® Outlook®- ja Outlook Express- sekä Mozilla Thunderbird™ -sähköpostiohjelmien, kuten myös POP3-, POP3-Web-sähköposti- ja MAPI (Microsoft Exchange Server) -sähköpostitilien 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.

Sinun ei tarvitse määrittää Anti-Spamia asentamisen jälkeen, mutta jos olet kokenut käyttäjä, haluat mahdollisesti säätää sen roskapostilta ja phishing-huijauksilta suojaavia kehittyneitä toimintoja omien mieltymystesi mukaan.

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	121
Roskapostiviestien tunnistustavan määrittäminen	123
Sähköpostin suodatus	131
Ystävien määrittäminen	133
Web-sähköpostitilien määrittäminen.....	137
Suodatettujen sähköpostiviestien käsitteleminen	141
Phishing-huijausten torjunnan asetusten määrittäminen.....	143

Anti-Spamin ominaisuudet

Roskapostin suodatus

Estä roskapostin pääsy Saapuneet-kansioosi. Anti-Spamin kehittyneet suodattimet päivitetään automaattisesti jokaista sähköpostitiliäsi varten. Voit luoda myös mukautettuja suodattimia varmistaaksesi, että kaikki roskapostiviestit suodatetaan, ja lähettää roskapostiviestit McAfeelle analysointia varten.

Phishing-suodatus

Tunnista mahdollisesti petolliset phishing-sivustot, jotka tavoittelevat 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 sähköpostiosoitteet ystäväluetteloon, jotta heidän lähettämiään sähköpostiviestejä ei suodateta.

LUKU 24

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

Suodatusasetusten määrittäminen	124
Henkilökohtaisten suodattimien käyttäminen	127
Poista roskapostin torjunta käytöstä.....	130

Suodatusasetusten määrittäminen

Säädä Anti-Spamin suodatusasetuksia, jos haluat suodattaa viestejä aggressiivisesti, määrittää roskapostin käsittelytavan ja etsiä tiettyjä merkistöjä roskapostia analysoitaessa.

Suodatustaso

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

Roskapostin käsittely

Anti-Spamin avulla voit mukauttaa roskapostiviestien käsittelyasetuksia. Voit esimerkiksi siirtää roskaposti- ja phishing-huijausviestit tiettyihin kansioihin, muuttaa sähköposti- ja phishing-huijausviestien otsikkorivillä olevaa tunnistetta, määrittää suodatettavien viestien enimmäiskoon ja määrittää roskapostisääntöjen päivitystiheyden.

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, länsieurooppalaisen merkistön valitseminen suodattaa myös englanniksi ja muilla länsieurooppalaista merkistöä käytävillä kielillä kirjoitetut viestit. Tässä tapauksessa et voi suodattaa vain italiankielisiä viestejä.

Huomautus: Merkistösuodattimen käyttöä 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** Valitse **Määritä roskapostin suodatustaso** -luettelosta haluamasi taso ja valitse **OK**.

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

Muokkaa roskapostin käsittely- ja merkintätapaa

Voit määrittää kansion, johon roskaposti- ja phishing-huijausviestit siirretään, muuttaa sähköposti- ja phishing-huijausviestien otsikkorivillä olevaa [SPAM]- tai [PHISH]-tunnistetta, määrittää suodatettavien viestien enimmäiskoon ja määrittää roskapostisääntöjen päivitystiheyden.

- 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 Muokkaa alla olevia asetuksia tai valitse ne, ja valitse sen jälkeen **OK**.

Toiminto	Toimenpide
Määritä sijainti, johon roskaposti- ja phishing-huijausviestit siirretään.	Valitse kansio Siirrä roskapostiviestit tähän kansioon -luettelosta. Oletuskansio on McAfee Anti-Spam.
Muuta roskapostiviestien otsikkoriviä	Määritä Merkitse roskapostiviestien aihe merkinnällä -kohdassa tunniste, jonka haluat lisätä roskapostiviestien otsikkoriville. Oletustunniste on [SPAM].
Muuta phishing-huijausviestien otsikkoriviä	Määritä Merkitse roskapostiviestien aihe merkinnällä -kohdassa tunniste, jonka haluat lisätä phishing-huijausviestien otsikkoriville. Oletustunniste on [PHISH].
Muuta suodatettavien sähköpostiviestien enimmäiskokoa	Määritä Määritä suurin suodatettava sähköpostiviesti (koko kilotavuina) -kohdassa suodatettavien sähköpostiviestien enimmäiskoko.
Päivitä roskapostisäännöt	Valitse Päivitä roskapostisäännöt (minuutteina) ja määritä roskapostisääntöjen päivitystiheys. Suositeltu päivitystiheys on 30 minuuttia. Jos käytät nopeata verkkoyhteyttä, saat parempia tuloksia määrittämällä suuremman päivitystiheyden, kuten 5 minuuttia.
Älä päivitä roskapostisääntöjä	Valitse Älä päivitä roskapostisääntöjä .

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

Henkilökohtainen suodatin määrittää, sallitaanko vai estetäänkö sähköpostiviestit tiettyjen sanojen tai lauseiden perusteella. Jos sähköpostiviesti sisältää sanan tai lauseen, jonka suodatin on määritetty estämään, viesti merkitään roskapostiksi ja jätetään Saapuneet-kansioon tai siirretään McAfee Anti-Spam -kansioon. Lisätietoja roskapostiviestien käsittelystä on kohdassa Muokkaa viestin käsittely- ja merkintätapaa (sivu 125).

Anti-Spamissa on kehittynyt suodatin, joka estää ei-toivottujen sähköpostiviestien toimittamisen Saapuneet-kansioon. Jos haluat kuitenkin säätää, mitkä viestit Anti-Spam tunnistaa roskapostiksi, voit luoda henkilökohtaisen suodattimen. Esimerkiksi jos lisäät laina-sanan sisältävän suodattimen, Anti-Spam suodattaa laina-sanan sisältävän viestit. Älä luo suodattimia asiallisissa sähköpostiviesteissä esiintyvillä tavallisilla sanoilla, sillä tällöin suodatetaan myös muut kuin roskapostiviestit. Kun olet luonut suodattimen, voit muokata sitä, jos se ei edelleenkaan 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 säännönmukaisten 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 -tietoalueelta **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 129) 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 -tietoalueelta **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 129) 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**.

Määritä henkilökohtainen suodatin

Tässä taulukossa kuvataan, mitä henkilökohtainen suodatin etsii sähköpostiviesteistä.

Toiminto	Toimenpide
Määritä sähköpostiviestin suodatettava osa	Valitse Sähköpostin osa -luettelosta kohta, jolla määrität, etsiikö suodatin sanoja tai ilmaisuja sähköpostiviestin aiheesta, tekstiosasta, lähettäjästä, otsikosta vai vastaanottajasta. Valitse Sähköpostin osa -luettelosta kohta, jolla määrität, etsiikö suodatin sähköpostiviestiä, joka joko sisältää tai ei sisällä määrittämiäsi sanoja tai ilmauksia.
Määritä suodattimen etsimät sanat tai lauseet	Kirjoita Sanat tai fraasit -ruutuun se, mitä viestistä etsitään. Jos esimerkiksi määrität <i>laina</i> , kaikki kyseisen sanan sisältävät sähköpostiviestit suodatetaan.
Määritä suodatin käyttämään säännönmukaisia lausekkeita	Valitse Tämä suodatin käyttää säännönmukaisia lausekkeita .
Valitse, haluatko estää tai sallia sähköpostiviestit suodattimessa määritettyjen sanojen tai lauseiden perusteella	Valitse Suorita tämä toiminto -kohdasta Estä tai Salli sen mukaan, haluatko estää tai sallia suodattimessa määritetyt sanat tai lauseet sisältävät sähköpostiviestit.

Poista roskapostin torjunta käytöstä

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

- 1 Valitse Lisävalikosta **Määritä**.
- 2 Valitse Määritä-ruudusta **Sähköposti ja pikaviestit**.
- 3 Valitse **Roskapostin torjunta on käytössä** -kohdasta **Ei käytössä**.

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

LUKU 25

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 merkitä sähköpostiviestit roskapostiksi tai ei-roskapostiksi Anti-Spamin työkalurivillä, muuttaa sijaintia, jonne roskapostiviestit siirretään, tai muuttaa otsikkorivillä näkyvää tunnistetta.

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

Tässä luvussa

Merkitse viesti Anti-Spam-työkaluriviltä.....	131
Poista Anti-Spam-työkalurivi käytöstä	132

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	Valitse Anti-Spam -valikosta Merkitse roskapostiksi tai Merkitse ei roskapostiksi .
Thunderbird	Napsauta Anti-Spam -työkalurivillä olevaa M -kuvaketta, valitse Merkitse ja sitten roskapostiksi tai ei roskapostiksi .

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 -tietoaalueelta **Määritä**.
3. Valitse Sähköposti ja pikaviesti -asetusikkunan **Roskapostin torjunta** -kohdasta **Lisäasetukset**.

2 Valitse Roskapostin torjunta -ikkunasta **Sähköpostin työkalurivit**.

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 26

Ystävien määrittäminen

Koska Anti-Spamin parannettu suodatin tunnistaa ja sallii asialliset sähköpostiviestit, sinun tarvitsee lisätä ystäväsi sähköpostiosoitteet ystäväluettelosi vain harvoin, halusitpa lisätä ne manuaalisesti tai tuoda osoitekirjoja. Jos kuitenkin lisäät ystäväsi sähköpostiosoitteen ja joku käyttää sitä väärin, Anti-Spam päästää kyseisestä sähköpostiosoitteesta tulevat viestit Saapuneet-kansioosi.

Jos haluat silti tuoda osoitekirjasi ja ne muuttuvat, sinun on tuotava ne uudelleen, sillä Anti-Spam ei automaattisesti päivitä ystäväluetteloa.

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

Tässä luvussa

Tuo osoitekirja.....	133
Ystävien määrittäminen manuaalisesti	134

Tuo osoitekirja

Tuo osoitekirjat, jos haluat Anti-Spamin lisäävän niissä olevat sähköpostiosoitteet ystäväluettelosi.

- 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 **Ystävät**.
- 3 Valitse Ystävät-ikkunasta **Tuo**.
- 4 Valitse tuotavan osoitekirjan tyyppi **Valitse tuotava osoitekirja** -luettelosta.
- 5 Valitse **Tuo nyt**.

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-sähköpostiohjelmaa, voit lisätä ystäviä Anti-Spam-työkaluriviltä.

Ystävän lisääminen ohjelmasta...	Valitse viesti ja sitten...
Outlook, Outlook Express, Windows Mail	Valitse Lisää ystävä .
Eudora	Valitse Anti-Spam -valikosta Lisää ystävä .
Thunderbird	Napsauta Anti-Spam -työkalurivillä olevaa M -kuvaketta, valitse Merkitse ja sitten ystäväksi .

Lisää ystävä manuaalisesti

Jos et halua lisätä ystävää suoraan työkaluriviltä tai unohdit tehdä niin, kun sait sähköpostiviestin, voit silti lisätä ystävän ystäväluettelosi.

- 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 ystävän tietoja

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, jonka tietoja 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 -tietoalueelta **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 -tietoalueelta **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**.

LUKU 27

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 muun muassa Yahoo®-, MSN®/Hotmail®-, Windows® Mail- ja Live™ Mail-, Microsoft® Outlook®- ja Outlook Express- sekä Mozilla Thunderbird™ -sähköpostiohjelmien, kuten myös POP3-, POP3-Web-sähköposti- ja MAPI (Microsoft Exchange Server) -sähköpostitilien 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 Web-sähköpostitilisi 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.

Tässä luvussa

Lisää Web-sähköpostitili	137
Muokkaa Web-sähköpostitiliä	138
Poista Web-sähköpostitili	139
Web-sähköpostitilin tietojen ymmärtäminen	139

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 139) ja valitse **Seuraava**.
- 5 Määritä **Tarkistusasetukset**-kohdassa, milloin haluat Anti-Spamin tarkistavan tilisi roskapostin varalta (sivu 139).
- 6 Jos käytät puhelinverkkoyhteyttä, määritä, miten Anti-Spam muodostaa yhteyden Internetiin (sivu 139).
- 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 139) ja valitse **Seuraava**.
- 5 Määritä **Tarkistusasetukset**-kohdassa, milloin haluat Anti-Spamin tarkistavan tilisi roskapostin varalta (sivu 139).
- 6 Jos käytät puhelinverkkoyhteyttä, määritä, miten Anti-Spam muodostaa yhteyden Internetiin (sivu 139).
- 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.

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 tarkastella, viedä ja poistaa suodatettuja sähköpostiviestejä. Tämä on käytännöllistä silloin, jos et ole varma, oletko suodattanut asiallisen viestin, tai kun haluat tietää, milloin viesti on suodatettu.

Tässä luvussa

Ilmoita sähköpostiviesteistä McAfeelle	141
Tarkastele, vie tai poista suodatettuja Web-sähköpostiviestejä	142
Näytä suodatettujen Web-sähköpostiviestien tapahtumat	142

Ilmoita sähköpostiviesteistä McAfeelle

Voit ilmoittaa sähköpostiviesteistä McAfeelle, kun merkitset ne roskapostiksi tai ei roskapostiksi, jotta voimme analysoida ne tarkemmin luodessamme 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 **Sähköpostin työkalurivit**.
- 3 Valitse **Autu parantamaan Anti-Spamia** -ikkunasta haluamasi valintaruudut ja valitse sen jälkeen **OK**.

Toiminto	Toimenpide
Ilmoitus McAfeelle aina, kun viesti merkitään roskapostiksi.	Valitse Merkitse sähköpostiviestit roskapostiksi .
Ilmoitus McAfeelle aina, kun viesti merkitään ei roskapostiksi.	Valitse Merkitse sähköpostiviestit ei roskapostiksi .

Toiminto	Toimenpide
Lähetä koko sähköpostiviesti (ei ainoastaan otsikko) McAfeelle, kun ilmoitat sähköpostiviestistä, joka ei ole roskapostiviesti.	Valitse Lähetä koko sähköpostiviesti (ei vain otsikkoa) .

Huomautus: Kun ilmoitat sähköpostiviestistä, joka ei ole roskapostiviesti, ja lähetät koko sähköpostiviestin McAfeelle, sähköpostiviestiä ei salata.

Tarkastele, vie tai poista suodatettuja Web-sähköpostiviestejä

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

- 1 Valitse **Yleiset tehtävät** -kohdasta **Raportit ja lokit**.
- 2 Valitse Raportit ja lokit -ruudun kohta **Suodatetut Web-sähköpostiviestit**.
- 3 Valitse viesti.
- 4 Suorita jokin seuraavista toimenpiteistä **Haluan**-kohdassa:
 - Valitse **Näytä**, jos haluat tarkastella viestiä oletusarvoisessa sähköpostiohjelmassa.
 - Valitse **Vie**, jos haluat kopioida viestin tietokoneeseen.
 - 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-suojauksia, sillä SiteAdvisor käyttää Anti-Spamin kaltaista phishing-suojauksia.

Tässä luvussa

Lisää Web-sivusto valkoiseen listaan.....	143
Muokkaa valkoisessa listassa olevia sivustoja.....	144
Poista Web-sivusto valkoisesta listasta.....	144
Poista phishing-huijausten torjunta käytöstä.....	144

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 eivätkä ohjelmistot ole keskenään yhteensopivia, voit poistaa Anti-Spamin phishing-suojauksen käytöstä.

- 1 Valitse SecurityCenterin Koti-ikkunasta **Internet ja verkko**.
- 2 Valitse Internet ja verkko -tietoaalueelta **Määritä**.
- 3 Valitse **Phishing-huijausten torjunta on käytössä** -kohdasta **Ei käytössä**.

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

LUKU 30

McAfee Parental Controls

Käytönvalvonta-asetukset 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. Käytönvalvonta-asetusten avulla voit valvoa, hallita ja kirjata luvattomia Web-selaustapoja, ja se toimii myös omien salasanojesi suojattuna säilytyspaikkana.

Voit tutustua käytönvalvonta-asetusten suosituimpiin ominaisuuksiin, ennen kuin alat käyttää sitä. Lisätietoja näiden ominaisuuksien määrittämisestä ja käyttämisestä on käytönvalvonta-asetusten 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

Parental Controlsin ominaisuudet	146
Lasten suojaaminen	147
Tietojen suojaaminen Internetissä	161
Salasanojen suojaaminen	163

Parental Controlsin ominaisuudet

Käytönvalvonta-asetukset

Suodata mahdollisesti epäsovikat kuvat, käytä ikäryhmälle sopivaa hakua, määritä käyttäjän ikä (joka määrää estettävän sisällön) ja aseta Web-selaukselle aikarajoitukset (päivät ja kellonajat, jolloin käyttäjällä on Internet-yhteys käytössään) SecurityCenterin käyttäjille. Käytönvalvonta-asetuksilla voit myös rajoittaa käyttäjien pääsyä Web-sivustoihin ja sallia tai estää käytön ikäryhmien käyttöoikeuksien tai avainsanojen perusteella.

Henkilökohtaisten tietojen suojaus

Estä arkaluontoisten ja luottamuksellisten tietojen (esimerkiksi luottokorttien numeroiden, pankkitilinumeroiden, osoitteiden ja niin edelleen) lähettämisen Internetin kautta.

Salasanasäilö

Tallenna salasanasi turvallisesti niin, ettei kukaan muu käyttäjä (ei edes järjestelmänvalvoja) saa niitä käyttöönsä.

LUKU 31

Lasten suojaaminen

Jos lapsesi käyttävät tietokonetta, käytönvalvonta-asetusten avulla voit säädellä, mitä kukin lapsi voi nähdä tai tehdä selatessaan Webiä. Voit esimerkiksi ottaa ikäryhmälle sopivan haun ja kuvien suodatuksen käyttöön tai poistaa sen käytöstä, valita sisältöluokitusryhmän ja määrittää Web-selaukselle aikarajoitukset.

Ikäryhmälle sopivan haun avulla voit varmistaa, että joidenkin suosittujen hakuohjelmien turvasuodattimet otetaan käyttöön, jolloin epäasialliset hakutulokset poistetaan automaattisesti lapsen hakutuloksista. 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. Voit myös suodattaa (estää tai sallia) tiettyjä Web-sivustoja kaikilta lapsilta.

Huomautus: Sinun on kirjaututtava Windowsiin järjestelmänvalvojana, jotta voit määrittää käytönvalvonta-asetukset suojaamaan lapsiasi. Jos päivität McAfee-tuotteen vanhemman version ja käytät edelleen McAfee-käyttäjiä, sinun on myös varmistettava, että olet kirjautunut tietokoneeseen McAfee-järjestelmänvalvojana.

Tässä luvussa

Web-sivustojen suodattaminen avainsanojen avulla	148
Web-sivustojen suodattaminen	149
Web-selauksen aikarajoitusten määrittäminen.....	152
Sisältöluokitusryhmän määrittäminen.....	153
Mahdollisesti sopimattomien Web-kuvien suodattaminen	154
Ikäryhmälle sopivan haun ottaminen käyttöön	155
Käyttäjien määrittäminen	157

Web-sivustojen suodattaminen avainsanojen avulla

Avainsanasuodatuksen avulla voit estää alaikäisiä käyttäjiä vierailemasta Web-sivustoissa, 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.

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**.

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**.

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 148). 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. Muista kuitenkin tyhjentää selaimesi selaushistoria testaamisen jälkeen.

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**.

Suodatetun Web-sivuston päivittäminen

Jos Web-sivuston osoite muuttuu tai jos kirjoitat 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**.

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**.

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-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 **Web-selauksen aikarajat** -kohdasta hiiren osoittimella päivät ja ajat, jolloin tietty käyttäjä ei voi selata Web-sivuja.

4 Valitse **OK**.

Sisältöluokitusryhmän määrittäminen

Käyttäjä voi kuulua johonkin seuraavista sisältöluokitusryhmistä:

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

Käytönvalvonta-asetukset 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 sisällön 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 149).

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 Sallitut Web-sivustot -luettelossa mainittuja sivustoja** -valintaruudun.

4 Valitse **OK**.

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 153).

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**.

Ikäryhmälle sopivan haun ottaminen käyttöön

Jotkin suositut hakukoneet, kuten Yahoo! ja Google, sisältävät turvallisen hakutoiminnon. Tämä hakuasetus estää mahdollisten asiattomien hakutulosten näkymisen hakuluetteloissa.

Hakukoneet antavat sinun tavallisesti valita, kuinka paljon haluat rajoittaa turvallisen haun suodatusta, mutta antavat sinulle ja muille käyttäjille myös mahdollisuuden poistaa se käytöstä.

Käytönvalvonta-asetusten ikäryhmälle sopiva haku on kätevä tapa varmistaa, että "turvallinen haku" on aina käytössä, kun käyttäjä käyttää seuraavia hakukoneita:

- Google™
- MSN®
- Windows® Live Search
- Yahoo!®

Jos otat ikäryhmälle sopivan haun käyttöön, varmistamme, että hakukoneen turvallisen haun suodatus on kyseisellä käyttäjällä käytössä ja määritetty käyttämään rajoittavinta asetusta. Jos käyttäjä yrittää poistaa toiminnon käytöstä (hakukoneen asetuksissa tai lisäasetuksissa), otamme sen uudelleen automaattisesti käyttöön.

Oletusarvoisesti ikäryhmälle sopiva haku otetaan käyttöön kaikille käyttäjille järjestelmänvalvoja ja Aikuinen-ikäryhmän jäseniä lukuun ottamatta. Lisätietoja käyttäjän ikäryhmistä on kohdassa Sisältöluokitusryhmän määrittäminen (sivu 153).

Ota ikäryhmälle sopiva haku käyttöön

Oletuksena uudet käyttäjät lisätään Aikuinen-ryhmään ja ikäryhmälle sopiva haku on poistettu käytöstä. Jos haluat varmistaa, että joidenkin suosittujen hakukoneiden sisältämä turvallisen haun suodatusta käytetään Aikuinen-ryhmään kuuluvan käyttäjän tapauksessa, voit ottaa ikäryhmälle sopivan haun käyttöön.

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 **Ikäryhmälle sopiva haku** -kohdasta **Käytössä**.
 - 4 Valitse **OK**.

LUKU 32

Käyttäjien määrittäminen

Voit määrittää käytönvalvonta-asetukset suojaamaan lapsiasi antamalla heille SecurityCenterissä tietyt käyttöoikeudet. Nämä käyttöoikeudet määräävät, mitä kukin lapsi voi nähdä tai tehdä Webissä.

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 tietokoneeseen Windowsin järjestelmänvalvojana, jotta voit määrittää käyttäjiä. Jos päivität McAfee-tuotteen vanhemman version ja käytät edelleen McAfee-käyttäjiä, sinun on myös varmistettava, että olet kirjautunut tietokoneeseen McAfee-järjestelmänvalvojana.

Tässä luvussa

McAfee-käyttäjien asetusten määrittäminen.....	158
Windows-käyttäjien asetusten määrittäminen.....	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, mutta McAfee suosittelee vaihtamista Windows-käyttäjiin. 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.

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**.

Vaihda McAfee-järjestelmänvalvojan salasana

Jos sinun on vaikeata muistaa McAfee-järjestelmänvalvojan salasanaa tai epäilet sen joutuneen väriin 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**.

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**.

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**.

Lisää McAfee-käyttäjä

Kun McAfee-käyttäjä on luotu, voit määrittää käyttäjälle käytönvalvonta-asetukset. Lisätietoja on käytönvalvonta-asetusten 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**.

Windows-käyttäjiin vaihtaminen

McAfee suosittelee vaihtamista Windows-käyttäjiin, sillä tämä helpottaa ylläpitoa. Tämän jälkeen et kuitenkaan enää voi 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.

Windows-käyttäjien asetusten määrittäminen

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 käyttäjien käytönvalvonta-asetukset SecurityCenterissä.

Jos olet päivittänyt SecurityCenterin aiemmasta versiosta, joka käytti McAfee-käyttäjiä, saat lisätietoja kohdasta McAfee-käyttäjien asetusten määrittäminen (sivu 158).

LUKU 33

Tietojen suojaaminen Internetissä

Voit estää henkilökohtaisten tietojen (kuten nimien, osoitteiden, luottokorttien ja pankkitilien numeroiden) lähettämisen Internetiin lisäämällä ne suojatulle tieto-alueelle.

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

Tässä luvussa

Henkilökohtaisten tietojen suojaaminen 162

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**.

LUKU 34

Salasanojen suojaaminen

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

Tässä luvussa

Salanasäilön asentaminen..... 164

Salanasäilön asentaminen

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

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

Nollaa salanasäilön salasana

Jos unohdat Salanasäilön salanan, 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-määrittelyt -ikkunan **Salanasäilö** -kohdasta **Lisäasetukset**.

2 Valitse **Unohditko salanasasi?**

3 Kirjoita uusi salasana Palauta salanasäilö -valintaikkunan **Salasana**-ruutuun ja kirjoita se sitten uudelleen **Anna salasana uudelleen** -ruutuun.

4 Valitse **Palauta**.

5 Valitse Salanan nollauksen vahvistus -valintaikkunasta **Kyllä**.

Vaihda Salanasäilön salasana

Voit vaihtaa Salanasäilön salanan 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-määrytykset -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**.

Poista salasana

Voit poistaa salasanvoja Salanasäilöstä milloin tahansa. Säilöstä poistettuja salasanvoja 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-määrytykset -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**.

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-määrittelyt -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**.

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 salasana **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**.

LUKU 35

McAfee Backup and Restore

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

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

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

Backup and Restoren ominaisuudet.....	168
Tiedostojen arkistointi.....	169
Arkistoitujen tiedostojen käsitteleminen	179

Backup and Restoren ominaisuudet

Ajoitettu paikallinen arkistointi

Suojaa tietojasi arkistoimalla tiedostoja ja kansioita CD- tai DVD-levyille, USB-asetalle, ulkoiselle kiintolevyille tai verkkoasemalle. Kun olet muodostanut ensimmäisen arkiston, lisäärkistointi 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 salaus

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

LUKU 36

Tiedostojen arkistointi

McAfee Backup and Restoren 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 Backup and Restoren suorittavan täydellisen arkistoinnin ja pika-arkistoinnin. Voit suorittaa manuaalisen arkistoinnin milloin tahansa.

Tässä luvussa

Paikallisen arkiston ottaminen käyttöön ja poistaminen käytöstä	170
Arkiston asetusten määrittäminen.....	171
Täydellisen arkistoinnin ja pika-arkistoinnin suorittaminen	175

Paikallisen arkiston ottaminen käyttöön ja poistaminen käytöstä

Kun käynnistät Backup and Restoren ensimmäisen kerran, voit määrittää Backup and Restoren käyttötavan mukaan, haluatko ottaa paikallisen arkiston käyttöön tai poistaa sen käytöstä. Kun olet kirjautunut sisään ja aloittanut Backup and Restoren käytön, voit ottaa paikallisen arkistoinnin käyttöön tai poistaa sen käytöstä milloin tahansa.

Jos et halua arkistoida tietokoneella olevista tiedostoista kopion CD- tai DVD-levylle, USB-asemalle, ulkoiselle kiintolevylle tai verkkoasemalle, voit poistaa paikallisen arkiston käytöstä.

Ota paikallinen arkisto käyttöön

Ota paikallinen arkisto käyttöön, jos haluat arkistoida tietokoneella olevista tiedostoista kopion CD- tai DVD-levylle, USB-asemalle, ulkoiselle kiintolevylle tai verkkoasemalle.

- 1 Valitse SecurityCenterin **Lisävalikko**-kohdasta **Määritä**.
- 2 Valitse Määritä-ruudusta **Tietokone ja tiedostot**.
- 3 Valitse Tietokone ja tiedostot -asetusikkunan **Paikallinen arkisto on poistettu käytöstä** -kohdasta **Käytössä**.

Poista paikallinen arkisto käytöstä

Poista paikallinen arkisto käytöstä, jos et halua arkistoida tietokoneella olevista tiedostoista kopiota CD- tai DVD-levylle, USB-asemalle, ulkoiselle kiintolevylle tai verkkoasemalle.

- 1 Valitse SecurityCenterin **Lisävalikko**-kohdasta **Määritä**.
- 2 Valitse Määritä-ruudusta **Tietokone ja tiedostot**.
- 3 Valitse Tietokone ja tiedostot -asetusikkunan **Paikallinen arkisto on poistettu käytöstä** -kohdasta **Ei käytössä**.

Arkiston asetusten määrittäminen

Ennen kuin aloitat tiedostojen arkistoinnin, sinun on määritettävä tietyt paikallisen arkiston asetukset. Sinun on esimerkiksi määritettävä tarkkailukohteet ja tarkkailtavat tiedostotyypit. Tarkkailukohteet ovat tietokoneessa olevia kansioita, joita Backup and Restore valvoo uusien tiedostojen ja tiedostojen muutosten varalta. Tarkkailtavat tiedostotyypit ovat tiedostotyyppiä (esimerkiksi .doc ja .xls), jotka Backup and Restore arkistoi tarkkailukohteissa. Oletusarvoisesti arkistoidaan seuraavat tiedostotyypit, mutta voit arkistoida myös muita tiedostotyyppiä.

- Microsoft® Word -asiakirjat (.doc, .docx)
- Microsoft Excel® -laskentataulukot (.xls, .xlsx)
- Microsoft PowerPoint® -esitykset (.ppt, .pptx)
- Microsoft Project® -tiedostot (.mpp)
- Adobe® PDF -tiedostot (.pdf)
- Tavalliset tekstitiedostot (.txt)
- HTML-tiedostot (.html)
- Joint Photographic Experts Group -tiedostot (.jpg, .jpeg)
- Tagged Image Format -tiedostot (.tif)
- MPEG Audio Stream III -tiedostot (.mp3)
- Videotiedostot (.vdo)

Huomautus: Seuraavia tiedostotyyppiä ei voi arkistoida: .ost ja .pst.

Voit määrittää kahdentyyppisiä tarkkailukohteita: ylemmän tason kansioita ja alikansioita sekä ainoastaan ylemmän tason kansioita. Jos määrität tarkkailukohteeksi ylemmän tason kansion ja sen alikansiot, Backup and Restore arkistoi kaikki kyseisen kansion ja sen alikansioiden tarkkailtavien tiedostotyyppien mukaiset tiedostot. Jos määrität tarkkailukohteeksi ylemmän tason kansion, Backup and Restore arkistoi ainoastaan kyseisen kansion tarkkailtavien tiedostotyyppien mukaiset tiedostot (ei alikansioita). Voit määrittää myös tarkkailukohteet, joita et halua lisätä paikalliseen arkistoon. Oletusarvoisesti Windowsin työpöytä ja Omat tiedostot määritetään ylemmän tason kansioiden ja alikansioiden tarkkailukohteiksi.

Kun olet määrittänyt tarkkailtavat tiedostotyypit 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: ylemmän tason kansioita ja alikansioita sekä ainoastaan ylemmän tason kansioita. Jos määrität tarkkailukohteeksi ylemmän tason kansion ja sen alikansiot, Backup and Restore valvoo kyseisen kansion ja sen alikansioiden sisältöä muutosten varalta. Jos määrität tarkkailukohteeksi ylemmän tason kansion, Backup and Restore valvoo ainoastaan kyseisen kansion sisältöä (ei alikansioita).

1 Valitse Paikallisarkistoinnin asetukset -valintaikkuna.

Miten?

1. Valitse **Paikallinen arkisto** -välilehti.
2. Valitse vasemmasta ruudusta **Asetukset**.

2 Valitse **Tarkkailtavat sijainnit**.

3 Valitse jokin seuraavista:

- Jos haluat arkistoida kansion ja sen alikansioiden sisällön, valitse **Arkistoi ylemmän tason kansiot ja alikansiot** -kohdasta **Lisää kansio**.
- Jos haluat arkistoida kansion sisällön, mutta et sen alikansioiden sisältöä, valitse **Arkistoi ylemmän tason kansiot** -kohdasta **Lisää kansio**.
- Jos haluat arkistoida koko tiedoston, valitse **Arkistoi ylemmän tason kansiot** -kohdasta **Lisää tiedosto**.

4 Siirry Etsi kansio -valintaikkunassa (tai Avaa-valintaikkunassa) tarkkailtavan kansion (tai tiedoston) kohdalle ja napsauta **OK**.

5 Valitse **OK**.

Vihje: Jos haluat Backup and Restoren 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 ylemmän tason kansioiden ja alikansioiden tai ylemmän tason kansioiden sijaintien tiedostotyyppit arkistoidaan. Voit valita olemassa olevasta tiedostotyyppien luettelosta tai lisätä luetteloon uuden tyyppin.

- 1 Valitse Paikallisarkistoinnin asetukset -valintaikkuna.

Miten?

1. Valitse **Paikallinen arkisto** -välilehti.
 2. Valitse vasemmasta ruudusta **Asetukset**.
- 2 Valitse **Tiedostotyyppit**.
 - 3 Laajenna tiedostotyyppien luettelot ja valitse arkistoitavien tiedostotyyppien vieressä olevat valintaruudut.
 - 4 Valitse **OK**.

Vihje: Jos haluat lisätä uuden tiedostotyyppin **Valitut tiedostotyyppit** -luetteloon, kirjoita tiedostotunniste **Lisää mukautettu tiedostotyyppi kohtaan Muut** -ruutuun, valitse **Lisää** ja sitten **OK**. Uusi tiedostotyyppi muuttuu automaattisesti tarkkailtavaksi tiedostotyyppiksi.

Sulje kohde arkistosta pois

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

- 1 Valitse Paikallisarkistoinnin asetukset -valintaikkuna.

Miten?

1. Valitse **Paikallinen arkisto** -välilehti.
 2. Valitse vasemmasta ruudusta **Asetukset**.
- 2 Valitse **Tarkkailtavat sijainnit**.
 - 3 Valitse **Varmuuskopioinnissa ohitetut kansiot** -kohdasta **Lisää kansio**.
 - 4 Siirry Etsi kansio -valintaikkunassa poissuljettavan kohteen kohdalle, valitse se ja napsauta **OK**.
 - 5 Valitse **OK**.

Vihje: Jos haluat Backup and Restoren 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*.

- 1 Valitse Paikallisarkistoinnin asetukset -valintaikkuna.

Miten?

1. Valitse **Paikallinen arkisto** -välilehti.
 2. Valitse vasemmasta ruudusta **Asetukset**.
- 2 Valitse **Muuta arkiston sijaintia**.
 - 3 Valitse Arkiston sijainti -valintaikkunassa yksi seuraavista vaihtoehdoista:
 - Valitse **Valitse tallentava CD/DVD-asema**, valitse tietokoneen CD- tai DVD-asema tietokoneen **Tallentava asema** -luettelosta ja valitse **OK**.
 - 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**.
 - 4 Vahvista uusi arkistointisijainti **Valittu arkistointisijainti** -kohdasta ja valitse **OK**.
 - 5 Valitse vahvistusvalintaikkunasta **OK**.
 - 6 Valitse **OK**.

Huomautus: Kun muutat arkiston sijaintia, aikaisemmin arkistoidut tiedostot merkitään **Tila**-sarakkeessa **Ei koskaan arkistoitu** column.

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.

- 1 Valitse Paikallisarkistoinnin asetukset -valintaikkuna.

Miten?

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

Huomautus: McAfee suosittelee, että et poista salausta ja pakkausta käytöstä tiedostoja arkistoitaessa.

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 Backup and Restore 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 Backup and Restorea 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.

- 1 Valitse Paikallisarkistoinnin asetukset -valintaikkuna.
Miten?
 1. Valitse **Paikallinen arkisto** -välilehti.
 2. Valitse vasemmasta ruudusta **Asetukset**.
- 2 Valitse **Yleinen**.
- 3 Jos haluat suorittaa täydellisen arkistoinnin päivittäin, viikoittain tai kuukausittain, valitse **Täydellinen arkistointi joka** -kohdasta yksi seuraavista:
 - **Päivä**
 - **Viikko**
 - **Kuukausi**
- 4 Valitse sen päivän vieressä oleva valintaruutu, jolloin haluat suorittaa täydellisen arkistoinnin.
- 5 Valitse arvo **Klo**-luettelosta ja määritä ajankohta, jolloin haluat suorittaa täydellisen arkistoinnin.
- 6 Jos haluat suorittaa pika-arkistoinnin päivittäin tai tunneittain, valitse **Pika-arkistointi**-kohdasta yksi seuraavista:
 - **Tunti**
 - **Päivä**
- 7 Kirjoita toistumistiheyttä ilmaiseva arvo **Pika-arkistointi joka** -ruutuun.
- 8 Valitse **OK**.

Huomautus: Voit poistaa ajoitetun arkistoinnin käytöstä valitsemalla **Täydellinen arkistointi joka** -kohdasta **Manuaalinen**.

Keskeytä automaattinen arkistointi

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

- 1 Valitse vasemmasta ruudusta **Keskeytä arkistointi**.
- 2 Valitse vahvistusvalintaikkunasta **Kyllä**.

Huomautus: **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 tiedostotyypit.

- 1 Valitse **Paikallinen arkisto** -välilehti.
- 2 Valitse jokin seuraavista:
 - Jos haluat suorittaa pika-arkistoinnin, valitse vasemmasta ruudusta **Pika-arkistointi**.
 - Jos haluat suorittaa täydellisen arkistoinnin, valitse vasemmasta ruudusta **Täydellinen arkistointi**.
- 3 Vahvista levytilasi ja asetukset Aloita arkistointi -valintaikkunasta ja valitse sitten **Jatka**.

LUKU 37

Arkistoitujen tiedostojen käsitteleminen

Kun olet arkistoinut tiedostot, voit käsitellä niitä Backup and Restorella. 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, katoaa tai vioittuu. Backup and Restore tarjoaa myös tietoja, jotka ovat välttämättömiä paikallisten arkistojen ja tallennusvälineiden hallintaan.

Tässä luvussa

Paikallisen arkiston hallintaohjelman käyttäminen.....	180
Arkistoitujen tiedostojen palauttaminen	181
Arkistojen hallinta	183

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. Backup and Restore 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.

- 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 **Alle 100 kt**, **Alle 1 Mt** tai **Yli 1 Mt**.
 - Valitse **Koko kilotavuina** ja määritä sopivat arvot ruutuihin.

- 4 Määritä tiedoston viimeisimmän arkistoinnin 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**.

Huomautus: 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 tärkeätä 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 CD- tai DVD-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 Backup and Restore tietokoneelle B ja liitettävä ulkoinen kiintolevyasema siihen. Sen jälkeen voit etsiä tiedostot Backup and Restoresta 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

Backup and Restoren paikallisen arkiston avulla voit noutaa paikallisen tietokoneesi tarkkailtavasta kansioista puuttuvat tiedot. Jos esimerkiksi tiedosto siirretään tarkkailtavasta kansioista tai se poistetaan, mutta se on jo arkistoitu, voit palauttaa sen 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.

- 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, suoritettiinko täydellinen arkistointi tai pika-arkistointi.

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

Valitussa sijainnissa olevat tiedostot tulevat näkyviin **Puuttuvat tiedostot** -luetteloon, ja ne voidaan palauttaa. Lisätietoja on kohdassa Palauta puuttuvia tiedostoja paikallisesta arkistosta (sivu 182).

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 siirrettiin tarkkailtavasta kansioista tai se poistettiin 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.

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

 LUKU 38

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 eheytyksen 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.....	186
Tietokoneen puhdistaminen	187
Tietokoneen eheyttäminen.....	191
Tehtävän ajoittaminen	193

QuickCleanin toiminnot

Tiedostojen puhdistusohjelma

Poista tarpeettomat tiedostot nopeasti ja turvallisesti erilaisten tyhjennysohjelmien avulla. Poistamalla nämä tiedostot voit lisätä tietokoneesi kiintolevyllä olevaa tilaa ja parantaa sen suorituskykyä.

LUKU 39

Tietokoneen puhdistaminen

QuickClean poistaa tiedostot, jotka voivat viedä tietokoneessa vain turhaan tilaa. 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 rikkiäiset 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 selatessa. 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.

Nimi	Toiminto
Evästeiden tyhjennysohjelma	<p>Poistaa evästeet. Nämä tiedostot tallennetaan tavallisesti väliaikaisina tiedostoina.</p> <p>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 hakkerit voivat myös käyttää niitä hyväkseen.</p>
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	<p>Poistaa viimeksi käytetyt tiedostot, jotka on luotu seuraavilla ohjelmilla:</p> <ul style="list-style-type: none"> ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
ActiveX-objektien tyhjennysohjelma	<p>Poistaa ActiveX-ohjausobjektit.</p> <p>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.</p>

Nimi	Toiminto
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.

Tässä luvussa

Puhdista tietokone 189

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.

LUKU 40

Tietokoneen eheyttäminen

Levyn eheytyks järjestää tietokoneessa olevat tiedostot ja kansiot siten, että ne eivät hajoa osiin (pirstoudu), kun ne tallennetaan tietokoneen kiintolevylle. Eheyttämällä kiintolevysi 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.

LUKU 41

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 oletusohjelmat 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 eheytetään 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

s -tehtävää

Voit muokata ajoitettua Levyn eheytys -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**.

LUKU 42

McAfee Shredder

McAfee Shredder poistaa pysyvästi (tuhoaa) 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 tietosuojaa 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	200
Tiedostojen, kansioden ja levyjen tuhoaminen.....	200

Shredderin toiminnot

Poista tiedostoja ja kansioita pysyvästi

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

Tiedostojen, kansioiden ja levyjen tuhoaminen

Shredder varmistaa, että Roskakorissa ja Väliaikaiset Internet-tiedostot -kansiossa olevia poistettuja tiedostoja ja kansioita ei voi palauttaa erikoistyökaluillakaan. 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.

LUKU 43

McAfee Network Manager

McAfee Network Manager esittää graafisen näkymän kotiverkon tietokoneista ja muista laitteista. Network Managerin avulla voit hallita etäältä kunkin verkkosi hallitun tietokoneen suojauksen tilaa ja korjata raportoituja tietoturvan puutteita. Jos olet asentanut McAfee Total Protectionin, Network Managerin avulla voit suojata verkkoasi myös tunkeutujilta (tietokoneilta tai laitteilta, joita et tunnista tai joihin et luota), jotka yrittävät muodostaa yhteyden verkkoosi.

Voit tutustua Network 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	204
Network Managerin kuvakkeiden toiminta	205
Hallitun verkon määrittäminen.....	207
Verkon etähallinta.....	213
Verkkojen valvonta	219

Network Managerin ominaisuudet

- Graafinen verkkokartta** Tarkastele graafista näkymää kotiverkkosi tietokoneiden ja muiden laitteiden 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 laitteisiin liittyviä tietoja.
- Etähallinta** Hallitse kotiverkkosi tietokoneiden suojaustilaa. Voit kutsua tietokoneen hallittuun verkkoon, valvoa hallitun tietokoneen suojaustilaa ja korjata tunnettuja tietoturvan puutteita verkkosi etätietokoneelta.
- Verkon valvonta** Jos Network Manager on käytettävissä, anna sen valvoa verkkojasi ja pyydä sitä ilmoittamaan sinulle, kun ystävät tai tunkeutajat muodostavat niihin yhteyden. Verkon valvonta on käytettävissä vain silloin, jos olet hankkinut McAfee Total Protectionin.

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

LUKU 44

Hallitun verkon määrittäminen

Voit määrittää hallitun verkon luottamalla verkkoon (jos et ole vielä tehnyt niin) ja lisäämällä siihen jäseniä (tietokoneita). 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 kohteisiin liittyviä tietoja, vaikka teet muutoksia verkkoon (esimerkiksi lisäät siihen tietokoneen).

Tässä luvussa

Verkkokartan käyttäminen.....	208
Hallittuun verkkoon liittyminen.....	210

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 nimi, joka on liitetty verkkoon ja johon on asennettu SecurityCenter. Voit kuitenkin nimetä verkon milloin tahansa uudelleen.

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 kohteita. Voit myös tarkastella verkkokartassa näkyviin kohteisiin liittyviä tietoja.

Käytä verkkokarttaa

Verkkokartta on graafinen esitys kotiverkon tietokoneista ja laitteista.

- Valitse Perus- tai Lisävalikon kohta **Verkonhallinta**.

Huomautus: Jos et ole vielä luottanut verkkoon (McAfee Personal Firewallin avulla), sinua kehoitetaan tekemään niin, kun käytät verkkokarttaa ensimmäisen kerran.

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 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 **Nimeä verkko 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 laitteet 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 kohteesta valitsemalla sen verkkokartalta. Näitä tietoja ovat muun muassa kohteen nimi, sen suojauksen tila ja muut kohteen 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 suojaustilansa, siitä tulee verkon hallittu jäsen. Jos tietokone ei suostu paljastamaan suojaustilansa, 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 myös määrittää, haluatko muiden tässä verkossa olevien tietokoneiden hallitsevan tämän tietokoneen suojausasetuksia.

- 1 Varmista, että Hallittu verkko -valintaikkunan **Salli jokaisen tässä verkossa olevan tietokoneen hallita 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 **Hallitse 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 45

Verkon etähallinta

Kun olet asentanut hallitun verkon, voit etähallita verkon tietokoneita ja laitteita. Voit hallita tietokoneiden ja laitteiden tilaa ja oikeustasoja sekä korjata useimmat tietoturvan puutteet etäältä.

Tässä luvussa

Tilojen ja oikeuksien hallinta	214
Tietoturvan puutteiden korjaaminen	216

Tilojen ja oikeuksien hallinta

Hallitussa verkossa on hallittuja ja hallinnan piiriin kuulumattomia jäseniä. Hallitut jäsenet sallivat muiden verkon tietokoneiden hallita 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). Hallitun verkon tietokone, jolla on järjestelmänvalvojan oikeudet, voi milloin tahansa kutsua hallinnan piiriin kuulumattoman tietokoneen hallituksi tietokoneeksi. Samoin hallitusta tietokoneesta, jolla on järjestelmänvalvojan oikeudet, 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.

Hallitse tietokoneen suojauksen tilaa

Jos tietokoneen suojauksen tilaa ei hallita verkossa (tietokone ei ole verkon jäsen tai se on hallinnan piiriin kuulumaton verkon jäsen), sen hallintaa voi pyytää.

- 1 Napsauta verkkokartalla näkyvää hallinnan piiriin kuulumattoman tietokoneen kuvaketta.
- 2 Valitse **Haluan**-kohdasta **Hallitse tätä tietokonetta**.

Lopeta tietokoneen suojauksen tilan hallinta

Voit lopettaa verkossa olevan hallitun tietokoneen hallinnan, mutta tällöin tietokoneesta tulee hallinnan piiriin kuulumaton, jolloin et voi hallita sen suojauksen tilaa etäyhteyden kautta.

- 1 Napsauta verkkokartalla näkyvää hallitun tietokoneen kuvaketta.
- 2 Valitse **Haluan**-kohdasta **Lopeta tämän tietokoneen hallinta**.
- 3 Valitse vahvistusvalintaikkunasta **Kyllä**.

Muokkaa hallitun tietokoneen oikeuksia

Voit muuttaa hallitun tietokoneen oikeuksia milloin tahansa. Oikeuksien avulla voit määrittää, mitkä tietokoneet hallitsevat 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 hallita toistensa suojauksen tilaa valitsemalla tai poistamalla valinta käyttöoikeuksien muuttamisen valintaikkunan valintaruudusta.
- 4 Valitse **OK**.

Hallitse laitetta

Voit hallita laitetta käyttämällä sen hallinnan Web-sivua verkkokartalta 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 McAfee 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 hallita verkossa olevien toisten hallittujen tietokoneiden McAfee-suojastasoja ja korjata raportoituja tietoturvan puutteita. Jos esimerkiksi hallitun tietokoneen McAfee-suojastaso 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. Tietyt 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 uutta versiota, niiden suojauksen tilaa ei voida hallita etäyhteyden kautta. Jos haluat hallita kyseisiä tietokoneita etäyhteydettä käyttäen, niihin täytyy asentaa SecurityCenterin uusi versio.

- 1** Varmista, että noudatat näitä ohjeita tietokoneessa, jota haluat hallita etäältä.
- 2** Pidä McAfee-kirjautumistietosi käsillä. Tällä tarkoitetaan sähköpostiosoitetta ja salasanaa, joita käytit, kun aktivoit McAfee-ohjelmiston ensimmäisen kerran.
- 3** Siirry selaimella McAfeen Web-sivustoon, kirjaudu sisään ja napsauta **Oma tili** -painiketta.
- 4** Etsi asennettava tuote, napsauta sen **Lataa**-kuvaketta ja noudata sitten näytön ohjeita.

Vihje: Voit perehtyä myös McAfee-tietoturvaohjelmistojen asennukseen etätietokoneisiin avaamalla verkkokarttasi ja valitsemalla **Haluan**-kohdasta **Suojaa tietokoneeni**.

LUKU 46

Verkkojen valvonta

Jos olet asentanut McAfee Total Protectionin, Network Manager valvoo verkkojasi myös tunkeutujien varalta. Jos tuntematon tietokone tai laite muodostaa yhteyden verkkoosi, saat siitä ilmoituksen, jotta voit päättää, haluatko merkitä tietokoneen tai laitteen ystäväksi tai tunkeutujaksi. Ystävä on tietokone tai laite, jonka tunnistat ja johon luotat, kun taas tunkeutuja on tietokone tai laite, jota et tunnista ja johon et luota. Jos merkitset tietokoneen tai laitteen ystäväksi, voit päättää, haluatko saada aina ilmoituksen, kun ystävä muodostaa yhteyden verkkoon. Jos merkitset tietokoneen tai laitteen tunkeutujaksi, ilmoitamme sinulle aina automaattisesti, kun se muodostaa yhteyden verkkoon.

Kun muodostat yhteyden verkkoon ensimmäisen kerran Total Protectionin tämän version asentamisen tai päivittämisen jälkeen, merkitsemme jokaisen tietokoneen tai laitteen automaattisesti ystäväksi emmekä ilmoita, kun ne muodostavat myöhemmin yhteyden verkkoon. Kolmen päivän kuluttua alamme ilmoittaa sinulle jokaisesta verkkoon yhteyden muodostavasta tuntemattomasta tietokoneesta tai laitteesta, jotta voit merkitä ne itse.

Huomautus: Verkon valvonta on Network Managerin toiminto, joka on käytettävissä vain McAfee Total Protectionin kanssa. Lisätietoja Total Protectionista on Web-sivustossamme.

Tässä luvussa

Lopeta verkkojen valvonta	219
Ota uudelleen käyttöön verkon valvontaan liittyvät ilmoitukset	220
Merkitse tunkeutujaksi	221
Merkitse ystäväksi	221
Lopeta uusien ystävien etsintä	221

Lopeta verkkojen valvonta

Jos poistat verkon valvonnan käytöstä, emme enää pysty ilmoittamaan sinulle, kun tunkeutujat muodostavat yhteyden kotiverkkoosi tai muihin verkkoihin, joihin muodostat yhteyden.

1 Avaa Internet ja verkko -asetusikkuna.

Miten?

1. Valitse **Yleiset tehtävät** -kohdasta **Koti**.
 2. Valitse SecurityCenterin Koti-ikkunasta **Internet ja verkko**.
 3. Valitse Internet ja verkko -osasta **Määritä**.
- 2 Valitse **Verkon valvonta** -kohdasta **Ei käytössä**.

Ota uudelleen käyttöön verkon valvontaan liittyvät ilmoitukset

Vaikka voit poistaa verkon valvontaan liittyvät ilmoitukset käytöstä, se ei ole suositeltavaa. Jos teet niin, emme välttämättä pysty kertomaan sinulle, kun tuntemattomat tietokoneet tai tunkeutujat muodostavat yhteyden verkkoon. Jos poistat nämä ilmoitukset vahingossa käytöstä (esimerkiksi valitsemalla ilmoituksen **Älä näytä tätä hälytystä uudelleen** -valintaruudun), voit ottaa ne milloin tahansa uudelleen käyttöön.

- 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 Varmista Tiedottavat hälytykset -ikkunassa, että seuraavien valintaruutujen valinnat on poistettu:
 - **Älä näytä hälytyksiä, kun uudet tietokoneet tai laitteet muodostavat yhteyden verkkoon**
 - **Älä näytä hälytyksiä, kun tunkeutujat muodostavat yhteyden verkkoon**
 - **Älä näytä hälytyksiä ystävistä, joista haluan yleensä saada ilmoituksen**
 - **Älä muistuta minua, kun tuntemattomia tietokoneita tai laitteita havaitaan**
 - **Älä ilmoita minulle, kun McAfee on lopettanut uusien ystävien etsinnän**
- 4 Valitse **OK**.

Merkitse tunkeutujaksi

Merkitse verkossa oleva tietokone tai laite tunkeutujaksi, jos et tunnista sitä etkä luota siihen. Ilmoitamme sinulle automaattisesti aina, kun se muodostaa yhteyden verkkoon.

- 1 Valitse Perus- tai Lisävalikon kohta **Verkonhallinta**.
- 2 Napsauta kohdetta verkkokartalla.
- 3 Valitse **Haluan**-kohdasta **Merkitse ystäväksi tai tunkeutujaksi**.
- 4 Valitse valintaikkunasta **Tunkeutuja**.

Merkitse ystäväksi

Merkitse verkossa oleva tietokone tai laite ystäväksi vain silloin, jos tunnistat sen ja luostat siihen. Kun merkitset tietokoneen tai laitteen ystäväksi, voit myös päättää, haluatko saada aina ilmoituksen, kun se muodostaa yhteyden verkkoon.

- 1 Valitse Perus- tai Lisävalikon kohta **Verkonhallinta**.
- 2 Napsauta kohdetta verkkokartalla.
- 3 Valitse **Haluan**-kohdasta **Merkitse ystäväksi tai tunkeutujaksi**.
- 4 Valitse valintaikkunasta **Ystävä**.
- 5 Jos haluat saada ilmoituksen aina, kun tämä ystävä muodostaa yhteyden verkkoon, valitse **Ilmoita, kun tämä tietokone tai laite muodostaa yhteyden verkkoon**-valintaruutu.

Lopeta uusien ystävien etsintä

Kun muodostat yhteyden verkkoon ensimmäisen kolmen päivän ajan, jonka Total Protection on ollut asennettuna, merkitsemme jokaisen tietokoneen tai laitteen automaattisesti ystäväksi, josta et halua saada erillistä ilmoitusta. Voit poistaa tämän automaattisen merkintätoiminnon käytöstä ensimmäisen kolmen päivän aikana milloin tahansa, mutta et voi ottaa sitä uudelleen käyttöön.

- 1 Valitse Perus- tai Lisävalikon kohta **Verkonhallinta**.
- 2 Valitse **Haluan**-kohdasta **Lopeta uusien ystävien etsintä**.

LUKU 47

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	224
EasyNetworkin asentaminen	225
Tiedostojen jakaminen ja lähettäminen.....	229
Tulostinten jakaminen	235

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.

LUKU 48

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.....	225
Hallittuun verkkoon liittyminen.....	226
Hallitusta verkosta poistuminen	228

Avaa EasyNetwork

Voit avata EasyNetworkin Windowsin Käynnistä-valikosta tai napsauttamalla ohjelmiston työpöydällä olevaa kuvaketta.

- Valitse **Käynnistä**-valikosta **Ohjelmat, McAfee** ja valitse **McAfee EasyNetwork**.

Vihje: Voit avata EasyNetworkin myös kaksoisnapsauttamalla työpöydällä 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 liittymispyyntön. 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). Järjestelmänvalvojoikeuksien 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 liityt 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 226).

Poistu hallitusta verkosta

Voit poistua hallitusta verkosta, johon olet aiemmin liittynyt.

1 Irrota tietokone verkosta.

2 Valitse EasyNetworkin **Työkalut**-valikosta **Poistu verkosta**.

3 Valitse Poistu verkosta -valintaikkunasta sen verkon nimi, josta haluat poistua.

4 Valitse **Poistu verkosta**.

LUKU 49

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.....	230
Tiedostojen lähettäminen toisiin tietokoneisiin.....	232

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 231).
- 3 Kirjoita tiedoston tai tiedostopolun nimi osittain tai kokonaan **Tiedoston tai tiedostopolun nimi** -luetteloon.
- 4 Valitse **Tyyppi**-luettelosta haluamasi tiedostotyyppi (sivu 231).
- 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 233).

- 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 50

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 käyttäminen236

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 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 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 kaistassa. Vaikka tiedonsiirron nopeus on pienempi kuin 802.11a-standardissa, laajennuksen kantoalue on paljon suurempi.

802.1x

Tavallisten ja langattomien verkkojen todennusstandardi. 802.1x-standardia käytetään yleensä langattoman 802.11-verkon kanssa. Katso myös todennus (sivu 247).

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. Vertaa varmuuskopiointiin (sivu 248).

asiakas

Ohjelma, 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 (sivu 248), WPA (sivu 249), WPA2 (sivu 250), WPA2-PSK (sivu 250) ja WPA-PSK (sivu 250).

D

DAT

Tunnistumääritystiedostot, joita kutsutaan myös allekirjoitustiedostoiksi, sisältävät virusten, Troijan hevosten, vakoiluohjelmien, mainosohjelmien ja muiden mahdollisten haittaohjelmien (PUP) tunnistamiseen, havaitsemiseen ja korjaamiseen tarvittavat määritykset.

DNS

Domain Name System. Tietokantajärjestelmä, joka muuntaa IP-osoitteen, esimerkiksi 11.2.3.44, toimialueen nimeksi, kuten www.mcafee.com.

E

ESS

Extended Service Set. Vähintään kaksi verkkoa, jotka muodostavat yhtenäisen aliverkon.

estettyjen osoitteiden luettelo

Anti-Spamissa luettelo sellaisista sähköpostiosoitteista, joista et halua saada viestejä, sillä uskot niiden olevan roskapostia. Phishing-huijaussuojauksessa haitallisina pidettyjen Web-sivustojen luettelo. Vertaa sallittujen osoitteiden luetteloon (sivu 245).

eväste

Monissa Web-sivustoissa käytettävä pieni tekstitiedosto, johon tallennetaan tietoja vierailuista sivuista. Eväste tallennetaan Internetiä käyttävän henkilön tietokoneeseen, ja se voi sisältää kirjautumis- tai rekisteröintitietoja, ostoskärryyn liittyviä tietoja tai käyttäjän asetuksia. Web-sivustot käyttävät evästeitä lähinnä aikaisemmin sivustoon rekisteröityneiden tai siellä käyneiden henkilöiden tunnistamiseen, mutta hakkerit voivat myös käyttää niitä hyväkseen.

I

intranet

Yleensä organisaation sisäinen yksityinen tietokoneverkko, joka on vain hyväksytyjen 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

Internet Protocol -osoite. Osoite, jota käytetään TCP/IP-verkkoon liitetyn tietokoneen tai laitteen tunnistamiseen. IP-osoitteet ovat 32-bittisessä numeerisessa osoitemuodossa, jossa neljän numeron sarjat erotellaan pisteillä. Jokainen numero voi olla 0–255 (esimerkiksi 192.168.1.100).

J

jaettu salaisuus

Merkkijono tai avain (yleensä salasana), joka on sovittu kahden keskustelevalle osapuolen välillä ennen kommunikoinnin aloittamista. Sitä käytetään RADIUS-viestien arkaluonteisten osien suojaamiseen. Katso myös RADIUS (sivu 244).

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 sähköpostiviestin Backup and Restorelta, jossa heille kerrotaan jaettavista tiedostoista. Sähköpostiviesti sisältää linkin, josta jaettavat tiedostot voidaan ladata.

julkaiseminen

Varmuuskopioidun tiedoston julkaiseminen Internetissä. Voit etsiä julkaistuja tiedostoja Backup and Restore -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 (läpisyöttö), joka voidaan siirtää tietyssä ajassa.

karanteeni

Viruksen, roskapostiviestin, epäilyttävän sisällön tai mahdollisen haittaohjelman sisältävän tiedoston tai kansion eristäminen, jotta tiedostoja tai kansioita ei voi avata tai suorittaa.

komentosarja

Komentoluettelo, joka voidaan suorittaa automaattisesti (ilman käyttäjän toimintaa). Toisin kuin ohjelmat, komentosarjat tallennetaan yleensä tekstimuotoisena ja käännetään suoritukseen 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 (sivu 241).

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.

L

laajennus

Pieni ohjelmisto, joka lisää uusia toimintoja suurempaan ohjelmistoon tai parantaa sen toimintaa. Esimerkiksi laajennukset antavat Web-selaimen käyttää ja suorittaa HTML-asiakirjoihin upotettuja tiedostoja, jotka ovat selaimen tunnistamattomassa muodossa (esimerkiksi animaatio-, video- ja äänitiedostot).

langaton PCI-verkkosovitinkortti

Peripheral Component Interconnect. Langaton sovitinkortti, joka liitetään tietokoneen sisällä olevaan PCI-laajennuspaikkaan.

langaton USB-verkkosovitinkortti

Langaton sovitinkortti, joka liitetään tietokoneen USB-porttiin.

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.

laukaisualusta

U3-liittymän komponentti, joka toimii U3 USB -ohjelmien käynnistämisen ja hallinnan aloituspisteenä.

luotettujen luettelo

Luettelo kohteista, joihin luotat ja joihin ei sovelleta tunnistusta. Jos merkitset kohteen (esimerkiksi mahdollisen haittaohjelman tai rekisterimuutoksen) luotettavaksi vahingossa tai haluat, että kohde tunnistetaan uudelleen, kohde on poistettava tästä luettelosta.

luvaton käyttöpiste

Ilman lupaa asennettu käyttöpiste. Luvattomat käyttäjät voivat asentaa luvattomia käyttöpisteitä suojattuun yritysverkkoon saadakseen verkon käyttöoikeudet. Hyökkääjät voi luoda niitä myös MITM-hyökkäyksen toteuttamista varten.

lähiverkko

Paikallisverkko. 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

Media Access Control -osoite. Yksilöivä sarjanumero, joka on määritetty verkkoa käyttävälle fyysiselle laitteelle (verkkokortille).

mahdollinen haittaohjelma (PUP)

Ohjelmisto, joka voi olla ei-toivottu siitä huolimatta, että käyttäjät ovat sallineet sen lataamisen. Ohjelmisto voi muuttaa sen tietokoneen suojaus- ja tietosuoja-asetuksia, johon se asennetaan. Mahdollisiin haittaohjelmiin kuuluvat muun muassa vakoiluohjelmat, mainosohjelmat ja piilosoittajat, jotka voivat latautua käyttäjän haluaman ohjelman mukana.

MAPI

Messaging Application Programming Interface. Microsoftin liittymämääritys, jonka avulla eri viestintä- ja työryhmäohjelmat (kuten sähköposti, ääniviesti ja faksi) toimivat yhden asiakkaan, esimerkiksi Exchange-asiakkaan, kautta.

mato

Virus, joka leviää tekemällä itsestään kopioita muihin asemiin, järjestelmiin tai verkkoihin. Joukkopostitusmato vaatii levitäkseen käyttäjän toimenpiteitä, esimerkiksi liitteen avaamista tai ladatun tiedoston suorittamista. Useimmat sähköpostivirukset ovat tänä päivänä matoja. Itseleviävä mato ei vaadi käyttäjän toimenpiteitä levitäkseen. Esimerkkejä itseleviävistä madoista ovat Blaster ja Sasser.

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. Verkkokortti, joka liitetään kannettavaan tietokoneeseen tai muuhun laitteeseen ja jonka avulla laite voidaan liittää lähiverkkoon.

P

pakkaus

Prosessi, jossa tiedostot pakataan sellaiseen muotoon, joka minimoi niiden tallentamiseen tai siirtämiseen vaadittavan levytilan määrän.

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.

palvelunestohyökkäys (DOS)

Tietokoneeseen, palvelimeen tai verkkoon kohdistuva hyökkäystyyppi, joka hidastaa verkkoliikennettä tai keskeyttää sen kokonaan. Palvelunestohyökkäyksessä verkkoon tulvii liikaa ylimääräisiä pyyntöjä, minkä vuoksi tavanomainen liikenne hidastuu tai keskeytyy täysin. Hyökkäyksen kohteeseen saapuu niin paljon virheellisiä yhteyspyyntöjä, että asiallisia pyyntöjä ei oteta huomioon.

perusteksti

Teksti, jota ei ole salattu. Katso myös salaus (sivu 245).

phishing-huijaus

Salasanojen, sosiaaliturvatunnusten ja luottokorttitietojen kaltaisten henkilökohtaisten tietojen petollinen hankkimistapa. Vastaanottajalle lähetetään tekaistuja sähköpostiviestejä, jotka näyttävät olevan peräisin pankkien tai muiden laillisesti toimivien yritysten kaltaisista luotettavista lähteistä. Phishing-huijausviesteissä vastaanottajaa pyydetään tavallisesti napsauttamaan sähköpostiviestissä olevaa linkkiä yhteystietojen tai luottokorttitietojen tarkistamista tai päivittämistä varten.

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.

piilosoittajat

Ohjelmisto, joka ohjaa Internet-yhteydet muulle kuin käyttäjän oletusarvoiselle palveluntarjoajalle periäkseen ylimääräisiä yhteismaksuja sisällöntarjoajalle, toimittajalle tai muulle kolmannelle osapuolelle.

pikakuvake

Tiedosto, joka sisältää vain tietokoneessasi olevan toisen tiedoston sijaintitiedot.

ponnahdusikkunat

Pieniä ikkunoita, jotka avautuvat tietokoneen näytössä olevien muiden ikkunoiden päälle. Ponnahdusikkunoita käytetään useimmiten mainosten näyttämiseen Web-selaimissa.

POP3

Post Office Protocol 3. Sähköpostiasiakasohjelman ja sähköpostipalvelimen välinen liittymä. Useimmilla kotikäyttäjillä on POP3-sähköpostitili. POP3-tili tunnetaan myös tavanomaisena sähköpostitilinä.

portti

Paikka laitteistossa, jonka kautta tietotekniikkalaitte vastaanottaa ja lähettää tietoja. Henkilökohtaisissa tietokoneissa on erilaisia portteja, kuten levyasemien, näyttöjen ja näppäimistöjen liittämiseen tarkoitettuja sisäisiä portteja sekä modeemien, tulostimien, hiirten ja muiden oheislaitteiden liittämiseen tarkoitettuja ulkoisia portteja.

PPPoE

Point-to-Point Protocol Over Ethernet. Point-to-Point Protocol (PPP) -soittoprotokollan käyttötapa Ethernet-yhteyden kautta.

protokolla

Tietokoneiden tai laitteiden tiedonsiirtoa koskevien sääntöjen kokoelma. Useista kerroksista muodostuvissa verkoissa (Open System Interconnection -malli) jokaisella kerroksella on oma protokollansa, joka määrää kyseisen kerroksen tiedonsiirtotavan. Tietokoneen tai laitteen on tuettava oikeata protokollaa, jotta se pystyy kommunikoimaan muiden tietokoneiden kanssa. Katso myös Open Systems Interconnection (OSI).

puskurin ylivuoto

Tilanne, joka esiintyy käyttöjärjestelmässä tai sovelluksessa, kun epäilyttävät ohjelmat tai prosessit yrittävät tallentaa puskuriin (tietojen väliaikaiseen tallennusalueeseen) enemmän tietoja kuin siihen mahtuu. Puskurin ylivuoto vioittaa muistia tai korvaa vierekkäisissä puskuureissa olevat tiedot.

R

RADIUS

Remote Access Dial-In User Service. Protokolla, jonka avulla käyttäjät voidaan todentaa. Protokollaa käytetään useimmiten etäyhteyksien yhteydessä. Protokolla kehitettiin alunperin etäkäyttöpalvelimia varten, mutta nykyään sitä käytetään useissa erilaisissa todennusympäristöissä, kuten langattoman verkon käyttäjän jaetun salaisuuden todentamisessa 802.1x-standardin yhteydessä. Katso myös jaettu salaisuus.

reaaliaikainen tarkistus

Tiedostojen ja kansioiden tarkistus virusten ja muun toiminnan varalta, kun käyttäjä tai tietokone käyttää niitä.

reititin

Verkkolaitte, joka välittää datapaketteja verkosta toiseen. Reitittimet lukevat jokaisen saapuvan paketin ja määrittävät sen välitystavan lähde- ja kohdeosoitteiden sekä vallitsevien tietoliikenneolosuhteiden mukaan. Reititintä kutsutaan joskus käyttöpisteeksi.

rekisteri

Windowsin käyttämä tietokanta, joka sisältää jokaisen tietokoneen käyttäjän kokoonpanotiedot sekä tietoja järjestelmän laitteista, asennetuista ohjelmista ja ominaisuuksien asetuksista. Tietokanta muodostuu avaimista, joiden arvot on määritetty. Haittaohjelmat voivat muuttaa rekisteriavaimien arvoja tai luoda uusia rekisteriarvoja haitallisen koodin suorittamista varten.

roaming

Siirtyminen yhden käyttöpisteen käyttöalueelta toiselle ilman palvelukatkoja tai yhteyden menetyksiä.

rootkit

Työkalukokoelma (tai ohjelmakokoelma), joka takaa käyttäjälle järjestelmänvalvojaoikeudet tietokoneeseen tai tietokoneverkkoon. Ne voivat olla vakoiluohjelmia ja muita mahdollisia haittaohjelmia, jotka voivat aiheuttaa suojaus- ja tietoturvariskejä tietokoneelle ja sen tiedoille.

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 salasanasi 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). Katso myös salaus (sivu 245).

salaus

Koodausmenetelmä, jonka avulla estetään tietojen luvaton käyttö. Tietojen koodauksessa käytetään ”avainta” ja matemaattisia algoritmeja. Salattujen tietojen salausta ei voi purkaa ilman oikeata avainta. Virukset käyttävät joskus salausta, jotta niitä ei tunnisteta.

sallittujen osoitteiden luettelo

Turvallisina pidettyjen Web-sivustojen tai sähköpostiosoitteiden luettelo. Sallittujen osoitteiden luettelossa on sellaisia Web-osoitteita, joita käyttäjillä on lupa käyttää. Sallittujen osoitteiden luettelossa olevat sähköpostiosoitteet ovat luotettavista lähteistä, joista haluat ottaa viestejä vastaan. Vertaa estettyjen osoitteiden luetteloon (sivu 239).

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 nuori 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. Verkon järjestelmänvalvoja määrittää SSID-tunnuksen. 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

Varmuuskopioitujen tiedostoversioiden ja paikalliseen tietokoneeseen tallennettujen tiedostoversioiden tietojen yhtenäistäminen. Tiedostot kannattaa synkronoida silloin, kun online-varmuuskopiovarastossa oleva tiedostoversio on uudempi kuin muissa tietokoneissa oleva tiedostoversio.

SystemGuard

McAfee-hälytykset, jotka tunnistavat tietokoneeseen tehdyt luvattomat muutokset ja varoittavat niistä.

sähköposti

Sähköposti. Tietokoneverkon kautta sähköisesti lähetetyt ja vastaanotetut viestit. Katso myös webmail (sivu 248).

sähköpostiasiakas

Tietokoneessa suoritettava ohjelma sähköpostiviestien lähettämistä ja vastaanottamista varten (esimerkiksi Microsoft Outlook).

T

tapahtuma

Tietokonejärjestelmässä tai ohjelmassa ilmenevä tapaus tai esiintymä, joka voidaan havaita tietoturvaohjelmiston avulla käyttämällä esimääritettyjä ehtoja. Tyypillisesti tapahtuma laukaisee toiminnon, kuten ilmoituksen lähettämisen tai merkinnän lisäämisen tapahtumalokiin.

tarkkailtavat tiedostotyypit

Tarkkailtavat tiedostotyypit ovat tiedostotyyppisiä (esimerkiksi .doc ja .xls), jotka Backup and Restore varmuuskopioi tai arkistoi tarkkailukohteissa.

tarkkailukohteet

Tietokoneen kansiot, joita Backup and Restore tarkkailee.

tarvepohjainen tarkistus

Valittujen tiedostojen, sovellusten tai verkkolaitteiden ajoitettu tarkistus, jonka tavoitteena on löytää uhat, tietoturvan puutteet tai muut mahdollisesti haitalliset koodit. Tarkistus voidaan suorittaa välittömästi, määrättyyn aikaan tulevaisuudessa tai säännöllisin aikavälein. Vertaa käytönaikaiseen tarkistukseen. Katso myös tietoturvan puutteet.

tavallinen sähköpostitili

Katso POP3 (sivu 243).

tiedostopirstaleet

Levyille tallennettujen tiedostojen jäänteitä. Tiedostot pirstoutuvat, kun tiedostoja lisätään ja poistetaan. Levyn pirstoutuminen voi hidastaa tietokoneen suorituskykyä.

TKIP

Temporal Key Integrity Protocol (äännetään tee-kip). Langattomien lähiverkkojen 802.11i-salausstandardin osa. TKIP on seuraavan sukupolven WEP, jota käytetään 802.11-standardia soveltavien langattomien lähiverkkojen suojaamiseen. TKIP sisältää pakettikohtaisen avainten hajautuksen, viestien yhtenäisyyden tarkistuksen ja avainten kierrätysmahdollisuuden, jolla korvataan WEP-protokollan puutteet.

todennus

Lähettäjän digitaalisen henkilöllisyyden tarkistaminen sähköisessä viestinnässä.

toimialue

Paikallinen aliverkko tai kuvaus Internet-sivustoja varten. Lähiverkossa (LAN) toimialue on asiakas- ja palvelintietokoneista koostuva aliverkko, jota valvoo yksi suojaustietokanta. Internetissä toimialue kuuluu osana jokaiseen Web-osoitteeseen. Esimerkiksi osoitteessa www.mcafee.com toimialue on mcafee.

Trojialainen, Troijan hevonen

Ohjelma, joka ei replikoi, vaan aiheuttaa vahinkoja tai vaarantaa tietokoneen tietoturvan. Tavallisesti joku lähettää Troijan hevosen sinulle, se ei lähetä itseään. Voit myös ladata Troijan hevosen Web-sivustosta tai vertaisverkosta tietämättäsi.

U

U3

You: Simplified, Smarter, Mobile. 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 koneeseen asennettu tai tallennettu.

ulkoinen kiintolevyasema

Kiintolevyasema, joka sijaitsee tietokoneen ulkopuolella.

URL

Uniform Resource Locator. Internet-osoitteiden standardimuoto.

USB

Universal Serial Bus. Useimmissa nykyaikaisissa tietokoneissa käytettävä standardinmukainen liitäntätapa, jonka avulla voidaan liittää useita laitteita, kuten näppäimistöjä, hiiriä, verkkokameroita, skannereita ja tulostimia.

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 ajelee ympäri kaupunkeja mukanaan Wi-Fi-tietokone sekä erityisohjelmistoja ja -laitteita.

V

varmuuskopiointi

Kopioiden luominen tärkeistä tiedostoista, tavallisesti suojattuun online-palvelimeen. Vertaa arkistointiin (sivu 238).

W

webmail

Web-pohjainen sähköposti. Sähköinen postipalvelu, jota käytetään lähinnä Web-selaimen kautta tietokoneessa olevan sähköpostiohjelman (esimerkiksi Microsoft Outlookin) sijaan. Katso myös sähköposti (sivu 246).

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 toisesta päätepisteestä toiseen. Viime aikoina on kuitenkin huomattu, että WEP-salaus ei ole aivan niin turvallinen kuin aiemmin on uskottu.

V

verkko

IP-pohjaisten järjestelmien (kuten reitittimien, kytkimien, palvelimien ja palomuurien) kokoelma, jotka on ryhmitelty loogiseksi yksiköksi. Esimerkiksi ”talousverkko” voi sisältää kaikki talousosastoa palvelevat palvelimet, reitittimet ja järjestelmät. Katso myös kotiverkko (sivu 240).

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 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 asiakasohjelmisto on myös 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

Tietokoneohjelma, joka pystyy kopioimaan itsensä ja tartuttamaan tietokoneen ilman käyttäjän lupaa tai hänen tietämättään.

W

WLAN

Wireless Local Area Network. Lähiverkko, johon voidaan muodostaa langaton yhteys. 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 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 aloitussalasanan manuaalisesti aktivoitakseen suojatun langattoman verkkoyhteyden esijaetun avaintilan ja vaihtaa sitten verkon jokaisen langattoman tietokoneen ja käyttöpiestin salasanaa säännöllisesti. Katso myös WPA2-PSK (sivu 250) ja TKIP (sivu 247).

WPA2

WPA-tietosuojastandardin päivitys, joka perustuu 802.11i-standardiin.

WPA2-PSK

Eriyinen 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 tietoliikenneverkko, joka on määritetty isäntäverkon (esimerkiksi Internetin) välityksellä. VPN-yhteyden kautta kulkevat tiedot on salattu ja niitä luonnehtivat vahvat tietoturvaominaisuudet.

väliaikainen tiedosto

Käyttöjärjestelmän tai jonkin muun ohjelman muistiin tai levyille luoma tiedosto, jota käytetään istunnon aikana ja joka sen jälkeen poistetaan.

välimuisti

Tietokoneessa oleva alue, jota käytetään usein tai hiljattain käytettyjen tietojen väliaikaiseen tallennukseen. 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 luvatonta 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 (sivu 250).

[väsytyksen menetelmähyökkäys](#)

Salasanojen tai salausavainten etsimiseen käytettävä tietomurtomenetelmä, jossa kokeillaan kaikkia mahdollisia merkkiyhdistelmiä niin kauan, kunnes salaus on murrettu.

Y

[yhdistetty yhdyskäytävä](#)

Laite, joka yhdistää langattoman käyttöpisteen, reitittimen ja palomuurin toiminnot. Jotkin laitteet sisältävät myös suojausparannuksia ja siltausominaisuuksia.

Ä

[älykäs asema](#)

Katso USB-asema (sivu 248).

Tietoja McAfeesta

McAfee, Inc.:n pääkonttori sijaitsee Santa Clarassa, Kaliforniassa. McAfee on maailman johtavia tietomurtojen esto- ja tietoturvariskien hallintasovellusten 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.

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 MYYNTI-, MYYNTITILAUS- 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 ASENN A OHJELMISTOA. TIETYISSÄ TAPAUKSISSA VOIT PALAUTTAA TUOTTEEN MCAFEE-YHTIÖLLE TAI OSTOAIKKAAN JA SAADA TÄYDEN HYVITYKSEN MAKSUSTASI.

Copyright

Copyright © 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.

LUKU 51

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 (ongelmatyyppin 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 kirjaututtava 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.....256

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.

Käynnistä Virtual Technician

Virtual Technician kerää tietoja tietokoneeseesi asennetuista SecurityCenter-ohjelmista ja auttaa sinua ratkaisemaan tietokoneesi suojausongelmat. Yksityisyytesi turvaamiseksi näihin tietoihin ei sisälly henkilö- tai tunnistetietoja.

- 1 Valitse **Yleiset tehtävät** -kohdasta **McAfee Virtual Technician**.
- 2 Lataa Virtual Technician toimimalla näytön ohjeiden mukaan.

Lisätietoja oman maasi tai alueesi McAfeen tuki- ja lataussivustoista sekä käyttöoppaiden lataussivustoista on seuraavissa taulukoissa.

Tuki ja lataukset

Maa/alue	McAfee-tuki	McAfee-lataussivustot
Australia	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brasilia	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Espanja	www.mcafeeayuda.com	es.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
Kanada (englanti)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp

Kanada (ranska)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp?langid=48
Kiina (yksinkertaistettu kiina)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
Korea	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Kreikka	www.mcafeehelp.com	el.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
Portugali	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
Puola	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp
Ranska	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Ruotsi	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Saksa	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Slovakia	www.mcafeehelp.com	sk.mcafee.com/root/downloads.asp
Suomi	www.mcafeehelpfinland.com	fi.mcafee.com/root/downloads.asp
Taiwan	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Tanska	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Tsekin tasavalta	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Turkki	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
Unkari	www.mcafeehelp.com	hu.mcafee.com/root/downloads.asp
Venäjä	www.mcafeehelp.com	ru.mcafee.com/root/downloads.asp
Yhdysvallat	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

McAfee Total Protection -käyttöoppaat

Maa/alue	McAfee-käyttöoppaat
Alankomaat	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Australia	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brasilia	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Espanja	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Iso-Britannia	download.mcafee.com/products/manuals/en-uk/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
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 (yksinkertaistettu kiina)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Kreikka	download.mcafee.com/products/manuals/el/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
Portugali	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Puola	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
Ranska	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Ruotsi	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Saksa	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Slovakia	download.mcafee.com/products/manuals/sk/MTP_userguide_2008.pdf
Suomi	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf

Taiwan	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Tanska	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Tsekin tasavalta	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Turkki	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Unkari	download.mcafee.com/products/manuals/hu/MTP_userguide_2008.pdf
Venäjä	download.mcafee.com/products/manuals/ru/MTP_userguide_2008.pdf
Yhdysvallat	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

McAfee Internet Security -käyttöoppaat

Maa/alue	McAfee-käyttöoppaat
Alankomaat	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Australia	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brasilia	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Espanja	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Iso-Britannia	download.mcafee.com/products/manuals/en-uk/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
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 (yksinkertaistettu kiina)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Kreikka	download.mcafee.com/products/manuals/el/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
Portugali	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
Puola	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Ranska	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Ruotsi	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Saksa	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf
Slovakia	download.mcafee.com/products/manuals/sk/MIS_userguide_2008.pdf
Suomi	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Tanska	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Tsekin tasavalta	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Turkki	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Unkari	download.mcafee.com/products/manuals/hu/MIS_userguide_2008.pdf
Venäjä	download.mcafee.com/products/manuals/ru/MIS_userguide_2008.pdf
Yhdysvallat	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

McAfee VirusScan Plus -käyttöoppaat

Maa/alue	McAfee-käyttöoppaat
Alankomaat	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Australia	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brasilia	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Espanja	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Iso-Britannia	download.mcafee.com/products/manuals/en-uk/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
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 (yksinkertaistettu kiina)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Kreikka	download.mcafee.com/products/manuals/el/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
Portugali	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
Puola	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Ranska	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Ruotsi	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Saksa	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Slovakia	download.mcafee.com/products/manuals/sk/VSP_userguide_2008.pdf
Suomi	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Tanska	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Tsekin tasavalta	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
Turkki	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
Unkari	download.mcafee.com/products/manuals/hu/VSP_userguide_2008.pdf
Venäjä	download.mcafee.com/products/manuals/ru/VSP_userguide_2008.pdf

Yhdysvallat	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf
-------------	--

McAfee VirusScan -käyttöoppaat

Maa/alue	McAfee-käyttöoppaat
Alankomaat	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Australia	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brasilia	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Espanja	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Iso-Britannia	download.mcafee.com/products/manuals/en-uk/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
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 (yksinkertaistettu kiina)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Kreikka	download.mcafee.com/products/manuals/el/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
Portugali	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
Puola	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Ranska	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Ruotsi	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Saksa	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf

Slovakia	download.mcafee.com/products/manuals/sk/VS_userguide_2008.pdf
Suomi	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Tanska	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Tsekin tasavalta	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Turkki	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Unkari	download.mcafee.com/products/manuals/hu/VS_userguide.2008.pdf
Venäjä	download.mcafee.com/products/manuals/ru/VS_userguide_2008.pdf
Yhdysvallat	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

Lisätietoja oman maasi tai alueesi McAfee Threat Centeristä ja virustietoja sisältävistä sivustoista on seuraavassa taulukossa.

Maa/alue	Tietoturvasivustot	Virustietoja
Alankomaat	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Australia	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brasilia	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Espanja	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Iso-Britannia	www.mcafee.com/us/threat_center	uk.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
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 (yksinkertaistettu kiina)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
Korea	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Kreikka	www.mcafee.com/us/threat_center	gr.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
Portugali	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
Puola	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
Ranska	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Ruotsi	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Saksa	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Slovakia	www.mcafee.com/us/threat_center	sk.mcafee.com/virusInfo
Suomi	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
Taiwan	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Tanska	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Tsekin tasavalta	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Turkki	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Unkari	www.mcafee.com/us/threat_center	hu.mcafee.com/virusInfo
Venäjä	www.mcafee.com/us/threat_center	ru.mcafee.com/virusInfo
Yhdysvallat	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

Lisätietoja oman maasi tai alueesi HackerWatch-sivustoista on seuraavassa taulukossa.

Maa/alue	HackerWatch
Alankomaat	www.hackerwatch.org/?lang=nl
Australia	www.hackerwatch.org

Brasilia	www.hackerwatch.org/?lang=pt-br
Espanja	www.hackerwatch.org/?lang=es
Iso-Britannia	www.hackerwatch.org
Italia	www.hackerwatch.org/?lang=it
Japani	www.hackerwatch.org/?lang=jp
Kanada (englanti)	www.hackerwatch.org
Kanada (ranska)	www.hackerwatch.org/?lang=fr-ca
Kiina (yksinkertaistettu kiina)	www.hackerwatch.org/?lang=zh-cn
Korea	www.hackerwatch.org/?lang=ko
Kreikka	www.hackerwatch.org/?lang=el
Meksiko	www.hackerwatch.org/?lang=es-mx
Norja	www.hackerwatch.org/?lang=no
Portugali	www.hackerwatch.org/?lang=pt-pt
Puola	www.hackerwatch.org/?lang=pl
Ranska	www.hackerwatch.org/?lang=fr
Ruotsi	www.hackerwatch.org/?lang=sv
Saksa	www.hackerwatch.org/?lang=de
Slovakia	www.hackerwatch.org/?lang=sk
Suomi	www.hackerwatch.org/?lang=fi
Taiwan	www.hackerwatch.org/?lang=zh-tw
Tanska	www.hackerwatch.org/?lang=da
Tsekin tasavalta	www.hackerwatch.org/?lang=cs
Turkki	www.hackerwatch.org/?lang=tr
Unkari	www.hackerwatch.org/?lang=hu
Venäjä	www.hackerwatch.org/?lang=ru
Yhdysvallat	www.hackerwatch.org

Hakemisto

8

802.11	238
802.11a.....	238
802.11b	238
802.1x.....	238

A

ActiveX-komponentti.....	238
Ajoita automaattinen arkistointi.....	176
Ajoita Levyn eheytytys -tehtävä	195
Ajoita QuickClean-tehtävä	193
Aktivoi tuotteesi.....	11
Analysoi saapuvaa ja lähtevää tietoliikennettä	114
Anti-Spamin ominaisuudet.....	121
arkistointi	238, 248
Arkistoitujen tiedostojen käsitteleminen	179
Arkistoitujen tiedostojen palauttaminen	181
Arkistojen hallinta	183
Arkiston asetusten määrittäminen	171
Asenna käytettävissä oleva verkkotulostin	236
Asenna McAfee-tietoturvaohjelmisto etätietokoneisiin	217
asiakas	238
Asiakaspalvelu ja tekninen tuki.....	255
Avaa arkistoitu tiedosto	181
Avaa EasyNetwork.....	225
avain	238
Avainsanojen suodatuksen poistaminen käytöstä	149

B

Backup and Restoren ominaisuudet ...	168
--------------------------------------	-----

C

Copyright.....	254
----------------	-----

D

DAT	239
DNS.....	239

E

EasyNetworkin asentaminen	225
---------------------------------	-----

EasyNetworkin ominaisuudet.....	224
Eheyttä tietokoneesi	191
Eristettyjen ohjelmien ja evästeiden käsitteleminen.....	39
Eristettyjen tiedostojen käsitteleminen	38
ESS	239
estettyjen osoitteiden luettelo.....	239, 245
Estä käyttöoikeudet äskettäisten tapahtumien lokista.....	91
Estä ohjelman käyttöoikeudet	90
Estä olemassa olevan järjestelmäpalveluportin käyttö	103
Estä tietokone saapuvien tapahtumien lokista	100
Estä tietokone tietomurtojen havainnoinnin tapahtumien lokista	100
Estä uuden ohjelman käyttöoikeudet ...	90
Estä Web-sivustot avainsanojen perusteella	148
Etsi arkistoitua tiedostoa	180
eväste	239

H

Hae jaettu tiedosto	231
Hae ohjelmatietoja lähtevien tapahtumien lokista.....	92
Hakuehdot	231
Hallitse laitetta.....	215
Hallitse tietokoneen suojauksen tilaa .	214
Hallittuun verkkoon liittyminen .	210, 226, 228
Hallitun verkon määrittäminen.....	207
Hallitusta verkosta poistuminen	228
Hanki ohjelmatietoja	92
Hanki tietokoneen rekisteröintitiedot.	111
Hanki tietokoneen verkkotiedot	111
Henkilökohtaisten suodattimien käyttäminen.....	127
Henkilökohtaisten tietojen suojaaminen	162
Hyväksy tiedosto toisesta tietokoneesta	232, 233
Hälytyksiin liittyvien suositusten asetusten määrittäminen	77
Hälytysasetusten määrittäminen	24
Hälytysten käsitteleminen.....	14, 21, 69

I

Ikäryhmälle sopivan haun ottaminen käyttöön	155
Ilmoita sähköpostiviesteistä McAfeelle	141
Ilmoituksen saaminen tiedoston lähettämisestä	233
Internet-tietoliikenteen jäljittäminen	110
Internet-tietoliikenteen valvonta.....	113
intranet	239
IP-huijausyritys.....	239
IP-osoite	239

J

Jaa tiedosto.....	230
jaettu salaisuus	240
Jaettujen tulostinten käyttäminen.....	236
jakaminen	240
julkaiseminen	240
Jäljitä tietokone saapuvien tapahtumien lokista	112
Jäljitä tietokone tietomurtojen havainnoinnin tapahtumien lokista	112
Jäljitä valvottu IP-osoite.....	113
Jäljitä verkkotietokone maantieteellisesti	111
järjestelmän palautuspiste	240
Järjestelmäpalveluiden hallinta	101
Järjestelmäpalveluporttien asetusten määrittäminen	102

K

kaistanleveys	240
karanteeni	240
Keskeytä automaattinen arkistointi	176
Kirjaus, valvonta ja analyysi	107
komentosarja	240
Kopioi jaettu tiedosto.....	231
Korjaa suojausongelmat automaattisesti	18
Korjaa suojausongelmat manuaalisesti	19
Korjaa tietoturvan puutteet.....	216
kotiverkko.....	240, 249
Kutsu tietokone hallittuun verkkoon ..	211
Käynnistä HackerWatch-opetusohjelma	118
Käynnistä komentosarjatarkistussuojaus	44
Käynnistä pikaviestisuojaus	45
Käynnistä sähköpostisuojaus.....	44
Käynnistä vakoiluohjelasuojaus.....	44
Käynnistä Virtual Technician.....	256
Käyttäjien määrittäminen	157
Käyttöoikeus	253

käyttöpiste.....	240
Käytä merkistösuodattimia	126
Käytä verkkokarttaa.....	208

L

laajennus	241
Lajittele arkistoidut tiedostot	180
Lakkaa luottamasta verkon tietokoneisiin	212
langaton PCI-verkkosovitinkortti	241
langaton USB-verkkosovitinkortti	241
langaton verkkopiste.....	241
langaton verkkosovitin	241
Lasten suojaaminen	147
laukaisualusta	241
Liity hallittuun verkkoon	210
Liity verkkoon	227
Lisäsuojaus käytäminen.....	43
Lisää estetty tietokoneyhteys	98
Lisää henkilökohtainen suodatin	128
Lisää kohde arkistoon	172
Lisää McAfee-käyttäjä.....	159
Lisää salasana	166
Lisää tietokone saapuvien tapahtumien lokista	96
Lisää tietokoneyhteys.....	95
Lisää toimialue	135
Lisää Web-sivusto valkoiseen listaan ..	143
Lisää Web-sähköpostitili	137
Lisää ystävä Anti-Spam-työkaluriviltä	134
Lisää ystävä manuaalisesti	134
Lopeta reaaliaikainen virustorjunta	49
Lopeta tiedoston jakaminen	230
Lopeta tietokoneen suojaus tilan hallinta	214
Lopeta tulostimen jakaminen	236
Lopeta uusien ystävien etsintä.....	221
Lopeta verkkojen valvonta	219
Lukitse palomuri välittömästi.....	82
luotettujen luettelo.....	241
Luotettujen luetteloiden hallinta.....	61
Luotettujen luetteloiden käyttäminen ..	60
luvaton käyttöpiste.....	241
Lähetä tiedosto toiseen tietokoneeseen	232
lähiverkko	240, 241

M

MAC-osoite	242
mahdollinen haittaohjelma (PUP)	242
Mahdollisesti sopimattomien Web-kuvien suodattaminen	154
Mahdollisten haittaohjelmien käsitteleminen.....	38

- MAPI 242
mato 242
McAfee Anti-Spam 119
McAfee Backup and Restore..... 167
McAfee EasyNetwork 223
McAfee Network Manager 203
McAfee Parental Controls..... 145
McAfee Personal Firewall 65
McAfee QuickClean..... 185
McAfee SecurityCenter 5
McAfee Shredder 199
McAfee Total Protection 3
McAfee Virtual Technician -palvelun
käyttö..... 256
McAfee VirusScan..... 29
McAfee-käyttäjien asetusten
määrittäminen 158, 160
McAfee-tilisi käyttäminen 11
Merkitse tunkeutujaksi 221
Merkitse viesti Anti-Spam-työkalariviltä
..... 131
Merkitse ystäväksi 221
MITM-hyökkäys 242
MSN 242
Mukautettujen tarkistusasetusten
määrittäminen41, 50
Muokkaa estettyä tietokoneyhteyttä 99
Muokkaa hallitun tietokoneen oikeuksia
..... 215
Muokkaa henkilökohtaista suodatinta 128
Muokkaa järjestelmäpalveluporttia 105
Muokkaa laitteen näytön ominaisuuksia
..... 215
Muokkaa Levyn eheytyksen tehtävää 196
Muokkaa McAfee-käyttäjän tilitietoja. 159
Muokkaa QuickClean-tehtävää 194
Muokkaa roskapostin käsittely- ja
merkintätapaa 125, 127
Muokkaa salasanaa 165
Muokkaa tietokoneyhteyttä 96
Muokkaa toimialuetta..... 136
Muokkaa valkoisessa listassa olevia
sivustoja 144
Muokkaa Web-sähköpostitiliä 138
Muokkaa ystävän tietoja..... 135
Muuta arkiston sijaintia..... 174
Muuta suodatustasoa..... 124
Myönnä ohjelmalle täydet käyttöoikeudet
..... 86
Myönnä ohjelmalle vain lähtevän
tietoliikenteen käyttöoikeudet..... 88
Myönnä täydet käyttöoikeudet lähtevien
tapahtumien lokista..... 88
Myönnä täydet käyttöoikeudet
äskettäisten tapahtumien lokista 87
Myönnä uudelle ohjelmalle täydet
käyttöoikeudet..... 87
Myönnä vain lähtevän tietoliikenteen
käyttöoikeudet lähtevien tapahtumien
lokista 89
Myönnä vain lähtevän tietoliikenteen
oikeudet äskettäisten tapahtumien
lokista 89
Myönnä verkon käyttöoikeudet..... 227
Määritä arkistotiedostojen tyypit..... 173
Määritä automaattiset päivitykset 14
Määritä henkilökohtainen suodatin... 128,
129
Määritä käyttäjän sisältöluokitusryhmä
..... 153
Määritä mukautetun tarkistuksen
asetukset 51
Määritä palomuurin suojauksen tilan
asetukset 81
Määritä ping-pyyntöjen asetukset..... 80
Määritä reaaliaikaisen tarkistuksen
asetukset 48
Määritä SystemGuards-asetukset..... 56
Määritä tapahtumalokin asetukset..... 108
Määritä tietomurtojen havainnoinnin
asetukset 81
Määritä UDP-asetukset..... 80
Määritä uuden järjestelmäpalveluportin
asetukset 104
- N**
- Network Managerin kuvakkeiden
toiminta..... 205
Network Managerin ominaisuudet 204
NIC 242
Nimeä verkko uudelleen..... 209, 228
Nollaa salasanasäilön salasana 164
Nouda McAfee-järjestelmänvalvojan
salasana..... 158
Näytä arkistointitoimintojen yhteenveto
..... 183
Näytä hälytykset pelaamisen aikana 71
Näytä kohteen tiedot..... 209
Näytä suodatettujen
Web-sähköpostiviestien tapahtumat142
Näytä suositukset 78
Näytä tai piilota kohde verkkokartalla 209
Näytä tai piilota tiedottavat hälytykset . 22
Näytä tai piilota tiedottavat hälytykset
pelejä pelattaessa 23
Näytä tarkistuksen tulokset 35

O

Ohita suojausongelma	19
Ohitettujen ongelmien näyttäminen tai piilottaminen.....	20
Ohjelmien Internet-käyttöoikeuden estäminen	90
Ohjelmien Internet-käyttöoikeuden salliminen	86
Ohjelmien ja käyttöoikeuksien hallinta	85
Ohjelmien käyttöoikeuksien poistaminen	91
Opas	237
Ota ikäryhmälle sopiva haku käyttöön	155
Ota paikallinen arkisto käyttöön.....	170
Ota suositukset käyttöön	77
Ota SystemGuards-suojaus käyttöön....	55
Ota uudelleen käyttöön verkon valvontaan liittyvät ilmoitukset.....	220

P

Paikallisen arkiston hallintaohjelman käyttäminen.....	180
Paikallisen arkiston ottaminen käyttöön ja poistaminen käytöstä	170
pakkaus.....	242
Palauta palomuurin asetukset	83
Palauta puuttuvia tiedostoja paikallisesta arkistosta.....	182
Palauta tiedoston aikaisempi versio paikallisesta arkistosta.....	182
palomuuuri.....	243
Palomuurin käynnistäminen	67
Palomuurin lukitseminen ja palauttaminen	82
Palomuurin suojauksen optimointi	79
Palomuurin tietoturvasojen hallinta..	74
Palomuurisuojauksen asetusten määrittäminen	73
Palomuurisuojauksen käynnistäminen	67
Palomuurisuojauksen pysäyttäminen ..	68
palvelin	243
palvelunestohyökkäys (DOS)	243
Parental Controlsin ominaisuudet	146
Perehtyminen Internet-tietoturvaan..	117
Perehtyminen ohjelmiin.....	92
Personal Firewallin ominaisuudet.....	66
perusteksti.....	243
phishing-huijaus	243
Phishing-huijausten torjunnan asetusten määrittäminen	143
piilojäljitteet	243
piilosoittajat	243
Piilota aloitusnäyttö käynnistyksessä....	24

Piilota tiedottavat hälytykset.....	72
Piilota tietoturvailmoitukset	25
Piilota virusesiintymähälytykset	25
pikakuvake	243
Poista Anti-Spam-työkalurivi käytöstä	132
Poista arkiston salaus ja pakkaus käytöstä	174
Poista automaattiset päivitykset käytöstä	14
Poista estetty tietokoneyhteys.....	99
Poista henkilökohtainen suodatin.....	128
Poista järjestelmäpalveluportti	106
Poista Levyn eheytyksen tehtävä.....	197
Poista McAfee-käyttäjä	159
Poista ohjelman käyttöoikeudet	91
Poista paikallinen arkisto käytöstä	170
Poista palomuurin lukitus välittömästi.	82
Poista phishing-huijausten torjunta käytöstä	144
Poista QuickClean-tehtävä.....	195
Poista roskapostin torjunta käytöstä...	130
Poista salasana.....	165
Poista suositukset käytöstä.....	78
Poista tiedostoja Puuttuvat tiedostot -luettelosta.....	183
Poista tietokoneyhteys	97
Poista Web-sivusto valkoisesta listasta	144
Poista Web-sähköpostitili.....	139
Poista ystävä.....	136
Poistu hallitusta verkosta.....	228
ponnahdusikkunat	243
POP3	244, 247
portti	244
PPPoE	244
protokolla	244
Puhdista tietokone	189
puskurin ylivuoto	244
Päivitä verkkokartta.....	208

Q

QuickCleanin toiminnot.....	186
-----------------------------	-----

R

RADIUS.....	240, 244
reaaliaikainen tarkistus.....	244
Reaaliaikaisen tarkistuksen asetusten määrittäminen	40, 48
reititin	244
rekisteri.....	245
roaming	245
rootkit	245
roskakori.....	245
Roskapostiviestien tunnistustavan määrittäminen	123

S

salasana	245
salanasäilö	245
Salanasäilön asentaminen	164
Salasanojen suojaaminen	163
salattu teksti	245
salaus	243, 245
Salli olemassa olevan järjestelmäpalveluportin käyttö	103
sallittujen osoitteiden luettelo	239, 245
sanakirjahyökkäys	245
SecurityCenterin käyttäminen	7
SecurityCenterin ominaisuudet	6
SecurityCenterin päivittäminen	13
selain	246
Shredderin toiminnot	200
sisältöluokitus-ryhmä	246
Sisältöluokitusryhmän määrittäminen	153, 154, 155
SMTP	246
Soita ääni hälytyksen esiintyessä	24
solmu	246
SSID	246
SSL	246
Sulje kohde arkistosta pois	173
Suodata mahdollisesti sopimattomat Web-kuvat	154
Suodatettujen sähköpostiviestien käsitteleminen	141
Suodatetun Web-sivuston poistaminen	150
Suodatetun Web-sivuston päivittäminen	150
Suodatusasetusten määrittäminen	124
Suojaa henkilökohtaisia tietoja	162
Suojaa tietokonetta käynnistyksen aikana	79
Suojauksen tilan toiminta	7, 8, 9
Suojausluokkien toiminta	7, 9, 27
Suojausongelmien korjaaminen	8, 18
Suojausongelmien korjaaminen ja ohittaminen	8, 17
Suojausongelmien ohittaminen	19
Suojauspalveluiden toiminta	10
Suojaustason määrittäminen Automaattinen-tasolle	76
Suojaustason määrittäminen Normaali-tasolle	75
Suojaustason määrittäminen Vaikeasti havaittava -tasolle	75
Suorita manuaalinen arkistointi	177
synkronointi	246
SystemGuard	246

SystemGuards-toimintojen asetukset ...	54
sähköposti	246, 248
sähköpostiasiakas	246
Sähköpostin suodatus	131

T

tapahtuma	247
Tapahtumien kirjaus	108
Tapahtumien näyttäminen	18, 27
Tarkastele kaikkia tapahtumia	27
Tarkastele lähteviä tapahtumia	87, 109
Tarkastele maailman Internet-porttitapahtumia	110
Tarkastele maailman tietoturvatapahtumien tilastotietoja	110
Tarkastele saapuvia tapahtumia	109
Tarkastele tietomurtojen havainnoinnin tapahtumia	109
Tarkastele äskettäisiä tapahtumia	27, 108
Tarkastele, vie tai poista suodatettuja Web-sähköpostiviestejä	142
Tarkista päivitykset	13, 14
Tarkista tietokone	32, 41
Tarkistuksen ajoittaminen	41, 53
Tarkistuksen tulosten käyttäminen	37
Tarkistustavat	34, 40
tarkkailtavat tiedostotyypit	247
tarkkailukohteet	247
tarvepohjainen tarkistus	247
tavallinen sähköpostitili	247
Tehtävän ajoittaminen	193
Tiedostojen arkistointi	169
Tiedostojen jakaminen	230
Tiedostojen jakaminen ja lähettäminen	229
Tiedostojen lähettäminen toisiin tietokoneisiin	232
Tiedostojen, kansiodien ja levyjen tuhoaminen	200
tiedostopirstaleet	247
Tiedottavien hälytysten hallinta	71
Tiedottavien hälytysten näyttäminen ja piilottaminen	22
Tietoja hälytyksistä	70
Tietoja luotettujen luetteloiden tyypeistä	61, 62
Tietoja McAfeesta	253
Tietoja SystemGuards-tyypeistä	56, 57
Tietoja tietokoneyhteyksistä	94
Tietoja tietoliikenneanalyysin kaaviosta	114
Tietojen suojaaminen Internetissä	161
Tietokoneen eheyttäminen	191
Tietokoneen puhdistaminen	187

- Tietokoneen tarkistaminen 31
- Tietokoneyhteyksien estäminen..... 98
- Tietokoneyhteyksien hallinta..... 93
- Tietoturvan puutteiden korjaaminen . 216
- Tilastotietojen käsitteleminen 110
- Tilausten hallinta.....10, 18
- Tilojen ja oikeuksien hallinta 214
- TKIP 247, 250
- todennus 238, 247
- toimialue 247
- Trojialainen, Troijan hevonen 247
- Tuhoa koko levy..... 201
- Tuhoa tiedostoja ja kansioita 200
- Tulostinten jakaminen..... 235
- Tuo osoitekirja 133
- Täydellisen arkistoinnin ja
pika-arkistoinnin suorittaminen 175
- U**
- U3 248
- ulkoinen kiintolevyasema 248
- URL 248
- USB 248
- USB-asema..... 248, 251
- Uudista tilauksesi 11
- V,W**
- Vahvista tilaus..... 11
- Vaihda McAfee-järjestelmänvalvojan
salasana..... 158
- Vaihda Salanasäilön salasana..... 164
- Vain lähtevän tietoliikenteen
käyttöoikeuksien myöntäminen 88
- Valvo ohjelman kaistanleveyttä 115
- Valvo ohjelmatapahtumia 115
- wardriver-verkkovaras 248
- varmuuskopiointi 238, 248
- webmail 246, 248
- Web-selauksen aikarajoitusten
määrittäminen 152
- Web-sivustojen suodattaminen... 149, 153
- Web-sivustojen suodattaminen
avainsanojen avulla 148, 149
- Web-sivuston estäminen 151
- Web-sivuston salliminen 150
- Web-sähköpostitilien määrittäminen. 137
- Web-sähköpostitilin tietojen
ymmärtäminen 138, 139
- WEP..... 238, 248
- verkko 249
- verkkosema 249
- Verkkojen valvonta..... 219
- Verkkokartan käyttäminen 208
- verkkokartta 249
- Verkon etähallinta 213
- viestin todennuskoodi (MAC) 249
- Wi-Fi 249
- Wi-Fi Alliance..... 249
- Wi-Fi Certified 249
- Windows-käyttäjien asetusten
määrittäminen 160
- Windows-käyttäjiin vaihtaminen 160
- virus 249
- VirusScan-ohjelman ominaisuudet..... 30
- Virusten ja troijalaisten käsitteleminen 37
- Virustorjunnan määrittäminen31, 47
- WLAN..... 249
- WPA..... 238, 250
- WPA2..... 238, 250
- WPA2-PSK 238, 250
- WPA-PSK 238, 250
- VPN 250
- väliaikainen tiedosto 250
- välimuisti..... 250
- välimuistipalvelin 250, 251
- välityspalvelin 251
- väsytyksen menetelmähyökkäys..... 251
- Y**
- yhdistetty yhdyskäytävä..... 251
- Ystävien määrittäminen 133
- Ystävien määrittäminen manuaalisesti
..... 134
- Ä**
- älykäs asema 251