

McAfee® **Total Protection**

Kullanıcı Kılavuzu

İçindekiler

McAfee Total Protection

3

McAfee SecurityCenter.....	5
SecurityCenter özellikleri	6
SecurityCenter'i kullanma	7
Koruma sorunlarını onarma veya yok sayma	17
Uyarılarla çalışma	21
Olayları görüntüleme	27
McAfee VirusScan.....	29
VirusScan özellikleri.....	30
Bilgisayarınızı tarama	31
Tarama sonuçlarıyla çalışma	35
Tarama türleri	38
Ek koruma kullanma.....	41
Virüsten korumayı ayarlama.....	45
McAfee Personal Firewall	61
Personal Firewall özellikleri	62
Firewall'u Başlatma	63
Uyarılarla çalışma	65
Bilgi uyarılarını yönetme	67
Firewall korumasını yapılandırma	69
Programları ve izinleri yönetme	79
Bilgisayar bağlantılarını yönetme	85
Sistem hizmetlerini yönetme	93
Günlüğe kaydetme, izleme ve analiz	99
Internet güvenliği hakkında bilgi alma	109
McAfee Anti-Spam	111
Anti-Spam özellikleri.....	112
Spam algılamayı yapılandırma	113
E-posta filtreleme.....	121
Arkadaşları ayarlama	123
Web posta hesaplarınızı ayarlama	127
Filtrelenen e-posta ile çalışma	131
Phishing korumasını yapılandırma	133
McAfee Parental Controls.....	135
Ebeveyn Denetimleri özellikleri	136
Çevrimiçi ortamda çocuklarınızı koruma	137
Web'de bilgileri koruma	153
Parolaları koruma.....	155
McAfee Yedekleme ve Geri Yüklemesi	159
Backup and Restore özellikleri	160
Dosyaları arşivleme	161
Arşivlenen dosyalarla çalışma	171
McAfee QuickClean	177
QuickClean özellikleri	178
Bilgisayarınızı temizleme	179
Bilgisayarınızı birleştirme.....	183
Görev zamanlama	185

McAfee Shredder	191
Shredder zellikleri	192
Dosyaları, klasrleri ve diskleri paralama	192
McAfee Network Manager	195
Network Manager zellikleri	196
Network Manager simgeleri hakkında bilgi	197
Ynetilen bir ađ kurma	199
Ađı uzaktan ynetme	205
Ađlarınızı izleme	211
McAfee EasyNetwork	215
EasyNetwork zellikleri	216
EasyNetwork' ayarlama	217
Dosyaları paylařma ve gnderme	221
Yazıcıları paylařma	227
Başvuru	229

Szlk **230**

McAfee Hakkında **243**

Lisans	243
Telif Hakkı	244
Mřteri Desteđi ve Teknik Destek	245
McAfee Virtual Technician'ı kullanma	246

Dizin **256**

B Ö L Ü M 1

McAfee Total Protection

Bilgisayarınız için güvenliğin ötesinde bir öneme sahip Total Protection, çevrimiçi ortamda çalışırken veya oyun oynarken, siz ve aileniz için eksiksiz bir koruma sistemi sağlar. Total Protection'ı kullanarak bilgisayarınızı virüsler, korsanlar ve casus yazılımlardan koruyabilir; İnternet trafiğinde şüpheli etkinliği izleyebilir; ailenizin gizliliğini koruyabilir; riskli Web sitelerini engelleyebilir ve daha pek çok şey yapabilirsiniz.

Bu bölümde

McAfee SecurityCenter.....	5
McAfee VirusScan.....	29
McAfee Personal Firewall.....	61
McAfee Anti-Spam.....	111
McAfee Parental Controls.....	135
McAfee Yedekleme ve Geri Yükleme.....	159
McAfee QuickClean.....	177
McAfee Shredder.....	191
McAfee Network Manager.....	195
McAfee EasyNetwork.....	215
Başvuru.....	229
McAfee Hakkında.....	243
Müşteri Desteği ve Teknik Destek.....	245

B Ö L Ü M 2

McAfee SecurityCenter

McAfee SecurityCenter, bilgisayarınızın güvenlik durumunu izlemenize, bilgisayarınızdaki virüs, casus yazılım, e-posta ve güvenlik duvarı koruma hizmetlerinin güncel olup olmadığını anında öğrenmenize, olası güvenlik açıklarını düzeltmenize olanak verir. Bilgisayarınızda tüm koruma alanlarını koordine etmek ve yönetmek için gereksinim duyduğunuz gezinti araçlarını ve denetimlerini sağlar.

Bilgisayarınızın korumasını yapılandırmaya ve yönetmeye başlamadan önce, SecurityCenter arabirimini inceleyin ve korunma durumu, korunma kategorileri ve korunma hizmetleri arasındaki farkı bildiğinizden emin olun. Sonra McAfee tarafından sunulan en son korumaya sahip olmak için SecurityCenter'ı güncelleştirin.

Başlangıç yapılandırması görevlerini tamamlayınca, bilgisayarınızın korunma durumunu izlemek için SecurityCenter'ı kullanın. SecurityCenter bir sorun algırsa, sorunu çözmeniz veya yok saymanız (önem düzeyine göre) için sizi uyarır. Ayrıca olay günlüğünde, virüs taraması yapılandırma değişiklikleri gibi SecurityCenter olaylarını da inceleyebilirsiniz.

Not: SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde

SecurityCenter özellikleri.....	6
SecurityCenter'ı kullanma	7
Koruma sorunlarını onarma veya yok sayma.....	17
Uyarılarla çalışma	21
Olayları görüntüleme	27

SecurityCenter özellikleri

Basitleştirilmiş koruma durumu

Kolayca bilgisayarınızın korunma durumunu inceleyin, güncelleştirmeleri denetleyin ve korunma sorunlarını düzeltin.

Otomatik güncelleştirmeler ve yükseltmeler

SecurityCenter, programlarınız için güncelleştirmeleri otomatik olarak yükleyip kurar. Bir McAfee programının yeni sürümü çıktığında, aboneliğiniz geçerli olduğu sürece otomatik olarak bilgisayarınıza aktarılır ve böylece her zaman en güncel korumaya sahip olduğunuzdan emin olursunuz.

Gerçek zamanlı uyarılar

Güvenlik uyarıları, acil virüs saldırılarını ve güvenlik tehditlerini size bildirir.

B Ö L Ü M 3

SecurityCenter'ı kullanma

SecurityCenter'ı kullanmaya başlamadan önce, bilgisayarınızın korunma durumunu yönetmek için kullanacağınız bileşenleri ve yapılandırma alanlarını inceleyin. Bu görüntüde kullanılan terminoloji hakkında ayrıntılı bilgi için bkz. Koruma durumu hakkında bilgi (sayfa 8) ve Koruma kategorileri hakkında bilgi (sayfa 9). Sonra, McAfee hesabı bilgilerinizi inceleyebilir ve aboneliğinizin geçerliliğini doğrulayabilirsiniz.

Güncelleştir Düğmesi
SecurityCenter güncelleştirmelerini denetleyin ve yükleyin.

Tara Düğmesi
Bilgisayarınızda virüsleri, Truva atlarını ve diğer güvenlik tehditlerini tarayın (VirusScan yüklüyse).

Ortak Görevler
Giriş bölümüne dönün, son olayları görüntüleyin ve başka popüler görevler gerçekleştirin.

Yüklü Bileşenler Alanı
Bilgisayarınızın hangi McAfee programları tarafından korunduğunu öğrenin.

Gelişmiş Menü
Daha gelişmiş bir yapılandırma seçenekleri menüsüne geçin.

Koruma Durumu Alanı
Bilgisayarınızın genel koruma durumunu (kırmızı, sarı veya yeşil) izleyin ve koruma sorunlarını otomatik olarak düzeltin.

Koruma Kategorileri
Her kategorinin koruma durumunu (Korumalı, Dikkat, Eylem Gerekli) izleyin.

Koruma Kategorisi Bilgi Alanı
Bir kategorinin koruma hizmetlerini ve koruma sorunlarını görüntüleyin.

SecurityCenter Bilgi Alanı
Bilgisayarınızın en son ne zaman güncelleştirildiğini, en son taramanın ne zaman yapıldığını (VirusScan yüklüyse), aboneliğinizin süresinin ne zaman dolacağını ve kaç adet bilgisayar koruyabileceğinizi öğrenin.

Bu bölümde

Koruma durumu hakkında bilgi	8
Koruma kategorileri hakkında bilgi	9
Koruma hizmetleri hakkında bilgi.....	10
Aboneliklerinizi yönetme.....	11
SecurityCenter'ı güncelleştirme	13

Koruma durumu hakkında bilgi

Bilgisayarınızın koruma durumu, SecurityCenter Giriş bölümündeki koruma durumu alanında gösterilir. Burada, bilgisayarınızın en son güvenlik tehditlerinden tam olarak korunup korunmadığı ve dış güvenlik saldırıları, diğer güvenlik programları ve Internet'e erişebilen programlar gibi etkilere açık olup olmadığı belirtilir.

Bilgisayarınızın koruma durumu kırmızı, sarı veya yeşil olabilir.

Koruma Durumu	Açıklama
Kırmızı	<p>Bilgisayarınız korunmuyor. SecurityCenter Giriş bölümündeki koruma durumu alanı kırmızıdır ve korunmadığınızı belirtir. SecurityCenter, en az bir kritik güvenlik sorunu bildirir.</p> <p>Tam korumaya ulaşmak için her bir koruma kategorisindeki tüm kritik güvenlik sorunlarını düzeltmeniz gerekir (sorun kategorisinin durumu yine kırmızı renkte Eylem Gerekli seçeneğine ayarlıdır). Koruma sorunlarını düzeltme hakkında bilgi için bkz. Koruma sorunlarını onarma (sayfa 18).</p>
Sarı	<p>Bilgisayarınız kısmen korunuyor. SecurityCenter Giriş bölümündeki koruma durumu alanı sarıdır ve korunmadığınızı belirtir. SecurityCenter, en az bir kritik olmayan güvenlik sorunu bildirir.</p> <p>Tam korumaya ulaşmak için her bir koruma kategorisiyle ilişkili kritik olmayan güvenlik sorunlarını düzeltmeniz veya yok saymanız gerekir. Koruma sorunlarını düzeltme veya yok sayma hakkında bilgi için bkz. Koruma sorunlarını onarma veya yok sayma (sayfa 17).</p>
Yeşil	<p>Bilgisayarınız tam olarak korunuyor. SecurityCenter Giriş bölümündeki koruma durumu alanı yeşildir ve korunduğunuzu belirtir. SecurityCenter, kritik veya kritik olmayan güvenlik sorunu bildirmez.</p> <p>Her koruma kategorisinde, bilgisayarınızı koruyan hizmetler listelenir.</p>

Koruma kategorileri hakkında bilgi

SecurityCenter'ın koruma hizmetleri dört kategoriye ayrılır: Bilgisayar ve Dosyalar, İnternet ve Ağ, E-posta ve Anlık İleti, Ebeveyn Denetimleri. Bu kategoriler, bilgisayarınızı koruyan güvenlik hizmetlerine göz atmanıza ve bunları yapılandırmanıza yardımcı olur.

Koruma hizmetlerini yapılandırmak için bir kategori adını tıklayın ve varsa bu hizmetlerle ilgili algılanan güvenlik sorunlarını görüntüleyin. Bilgisayarınızın koruma durumu kırmızı veya sarı ise, bir veya birkaç kategoride *Eylem Gerekli* veya *Dikkat* iletisi görüntülenir; bu, SecurityCenter'ın bu kategori içinde bir sorun algıladığını gösterir. Koruma durumu hakkında ayrıntılı bilgi için bkz. Koruma durumu hakkında bilgi (sayfa 8).

Koruma Kategorisi	Açıklama
Bilgisayar ve Dosyalar	Bilgisayar ve Dosyalar kategorisi, şu koruma hizmetlerini yapılandırmanızı sağlar: <ul style="list-style-type: none"> Virüsten Koruma Casus Yazılımdan Koruma Sistem Koruması Windows Koruması PC Sağlığı
İnternet ve Ağ	İnternet ve Ağ kategorisi, şu koruma hizmetlerini yapılandırmanızı sağlar: <ul style="list-style-type: none"> Güvenlik Duvarı Koruması Phishing Koruması Kimlik Koruma
E-posta ve Anlık İleti	E-posta ve Anlık İleti kategorisi, şu koruma hizmetlerini yapılandırmanızı sağlar: <ul style="list-style-type: none"> E-Posta Virüsünden Koruma IM Virüsten Koruma E-Posta Casus Yazılımdan Koruma IM Casus Yazılımdan Koruma Spam'den Korunma
Ebeveyn Denetimleri	Ebeveyn Denetimleri kategorisi, şu koruma hizmetlerini yapılandırmanızı sağlar: <ul style="list-style-type: none"> İçerik Engelleme

Koruma hizmetleri hakkında bilgi

Koruma hizmetleri, bilgisayarınızı ve dosyalarınızı korumak için yapılandığımız çeşitli güvenlik bileşenleridir. Koruma hizmetleri, doğrudan McAfee programlarıyla ilişkilidir. Örneğin VirusScan yüklediğinizde, şu koruma hizmetlerini kullanabilirsiniz: Virus Protection, Spyware Protection, Sistem Koruması ve Komut Dosyası Tarama. Bu özel koruma hizmetleri hakkında ayrıntılı bilgi için VirusScan yardımına bakın.

Varsayılan olarak, bir programı yüklediğinizde bu programla ilişkili tüm koruma hizmetleri etkindir; ancak istediğiniz zaman koruma hizmetini devre dışı bırakabilirsiniz. Örneğin Ebeveyn Denetimleri yüklerseniz, İçerik Engelleme ve Kimlik Koruma etkindir. İçerik Engelleme koruma hizmetini kullanmayı düşünmüyorsanız, bunu tamamen devre dışı bırakabilirsiniz. Ayrıca ayar veya bakım görevleri gerçekleştirirken de bir koruma hizmetini geçici olarak devre dışı bırakabilirsiniz.

Aboneliklerinizi yönetme

Satın aldığımız her McAfee koruma ürünü, ürünü belli bir süre boyunca belirli sayıda bilgisayarda kullanmanızı sağlayan bir abonelikte birlikte gelir. Aboneliğinizin süresi satın aldığımız ürüne göre değişir, ancak genellikle ürününüzü etkinleştirdiğinizde başlar. Etkinleştirme basit ve ücretsiz bir işlemdir (yalnızca Internet bağlantınızın olması yeterlidir), ancak size bilgisayarınızı en son tehditlerden koruyan düzenli ve otomatik ürün güncelleştirmeleri alma hakkı tanıdığı için son derece önemlidir.

Etkinleştirme, normalde ürün yüklendiği zaman gerçekleşir, ancak beklemeye karar verirsiniz (örneğin Internet bağlantınız olmadığı için) etkinleştirme için 15 gün süreniz vardır. 15 gün içinde etkinleştirmeszeniz, ürünleriniz artık kritik güncelleştirmeleri almaz veya taramalar gerçekleştirmez. Ayrıca aboneliğinizin süresi sona ermeye yaklaştığında size bunu düzenli aralıklarla (ekran iletileriyle) bildiririz. Bu yolla, aboneliğinizi erkenden yenileyerek veya Web sitemizde otomatik yenilemeyi ayarlayarak, korumanızda kesinti olmasını önleyebilirsiniz.

SecurityCenter'da etkinleştirmenizi isteyen bir bağlantı görürseniz, aboneliğiniz henüz etkinleştirilmemiş demektir. Aboneliğinizin süresinin ne zaman dolacağını görmek için Hesabım sayfanızı denetleyebilirsiniz.

McAfee hesabınıza erişme

McAfee hesap bilgilerinize (Hesabım sayfanız), SecurityCenter'dan kolayca erişebilirsiniz.

- 1 **Ortak Görevler** altında **Hesabım**'ı tıklatın.
- 2 McAfee hesabınızda oturumu açın.

Ürününüzü etkinleştirme


Etkinleştirme normalde ürününüzü yüklediğinizde gerçekleşir. Ancak gerçekleşmezse, SecurityCenter'da etkinleştirmenizi isteyen bir bağlantı görürsünüz. Ayrıca bunu size düzenli olarak bildiririz.

- SecurityCenter Giriş bölümünde **SecurityCenter Bilgisi** altında **Lütfen aboneliğinizi etkinleştirin**'i tıklatın.

İpucu: Düzenli olarak görüntülenen uyarıdan da etkinleştirebilirsiniz.

Aboneliğinizi doğrulama

Süresinin sona ermediğinden emin olmak için aboneliğinizi doğrularsınız.

- Görev çubuğunun sağ ucundaki bildirim alanında bulunan SecurityCenter simgesini  sağ tıklatın ve sonra **Aboneliği Doğrula**'yı tıklatın.

Aboneliđinizi yenileme

Aboneliđinizin süresi dolmadan kısa bir süre önce, SecurityCenter'da yenilemenizi isteyen bir bağlantı görürsünüz. Ayrıca yaklaşan süre sonunu size uyarılarla düzenli olarak bildiririz.

- SecurityCenter Giriş bölümünde **SecurityCenter Bilgisi** altında **Yenile**'yi tıkladın.

İpucu: Ürününüzü düzenli olarak görüntülenen bildirim iletisinden de yenileyebilirsiniz. Ayrıca Hesabım sayfanıza giderek yenileyebilir veya otomatik yenilemeyi ayarlayabilirsiniz.

B Ö L Ü M 4

SecurityCenter'ı güncelleştirme

SecurityCenter, dört saatte bir çevrimiçi güncelleştirmeleri denetleyip yükleyerek, kayıtlı McAfee programlarınızın güncel olmasını sağlar. yüklediğiniz veya etkinleştirdiğiniz programlara bağlı olarak, çevrimiçi güncelleştirmeler en son virüs tanımlarını ve korsan, spam, casus yazılım veya gizlilik koruması yükseltmelerini içerebilir. Varsayılan dört saatlik süre içinde güncelleştirmeleri denetlemek istiyorsanız, bunu istediğiniz zaman yapabilirsiniz. SecurityCenter güncelleştirmeleri denetlerken, siz başka görevler gerçekleştirmeye devam edebilirsiniz.

Bu önerilmesine de, SecurityCenter'ın güncelleştirmeleri denetleme ve yükleme biçimini değiştirebilirsiniz. Örneğin, SecurityCenter'ı güncelleştirmeleri yükleyecek ancak kurmayacak ya da güncelleştirmeleri yüklemeyen veya kurmadan önce size bildirecek şekilde yapılandırabilirsiniz. Ayrıca otomatik güncelleştirmeyi devre dışı bırakabilirsiniz.

Not: McAfee Ürününüzü CD'den yüklediyseniz, 15 gün içinde etkinleştirmeniz gerekir; aksi halde ürünleriniz kritik güncelleştirmeleri almaz veya taramalar gerçekleştirmez.


Bu bölümde

Güncelleştirmeleri denetleme.....	13
Otomatik güncelleştirmeleri yapılandırma.....	14
Otomatik güncelleştirmeleri devre dışı bırakma	15

Güncelleştirmeleri denetleme

Varsayılan olarak, bilgisayarınız Internet'e bağlı olduğunda, SecurityCenter dört saatte bir güncelleştirmeleri otomatik olarak denetler; ancak dört saatlik süre içinde güncelleştirmeleri denetlemek isterseniz, bunu yapabilirsiniz. Otomatik güncelleştirmeleri devre dışı bıraktıysanız, güncelleştirmeleri düzenli olarak denetlemek sizin sorumluluğunuzdadır.

- SecurityCenter Giriş bölümünde **Güncelleştir**'i tıklatın.

İpucu: Görev çubuğunun sağ ucundaki bildirim alanında bulunan SecurityCenter simgesini  sağ tıklayıp, ardından **Güncelleştirmeler**'i tıklayarak, SecurityCenter'ı başlatmadan güncelleştirmeleri denetleyebilirsiniz.

Otomatik gncelleřtirmeleri yapılandırma

Varsayılan olarak, bilgisayarınız İnternet'e baęlı olduęunda, SecurityCenter drt saatte bir gncelleřtirmeleri otomatik olarak denetler ve ykler. Bu varsayılan davranıřı deęiřtirmek isterseniz, gncelleřtirmeleri otomatik olarak ykleyip ardından gncelleřtirmeler kurulmak zere hazır olunca size bunu bildirecek veya gncelleřtirmeleri yklemeden nce bildirecek řekilde SecurityCenter'ı yapılandırabilirsiniz.

Not: Gncelleřtirmeler karřıdan yklenmek veya kurulmak zere hazır olunca, SecurityCenter uyarıları kullanarak bunu size bildirir. Uyarılardan gncelleřtirmeleri ykleyebilir veya kurabilir ya da gncelleřtirmeleri erteleyebilirsiniz. Programlarınızı uyarıdan gncelleřtirince, gncelleřtirmeyi ykleyip kurmadan nce abonelięinizi doęrulamanız istenebilir. Ayrıntılı bilgi iin bkz. Uyarılarla alıřma (sayfa 21).

- 1** SecurityCenter Yapılandırma blmesini aın.
Nasıl?
 1. **Ortak Grevler** blmnde **Giriř**'i tıklatın.
 2. Saędaki blmede, **SecurityCenter Bilgisi** altında **Yapılandır**'ı tıklatın.
- 2** SecurityCenter Yapılandırma blmesinde, **Otomatik gncelleřtirmeler devre dıřı** altında **Aık**'ı ve sonra **Geliřmiř**'i tıklatın.
- 3** Ařaęıdaki dęmelerden birini tıklatın:
 - **Gncelleřtirmeler otomatik olarak ykle ve hizmetlerim gncelleřtirildięinde bana bildir (nerilir)**
 - **Gncelleřtirmeleri otomatik olarak karřıdan ykle ve yklemeye hazır olduęunda bana bildir**
 - **Gncelleřtirmeleri karřıdan yklemeden nce bana bildir**
- 4** **Tamam**'ı tıklatın.

Otomatik gncelleřtirmeleri devre dıřı bırakma

Otomatik gncelleřtirmeleri devre dıřı bırakırsanız, gncelleřtirmeleri dzenli olarak denetlemek sizin sorumluluęunuzdadır; aksi halde, bilgisayarınızda en son gvenlik koruması olmaz. Gncelleřtirmeleri el ile denetleme hakkında ayrıntılı bilgi iin bkz. Gncelleřtirmeleri denetleme (sayfa 13).

1 SecurityCenter Yapılandırma blmesini aın.

Nasıl?

1. **Ortak Grevler** blmnde **Giriř**'i tıklatın.
2. Saędaki blmede, **SecurityCenter Bilgisi** altında **Yapılandır**'ı tıklatın.

2 SecurityCenter Yapılandırma blmesinde, **Otomatik gncelleřtirmeler etkin** altında **Kapalı**'yı tıklatın.

3 Onay iletiřim kutusunda **Evet**'i tıklatın.

İpucu: **Aık** dęmesini tıklatarak veya Gncelleřtirme Seenekleri blmesinde **Otomatik gncelleřtirmeyi devreden ıkar ve gncelleřtirmeleri el ile denetlememe izin ver**'in iřaretini kaldırarak otomatik gncelleřtirmeleri etkinleřtirirsiniz.

B Ö L Ü M 5

Koruma sorunlarını onarma veya yok sayma

SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Kritik sorunlarla hemen ilgilenilmesi gerekir ve bunlar koruma durumunuzu tehlikeye atar (rengi kırmızıya dönüşür). Kritik olmayan sorunlarla hemen ilgilenilmesi gerekmez ve bunlar koruma durumunuzu tehlikeye atabilir veya atmayabilir (sorunun türüne göre). Yeşil koruma durumuna ulaşmak için tüm kritik sorunları düzeltmeniz ve tüm kritik olmayan sorunları düzeltmeniz veya yok saymanız gerekir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz. McAfee Virtual Technician hakkında ayrıntılı bilgi için McAfee Virtual Technician yardımına bakın.

Bu bölümde

Koruma sorunlarını onarma	18
Koruma sorunlarını yok sayma	19

Koruma sorunlarını onarma

Güvenlik sorunlarının çoğu otomatik olarak düzeltilebilir; ancak bazı sorunlarla sizin ilgilenmeniz gerekebilir. Örneğin Güvenlik Duvarı Koruması devre dışıysa, SecurityCenter bunu otomatik olarak etkinleştirebilir; ancak Güvenlik Duvarı Koruması yüklü değilse bunu yüklemeniz gerekir. Aşağıdaki tabloda, koruma sorunlarını el ile düzeltirken gerçekleştirebileceğiniz diğer bazı eylemler açıklanmaktadır:

Sorun	Eylem
Son 30 gün içinde bilgisayarınızda tam tarama yapılmadı.	Bilgisayarınızı el ile tarayın. Ayrıntılı bilgi için VirusScan yardımına bakın.
Algılama imza dosyalarınız (DAT) eski.	Korumanızı el ile güncelleştirin. Ayrıntılı bilgi için VirusScan yardımına bakın.
Bir program yüklü değil.	Programı McAfee Web sitesinden veya CD'den yükleyin.
Bir programın bileşenleri eksik.	Programı McAfee Web sitesinden veya CD'den yeniden yükleyin.
Bir program etkinleştirilmemiş ve tam koruma alamıyor.	Programı McAfee Web sitesinde etkinleştirin.
Aboneliğiniz sona erdi.	Hesap durumunuzu McAfee Web sitesinde denetleyin. Ayrıntılı bilgi için bkz. Aboneliklerinizi yönetme (sayfa 11).

Not: Genellikle bir tek koruma sorunu birden çok koruma kategorisini etkiler. Bu durumda, sorunu bir kategoride düzelttiğinizde, bu sorun diğer tüm kategorilerden silinir.

Koruma sorunlarını otomatik olarak onarma

SecurityCenter, koruma sorunlarının çoğunu otomatik olarak düzeltebilir. SecurityCenter'ın koruma sorunlarını otomatik olarak düzeltirken yaptığı yapılandırma değişiklikleri, olay günlüğüne kaydedilmez. Olaylar hakkında ayrıntılı bilgi için bkz. Olayları görüntüleme (sayfa 27).

- 1 **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
- 2 SecurityCenter Giriş bölümünde, koruma durumu alanında **Onar**'ı tıklatın.

Koruma sorunlarını el ile onarma

Otomatik olarak düzeltmeyi denedikten sonra bir veya birkaç koruma sorunu devam ederse, bunları el ile düzeltebilirsiniz.

- 1 **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
- 2 SecurityCenter Giriş bölümünde, SecurityCenter'ın sorunu bildirdiği koruma kategorisini tıklatın.
- 3 Sorun açıklamasının yanındaki bağlantıyı tıklatın.

Koruma sorunlarını yok sayma

SecurityCenter kritik olmayan bir sorun algılırsa, bunu düzeltebilir veya yok sayabilirsiniz. Diğer kritik olmayan sorunlar (örneğin, Anti-Spam veya Ebeveyn Denetimleri yüklü değilse) otomatik olarak yok sayılır. Bilgisayarınızın koruma durumu yeşil olmadığı sürece, yok sayılan sorunlar SecurityCenter Giriş bölümündeki koruma kategorisi alanında gösterilmez. Bir sorunu önce yok sayıp, daha sonra bilgisayarınızın koruma durumu yeşil olmasa bile bunun koruma kategorisi bilgi alanında görüntülenmesini istediğinize karar verirsiniz, yok sayılan sorunu gösterebilirsiniz.

Koruma sorununu yok sayma

SecurityCenter kritik olmayan bir sorun algılırsa ve bunu düzeltmeyi düşünmüyorsanız yok sayabilirsiniz. Yok saydığımızda, sorun SecurityCenter'da koruma kategorisi bilgi alanından kaldırılır.

- 1 **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
- 2 SecurityCenter Giriş bölümünde, sorunun bildirildiği koruma kategorisini tıklatın.
- 3 Koruma sorununun yanındaki **Yoksay** bağlantısını tıklatın.

Yok sayılan sorunları gösterme veya gizleme

Önem düzeyine bağlı olarak, yok sayılan koruma sorununu gösterebilir veya gizleyebilirsiniz.

- 1 Uyarı Seçenekleri bölümünü açın.
Nasıl?
 1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. Sağdaki bölmede, **SecurityCenter Bilgisi** altında **Yapılandır**'i tıklatın.
 3. **Uyarılar** altında **Gelişmiş**'i tıklatın.
- 2 SecurityCenter Yapılandırma bölümünde **Yoksayılan Sorunlar**'i tıklatın.
- 3 Yoksayılan Sorunlar bölümünde aşağıdakileri yapın:
 - Bir sorunu yok saymak için onay kutusunu işaretleyin.
 - Koruma kategorisi bilgi alanında bir sorunu bildirmek için onay kutusunun işaretini kaldırın.
- 4 **Tamam**'i tıklatın.

İpucu: Koruma kategorisi bilgi alanında bildirilen sorunun yanındaki **Yoksay** bağlantısını tıklatarak da sorunu yok sayabilirsiniz.

B Ö L Ü M 6

Uyarılarla çalışma

Uyarılar, belirli SecurityCenter olayları gerçekleştiğinde, ekranınızın sağ alt köşesinde açılan küçük iletişim kutularıdır. Uyarı, olay hakkında ayrıntılı bilgilerin yanı sıra, olayla ilişkili olabilecek sorunları çözmeye yönelik öneriler ve seçenekler de sağlar. Bazı uyarılar, olayla ilgili ek bilgilere bağlantılar da içerir. Bu bağlantılar, McAfee'nin genel Web sitesini açmanızı veya sorunu gidermek için McAfee'ye bilgi göndermenizi sağlar.

Üç tür uyarı vardır: kırmızı, sarı ve yeşil.

Uyarı Türü	Açıklama
Kırmızı	Kırmızı uyarı, sizden yanıt vermenizi isteyen kritik bir bildirimdir. SecurityCenter koruma sorununun otomatik olarak nasıl çözüleceğini belirleyemediği zaman kırmızı uyarılar oluşur.
Sarı	Sarı uyarı, genellikle sizden yanıt vermenizi isteyen kritik olmayan bir bildirimdir.
Yeşil	Yeşil uyarı, genellikle sizden yanıt vermenizi istemeyen kritik olmayan bir bildirimdir. Yeşil uyarılar, olayla ilgili temel bilgiler verir.

Uyarılar koruma durumunuzun izlenmesi ve yönetilmesinde çok önemli bir rol oynadığı için bunları devre dışı bırakamazsınız. Ancak belirli bilgi uyarılarının görüntülenip görüntülenmemesini kontrol edebilir ve diğer bazı uyarı seçeneklerini yapılandırabilirsiniz (SecurityCenter'ın uyarıyla birlikte ses çıkarıp çıkarmayacağı veya başlangıçta McAfee giriş ekranını görüntüleyip görüntülemeyeceği gibi).

Bu bölümde

Bilgi uyarılarını gösterme ve gizleme	22
Uyarı seçeneklerini yapılandırma	23

Bilgi uyarılarını gösterme ve gizleme

Bilgi uyarıları, bilgisayarınızın güvenliğini tehdit etmeyen olaylar olduğunda bunu size bildirir. Örneğin, Güvenlik Duvarı korumasını ayarladıysanız, bilgisayarınızdaki bir programa Internet erişimi verildiğinde varsayılan olarak bilgi uyarısı görüntülenir. Belirli bir bilgi uyarısı türünün görüntülenmesini istemiyorsanız bunu gizleyebilirsiniz. Hiçbir bilgi uyarısının görüntülenmesini istemiyorsanız tümünü gizleyebilirsiniz. Bilgisayarınızda tam ekran modunda oyun oynarken de tüm bilgi uyarılarını gizleyebilirsiniz. Oyununuz bitince tam ekran modundan çıktığınızda, SecurityCenter bilgi uyarılarını yeniden görüntülemeye başlar.

Bir bilgi uyarısını yanlışlıkla gizlediyseniz, bunu istediğiniz zaman yeniden gösterebilirsiniz. Varsayılan olarak, SecurityCenter tüm bilgi uyarılarını gösterir.

Bilgi uyarılarını gösterme veya gizleme

SecurityCenter'ı, bazı bilgi uyarılarını gösterecek veya gizleyecek ya da tüm bilgi uyarılarını gizleyecek şekilde yapılandırabilirsiniz.

1 Uyarı Seçenekleri bölmesini açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
2. Sağdaki bölmede, **SecurityCenter Bilgisi** altında **Yapılandır**'ı tıklatın.
3. **Uyarılar** altında **Gelişmiş**'i tıklatın.

2 SecurityCenter Yapılandırma bölmesinde **Bilgi Uyarıları**'ni tıklatın.

3 Bilgi Uyarıları bölmesinde aşağıdakileri yapın:

- Bir bilgi uyarısını göstermek için onay kutusunu temizleyin.
- Bir bilgi uyarısını gizlemek için onay kutusunu işaretleyin.
- Tüm bilgi uyarılarını gizlemek için **Bilgi uyarılarını gösterme** onay kutusunu işaretleyin.

4 **Tamam**'ı tıklatın.

İpucu: Uyarının içinden **Bu uyarıyı bir daha gösterme** onay kutusunu işaretleyerek de bilgi uyarısını gizleyebilirsiniz. Bunu yaptığımızda, Bilgi Uyarıları bölmesinde uygun onay kutusunun işaretini kaldırarak, bilgi uyarısını yeniden gösterebilirsiniz.

Oyun oynarken bilgi uyarılarını gösterme veya gizleme

Bilgisayarınızda tam ekran modunda oyun oynarken de bilgi uyarılarını gizleyebilirsiniz. Oyununuz bitince tam ekran modundan çıktığınızda, SecurityCenter bilgi uyarılarını yeniden görüntülemeye başlar.

- 1 Uyarı Seçenekleri bölmesini açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. Sağdaki bölmede, **SecurityCenter Bilgisi** altında **Yapılandır**'i tıklatın.
 3. **Uyarılar** altında **Gelişmiş**'i tıklatın.
- 2 Uyarı Seçenekleri bölümünde **Oyun modu algılandığında bilgilendirme uyarılarını göster** onay kutusunu işaretleyin veya işaretini kaldırın.
 - 3 **Tamam**'i tıklatın.

Uyarı seçeneklerini yapılandırma

Uyarıların görünümü ve sıklığı, SecurityCenter tarafından yapılandırılır; ancak bazı temel uyarı seçeneklerini ayarlayabilirsiniz. Örneğin, uyarılarla birlikte sesi açabilir veya Windows başlatıldığında giriş ekranı uyarısının görüntülenmesini engelleyebilirsiniz. Size çevrimiçi topluluktaki virüs saldırılarını ve diğer güvenlik tehditlerini bildiren uyarıları da gizleyebilirsiniz.

Uyarılarla birlikte sesi açma

Uyarının size sesle birlikte bildirilmesini istiyorsanız, her uyarıyla birlikte ses çıkarması için SecurityCenter'ı yapılandırabilirsiniz.

- 1 Uyarı Seçenekleri bölmesini açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. Sağdaki bölmede, **SecurityCenter Bilgisi** altında **Yapılandır**'i tıklatın.
 3. **Uyarılar** altında **Gelişmiş**'i tıklatın.
- 2 Uyarı Seçenekleri bölümünde, **Ses** altında **Bir uyarı oluştuğunda ses çal** onay kutusunu işaretleyin.

Başlangıçta giriş ekranını gizleme

Varsayılan olarak, Windows başlatıldığında, SecurityCenter'ın bilgisayarınızı koruduğunu size bildiren McAfee giriş ekranı kısaca görüntülenir. Ancak bunun görüntülenmesini istemiyorsanız giriş ekranını gizleyebilirsiniz.

1 Uyarı Seçenekleri bölmesini açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
2. Sağdaki bölmede, **SecurityCenter Bilgisi** altında **Yapılandır**'ı tıklatın.
3. **Uyarılar** altında **Gelişmiş**'i tıklatın.

2 Uyarı Seçenekleri bölmesinde, **Giriş Ekranı** altında **Windows başlangıcında McAfee giriş ekranını göster** onay kutusunun işaretini kaldırın.

İpucu: **Windows başlangıcında McAfee giriş ekranını göster** onay kutusunu işaretleyerek, istediğiniz zaman giriş ekranını yeniden gösterebilirsiniz.

Virüs saldırısı uyarılarını gizleme

Size çevrimiçi topluluktaki virüs saldırılarını ve diğer güvenlik tehditlerini bildiren uyarıları gizleyebilirsiniz.

1 Uyarı Seçenekleri bölmesini açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
2. Sağdaki bölmede, **SecurityCenter Bilgisi** altında **Yapılandır**'ı tıklatın.
3. **Uyarılar** altında **Gelişmiş**'i tıklatın.

2 Uyarı Seçenekleri bölmesinde **Virüs veya güvenlik tehditi oluştuğunda beni uyar** onay kutusunun işaretini kaldırın.

İpucu: **Virüs veya güvenlik tehditi oluştuğunda beni uyar** onay kutusunu işaretleyerek, istediğiniz zaman virüs saldırısı uyarılarını yeniden gösterebilirsiniz.

Güvenlik iletilerini gizleme

Ev ağınızda daha fazla bilgisayarı koruma hakkındaki güvenlik bildirimlerini gizleyebilirsiniz. Bu iletiler aboneliğiniz, aboneliğinizle koruyabileceğiniz bilgisayarların sayısı ve kapsamını genişletme daha fazla bilgisayarı koruyacak şekilde aboneliğinizin hakkında bilgiler sağlar.

1 Uyarı Seçenekleri bölmesini açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
2. Sağdaki bölmede, **SecurityCenter Bilgisi** altında **Yapılandır**'ı tıklatın.
3. **Uyarılar** altında **Gelişmiş**'i tıklatın.

2 Uyarı Seçenekleri bölümünde **Virüs önerilerini veya diğer güvenlik iletilerini göster** onay kutusunun işaretini kaldırın.

İpucu: **Virüs önerilerini veya diğer güvenlik iletilerini göster** onay kutusunu işaretleyerek, istediğiniz zaman bu güvenlik iletilerini gösterebilirsiniz.

B Ö L Ü M 7

Olayları görüntüleme

Olay, koruma kategorisinde ve ilişkili koruma hizmetlerinde gerçekleşen eylem veya yapılandırma değişikliğidir. Farklı koruma hizmetleri, farklı türde olayları kaydeder. Örneğin, bir koruma hizmeti etkinleştirilir veya devre dışı bırakılırsa, SecurityCenter olay kaydeder; Virus Protection, virüs algılandığında ve kaldırıldığında olay kaydeder; Firewall Protection ise, Internet'e bağlanma denemesi engellendiğinde olay kaydeder. Koruma kategorileri hakkında ayrıntılı bilgi için bkz. Koruma kategorileri hakkında bilgi (sayfa 9).

Yapılandırma sorunlarını giderirken ve başka kullanıcılar tarafından gerçekleştirilen işlemleri incelerken olayları görüntüleyebilirsiniz. Pek çok ebeveyn, çocuklarının Internet'teki davranış biçimini izlemek için olay günlüğünü kullanır. Yalnızca gerçekleşen en son 30 olayı incelemek istiyorsanız son olayları görüntülersiniz. Gerçekleşen tüm olayların kapsamlı listesini incelemek istiyorsanız tüm olayları görüntülersiniz. Tüm olayları görüntülediğinizde, SecurityCenter olayları gerçekleştikleri koruma kategorisine göre sıralayan olay günlüğünü başlatır.

Bu bölümde

Son olayları görüntüleme	27
Tüm olayları görüntüleme	27

Son olayları görüntüleme

Yalnızca gerçekleşen en son 30 olayı incelemek istiyorsanız son olayları görüntülersiniz.

- **Ortak Görevler** altında **Son Olayları Görüntüle**'yi tıklatın.

Tüm olayları görüntüleme

Gerçekleşen tüm olayların kapsamlı listesini incelemek istiyorsanız tüm olayları görüntülersiniz.

- 1 Ortak Görevler** altında **Son Olayları Görüntüle**'yi tıklatın.
- 2 Son Olaylar** bölümünde **Günlüğü Görüntüle**'yi tıklatın.
- 3 Olay günlüğünün** soldaki bölümünde, görüntülemek istediğiniz olay türlerini tıklatın.

B Ö L Ü M 8

McAfee VirusScan

VirusScan'in gelişmiş algılama ve koruma hizmetleri, sizi ve bilgisayarınızı virüsler, Truva atları, izleme tanımlama bilgileri, casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programlar gibi en son güvenlik tehditlerinden korur. Koruma, masaüstü bilgisayarınızdaki dosya ve klasörlerin ötesine geçerek, e-posta, anlık iletiler ve Web gibi farklı giriş noktalarından gelen tehditleri hedefler.

VirusScan ile bilgisayarınızda anında ve sürekli koruma sağlanır (zahmetli yönetim gerekmez). Siz çalışırken, oyun oynarken, Web'de gezinirken veya e-postanızı kontrol ederken, program arka planda çalışır ve olası zararları gerçek zamanlı izler, tarar ve algılar. Kapsamlı taramalar zamanlamaya göre çalışır ve birtakım gelişmiş seçenekler kullanarak bilgisayarınızı düzenli olarak denetler. VirusScan, isterseniz size bu davranışı özelleştirme esnekliği sağlar; ancak özelleştirme yapmasanız da bilgisayarınız korunur.

Normal bilgisayar kullanımı sırasında virüsler, solucanlar ve diğer olası tehditler bilgisayarınıza sızabilir. VirusScan, bu durumda size tehdidi bildirir ve genellikle bunu sizin için ele alarak herhangi bir zarara yol açmadan virüs bulaşan öğeleri temizler veya karantinaya alır. Nadiren daha fazla işlem gerekebilir. VirusScan, bu tür durumlarda ne yapılması gerektiğine (bilgisayarınızı bir daha başlattığınızda yeniden tarama yapmak, algılanan öğeyi saklamak veya algılanan öğeyi kaldırmak) karar vermenize olanak tanır.

Not: SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde

VirusScan özellikleri.....	30
Bilgisayarınızı tarama.....	31
Tarama sonuçlarıyla çalışma.....	35
Tarama türleri.....	38
Ek koruma kullanma.....	41
Virüsten korumayı ayarlama.....	45

VirusScan özellikleri

Kapsamlı virüsten koruma

Kendinizi ve bilgisayarınızı virüsler, Truva atları, izleme tanımlama bilgileri, casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programlar gibi tehditlere karşı savunun. Koruma, masaüstü bilgisayarınızdaki dosya ve klasörlerin ötesine geçerek, e-posta, anlık iletiler ve Web gibi farklı giriş noktalarından gelen tehditleri hedefler. Zahmetli yönetim gerektirmez.

Kaynakları bilen tarama seçenekleri

İsterseniz tarama seçeneklerini özelleştirin ancak özelleştirme yapmasanız da bilgisayarınız korunur. Tarama hızı yavaşlarsa, minimum bilgisayar kaynağının kullanılması için seçeneği devre dışı bırakabilirsiniz; ancak virüs korumasına diğer görevlerden daha fazla öncelik tanınacağını unutmayın.

Otomatik düzeltmeler

VirusScan tarama çalıştırırken bir güvenlik tehdidi algırsa, tehdit türüne göre tehdidi otomatik olarak ele almayı dener. Bu yolla, pek çok tehdit algılanabilir ve sizin müdahaleniz olmadan etkisiz hale getirilebilir. Nadiren VirusScan tehdidi kendi başına etkisiz hale getiremeyebilir. VirusScan, bu tür durumlarda ne yapılması gerektiğine (bilgisayarınızı bir daha başlattığınızda yeniden tarama yapmak, algılanan öğeyi saklamak veya algılanan öğeyi kaldırmak) karar vermenize olanak tanır.

Tam ekran modunda görevleri duraklatma

Film izlemek, bilgisayarınızda oyun oynamak gibi etkinliklerin veya bilgisayar ekranınızın tamamını kaplayan herhangi bir etkinliğin keyfini çıkarırken, VirusScan el ile taramalar gibi çeşitli görevleri duraklatır.

B Ö L Ü M 9

Bilgisayarınızı tarama

SecurityCenter'ı ilk kez başlatmadan önce bile, VirusScan'in gerçek zamanlı virüsten koruması, bilgisayarınızı olası zararlı virüslerden, Truva atlarından ve diğer güvenlik tehditlerinden korumaya başlar. Gerçek zamanlı virüsten korumayı devre dışı bırakmadığınız sürece, VirusScan ayarladığımız gerçek zamanlı tarama seçeneklerini kullanarak, siz veya bilgisayarınız dosyalara erişince bunları tarar ve bilgisayarınızda virüs etkinliğini sürekli izler. Bilgisayarınızın en son güvenlik tehditlerine karşı korunduğundan emin olmak için gerçek zamanlı virüsten korumayı açık bırakın ve düzenli, daha kapsamlı el ile taramalar için zamanlama yapın. Tarama seçeneklerini ayarlama hakkında ayrıntılı bilgi için bkz. Virüsten korumayı ayarlama (sayfa 45).

VirusScan, düzenli aralıklarla daha kapsamlı taramalar çalıştırmanıza olanak vererek, virüsten korumaya yönelik daha ayrıntılı tarama seçenekleri sunar. SecurityCenter'dan tam, hızlı, özel veya zamanlanmış tarama çalıştırabilirsiniz. El ile taramaları, çalıştığınız sırada Windows Gezgini'nden de çalıştırabilirsiniz. SecurityCenter'da tarama yapmak, tarama seçeneklerini anında değiştirme avantajı sağlar. Windows Gezgini'nden tarama yapmak ise bilgisayar güvenliği açısından rahat bir yaklaşım sunar.

Taramayı ister SecurityCenter'dan isterseniz Windows Gezgini'nden çalıştırın, işlem tamamlandığında tarama sonuçlarını görüntüleyebilirsiniz. VirusScan'in virüs, Truva atı, casus yazılım, reklam yazılım, tanımlama bilgisi ve başka olası istenmeyen program algılayıp algılamadığını, onarıp onarmadığını veya karantinaya alıp almadığını belirlemek için tarama sonuçlarını görüntülersiniz. Tarama sonuçları farklı yollarla görüntülenebilir. Örneğin, tarama sonuçlarının temel özetini veya virüs bulaşma durumu ve türü gibi ayrıntılı bilgileri görüntüleyebilirsiniz. Ayrıca, genel tarama ve algılama istatistiklerini de görüntüleyebilirsiniz.

Bu bölümde

PC'nizi tarama	32
Tarama sonuçlarını görüntüleme.....	34

PC'nizi tarama

VirusScan, gerçek zamanlı tarama (PC'nizde sürekli tehdit etkinliğini izleyen), Windows Gezgini'nden el ile tarama ve SecurityCenter'dan tam, hızlı, özel veya zamanlanmış tarama gibi eksiksiz bir dizi tarama seçeneği sağlar.

Bunu yapmak için...	Bunu yapın...
Siz veya bilgisayarınız dosyalara erişince bunları tarayarak, bilgisayarınızda virüs etkinliğini sürekli izlemek için Gerçek zamanlı taramayı başlatmak	<p>1. Bilgisayar ve Dosyalar Yapılandırma bölümünü açın.</p> <p>Nasıl?</p> <ol style="list-style-type: none"> 1. Soldaki bölmede Gelişmiş Menü'yü tıklayın. 2. Yapılandır'ı tıklayın. 3. Yapılandır bölümünde Bilgisayar ve Dosyalar'ı tıklayın. <p>2. Virüsten koruma altında Açık'ı tıklayın.</p> <p>Not: Gerçek zamanlı tarama varsayılan olarak etkindir.</p>
Bilgisayarınızda tehditleri hızla denetlemek için Hızlı Tarama başlatmak	<ol style="list-style-type: none"> 1. Temel menüde Tara'yı tıklayın. 2. Tarama Seçenekleri bölümünde Hızlı Tarama altında Başlat'ı tıklayın.
Bilgisayarınızda tehditleri kapsamlı olarak denetlemek için Tam Tarama başlatmak	<ol style="list-style-type: none"> 1. Temel menüde Tara'yı tıklayın. 2. Tarama Seçenekleri bölümünde Tam Tarama altında Başlat'ı tıklayın.
Ayarlarınızı temel alan bir Özel Tarama başlatmak	<ol style="list-style-type: none"> 1. Temel menüde Tara'yı tıklayın. 2. Tarama Seçenekleri bölümünde Ben Seçeceğim altında Başlat'ı tıklayın. 3. Şunları işaretleyerek veya işaretini kaldırarak taramayı özelleştirin: <ul style="list-style-type: none"> Dosyalardaki Tüm Tehditler Bilinmeyen Virüsler Arşiv Dosyaları Casus Yazılımlar ve Olası Tehditler İzleme Tanımlama Bilgileri Görünmez Programlar 4. Başlat'ı tıklayın.

Bunu yapmak için...	Bunu yapın...
Dosyalarda, klasörlerde veya sürücülerde tehditleri denetlemek için El İle Tarama başlatmak	<ol style="list-style-type: none"> 1. Windows Gezgin'i açın. 2. Dosyayı, klasörü veya sürücüyü sağ tıklayın ve sonra Tara'yı tıklayın.
Bilgisayarınızda tehditleri düzenli aralıklarla taramak için Zamanlanan Tarama başlatmak	<ol style="list-style-type: none"> 1. Zamanlanan Tarama bölümünü açın. Nasıl? <ol style="list-style-type: none"> 1. Ortak Görevler bölümünde Giriş'i tıklayın. 2. SecurityCenter Giriş bölümünde Bilgisayar ve Dosyalar'ı tıklayın. 3. Bilgisayar ve Dosyalar bilgi alanında Yapılandır'ı tıklayın. 4. Bilgisayar ve Dosyalar Yapılandırma bölümünde, virüsten korumanın etkin olduğundan emin olun ve Gelişmiş'i tıklayın. 5. Virüsten Koruma bölümünde Zamanlanan Tarama'yı tıklayın. 2. Zamanlanan taramayı etkinleştir'i seçin. 3. Normalde tarama işlemi için kullanılan işlemci miktarını azaltmak için En az bilgisayar kaynağı kullanarak tara'yı seçin. 4. Bir veya birkaç gün seçin. 5. Başlangıç zamanını belirtin. 6. Tamam'ı tıklayın.

Tarama sonuçları, Tarama tamamlandı uyarısında görüntülenir. Sonuçlar; taranan, algılanan, onarılan, karantinaya alınan ve kaldırılan öğelerin sayısını içerir. Tarama sonuçları hakkında ayrıntılı bilgi almak veya virüslü öğeler üzerinde çalışmak için **Tarama ayrıntılarını görüntüle'yi** tıklayın.

Not: Tarama seçenekleri hakkında daha fazla bilgi almak için bkz. Tarama Türleri. (sayfa 38)

Tarama sonuçlarını görüntüleme

Tarama bitince, taramada neler bulunduğunu belirlemek ve bilgisayarınızın geçerli koruma durumunu analiz etmek için sonuçları görüntülersiniz. Tarama sonuçları size VirusScan'ın virüs, Truva atı, casus yazılım, reklam yazılım, tanımlama bilgisi ve başka olası istenmeyen program algılayıp algılamadığını, onarıp onarmadığını veya karantinaya alıp almadığını söyler.

Temel veya Gelişmiş menüde **Tara**'yı tıklatın ve sonra aşağıdakilerden birini yapın:

Bunu yapmak için...	Bunu yapın...
Tarama sonuçlarını uyarıda görüntülemek	Tarama sonuçlarını, Tarama tamamlandı uyarısında görüntüleyin.
Tarama sonuçları hakkında ayrıntılı bilgi görüntülemek	Tarama tamamlandı uyarısında Tarama ayrıntılarını görüntüle 'yi tıklatın.
Tarama sonuçlarının hızlı özetini görüntülemek	Görev çubuğunuzdaki bildirim alanında Tarama tamamlandı simgesine gidin.
Tarama ve algılama istatistiklerini görüntülemek	Görev çubuğunuzdaki bildirim alanında Tarama tamamlandı simgesini çift tıklatın.
Algılanan öğeler, bulaşma durumu ve türü hakkında ayrıntılı bilgi görüntülemek	1. Görev çubuğunuzdaki bildirim alanında Tarama tamamlandı simgesini çift tıklatın. 2. Tam Tarama, Hızlı Tarama, Özel Tarama veya El İle Tarama bölümünde Ayrıntılar 'ı tıklatın.
En son taramanızla ilgili ayrıntıları görüntülemek	Görev çubuğunuzdaki bildirim alanında Tarama tamamlandı simgesini çift tıklatın ve Tam Tarama, Hızlı Tarama, Özel Tarama veya El İle Tarama bölümünde Taramanız altında en son taramanızın ayrıntılarını görüntüleyin.

B Ö L Ü M 1 0

Tarama sonuçlarıyla çalışma

VirusScan tarama çalıştırırken bir güvenlik tehdidi algırsa, tehdit türüne göre tehdidi otomatik olarak ele almayı dener. Örneğin, VirusScan bilgisayarınızda bir virüs, Truva atı veya izleme tanımlama bilgisi algırsa, virüslü dosyayı temizlemeyi dener. VirusScan bir dosyayı temizlemeyi denemeden önce her zaman onu karantinaya alır. Temiz değilse dosya karantinaya alır.

Bazı güvenlik tehditlerinde, VirusScan dosyayı başarıyla temizleyemeyebilir veya karantinaya alamayabilir. Bu durumda, VirusScan sizden güvenlik tehdidini ele almanızı ister. Tehdit türüne bağlı olarak farklı eylemler gerçekleştirebilirsiniz. Örneğin bir dosyada virüs algılanırsa ancak VirusScan dosyayı başarıyla temizleyemez veya karantinaya alamazsa, buna erişimi reddeder. Tanımlama bilgileri algılanırsa ancak VirusScan tanımlama bilgilerini başarıyla temizleyemez veya karantinaya alamazsa, bunları kaldırma veya bunlara güvenme kararını siz verebilirsiniz. Olası istenmeyen programlar algılanırsa, VirusScan otomatik eylem gerçekleştirmez; bunun yerine, programı karantinaya alma veya programa güvenme kararını size bırakır.

VirusScan öğeleri karantinaya alınca, bunları şifreler ve sonra dosyaların, programların veya tanımlama bilgilerinin bilgisayarınıza zarar vermesini engellemek için bunları bir klasörde izole eder. Karantinadaki öğeleri geri yükleyebilir veya kaldırabilirsiniz. Genellikle karantinadaki bir tanımlama bilgisini bilgisayarınızı etkilemeden silebilirsiniz; ancak VirusScan bildiğiniz ve kullandığınız bir programı karantinaya almışsa bunu geri yüklemeyi düşünün.

Bu bölümde

Virüsler ve Truva atlarıyla çalışma	36
Olası istenmeyen programlarla çalışma	36
Karantinadaki dosyalarla çalışma	37
Karantinadaki programlar ve tanımlama bilgileriyle çalışma	37

Virüsler ve Truva atlarıyla çalışma

VirusScan bilgisayarınızdaki bir dosyada virüs veya Truva atı algılsa, dosyayı temizlemeyi dener. VirusScan dosyayı temizleyemezse karantinaya almayı dener. Bu da başarısız olursa, dosyaya erişim reddedilir (yalnızca gerçek zamanlı taramalarda).

1 Tarama Sonuçları bölmesini açın.

Nasıl?

1. Görev çubuğunuzun en sağındaki bildirim alanında **Tarama tamamlandı** simgesini çift tıklatın.
2. Tarama İlerleyişi: El İle Tarama bölümünde **Sonuçları Görüntüle**'yi tıklatın.

2 Tarama sonuçları listesinde **Virüsler ve Truva Atları**'nı tıklatın.

Not: VirusScan'ın karantinaya aldığı dosyalarla çalışmak için bkz. Karantinadaki dosyalarla çalışma (sayfa 37).

Olası istenmeyen programlarla çalışma

VirusScan bilgisayarınızda olası istenmeyen bir program algılsa, programı kaldırabilirsiniz veya programa güvenebilirsiniz. Programı tanımiyorsanız, bunu kaldırmayı düşünmenizi öneririz. Olası istenmeyen program kaldırıldığında, gerçekte sisteminizden silinmez. Kaldırma işlemi, programı karantinaya alarak bilgisayarınıza veya dosyalarınıza daha fazla zarar vermesini engeller.

1 Tarama Sonuçları bölmesini açın.

Nasıl?

1. Görev çubuğunuzun en sağındaki bildirim alanında **Tarama tamamlandı** simgesini çift tıklatın.
2. Tarama İlerleyişi: El İle Tarama bölümünde **Sonuçları Görüntüle**'yi tıklatın.

2 Tarama sonuçları listesinde **Olası İstenmeyen Programlar**'ı tıklatın.

3 Olası istenmeyen programı seçin.

4 **Şunu yapmak istiyorum** altında **Kaldır**'ı veya **Güven**'i tıklatın.

5 Belirlediğiniz seçeneği onaylayın.

Karantinadaki dosyalarla çalışma

VirusScan virüslü dosyaları karantinaya alınca, bunları şifreler ve sonra dosyaların bilgisayarınıza zarar vermesini engellemek için bunları bir klasöre taşır. Daha sonra karantinadaki dosyaları geri yükleyebilir veya kaldırabilirsiniz.

1 Karantinadaki Dosyalar bölmesini açın.

Nasıl?

1. Soldaki bölmede **Gelişmiş Menü**'yü tıklatın.
2. **Geri Yükle**'yi tıklatın.
3. **Dosyalar**'ı tıklatın.

2 Karantinadaki bir dosyayı seçin.

3 Aşağıdakilerden birini gerçekleştirin:

- Virüslü dosyayı onarıp bilgisayarınızdaki özgün konumuna döndürmek için **Geri Yükle**'yi tıklatın.
- Virüslü dosyayı bilgisayarınızdan kaldırmak için **Kaldır**'ı tıklatın.

4 Belirlediğiniz seçimi onaylamak için **Evet**'i tıklatın.

İpucu: Birden çok dosyayı aynı anda geri yükleyebilir veya kaldırabilirsiniz.

Karantinadaki programlar ve tanımlama bilgileriyle çalışma

VirusScan olası istenmeyen programları veya izleme tanımlama bilgilerini karantinaya alınca, bunları şifreler ve sonra programların veya tanımlama bilgilerinin bilgisayarınıza zarar vermesini engellemek için bunları korunan bir klasöre taşır. Daha sonra karantinadaki öğeleri geri yükleyebilir veya kaldırabilirsiniz. Genellikle karantinadaki öğeyi sisteminizi etkilemeden silebilirsiniz.

1 Karantinadaki Programlar ve İzleme Tanımlama Bilgileri bölmesini açın.

Nasıl?

1. Soldaki bölmede **Gelişmiş Menü**'yü tıklatın.
2. **Geri Yükle**'yi tıklatın.
3. **Programlar ve Tanımlama Bilgileri**'ni tıklatın.

2 Karantinadaki bir programı veya tanımlama bilgisini seçin.

3 Aşağıdakilerden birini gerçekleştirin:

- Virüslü dosyayı onarıp bilgisayarınızdaki özgün konumuna döndürmek için **Geri Yükle**'yi tıklayın.
- Virüslü dosyayı bilgisayarınızdan kaldırmak için **Kaldır**'ı tıklayın.

4 İşlemi onaylamak için **Evet**'i tıklayın.

İpucu: Birden çok programı ve tanımlama bilgisini aynı anda geri yükleyebilir veya kaldırabilirsiniz.

Tarama türleri

VirusScan, gerçek zamanlı tarama (PC'nizde sürekli tehdit etkinliğini izleyen), Windows Gezgini'nden el ile tarama ve SecurityCenter'dan tam, hızlı, özel tarama çalıştırma veya zamanlanan taramaların gerçekleşeceği zamanı özelleştirme becerisi gibi virüsten korunmaya yönelik eksiksiz bir dizi tarama seçeneği sağlar. SecurityCenter'da tarama yapmak, tarama seçeneklerini anında değiştirme avantajı sağlar.

Gerçek Zamanlı Tarama:

Gerçek zamanlı virüsten koruma, siz veya bilgisayarınız dosyalara erişince bunları tarayarak, bilgisayarınızda virüs etkinliğini sürekli izler. Bilgisayarınızın en son güvenlik tehditlerine karşı korunduğundan emin olmak için gerçek zamanlı virüsten korumayı açık bırakın ve düzenli, daha kapsamlı el ile taramalar için zamanlama yapın.

Bilinmeyen virüsleri tarama ve izleme tanımlama bilgilerinde ve ağ sürücülerinde tehditleri denetleme gibi gerçek zamanlı tarama için varsayılan seçenekleri ayarlayabilirsiniz. Ayrıca varsayılan olarak etkin olan arabellek taşması korumasından da yararlanabilirsiniz (Windows Vista 64 bit işletim sistemi kullanmıyorsanız). Daha fazla bilgi için bkz. Gerçek zamanlı tarama seçeneklerini ayarlama (sayfa 46).

Hızlı Tarama

Hızlı Tarama, bilgisayarınızdaki işlemlerde, kritik Windows dosyalarında ve diğer hassas alanlarda tehdit etkinliğini denetlemenize olanak verir.

Tam Tarama

Tam Tarama, tüm bilgisayarınızda PC'nizin herhangi bir yerinde bulunan virüsleri, casus yazılımları ve diğer güvenlik tehditlerini kapsamlı olarak denetlemenize olanak verir.

Özel Tarama

Özel Tarama, PC'nizde tehdit etkinliğini denetlemek için tarama ayarlarınızı seçmenize olanak verir. Özel tarama seçenekleri tüm dosyalarda, arşiv dosyalarında ve tanımlama bilgilerinde tehditleri denetlemenin yanı sıra bilinmeyen virüsleri, casus yazılımları ve görünmez dosyaları taramayı içerir.

Bilinmeyen virüsleri, arşiv dosyalarını, casus yazılımları ve olası tehditleri, izleme tanımlama bilgilerini ve görünmez dosyaları tarama gibi özel tarama için varsayılan seçenekleri ayarlayabilirsiniz. Ayrıca en az bilgisayar kaynağı kullanarak tarama yapabilirsiniz. Daha fazla bilgi için bkz. Özel tarama seçeneklerini ayarlama (sayfa 48).

El İle Tarama

El İle Tarama, anında dosyalar, klasörler ve sürücülerdeki tehditleri Windows Gezgini'nden hızla denetlemenize olanak verir.

Zamanlanan Tarama

Zamanlanan taramalar, haftanın herhangi bir gününde ve saatinde bilgisayarınızda virüsleri ve diğer tehditleri kapsamlı olarak denetler. Zamanlanan taramalar, her zaman varsayılan tarama seçeneklerinizi kullanarak tüm bilgisayarınızı denetler. Varsayılan olarak, VirusScan haftada bir kez zamanlanan tarama gerçekleştirir. Tarama hızının yavaşladığını fark ederseniz, minimum bilgisayar kaynağının kullanılması için seçeneği devre dışı bırakmayı düşünün; ancak virüs korumasına diğer görevlerden daha fazla öncelik tanınacağını unutmayın. Daha fazla bilgi için bkz. Tarama zamanlama (sayfa 50).

Not: Sizin için en iyi tarama seçeneğini başlatma hakkında bilgi için bkz. PC'nizi tarama (sayfa 32).

B Ö L Ü M 1 1

Ek koruma kullanma

VirusScan, gerçek zamanlı virüsten korumanın yanı sıra, komut dosyalarına, casus yazılımlara ve olası zararlı e-posta ve anlık ileti eklerine karşı gelişmiş koruma sağlar. Varsayılan olarak, komut dosyası tarama özelliği, casus yazılım, e-posta ve anlık ileti koruması açıktır ve bilgisayarınızı korur.

Komut dosyası tarama

Komut dosyası tarama koruması, olası zararlı komut dosyalarını algılar ve bunların bilgisayarınızda veya web tarayıcınızda çalışmasını engeller. Bilgisayarınızda, dosyalar oluşturan, kopyalayan veya silen ya da Windows kayıt defterini açan komut dosyaları gibi şüpheli komut dosyası etkinliklerini izler ve herhangi bir zarar oluşmadan sizi uyarır.

Casus yazılım koruması

Casus yazılım koruması, casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programları algılar. Casus yazılım, davranışınızı izlemek, kişisel bilgilerinizi toplamak ve hatta ek yazılımlar yükleyerek veya tarayıcı etkinliğinizin yönünü değiştirerek bilgisayarınızın kontrolünü ele geçirmek için gizlice bilgisayarınıza yüklenebilen yazılımdır.

E-posta koruması

E-posta koruması, gönderdiğiniz e-posta iletileri ve eklerindeki şüpheli etkinliği algılar.

Anlık ileti koruması

Anlık ileti koruması, aldığınız anlık ileti eklerindeki olası güvenlik tehditlerini algılar. Ayrıca, anlık ileti programlarının kişisel bilgileri paylaşmasını engeller.

Bu bölümde

Komut dosyası tarama korumasını başlatma.....	42
Casus yazılım korumasını başlatma	42
E-posta korumasını başlatma	43
Anlık ileti korumasını başlatma	43

Komut dosyası tarama korumasını başlatma

Olası zararlı komut dosyalarını algılaması ve bunların bilgisayarınızda çalışmasını engellemesi için komut dosyası tarama korumasını açın. Komut dosyası tarama koruması, bir komut dosyası bilgisayarınızda dosyalar oluşturmaya, kopyalamaya veya silmeye ya da Windows kayıt defterinde değişiklik yapmaya çalıştığında bunu size bildirir.

1 Bilgisayar ve Dosyalar Yapılandırma bölmesini açın.

Nasıl?

1. Soldaki bölmede **Gelişmiş Menü**'yü tıklatın.
2. **Yapılandır**'ı tıklatın.
3. Yapılandır bölmesinde **Bilgisayar ve Dosyalar**'ı tıklatın.

2 Komut dosyası tarama koruması altında Açık'ı tıklatın.

Not: İstedığınız zaman komut dosyası tarama korumasını kapatabilmenize karşın, bunu yaparsanız bilgisayarınız zararlı komut dosyalarına karşı korumasız kalır.

Casus yazılım korumasını başlatma

Casus yazılımları, reklam yazılımları ve sizin bilginiz veya izniniz olmadan bilgi toplayan ve ileten diğer olası istenmeyen programları algılaması ve kaldırması için casus yazılım korumasını açın.

1 Bilgisayar ve Dosyalar Yapılandırma bölmesini açın.

Nasıl?

1. Soldaki bölmede **Gelişmiş Menü**'yü tıklatın.
2. **Yapılandır**'ı tıklatın.
3. Yapılandır bölmesinde **Bilgisayar ve Dosyalar**'ı tıklatın.

2 Komut dosyası tarama koruması altında Açık'ı tıklatın.

Not: İsteddiğiniz zaman casus yazılım korumasını kapatabilmenize karşın, bunu yaparsanız bilgisayarınız olası istenmeyen programlara karşı korumasız kalır.

E-posta korumasını başlatma

Solucanların yanı sıra giden (SMTP) ve gelen (POP3) e-posta iletileri ve eklerindeki olası tehditleri algılaması için e-posta korumasını açın.

1 E-posta ve Anlık İleti Yapılandırma bölümünü açın.

Nasıl?

1. Soldaki bölmede **Gelişmiş Menü**'yü tıklatın.
2. **Yapılandır**'i tıklatın.
3. Yapılandır bölümünde **E-posta ve Anlık İleti**'yi tıklatın.

2 E-posta koruması altında **Açık**'i tıklatın.

Not: İstedığınız zaman e-posta korumasını kapatabilmenize karşın, bunu yaparsanız bilgisayarınız e-posta tehditlerine karşı korumasız kalır.

Anlık ileti korumasını başlatma

Gelen anlık ileti eklerinde bulunabilen güvenlik tehditlerini algılaması için anlık ileti korumasını açın.

1 E-posta ve Anlık İleti Yapılandırma bölümünü açın.

Nasıl?

1. Soldaki bölmede **Gelişmiş Menü**'yü tıklatın.
2. **Yapılandır**'i tıklatın.
3. Yapılandır bölümünde **E-posta ve Anlık İleti**'yi tıklatın.

2 Anlık İleti koruması altında **Açık**'i tıklatın.

Not: İsteddiğiniz zaman anlık ileti korumasını kapatabilmenize karşın, bunu yaparsanız bilgisayarınız zararlı anlık ileti eklerine karşı korumasız kalır.

B Ö L Ü M 1 2

Virüsten korumayı ayarlama

Zamanlanan, özel ve gerçek zamanlı tarama için farklı seçenekler ayarlayabilirsiniz. Örneğin, gerçek zamanlı koruma bilgisayarınızı sürekli izlediği için isteğe bağlı el ile korumaya yönelik daha kapsamlı tarama seçeneklerini ayırarak, temel tarama seçeneklerinden oluşan bir grubu seçebilirsiniz.

Ayrıca VirusScan'in, Sistem Koruması veya Güvenilenler Listeleri kullanarak, PC'nizde olası yetkisiz veya istenmeyen değişiklikleri nasıl izlemesini ve yönetmesini istediğinize karar verebilirsiniz. Sistem Koruması, bilgisayarınızda Windows kayıt defterinde veya kritik sistem dosyalarında yapılan olası yetkisiz değişiklikleri izler, günlüğe kaydeder, bildirir ve yönetir. Yetkisiz kayıt defteri ve dosya değişiklikleri, bilgisayarınıza zarar verebilir, güvenliğini tehlikeye atabilir ve değerli sistem dosyalarını bozabilir. Güvenilenler Listelerini kullanarak, dosya veya kayıt defteri değişikliklerini (Sistem Koruması), programları veya arabellek taşmalarını algılayan kurallara güvenmek mi yoksa kaldırmak mı istediğinize karar verebilirsiniz. Öğe güvenir ve bu etkinlik hakkında başka bildirim almak istemediğinizi belirtirseniz, öğe güvenilenler listesine eklenir ve VirusScan artık bunu algılamaz ve etkinliği hakkında size bildirimde bulunmaz.

Bu bölümde

Gerçek zamanlı tarama seçeneklerini ayarlama	46
Özel tarama seçeneklerini ayarlama	48
Tarama zamanlama	50
Sistem Koruması seçeneklerini kullanma	51
Güvenilenler listelerini kullanma	57

Gerçek zamanlı tarama seçeneklerini ayarlama

Gerçek zamanlı virüsten korumayı başlattığınızda, VirusScan dosyaları taramak için varsayılan birtakım seçenekler kullanır; ancak varsayılan seçenekleri gereksinimlerinize uygun şekilde değiştirebilirsiniz.

Gerçek zamanlı tarama seçeneklerini değiştirmek için tarama sırasında VirusScan'ın neleri denetleyeceğini, tarayacağı konumları ve dosya türlerini belirlemeniz gerekir. Örneğin, VirusScan'ın davranışınızı izlemek için Web siteleri tarafından kullanılan bilinmeyen virüsleri veya tanımlama bilgilerini denetleyip denetlemeyeceğini ve bilgisayarınızla veya yalnızca yerel sürücülerle eşleştirilen ağ sürücülerini tarayıp taramayacağını belirleyebilirsiniz. Hangi dosya türlerinin (tüm dosyalar veya yalnızca çoğu virüsün algılandığı yer olan program dosyaları ve belgeler) taranacağını da belirleyebilirsiniz.

Gerçek zamanlı tarama seçeneklerini değiştirirken, bilgisayarınızda arabellek taşması koruması olmasının önemli olup olmadığını da belirlemeniz gerekir. Arabellek, bilgisayar bilgilerini geçici olarak tutmak için kullanılan bellek bölümüdür. Arabellek taşmaları, şüpheli programların ve işlemlerin arabellekte depoladığı bilgi miktarı arabellek kapasitesini aştığı zaman gerçekleşebilir. Bu olursa, bilgisayarınız güvenlik saldırılarına açık hale gelir.

Gerçek zamanlı tarama seçeneklerini ayarlama

Gerçek zamanlı tarama sırasında VirusScan'ın neleri arayacağını, tarayacağı konumları ve dosya türlerini özelleştirmek için gerçek zamanlı tarama seçeneklerini ayarlıyorsunuz. Seçenekler, bilinmeyen virüsleri ve tanımlama bilgilerini taramanın yanı sıra, arabellek taşma koruması sağlamayı içerir. Gerçek zamanlı taramayı, bilgisayarınızla eşleştirilen ağ sürücülerini denetlemesi için de yapılandırabilirsiniz.

1 Gerçek Zamanlı Tarama bölümünü açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
2. SecurityCenter Giriş bölümünde **Bilgisayar ve Dosyalar**'ı tıklatın.
3. Bilgisayar ve Dosyalar bilgi alanında **Yapılandır**'ı tıklatın.
4. Bilgisayar ve Dosyalar Yapılandırma bölümünde, virüsten korumanın etkin olduğundan emin olun ve sonra **Gelişmiş**'i tıklatın.

- 2 Gerçek zamanlı tarama seçeneklerinizi belirtin ve sonra **Tamam**'ı tıklatın.

Bunu yapmak için...	Bunu yapın...
Bilinmeyen virüsleri ve bilinen virüslerin yeni türevlerini algılamak	Bilinmeyen virüsleri tara 'yı seçin.
Tanımlama bilgilerini algılamak	İzleme tanımlama bilgilerini tara ve temizle 'yi seçin.
Ağımıza bağlı sürücülerde virüsleri ve diğer olası tehditleri algılamak	Ağ sürücülerini tara 'yı seçin.
Bilgisayarınızı arabellek taşmalarından korumak	Arabellek taşması korumasını etkinleştir 'i seçin.
Hangi dosya türlerinin taranacağını belirtmek	Tüm dosyalar (önerilir) veya Yalnızca program dosyaları ve belgeler 'i tıklatın.

Gerçek zamanlı virüsten korumayı durdurma

Nadiren gerçek zamanlı taramayı geçici olarak durdurmak isteyebilirsiniz (örneğin bazı tarama seçeneklerini değiştirmek veya bir performans sorununu gidermek için). Gerçek zamanlı virüsten koruma devre dışı bırakıldığında, bilgisayarınız korunmaz ve SecurityCenter koruma durumunuz kırmızı olur. Koruma durumu hakkında ayrıntılı bilgi için SecurityCenter yardımında bkz. "Koruma durumu hakkında bilgi".

Gerçek zamanlı virüsten korumayı kapatabilir ve sonra yeniden devam edeceği zamanı belirtebilirsiniz. Bilgisayarınız yeniden başlatıldıktan 15, 30, 45 veya 60 dakika sonra korumayı otomatik olarak devam ettirebilir veya hiçbir zaman devam ettirmeyebilirsiniz.

- 1 Bilgisayar ve Dosyalar Yapılandırma bölmesini açın.
Nasıl?
 1. Soldaki bölmede **Gelişmiş Menü**'yü tıklatın.
 2. **Yapılandır**'ı tıklatın.
 3. Yapılandır bölmesinde **Bilgisayar ve Dosyalar**'ı tıklatın.
- 2 **Virüsten koruma** altında **Kapalı**'yı tıklatın.
- 3 İletişim kutusunda, gerçek zamanlı taramanın devam edeceği zamanı seçin.
- 4 **Tamam**'ı tıklatın.

Özel tarama seçeneklerini ayarlama

Özel virüsten koruma, istediğinizde dosyaları sizin taramanıza olanak verir. Özel taramayı başlattığınızda, VirusScan daha kapsamlı birtakım tarama seçenekleri kullanarak bilgisayarınızda virüsleri ve diğer olası zararlı öğeleri denetler. Özel tarama seçeneklerini değiştirmek için VirusScan'ın tarama sırasında neleri denetleyeceğini belirlemeniz gerekir. Örneğin, VirusScan'ın virüsleri, casus yazılım veya reklam yazılım gibi olası istenmeyen programları, görünmez programları ve köke inme programlarını (bilgisayarınıza yetkisiz erişim verebilen) ve Web sitelerinin davranışınızı izlemek için kullanabileceği tanımlama bilgilerini arayıp aramayacağını belirleyebilirsiniz. Denetlenen dosya türlerini de belirlemeniz gerekir. Örneğin, VirusScan'ın tüm dosyaları mı yoksa yalnızca program dosyaları ve belgeleri mi (burası çoğu virüsün algılandığı yer olduğu için) belirleyebilirsiniz. Taramaya arşiv dosyalarının (örneğin .zip dosyaları) eklenip eklenmeyeceğini de belirtebilirsiniz.

Varsayılan olarak, VirusScan her özel tarama çalıştırdığında, bilgisayarınızdaki ve tüm ağ sürücülerindeki tüm sürücülerini ve klasörlerini denetler; ancak varsayılan konumları, gereksinimlerinize uygun olarak değiştirebilirsiniz. Örneğin, yalnızca kritik PC dosyalarını, masaüstünüzdeki öğeleri veya Program Files klasöründeki öğeleri tarayabilirsiniz. Her özel taramayı kendiniz başlatmak istemiyorsanız, taramalar için düzenli zamanlama ayarlayabilirsiniz. Zamanlanan taramalar, her zaman varsayılan tarama seçeneklerini kullanarak tüm bilgisayarınızı denetler. Varsayılan olarak, VirusScan haftada bir kez zamanlanan tarama gerçekleştirir.

Tarama hızının yavaşladığını fark ederseniz, minimum bilgisayar kaynağının kullanılması için seçeneği devre dışı bırakmayı düşünün; ancak virüs korumasına diğer görevlerden daha fazla öncelik tanınacağını unutmayın.

Not: Film izlemek, bilgisayarınızda oyun oynamak gibi etkinliklerin veya bilgisayar ekranınızın tamamını kaplayan herhangi bir etkinliğin keyfini çıkarırken, VirusScan otomatik güncelleştirmeler ve özel taramalar gibi çeşitli görevleri duraklatır.

Özel tarama seçeneklerini ayarlama

Özel tarama sırasında VirusScan'in neleri arayacağını, tarayacağı konumları ve dosya türlerini özelleştirmek için özel tarama seçeneklerini ayarlarsınız. Seçenekler; bilinmeyen virüsleri, dosya arşivlerini, casus yazılımları ve olası istenmeyen programları, izleme tanımlama bilgilerini, köke inme programlarını ve hayalet programları içerir. Özel tarama sırasında VirusScan'in virüsleri ve diğer zararlı öğeleri nerede arayacağını belirlemek için özel tarama konumunu da ayarlayabilirsiniz.

Bilgisayarınızdaki tüm dosyalar, klasörler ve sürücüler tarayabilir veya tarama işlemini belirli klasörler ve sürücülerle sınırlandırabilirsiniz.

1 Özel Tarama bölümünü açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
2. SecurityCenter Giriş bölümünde **Bilgisayar ve Dosyalar**'ı tıklatın.
3. Bilgisayar ve Dosyalar bilgi alanında **Yapılandır**'i tıklatın.
4. Bilgisayar ve Dosyalar Yapılandırma bölümünde, virüsten korumanın etkin olduğundan emin olun ve **Gelişmiş**'i tıklatın.
5. Virüsten Koruma bölümünde **El İle Tarama**'yı tıklatın.

2 Özel tarama seçeneklerinizi belirtin ve sonra **Tamam**'i tıklatın.

Bunu yapmak için...	Bunu yapın...
Bilinmeyen virüsleri ve bilinen virüslerin yeni türevlerini algılamak	Bilinmeyen virüsleri tara 'yı seçin.
.Zip ve diğer arşiv dosyalarındaki virüsleri algılamak ve kaldırmak	Arşiv dosyalarını tara 'yı seçin.
Casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programları algılamak	Casus yazılımları ve olası tehditleri tara 'yı seçin.
Tanımlama bilgilerini algılamak	İzleme tanımlama bilgilerini tara ve temizle 'yi seçin.
Varolan Windows sistem dosyalarını değiştirebilen ve kullanabilen köke inme programlarını ve hayalet programları algılamak	Görünmez programları tara 'yı seçin.
Taramalar için daha az işlemci gücü kullanmak diğer görevlere (Web'de gezinme veya dosyalar açma gibi) daha yüksek öncelik tanımak	En az bilgisayar kaynağı kullanarak tara 'yı seçin.

Bunu yapmak için...	Bunu yapın...
Hangi dosya türlerinin taranacağını belirtmek	Tüm dosyalar (önerilir) veya Yalnızca program dosyaları ve belgeler 'i tıklatın.

- 3** Taranacak Varsayılan Konum'u tıklatın, ardından taramak veya atlamak istediğiniz konumları seçin veya işaretini kaldırın ve sonra **Tamam**'i tıklatın:

Bunu yapmak için...	Bunu yapın...
Bilgisayarınızdaki tüm dosya ve klasörleri taramak	Bilgisayarım 'i seçin.
Bilgisayarınızdaki belirli dosyalar, klasörler ve sürücülerini taramak	Bilgisayarım onay kutusunun işaretini kaldırın ve bir veya birkaç klasör veya sürücü seçin.
Kritik sistem dosyalarını taramak	Bilgisayarım onay kutusunun işaretini kaldırın ve sonra Kritik Sistem Dosyaları onay kutusunu işaretleyin.

Tarama zamanlama

Haftanın herhangi bir gününde ve saatinde bilgisayarınızda virüsleri ve diğer tehditleri kapsamlı olarak denetlemek için taramalar zamanlayın. Zamanlanan taramalar, her zaman varsayılan tarama seçeneklerini kullanarak tüm bilgisayarınızı denetler. Varsayılan olarak, VirusScan haftada bir kez zamanlanan tarama gerçekleştirir. Tarama hızının yavaşladığını fark ederseniz, minimum bilgisayar kaynağının kullanılması için seçeneği devre dışı bırakmayı düşünün; ancak virüs korumasına diğer görevlerden daha fazla öncelik tanınacağını unutmayın.

Varsayılan tarama seçeneklerinizi kullanarak tüm bilgisayarınızda virüsleri ve diğer tehditleri kapsamlı olarak denetleyen taramalar zamanlayın. Varsayılan olarak, VirusScan haftada bir kez zamanlanan tarama gerçekleştirir.

- 1** Zamanlanan Tarama bölümünü açın.

Nasıl?

- Ortak Görevler** bölümünde **Giriş**'i tıklatın.
- SecurityCenter Giriş bölümünde **Bilgisayar ve Dosyalar**'i tıklatın.
- Bilgisayar ve Dosyalar bilgi alanında **Yapılandır**'i tıklatın.

4. Bilgisayar ve Dosyalar Yapılandırma bölümünde, virüsten korumanın etkin olduğundan emin olun ve **Gelişmiş'i** tıklatın.
5. Virüsten Koruma bölümünde **Zamanlanan Tarama'yı** tıklatın.

2 Zamanlanan taramayı etkinleştir'i seçin.

3 Normalde tarama işlemi için kullanılan işlemci miktarını azaltmak için **En az bilgisayar kaynağı kullanarak tara'yı** seçin.

4 Bir veya birkaç gün seçin.

5 Başlangıç zamanını belirtin.

6 **Tamam'ı** tıklatın.

İpucu: Sıfırla'yı tıklatarak varsayılan zamanlamayı geri yükleyebilirsiniz.

Sistem Koruması seçeneklerini kullanma

Sistem Koruması, bilgisayarınızda Windows kayıt defterinde veya kritik sistem dosyalarında yapılan olası yetkisiz değişiklikleri izler, günlüğe kaydeder, bildirir ve yönetir. Yetkisiz kayıt defteri ve dosya değişiklikleri, bilgisayarınıza zarar verebilir, güvenliğini tehlikeye atabilir ve değerli sistem dosyalarını bozabilir.

Kayıt defteri ve dosya değişiklikleri yaygındır ve bilgisayarınızda düzenli olarak gerçekleşebilir. Değişikliklerin pek çoğu zararsız olduğu için Sistem Koruması'nın varsayılan ayarları, önemli zarar olasılığı bulunan yetkisiz değişikliklere karşı güvenilir, akıllı ve somut koruma sağlamak üzere yapılandırılmıştır. Örneğin, Sistem Koruması yaygın olmayan ve önemli bir tehdit oluşturma olasılığı bulunan değişiklikler algıladığında, etkinlik hemen bildirilir ve günlüğe kaydedilir. Daha yaygın olan ancak yine de zarar verme olasılığı bulunan değişiklikler yalnızca günlüğe kaydedilir. Ancak standart ve düşük riskli değişikliklerin izlenmesi varsayılan olarak devre dışıdır. Sistem Koruması teknolojisinin korumasını, istediğiniz herhangi bir ortamı kapsayacak şekilde yapılandırabilirsiniz.

Üç tür Sistem Koruması vardır: Program Sistem Koruması, Windows Sistem Koruması ve Tarayıcı Sistem Koruması.

Program Sistem Koruması

Program Sistem Koruması, bilgisayarınızın kayıt defterindeki ve Windows tarafından kullanılan diğer kritik dosyalardaki olası yetkisiz değişiklikleri algılar. Bu önemli kayıt defteri öğeleri ve dosyaları; ActiveX yüklemelerini, başlangıç öğelerini, Windows kabuk yürütme kancalarını ve kabuk hizmeti nesne gecikme yüklemelerini içerir. Program Sistem Koruması teknolojisi, bunları izleyerek şüpheli ActiveX programlarının (Internet'ten yüklenen) yanı sıra casus yazılımları ve Windows başlatıldığında otomatik olarak açılabilen olası istenmeyen programları durdurur.

Windows Sistem Koruması

Windows Sistem Koruması da bilgisayarınızın kayıt defterindeki ve Windows tarafından kullanılan diğer kritik dosyalardaki olası yetkisiz değişiklikleri algılar. Bu önemli kayıt defteri öğeleri ve dosyalar; içerik menüsü işleyicileri, appInit DLL dosyaları ve Windows hosts dosyasını içerir. Windows Sistem Koruması teknolojisi, bunları izleyerek bilgisayarınızın Internet üzerinden yetkisiz veya kişisel bilgileri gönderip almasını engellemeye yardımcı olur. Ayrıca siz ve aileniz için önemli olan programların görünümünde ve davranışında istenmeyen değişiklikler yapabilen şüpheli programları durdurmaya yardımcı olur.

Tarayıcı Sistem Koruması

Program ve Windows Sistem Koruması gibi Sistem Koruması da bilgisayarınızın kayıt defterindeki ve Windows tarafından kullanılan diğer kritik dosyalardaki olası yetkisiz değişiklikleri algılar. Ancak Tarayıcı Sistem Koruması; Internet Explorer eklentileri, Internet Explorer URL'leri ve Internet Explorer güvenlik bölgeleri gibi önemli kayıt defteri öğeleri ve dosyalarındaki değişiklikleri izler. Tarayıcı Sistem Koruması teknolojisi, bunları izleyerek şüpheli Web sitelerine yeniden yönlendirme, tarayıcı ayarlarında ve seçeneklerinde habersiz değişiklik yapma ve şüpheli Web sitelerine istenmeyen şekilde güvenme gibi yetkisiz tarayıcı etkinliğini engellemeye yardımcı olur.

Sistem Koruması'nı etkinleştirme

Bilgisayarınızda olası istenmeyen Windows kayıt defteri ve dosya değişikliklerini algılayıp size bildirmesi için Sistem Koruması'nı etkinleştirin. Yetkisiz kayıt defteri ve dosya değişiklikleri, bilgisayarınıza zarar verebilir, güvenliğini tehlikeye atabilir ve değerli sistem dosyalarını bozabilir.

1 Bilgisayar ve Dosyalar Yapılandırma bölümünü açın.

Nasıl?

1. Soldaki bölmede **Gelişmiş Menü**'yü tıklayın.
2. **Yapılandır**'ı tıklayın.
3. Yapılandır bölümünde **Bilgisayar ve Dosyalar**'ı tıklayın.

2 Sistem Koruması altında **Açık**'ı tıklayın.

Not: **Kapalı**'yı tıklayarak Sistem Koruması'nı devre dışı bırakabilirsiniz.

Sistem Koruması seçeneklerini yapılandırma

Windows dosyaları, programları ve Internet Explorer ile ilişkili yetkisiz kayıt defteri ve dosya değişikliklerine karşı koruma, günlüğe kaydetme ve uyarı seçeneklerini yapılandırmak için Sistem Koruması bölümünü kullanın. Yetkisiz kayıt defteri ve dosya değişiklikleri, bilgisayarınıza zarar verebilir, güvenliğini tehlikeye atabilir ve değerli sistem dosyalarını bozabilir.

1 Sistem Koruması bölümünü açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklayın.
2. SecurityCenter Giriş bölümünde **Bilgisayar ve Dosyalar**'ı tıklayın.
3. Bilgisayar ve Dosyalar bilgi alanında **Yapılandır**'ı tıklayın.
4. Bilgisayar ve Dosyalar Yapılandırma bölümünde, Siste Koruması'nın etkin olduğundan emin olun ve **Gelişmiş**'i tıklayın.

2 Listedeki Sistem Koruması türünü seçin.

- **Program Sistem Koruması**
- **Windows Sistem Koruması**
- **Tarayıcı Sistem Koruması**

3 Şunu yapmak istiyorum altında aşağıdakilerden birini gerçekleştirin:

- Program, Windows ve Tarayıcı Sistem Koruması ile ilişkili yetkisiz kayıt defteri ve dosya değişikliklerini algılamak, günlüğe kaydetmek ve bildirmek için **Uyarıları göster**'i tıklatın.
- Program, Windows ve Tarayıcı Sistem Koruması ile ilişkili yetkisiz kayıt defteri ve dosya değişikliklerini algılamak ve günlüğe kaydetmek için **Değişiklikleri yalnızca günlüğe kaydet**'i tıklatın.
- Program, Windows ve Tarayıcı Sistem Koruması ile ilişkili yetkisiz kayıt defteri ve dosya değişikliklerini algılama özelliğini devre dışı bırakmak için **Bu Sistem Koruması'nı devre dışı bırak**'i tıklatın.

Not: Sistem Koruması türleri hakkında ayrıntılı bilgi için bkz. Sistem Koruması türleri hakkında (sayfa 54).

Sistem Koruması türleri hakkında

Sistem Koruması, bilgisayarınızın kayıt defterindeki ve Windows tarafından kullanılan diğer kritik dosyalardaki olası yetkisiz değişiklikleri algılar. Üç tür Sistem Koruması vardır: Program Sistem Koruması, Windows Sistem Koruması ve Tarayıcı Sistem Koruması

Program Sistem Koruması

Program Sistem Koruması teknolojisi, şüpheli ActiveX programlarının (İnternet'ten yüklenen) yanı sıra casus yazılımları ve Windows başlatıldığında otomatik olarak açılabilen olası istenmeyen programları durdurur.

Sistem Koruması	Şunları algılar...
ActiveX Yüklemeleri	Bilgisayarınıza zarar verebilen, güvenliğini tehlikeye atabilen ve değerli sistem dosyalarını bozabilen ActiveX yüklemelerinde yapılan yetkisiz kayıt defteri değişiklikleri.
Başlangıç Öğeleri	Başlangıç öğelerine dosya değişiklikleri yükleyerek, bilgisayarınızı başlattığınızda şüpheli programların çalışmasına izin verebilen casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programlar.
Windows Kabuk Yürütme Kancaları	Güvenlik programlarının düzgün şekilde çalışmasını engellemek için Windows kabuk yürütme kancaları yükleyebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Kabuk Hizmeti Nesne Gecikme Yükleme	Kabuk hizmeti nesne gecikme yüklemesi üzerinde kayıt defteri değişiklikleri yaparak, bilgisayarınızı başlattığınızda zararlı dosyaların çalışmasına izin verebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.

Windows Sistem Koruması

Windows Sistem Koruması teknolojisi, bilgisayarınızın Internet üzerinden yetkisiz veya kişisel bilgileri gönderip almasını engellemeye yardımcı olur. Ayrıca siz ve aileniz için önemli olan programların görünümünde ve davranışında istenmeyen değişiklikler yapabilen şüpheli programları durdurmaya yardımcı olur.

Sistem Koruması	Şunları algılar...
İçerik Menüsü İşleyicileri	Windows menülerinin görünümünü ve davranışını etkileyebilen Windows içerik menüsü işleyicilerinde yapılan yetkisiz kayıt defteri değişiklikleri. İçerik menüleri, bilgisayarınızda dosyaları sağ tıklamak gibi eylemler gerçekleştirmenize izin verir.
AppInit DLL'ler	Bilgisayarınızı başlattığınızda olası zararlı dosyaların çalışmasına izin verebilen Windows appInit DLL dosyalarında yapılan yetkisiz kayıt defteri değişiklikleri.
Windows Hosts Dosyası	Windows Hosts dosyanızda yetkisiz değişiklikler yaparak, tarayıcınızın şüpheli Web sitelerine yönlendirilmesine ve yazılım güncelleştirmelerinin engellenmesine izin verebilen casus yazılımlar, reklam yazılımlar ve olası istenmeyen programlar.
Winlogon Kabuğu	Winlogon kabuğu üzerinde kayıt defteri değişiklikleri yaparak, diğer programların Windows Explorer yerine geçmesine izin verebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Winlogon Kullanıcı Başlatma	Winlogon kullanıcı başlatma üzerinde kayıt defteri değişiklikleri yaparak, Windows oturumu açtığınızda şüpheli programların çalışmasına izin verebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Windows Protokolleri	Windows protokolleri üzerinde kayıt defteri değişiklikleri yaparak, bilgisayarınızın Internet'te bilgi gönderme ve alma biçimini etkileyebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Winsock Katmanlı Hizmet Sağlayıcıları	Internet'te gönderip aldığınız bilgileri ele geçirmek ve değiştirmek için Winsock Katmanlı Hizmet Sağlayıcıları (LSP) üzerine kayıt defteri değişiklikleri yükleyebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Windows Kabuk Açma Komutları	Solucanların ve diğer zararlı programların bilgisayarınızda çalışmasına izin verebilen Windows kabuk açma komutları üzerinde yapılan yetkisiz değişiklikler.
Paylaşılan Görev Zamanlayıcı	Paylaşılan görev zamanlayıcı üzerinde kayıt defteri ve dosya değişiklikleri yaparak, bilgisayarınızı başlattığınızda olası zararlı dosyaların çalışmasına izin verebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.

Sistem Koruması	Şunları algılar...
Windows Messenger Hizmeti	Windows messenger hizmeti üzerinde kayıt defteri değişiklikleri yaparak, bilgisayarınızda istenmeyen reklamlara ve uzaktan çalıştırılan programlara izin verebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Windows Win.ini Dosyası	Win.ini dosyasında değişiklikler yaparak, bilgisayarınızı başlattığınızda şüpheli programların çalışmasına izin verebilen casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programlar.

Tarayıcı Sistem Koruması

Tarayıcı Sistem Koruması teknolojisi, şüpheli Web sitelerine yeniden yönlendirme, tarayıcı ayarlarında ve seçeneklerinde habersiz değişiklik yapma ve şüpheli Web sitelerine istenmeyen şekilde güvenme gibi yetkisiz tarayıcı etkinliğini engellemeye yardımcı olur.

Sistem Koruması	Şunları algılar...
Tarayıcı Yardımcı Nesneleri	Web'de gezinmeyi izlemek ve istenmeyen reklamları göstermek için tarayıcı yardımcı nesneleri kullanabilen casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programlar.
Internet Explorer Çubukları	Internet Explorer'ın görünümünü ve davranışını etkileyebilen Ara ve Sık Kullanılanlar gibi Internet Explorer Çubuğu programlarında yapılan yetkisiz kayıt defteri değişiklikleri.
Internet Explorer Eklentileri	Web'de gezinmeyi izlemek ve istenmeyen reklamları göstermek için Internet Explorer eklentileri yükleyebilen casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programlar.
Internet Explorer ShellBrowser	Web tarayıcınızın görünümünü ve davranışını etkileyebilen Internet Explorer shell browser üzerinde yapılan yetkisiz kayıt defteri değişiklikleri.
Internet Explorer Web Tarayıcısı	Tarayıcınızın görünümünü ve davranışını etkileyebilen Internet Explorer Web tarayıcısı üzerinde yapılan yetkisiz kayıt defteri değişiklikleri.
Internet Explorer URL Arama Kancaları	Internet Explorer URL arama kancalarında kayıt defteri değişiklikleri yaparak, tarayıcınızın Web'de arama yaparken şüpheli Web sitelerine yönlendirilmesine izin verebilen casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programlar.
Internet Explorer URL'leri	Internet Explorer URL'lerinde kayıt defteri değişiklikleri yaparak tarayıcı ayarlarını etkileyebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.

Sistem Koruması	Şunları algılar...
Internet Explorer Kısıtlamaları	Internet Explorer kısıtlamaları üzerinde kayıt defteri değişiklikleri yaparak, tarayıcı ayarlarını ve seçeneklerini etkileyebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Internet Explorer Güvenlik Bölgeleri	Internet Explorer güvenlik bölgeleri üzerinde kayıt defteri değişiklikleri yaparak, bilgisayarınızı başlattığınızda olası zararlı dosyaların çalışmasına izin verebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Internet Explorer Güvenilir Siteleri	Internet Explorer güvenilir siteleri üzerinde kayıt defteri değişiklikleri yaparak, tarayıcınızın şüpheli Web sitelerine güvenmesine izin verebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.
Internet Explorer İlkesi	Internet Explorer ilkelerinde kayıt defteri değişiklikleri yaparak, tarayıcınızın görünümünü ve davranışını etkileyebilen casus yazılımlar, reklam yazılımlar veya diğer olası istenmeyen programlar.

Güvenilenler listelerini kullanma

VirusScan bir dosya veya kayıt defteri değişikliği (Sistem Koruması), program veya arabellek taşması algılsa, buna güvenmenizi veya bunu kaldırmanızı ister. Öğeye güvenir ve bu etkinlik hakkında başka bildirim almak istemediğinizi belirtirseniz, öğe güvenilenler listesine eklenir ve VirusScan artık bunu algılamaz ve etkinliği hakkında size bildirimde bulunmaz. Bir öğeyi güvenilenler listesine ekledikten sonra etkinliğini engellemek istediğinize karar verirseniz bunu yapabilirsiniz. Engellendiğinde, öğenin çalışması veya her girişimde bulunduğu size bildirmeden bilgisayarınızda değişiklik yapması önlenir. Bir öğeyi güvenilenler listesinden de kaldırabilirsiniz. Kaldırıldığında, VirusScan öğenin etkinliğini yeniden algılayabilir.

Güvenilenler listelerini yönetme

Önceden algılanan ve güvenilen öğelere güvenmek veya bunları engellemek için Güvenilenler Listeleri bölmesini kullanın. Bir öğeyi VirusScan'ın yeniden algılaması için güvenilenler listesinden de kaldırabilirsiniz.

1 Güvenilenler Listeleri bölmesini açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
2. SecurityCenter Giriş bölümünde **Bilgisayar ve Dosyalar**'ı tıklatın.
3. Bilgisayar ve Dosyalar bilgi alanında **Yapılandır**'ı tıklatın.

4. Bilgisayar ve Dosyalar Yapılandırma bölümünde, virüsten korumanın etkin olduğundan emin olun ve **Gelişmiş'i** tıklatın.
5. Virüsten Koruma bölümünde **Güvenilenler Listeleri'ni** tıklatın.

2 Aşağıdaki güvenilenler listesi türlerinden birini seçin:

- **Program Sistem Koruması**
- **Windows Sistem Koruması**
- **Tarayıcı Sistem Koruması**
- **Güvenilen Programlar**
- **Güvenilen Arabellek Taşmaları**

3 **Şunu yapmak istiyorum** altında aşağıdakilerden birini gerçekleştirin:

- Algılanan öğenin Windows kayıt defterinde veya bilgisayarınızdaki kritik sistem dosyalarında size bildirmeden değişiklik yapmasına izin vermek için **Güven'i** tıklatın.
- Algılanan öğenin Windows kayıt defterinde veya bilgisayarınızdaki kritik sistem dosyalarında size bildirmeden değişiklik yapmasını engellemek için **Engelle'yi** tıklatın.
- Algılanan öğeyi güvenilenler listelerinden kaldırmak için **Kaldır'ı** tıklatın.

4 **Tamam'ı** tıklatın.

Not: Güvenilenler listesi türleri hakkında ayrıntılı bilgi için bkz. Güvenilenler listesi türleri hakkında (sayfa 59).

Güvenilenler listesi türleri hakkında

Güvenilenler Listeleri bölümündeki Sistem Koruması, VirusScan tarafından önceden algılanan ancak sizin uyarıdan veya Tarama sonuçları bölümünden izin vermeyi seçtiğiniz, yetkisiz kayıt defteri ve dosya değişikliklerini yansıtır. Güvenilenler Listeleri bölümünden yönetebileceğiniz beş tür güvenilenler listesi türü vardır: Program Sistem Koruması, Windows Sistem Koruması, Tarayıcı Sistem Koruması, Güvenilen Programlar ve Güvenilen Arabellek Taşmaları.

Seçenek	Açıklama
Program Sistem Koruması	<p>Güvenilenler Listeleri bölümündeki Program Sistem Koruması, önceden VirusScan tarafından algılanan ancak sizin uyarıdan veya Tarama Sonuçları bölümünden izin vermeyi seçtiğiniz, yetkisiz kayıt defteri ve dosya değişikliklerini yansıtır.</p> <p>Program Sistem Koruması; ActiveX yüklemeleri, başlangıç öğeleri, Windows kabuk yürütme kancaları ve kabuk hizmeti nesne gecikme yükleme etkinliğiyle ilişkili yetkisiz kayıt defteri ve dosya değişikliklerini algılar. Bu türde yetkisiz kayıt defteri ve dosya değişiklikleri, bilgisayarınıza zarar verebilir, güvenliğini tehlikeye atabilir ve değerli sistem dosyalarını bozabilir.</p>
Windows Sistem Koruması	<p>Güvenilenler Listeleri bölümündeki Windows Sistem Koruması, VirusScan tarafından önceden algılanan ancak sizin uyarıdan veya Tarama Sonuçları bölümünden izin vermeyi seçtiğiniz, yetkisiz kayıt defteri ve dosya değişikliklerini yansıtır.</p> <p>Windows Sistem Koruması; içerik menüsü işleyicileri, appInit DLL dosyaları, Windows hosts dosyası, Winlogon kabuğu, Winsock Katmanlı Hizmet Sağlayıcıları (LSP) vb. ile ilişkili yetkisiz kayıt defteri ve dosya değişikliklerini algılar. Bu türde yetkisiz kayıt defteri ve dosya değişiklikleri, bilgisayarınızın Internet'te bilgi gönderme ve alma biçimini etkileyebilir, programların görünümünü ve davranışını değiştirebilir ve şüpheli programların bilgisayarınızda çalışmasına izin verebilir.</p>

Seenek	Aıklama
Tarayıcı Sistem Koruması	<p>Güvenilenler Listeleri bölümündeki Tarayıcı Sistem Koruması, VirusScan tarafından önceden algılanan ancak sizin uyarıdan veya Tarama Sonuçları bölümünden izin vermeyi seçtiğiniz, yetkisiz kayıt defteri ve dosya değişikliklerini yansıtır.</p> <p>Tarayıcı Sistem Koruması; Tarayıcı yardımcı nesnelere, İnternet Explorer eklentilerine, İnternet Explorer URL'leri, İnternet Explorer güvenlik bölgeleri vb. ile ilişkili yetkisiz kayıt defteri değişikliklerini ve diğer istenmeyen davranışları algılar. Bu türde yetkisiz kayıt defteri değişiklikleri, şüpheli Web sitelerine yeniden yönlendirme, tarayıcı ayarlarında ve seçeneklerinde değişiklikler ve şüpheli Web sitelerine güvenme gibi istenmeyen tarayıcı etkinliğine neden olabilir.</p>
Güvenilen Programlar	<p>Güvenilen programlar, VirusScan tarafından önceden algılanan ancak sizin uyarıdan veya Tarama Sonuçları bölümünden izin vermeyi seçtiğiniz olası istenmeyen programlardır.</p>
Güvenilen Arabellek Taşmaları	<p>Güvenilen arabellek taşmaları, VirusScan tarafından algılanan ancak sizin uyarıdan veya Tarama Sonuçları bölümünden izin vermeyi seçtiğiniz istenmeyen etkinliği yansıtır.</p> <p>Arabellek taşmaları bilgisayarınıza zarar verebilir ve dosyalarınızı bozabilir. Arabellek taşmaları, şüpheli programların ve işlemlerin arabellekte depoladığı bilgi miktarı arabellek kapasitesini aştığı zaman gerçekleşir.</p>

B Ö L Ü M 13

McAfee Personal Firewall

Personal Firewall, bilgisayarınız ve kişisel verileriniz için gelişmiş koruma sağlar. Personal Firewall, bilgisayarınızla Internet arasında bir engel oluşturarak, şüpheli etkinliklere karşı Internet trafiğini sessizce izler.

Not: SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde

Personal Firewall özellikleri	62
Firewall'u Başlatma.....	63
Uyarılarla çalışma	65
Bilgi uyarılarını yönetme	67
Firewall korumasını yapılandırma	69
Programları ve izinleri yönetme.....	79
Bilgisayar bağlantılarını yönetme	85
Sistem hizmetlerini yönetme.....	93
Günlüğe kaydetme, izleme ve analiz.....	99
Internet güvenliği hakkında bilgi alma.....	109

Personal Firewall özellikleri

Standart ve özel koruma düzeyleri	Firewall'un varsayılan veya özelleştirilebilir koruma ayarlarını kullanarak, izinsiz girişlerden ve şüpheli etkinliklerden korunun.
Gerçek zamanlı öneriler	Programlara Internet erişim izni vermeniz veya ağ trafiğine güvenmeniz gerekip gerekmediğine karar vermenize yardımcı olan dinamik öneriler alın.
Programlar için akıllı erişim yönetimi	Uyarılar ve olay günlükleri ile programların Internet erişimini yönetin ve belirli programların erişim izinlerini yapılandırın.
Oyun koruması	İzinsiz giriş denemeleri ve şüpheli etkinliklerle ilgili uyarıların, tam ekranda oyun oynarken dikkatinizi dağıtmasını engeller.
Bilgisayar başlangıç koruması	Windows® başlar başlamaz bilgisayarınızı izinsiz giriş denemelerinden, istenmeyen programlardan ve ağ trafiğinden koruyun.
Sistem hizmeti portunu kontrol etme	Bazı programlar için gereken açık ve kapalı sistem hizmeti portlarını yönetin.
Bilgisayar bağlantılarını yönetme	Başka bilgisayarlarla kendi bilgisayarınız arasında uzak bağlantılara izin verin ve bunları engelleyin.
HackerWatch bilgi tümleşmesi	Bilgisayarınızdaki programlar hakkında güncel güvenlik bilgilerinin yanı sıra genel güvenlik olayları ve Internet port istatistikleri de veren HackerWatch'un Web sitesi aracılığıyla, genel korsanlık hareketlerini ve izinsiz giriş desenlerini izleyin.
Güvenlik duvarını kilitleme	Bilgisayarınız ve Internet arasındaki tüm gelen ve giden trafiği anında engelleyin.
Firewall'u geri yükleme	Firewall'un özgün koruma ayarlarını anında geri yükleyin.
Gelişmiş Truva atı algılama	Truva atları gibi olası zararlı uygulamaları algılayıp, bunların kişisel verilerinizi Internet'e göndermesini engelleyin.
Olay günlüğü kaydetme	En son gelen ve giden Internet trafiğini, izinsiz giriş olaylarını izleyin.
Internet trafiğini izleme	Saldırıların kaynağını ve trafiği gösteren dünya haritalarını inceleyin. Bunun yanı sıra, IP adreslerinin kaynağını bulmak için ayrıntılı kullanıcı bilgilerine ve coğrafi verilere ulaşın. Ayrıca, gelen ve giden trafiği analiz edin; program bant genişliğini ve program etkinliğini izleyin.
İzinsiz girişleri engelleme	Gizliliğinizi olası Internet tehditlerinden koruyun. Sezgisel işlevler kullanarak, saldırı belirtileri veya korsanlık girişimi özellikleri sergileyen öğeleri engelleyip üçüncü bir koruma katmanı sağlıyoruz.
Karmaşık trafik analizi	Açık bağlantıları etkin şekilde dinleyenler de dahil, gelen ve giden Internet trafiğini ve program bağlantılarını inceleyin. Bu özellik, izinsiz girişlere karşı hassas olan programları görmenize ve gerekeni yapmanıza olanak verir.

B Ö L Ü M 14

Firewall'u Başlatma

Firewall yüklendikten sonra, bilgisayarınız izinsiz girişlerden ve istenmeyen ağ trafiğinden korunur. Ayrıca uyarıları işleyebilir; bilinen ve bilinmeyen programların gelen ve giden Internet erişimini yönetebilirsiniz. Akıllı Öneriler ve Otomatik güvenlik düzeyi (programların yalnızca giden Internet erişimine izin verme seçeneği belirlenmiş) otomatik olarak etkinleştirilir.

Internet ve Ağ Yapılandırması bölmesinden Firewall'u devre dışı bırakabilirsiniz; ancak bu durumda bilgisayarınız izinsiz girişlerden ve istenmeyen ağ trafiğinden korunmaz ve siz gelen ve giden Internet bağlantılarını etkili şekilde yönetemezsiniz. Güvenlik duvarı korumasını kaldırmanız gerekirse, bunu yalnızca zorunlu durumlarda ve geçici olarak yapın. Firewall'u aynı zamanda Internet ve Ağ Yapılandırması panelinden de etkinleştirebilirsiniz.

Firewall, Windows® Güvenlik Duvarı'nı otomatik olarak devre dışı bırakır ve kendisini varsayılan güvenlik duvarı olarak ayarlar.

Not: Firewall'u yapılandırmak için, Internet ve Ağ Yapılandırması bölümünü açın.

Bu bölümde

Güvenlik duvarı korumasını başlatma.....	63
Güvenlik duvarı korumasını durdurma	64

Güvenlik duvarı korumasını başlatma

Bilgisayarınızı izinsiz girişlerden ve istenmeyen ağ trafiğinden korumak, gelen ve giden Internet bağlantılarını yönetmek için Firewall'u etkinleştirebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı ve sonra **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruması devre dışı** altında **Açık**'ı tıklatın.

Güvenlik duvarı korumasını durdurma

Bilgisayarınızı izinsiz girişlerden ve istenmeyen ağ trafiğinden korumak istemiyorsanız Firewall'u devre dışı bırakabilirsiniz. Firewall devre dışı bırakıldığında, gelen ve giden Internet bağlantılarını yönetemezsiniz.

- 1** McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı ve sonra **Yapılandır**'ı tıklatın.
- 2** Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Kapalı**'yı tıklatın.

B Ö L Ü M 1 5

Uyarılarla çalışma

Firewall, güvenliğinizi yönetmenize yardımcı olmak için birtakım uyarılar yapar. Bu uyarılar, üç temel gruba ayrılabilir:

- Kırmızı uyarı
- Sarı uyarı
- Yeşil uyarı

Uyarılar, uyarıları nasıl işleyeceğinize karar vermenize veya bilgisayarınızda çalışan programlar hakkında bilgi almanıza yardımcı olan bilgiler de içerebilir.

Bu bölümde

Uyarılar hakkında..... 66

Uyarılar hakkında

Firewall'da üç temel uyarı türü vardır. Ayrıca, bazı uyarılar bilgisayarınızda çalışan programları öğrenmenize veya bunlarla ilgili bilgi almanıza yardımcı olan bilgiler içerir.

Kırmızı uyarı

Firewall bilgisayarınızda bir Truva atı algılayıp engellediğinde, ek tehditlere karşı tarama yapmanızı öneren bir kırmızı uyarı görüntülenir. Truva atı yasal program gibi görünür ancak bilgisayarınızı bozabilir, ona zarar verebilir ve yetkisiz erişim sağlayabilir. Bu uyarı, tüm güvenlik düzeylerinde gerçekleşir.

Sarı uyarı

En yaygın uyarı türü, Firewall tarafından algılanan bir program etkinliğini veya ağ olayını size bildiren sarı uyarıdır. Bu oluştuğunda, uyarı program etkinliğini veya ağ olayını açıklar ve sonra size yanıt vermenizi gerektiren bir veya birkaç seçenek sunar. Örneğin, Firewall yüklü bir bilgisayar yeni bir ağa bağlandığında, **Yeni Ağ Bağlantısı** uyarısı görüntülenir. Bu ağa atamak istediğiniz güven düzeyini belirtebilirsiniz ve sonra Ağlar listenizde bu ağ görüntülenir. Akıllı Öneriler etkinse, bilinen programlar otomatik olarak Program İzinleri bölümüne eklenir.

Yeşil uyarı

Pek çok durumda, yeşil uyarı bir olayla ilgili temel bilgiler verir ve sizden yanıt vermenizi istemez. Yeşil uyarılar varsayılan olarak devre dışıdır.

Kullanıcı Yardımı

Pek çok Firewall uyarısı, bilgisayarınızın güvenliğini yönetmenize yardım etmek için aşağıdaki gibi ek bilgiler içerir:

- **Bu program hakkında ek bilgi al:** Firewall'un bilgisayarınızda algıladığı bir program hakkında bilgi almak için, McAfee'nin genel güvenlik Web sitesini başlatın.
- **Bu program hakkında McAfee'yi bilgilendir:** Firewall'un bilgisayarınızda algıladığı bilinmeyen bir dosya hakkında McAfee'ye bilgi gönderin.
- **McAfee önerisi:** Uyarıların işlenmesiyle ilgili önerilerdir. Örneğin, uyarı size programa erişim izni vermenizi önerebilir.

B Ö L Ü M 1 6

Bilgi uyarılarını yönetme

Firewall, örneğin tam ekranda oyun gibi belirli olaylar sırasında izinsiz giriş denemeleri veya şüpheli etkinlik algılsa, bilgi uyarılarını görüntülenize veya gizlemenize olanak verir.

Bu bölümde

Oyun sırasında uyarıları görüntüleme	67
Bilgi uyarılarını gizleme	67

Oyun sırasında uyarıları görüntüleme

Tam ekranda oyun oynarken Firewall tarafından izinsiz giriş denemeleri veya şüpheli etkinlik algılandığında, bilgi uyarılarının görüntülenmesine izin verebilirsiniz.

- 1 McAfee SecurityCenter bölmesinde **Gelişmiş Menü**'yü tıklatın.
- 2 **Yapılandır**'ı tıklatın.
- 3 SecurityCenter Yapılandırma bölmesinde, **Uyarılar** altında **Gelişmiş**'i tıklatın.
- 4 Uyarı Seçenekleri bölmesinde **Oyun modu algılandığında bilgilendirme uyarılarını göster**'i seçin.
- 5 **Tamam**'ı tıklatın.

Bilgi uyarılarını gizleme

Firewall tarafından izinsiz giriş denemeleri veya şüpheli etkinlik algılandığında, bilgi uyarılarının görüntülenmesini engelleyebilirsiniz.

- 1 McAfee SecurityCenter bölmesinde **Gelişmiş Menü**'yü tıklatın.
- 2 **Yapılandır**'ı tıklatın.
- 3 SecurityCenter Yapılandırma bölmesinde, **Uyarılar** altında **Gelişmiş**'i tıklatın.
- 4 SecurityCenter Yapılandırma bölmesinde **Bilgi Uyarıları**'nı tıklatın.
- 5 Bilgi Uyarıları bölmesinde, aşağıdakilerden birini gerçekleştirin:
 - Tüm bilgi uyarılarını gizlemek için **Bilgi uyarılarını gösterme**'yi seçin.
 - Gizlemek için uyarının işaretini temizleyin.
- 6 **Tamam**'ı tıklatın.

B Ö L Ü M 17

Firewall korumasını yapılandırma

Firewall, güvenliğinizi yönetmek, güvenlik olayları ve uyarılara yanıt verme biçiminizi istediğiniz gibi değiştirmek için çeşitli yöntemler sunar.

Firewall'u ilk kez yüklediğinizde, bilgisayarınızın koruma düzeyi Otomatik seçeneğine ayarlıdır ve programlarınızın yalnızca giden Internet erişimine izin verilir. Ancak Firewall, kısıtlayıcı ile açık arasında değişen başka düzeyler de sunar.

Firewall, size uyarılar ve programların Internet erişimi hakkında öneriler alma fırsatı da sunar.

Bu bölümde

Firewall güvenlik düzeylerini yönetme.....	70
Akıllı Önerileri uyarılar için yapılandırma.....	72
Firewall güvenliğini iyileştirme	74
Firewall'u kilitleme ve geri yükleme.....	77

Firewall güvenlik düzeylerini yönetme

Firewall'un güvenlik düzeyleri, uyarıları ne düzeyde yönetmek ve bunlara ne kadar yanıt vermek istediğinizi kontrol eder. Program istenmeyen ağ trafiği, gelen ve giden Internet bağlantıları algıladığında bu uyarılar görüntülenir. Varsayılan olarak, Firewall'un güvenlik düzeyi yalnızca giden erişimine izin veren Otomatik seçeneğine ayarlıdır.

Otomatik güvenlik düzeyi ayarlıysa ve Akıllı Öneriler etkinse, sarı uyarılar gelen erişimi gerektiren bilinmeyen programlara erişim izni vermek veya erişimi engellemek için seçenek sunar. Yeşil uyarılar varsayılan olarak devre dışı olsa bile, bilinen programlar algılandığında bunlar görüntülenir ve otomatik olarak erişim izni verilir. Erişim izni verilmesi, programın giden bağlantılar oluşturmaya ve istenmeyen gelen bağlantıları dinlemesine olanak verir.

Genel olarak, güvenlik düzeyi ne kadar kısıtlayıcıysa (Görünmez ve Standart), görüntülenen ve dolayısıyla sizin tarafınızdan işlenmesi gereken seçeneklerin ve uyarıların sayısı o kadar artar.

Aşağıdaki tabloda, en kısıtlayıcı olandan en az kısıtlayıcı olana kadar, Firewall'un üç güvenlik düzeyi açıklanmaktadır:

Düzye	Açıklama
Görünmez	Açık portlar dışında tüm gelen Internet bağlantılarını engeller ve bilgisayarınızın Internet'teki varlığını gizler. Güvenlik duvarı, yeni programlar giden Internet bağlantıları denediğinde veya gelen bağlantı istekleri aldığıda sizi uyarır. Engellenen ve eklenen programlar, Program İzinleri bölümünde görüntülenir.
Standart	Gelen ve giden bağlantıları izler ve yeni programlar Internet'e erişmeye çalıştığıda sizi uyarır. Engellenen ve eklenen programlar, Program İzinleri bölümünde görüntülenir.
Otomatik	Programların gelen ve giden (tam) veya yalnızca giden Internet erişimine izin verir. Varsayılan güvenlik düzeyi, programların yalnızca giden erişimine izin verme seçeneği belirlenmiş durumda Otomatik olarak ayarlıdır. Bir programa tam erişim izni verilirse, Firewall programa otomatik olarak güvenir ve bunu Program İzinleri bölümünde izin verilen programlar listesine ekler. Bir programa yalnızca giden erişim izni verilirse, Firewall yalnızca giden Internet bağlantısı yaparken programa otomatik olarak güvenir. Gelen bağlantıya otomatik olarak güvenilmez.

Firewall, aynı zamanda Güvenlik Duvarı Varsayılanlarını Geri Yükle bölümünden, güvenlik düzeyinizi anında Otomatik seçeneğine sıfırlamanıza (ve yalnızca giden erişimine izin vermenize) olanak verir.

Güvenlik düzeyini Görünmez seçeneğine ayarlama

Açık portlar dışında tüm gelen ağ bağlantılarını engellemek ve bilgisayarınızın Internet'teki varlığını gizlemek için Firewall'un güvenlik düzeyini Görünmez seçeneğine ayarlayabilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Düzeyi bölümünde, **Görünmez** seçeneğinin geçerli düzey olarak görüntüleneceği şekilde kaydırma çubuğunu hareket ettirin.
- 4 **Tamam**'ı tıklatın.

Not: Görünmez modunda, yeni programlar giden Internet bağlantısı istediğinde veya gelen bağlantı istekleri aldığında Firewall sizi uyarır.

Güvenlik düzeyini Standart seçeneğine ayarlama

Gelen ve giden bağlantıları izlemek ve yeni programlar Internet'e erişmeye çalıştığında uyarı almak için güvenlik düzeyini Standart seçeneğine ayarlayabilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Düzeyi bölümünde, **Standart** seçeneğinin geçerli düzey olarak görüntüleneceği şekilde kaydırma çubuğunu hareket ettirin.
- 4 **Tamam**'ı tıklatın.

Güvenlik düzeyini Otomatik seçeneğine ayarlama

Tam erişim veya yalnızca giden ağ erişimi izni vermek için Firewall'un güvenlik düzeyini Otomatik seçeneğine ayarlayabilirsiniz.

- 1 McAfee SecurityCenter bölmesinde **Internet ve Ağ**'ı, ardından **Yapılandır**'i tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Düzeyi bölümünde, **Otomatik** seçeneğinin geçerli düzey olarak görüntüleneceği şekilde kaydırma çubuğunu hareket ettirin.
- 4 Aşağıdakilerden birini gerçekleştirin:
 - Tam gelen ve giden ağ erişimi izni vermek için **Tam Erişime İzin Ver**'i seçin.
 - Yalnızca giden ağ erişimi izni vermek için **Yalnızca Giden Erişimine İzin Ver**'i seçin.
- 5 **Tamam**'i tıklatın.

Not: Yalnızca Giden Erişimine İzin Ver, varsayılan seçenektir.

Akıllı Önerileri uyarılar için yapılandırma

Herhangi bir program Internet'e erişmeye çalıştığında, uyarılara öneriler eklemesi, eklememesi veya görüntülemesi için Firewall'u yapılandırabilirsiniz. Akıllı Önerilerin etkinleştirilmesi, uyarıları nasıl işleyeceğinize karar vermenize yardımcı olur.

Akıllı Öneriler uygulandığında (ve güvenlik düzeyi yalnızca giden erişimi etkin olarak Otomatik seçeneğine ayarlandığında), Firewall otomatik olarak bilinen programlara izin verir ve olası tehlikeli programları engeller.

Akıllı Öneriler uygulanmadığında, Firewall Internet erişimine izin vermez veya engellemez ve uyarının içinde öneri sağlamaz.

Akıllı Öneriler Göster seçeneğine ayarlandığında, uyarıyla erişime izin vermeniz veya engelleniz istenir ve Firewall uyarının içinde öneri sağlar.

Akıllı Önerileri etkinleştirme

Firewall'un otomatik olarak programlara erişim izni vermesi veya engellemesi ve tanınmayan ve tehlikeli olması olası programlar hakkında sizi uarması için Akıllı Öneriler'i etkinleştirebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'i tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Düzeyi bölümünde, **Akıllı Öneriler**'in altında **Akıllı Önerileri Uygula**'yı seçin.
- 4 **Tamam**'i tıklatın.

Akıllı Önerileri devre dışı bırakma

Firewall'un programlara erişim izni vermesi veya engellemesi ve tanınmayan ve tehlikeli olması olası programlar hakkında sizi uarması için Akıllı Öneriler'i devre dışı bırakabilirsiniz. Ancak uyarılar, programlara erişim izni verme hakkında herhangi bir öneri içermez. Firewall şüpheli veya tehdit olasılığı olduğu bilinen yeni bir program algılsa, programın Internet'e erişmesini otomatik olarak engeller.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'i tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Düzeyi bölümünde, **Akıllı Öneriler**'in altında **Akıllı Önerileri Uygulama**'yı seçin.
- 4 **Tamam**'i tıklatın.

Akıllı Önerileri görüntüleme

Uyarıların yalnızca uyarı içinde öneri görüntülemesi ve böylece tanınmayan ve tehlikeli olma olasılığı bulunan programlara izin verme veya engelleme kararını verebilmeniz için Akıllı Öneriler'i görüntüleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'i tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Düzeyi bölümünde, **Akıllı Öneriler**'in altında **Akıllı Önerileri Göster**'i seçin.
- 4 **Tamam**'i tıklatın.

Firewall güvenliğini iyileştirme

Bilgisayarınızın güvenliği çeşitli şekillerde tehlikeye girebilir. Örneğin, bazı programlar Windows® başlarken Internet'e bağlanmaya çalışabilir. Ayrıca deneyimli bilgisayar kullanıcıları, bilgisayarınızın ağa bağlı olup olmadığını belirlemek için onu izleyebilirler (ping işlemi yapabilirler). Bunun yanı sıra ileti birimleri (datagramlar) biçiminde UDP protokolünü kullanarak bilgisayarınıza bilgi gönderebilirler. Firewall, Windows başlarken programların Internet'e erişmelerini engelleyerek bu tür saldırılara karşı bilgisayarınızı korur; böylece başka kullanıcıların ağ üzerinde bilgisayarınızı algılamalarına yardımcı olan ping isteklerini engellenize ve başka kullanıcıların bilgisayarınıza ileti birimleri (datagramlar) biçiminde bilgi göndermelerini devre dışı bırakmanıza olanak verir.

Standart yükleme ayarları, Hizmet Reddi saldırıları veya suiistimler gibi en yaygın saldırı denemelerine karşı otomatik algılama özelliği içerir. Standart yükleme ayarlarının kullanılması, bu saldırılara ve taramalara karşı korunmanızı sağlar; ancak İzinsiz Giriş Tespiti bölümünde, bir veya daha fazla saldırı ya da tarama için otomatik algılamayı devre dışı bırakabilirsiniz.

Başlatma sırasında bilgisayarınızı koruma

Başlangıçta Internet erişimi bulunmayan ve şimdi buna gerek duyan yeni programları engellemek için Windows başlarken bilgisayarınızı koruyabilirsiniz. Firewall, Internet'e erişmek isteyen programlar için uygun uyarılar görüntülenir; böylece bunlara izin verebilir veya engelleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ'ı**, ardından **Yapılandır'ı** tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş'i** tıklatın.
- 3 Güvenlik Düzeyi bölümünde, **Güvenlik Ayarları** altında **Windows başlangıcında korumayı etkinleştir'i** seçin.
- 4 **Tamam'ı** tıklatın.

Not: Başlangıç koruması etkinleştirildiğinde, engellenen bağlantılar ve izinsiz girişler günlüğe kaydedilmez.

Ping isteđi ayarlarını yapılandırma

Ađ üzerinde bilgisayarınızın diđer bilgisayar kullanıcıları tarafından tespit edilmesine izin verebilir veya engelleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ađ'ı**, ardından **Yapılandır'ı** tıkladın.
- 2 Internet ve Ađ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş'i** tıkladın.
- 3 Güvenlik Düzeyi bölümünde, **Güvenlik Ayarları'nın** altında aşağıdakilerden birini gerçekleştirin:
 - Ping istekleri kullanarak bilgisayarınızın ađ üzerinde algılanmasına izin vermek için **ICMP ping isteklerine izin ver'i** seçin.
 - Ping istekleri kullanarak bilgisayarınızın ađ üzerinde algılanmasını önlemek için **ICMP ping isteklerine izin ver'i** temizleyin.
- 4 **Tamam'ı** tıkladın.

UDP ayarlarını yapılandırma

Diđer ađ bilgisayarı kullanıcılarının, UDP protokolünü kullanarak bilgisayarınıza ileti birimleri (datagramlar) göndermelerine izin verebilirsiniz. Ancak yalnızca bu protokolü engellemek için kapalı sistem hizmeti portunuz varsa bunu yapabilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ađ'ı**, ardından **Yapılandır'ı** tıkladın.
- 2 Internet ve Ađ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş'i** tıkladın.
- 3 Güvenlik Düzeyi bölümünde, **Güvenlik Ayarları'nın** altında aşağıdakilerden birini gerçekleştirin:
 - Diđer bilgisayar kullanıcılarının bilgisayarınıza ileti birimleri (datagramlar) göndermelerine izin vermek için **UDP izlemeyi etkinleştir'i** seçin.
 - Diđer bilgisayar kullanıcılarının bilgisayarınıza ileti birimleri (datagramlar) göndermelerini engellemek için **UDP izlemeyi etkinleştir'in** işaretini kaldırın.
- 4 **Tamam'ı** tıkladın.

İzinsiz giriş tespitini yapılandırma

Bilgisayarınızı saldırılardan ve yetkisiz taramalardan korumak için izinsiz giriş denemelerini tespit edebilirsiniz. Standart Firewall ayarı, Hizmet Reddi saldırıları veya suiistimaller gibi en yaygın saldırı denemelerine karşı otomatik algılama özelliği içerir; ancak bir veya daha çok saldırı veya tarama için otomatik algılamayı devre dışı bırakabilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Duvarı bölümünde **İzinsiz Giriş Tespiti**'ni tıklatın.
- 4 **İzinsiz Giriş Denemelerini Tespit Et** altında, aşağıdakilerden birini gerçekleştirin:
 - Otomatik olarak algılanacak saldırı veya taramanın adını seçin.
 - Saldırı veya taramanın otomatik olarak algılanmasını devre dışı bırakmak için adını temizleyin.
- 5 **Tamam**'i tıklatın.

Firewall Koruma Durumu ayarlarını yapılandırma

Firewall'u, bilgisayarınızda ortaya çıkan ve SecurityCenter'a bildirilmeyen belirli sorunları yok sayması için yapılandırabilirsiniz.

- 1 McAfee SecurityCenter bölümünde, **SecurityCenter Bilgisi** altında **Yapılandır**'i tıklatın.
- 2 SecurityCenter Yapılandırma bölümünde, **Koruma Durumu** altında **Gelişmiş**'i tıklatın.
- 3 Yoksayılan Sorunlar bölümünde, aşağıdaki seçeneklerden birini veya birkaçını belirleyin:
 - **Güvenlik Duvarı koruması devre dışı.**
 - **Güvenlik duvarı hizmeti çalışmıyor.**
 - **Güvenlik Duvarı Koruması bilgisayarınızda yüklü değil.**
 - **Windows Güvenlik Duvarı devre dışı.**
 - **Giden güvenlik duvarı bilgisayarınızda yüklü değil.**
- 4 **Tamam**'i tıklatın.


Firewall'u kilitleme ve geri yükleme

Kilitleme, Web sitelerine, e-postalara ve güvenlik güncelleştirmelerine erişim dahil olmak üzere tüm gelen ve giden ağ bağlantılarını anında engeller. Kilitleme, bilgisayarınızın ağ kablolarını çekmekle aynı etkiyi yapar. Bu ayarı kullanarak, Sistem Hizmetleri bölümündeki açık portları engelleyebilir ve bilgisayarınızdaki bir sorunu izole edip sorunu giderebilirsiniz.

Firewall'u anında kilitleme

Bilgisayarınız ve Internet dahil tüm ağlar arasındaki tüm ağ trafiğini anında engellemek için Firewall'u kilitleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde, **Ortak Görevler** altında **Güvenlik Duvarını Kilitle**'yi tıklatın.
- 2 Güvenlik Duvarını Kilitle bölümünde **Güvenlik Duvarı Kilitlemesini Etkinleştir**'i tıklatın.
- 3 Onaylamak için **Evet**'i tıklatın.

İpucu: Görev çubuğunun sağ ucundaki bildirim alanında bulunan SecurityCenter simgesini  sağ tıklayıp, ardından **Hızlı Bağlantılar**'ı ve sonra **Güvenlik Duvarını Kilitle**'yi tıklayarak da Firewall'u kilitleyebilirsiniz.

Firewall'un kilidini anında açma

Bilgisayarınız ve Internet dahil tüm ağlar arasındaki tüm ağ trafiğine anında izin vermek için Firewall'un kilidini açabilirsiniz.

- 1 McAfee SecurityCenter bölümünde, **Ortak Görevler** altında **Güvenlik Duvarını Kilitle**'yi tıklatın.
- 2 Kilit Etkin bölümünde **Güvenlik Duvarı Kilitlemesini Devre Dışı Bırak**'i tıklatın.
- 3 Onaylamak için **Evet**'i tıklatın.

Firewall ayarlarını geri yükleme

Firewall'u hızla özgün koruma ayarlarına geri yükleyebilirsiniz. Bu işlem, güvenlik düzeyinizi Otomatik seçeneğine sıfırlar ve yalnızca giden ağ erişimi izni verir, Akıllı Öneriler'i etkinleştirir, varsayılan programların ve izinlerinin listesini Program İzinleri bölümünde geri yükler, güvenilen ve yasaklı IP adreslerini kaldırır ve sistem hizmetlerini, olay günlüğü ayarlarını ve izinsiz giriş tespitini geri yükler.

- 1 McAfee SecurityCenter bölümünde **Güvenlik Duvarı Varsayılanlarını Geri Yükle**'yi tıklatın.**
- 2 Güvenlik Duvarı Koruması Varsayılanlarını Geri Yükle bölümünde **Varsayılanları Geri Yükle**'yi tıklatın.**
- 3 Onaylamak için **Evet**'i tıklatın.**
- 4 **Tamam**'ı tıklatın.**

B Ö L Ü M 1 8

Programları ve izinleri yönetme

Firewall, gelen ve giden Internet erişimi isteyen mevcut ve yeni programları yönetmenize ve bunlar için erişim izinleri oluşturmanıza olanak verir. Firewall, programların tam erişim veya yalnızca giden erişimini kontrol etmenizi sağlar. Ayrıca, programların erişimini engelleyebilirsiniz.

Bu bölümde

Programlara Internet erişim izni verme.....	80
Programlara yalnızca giden erişim izni verme	81
Programların Internet erişimini engelleme.....	82
Programların erişim izinlerini kaldırma	83
Programlar hakkında bilgi alma	84

Programlara İnternet erişim izni verme

İnternet tarayıcıları gibi bazı programların düzgün çalışabilmesi için İnternet'e erişmeleri gerekir.

Firewall, Program İzinleri sayfasını kullanarak aşağıdakileri yapmanıza olanak verir:

- Programlara erişim izni vermek
- Programlara yalnızca giden erişim izni vermek
- Programların erişimini engellemek

Bir programa Giden Olaylar ve Son Olaylar günlüğünden tam ve yalnızca giden İnternet erişim izni de verebilirsiniz.

Bir programa tam erişim izni verme

Bilgisayarınızdaki engellenen bir programa tam gelen ve giden İnternet erişim izni verebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **İnternet ve Ağ'ı**, ardından **Yapılandır'ı** tıklatın.
- 2 İnternet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş'i** tıklatın.
- 3 Güvenlik Duvarı bölümünde **Program İzinleri'ni** tıklatın.
- 4 **Program İzinleri'nin** altında, **Engellenen** veya **Yalnızca Giden Erişimi** seçeneğine ayarlı bir program seçin.
- 5 **Eylem** altında **Erişime İzin Ver'i** tıklatın.
- 6 **Tamam'ı** tıklatın.

Yeni bir programa tam erişim izni verme

Bilgisayarınızdaki yeni bir programa tam gelen ve giden İnternet erişim izni verebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **İnternet ve Ağ'ı**, ardından **Yapılandır'ı** tıklatın.
- 2 İnternet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş'i** tıklatın.
- 3 Güvenlik Duvarı bölümünde **Program İzinleri'ni** tıklatın.
- 4 **Program İzinleri** altında **İzin Verilen Program Ekle'yi** tıklatın.
- 5 **Program Ekle** iletişim kutusunda, eklemek istediğiniz programa gidip seçin ve sonra **Aç'ı** tıklatın.

Not: Yeni eklenen programın izinlerini, mevcut bir programın izinleri gibi değiştirebilirsiniz; bunun için programı seçin ve sonra **Eylem** altında **Yalnızca Giden Erişimine İzin Ver'i** veya **Erişimi Engelle'yi** tıklatın.

Son Olaylar günlüğünden tam erişim izni verme

Son Olaylar günlüğünde görüntülenen engellenen bir programa tam gelen ve giden Internet erişim izni verebilirsiniz.

- 1 McAfee SecurityCenter bölmesinde **Gelişmiş Menü**'yü tıklayın.
- 2 **Raporlar ve Günlükler**'i tıklayın.
- 3 **Son Olaylar** altında, olay açıklamasını seçin ve ardından **Erişime İzin Ver**'i tıklayın.
- 4 Onaylamak için Program İzinleri iletişim kutusunda **Evet**'i tıklayın.

İlgili konular

- Giden olayları görüntüleme (sayfa 101)

Giden Olaylar günlüğünden tam erişim izni verme

Giden Olaylar günlüğünde görüntülenen engellenen bir programa tam gelen ve giden Internet erişim izni verebilirsiniz.

- 1 McAfee SecurityCenter bölmesinde **Gelişmiş Menü**'yü tıklayın.
- 2 **Raporlar ve Günlükler**'i tıklayın.
- 3 **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklayın.
- 4 **Internet ve Ağ**'ı tıklayın ve sonra **Giden Olaylar**'ı tıklayın.
- 5 Bir program seçin ve **Şunu yapmak istiyorum** altında **Erişime İzin Ver**'i tıklayın.
- 6 Onaylamak için Program İzinleri iletişim kutusunda **Evet**'i tıklayın.

Programlara yalnızca giden erişim izni verme

Bilgisayarınızda bulunan bazı programlar, giden Internet erişim izni ister. Firewall, programı yalnızca giden Internet erişim izni verecek şekilde yapılandırmanızı sağlar.

Bir programa yalnızca giden erişim izni verme

Bir programa yalnızca giden Internet erişim izni verebilirsiniz.

- 1 McAfee SecurityCenter bölmesinde **Internet ve Ağ**'ı, ardından **Yapılandır**'i tıklayın.
- 2 **Internet ve Ağ Yapılandırması** bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklayın.
- 3 **Güvenlik Duvarı** bölümünde **Program İzinleri**'ni tıklayın.
- 4 **Program İzinleri** altında, **Engellenen** veya **Tam Erişim** seçeneğine ayarlı bir program seçin.
- 5 **Eylem** altında **Yalnızca Giden Erişimine İzin Ver**'i tıklayın.
- 6 **Tamam**'i tıklayın.

Son Olaylar günlüğünden yalnızca giden erişim izni verme

Son Olaylar günlüğünde görüntülenen engellenen bir programa yalnızca giden Internet erişim izni verebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Gelişmiş Menü'yü** tıklatın.
- 2 **Raporlar ve Günlükler'i** tıklatın.
- 3 **Son Olaylar** altında olay açıklamasını seçin ve sonra **Yalnızca Giden Erişimine İzin Ver'i** tıklatın.
- 4 Onaylamak için Program İzinleri iletişim kutusunda **Evet'i** tıklatın.

Giden Olaylar günlüğünden yalnızca giden erişim izni verme

Giden Olaylar günlüğünde görüntülenen engellenen bir programa yalnızca giden Internet erişim izni verebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Gelişmiş Menü'yü** tıklatın.
- 2 **Raporlar ve Günlükler'i** tıklatın.
- 3 **Son Olaylar** bölümünde, **Günlüğü Görüntüle'yi** tıklatın.
- 4 **Internet ve Ağ'ı** tıklatın ve sonra **Giden Olaylar'ı** tıklatın.
- 5 Bir program seçin ve **Şunu yapmak istiyorum** altında **Yalnızca Giden Erişimine İzin Ver'i** tıklatın.
- 6 Onaylamak için Program İzinleri iletişim kutusunda **Evet'i** tıklatın.

Programların Internet erişimini engelleme

Firewall, programların Internet'e erişmesini engellemeye olanak verir. Bir programı engellediğinizde, bunun ağ bağlantınıza veya düzgün çalışabilmesi için Internet erişimine gereksinim duyan başka bir programa engel olmayacağından emin olun.

Bir programın erişimini engelleme

Bir programın gelen ve giden Internet erişimini engelleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ'ı**, ardından **Yapılandır'ı** tıklatın.
- 2 **Internet ve Ağ Yapılandırması** bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş'i** tıklatın.
- 3 **Güvenlik Duvarı** bölümünde **Program İzinleri'ni** tıklatın.
- 4 **Program İzinleri** altında, **Tam Erişim** veya **Yalnızca Giden Erişimi** seçeneğine ayarlı bir program seçin.
- 5 **Eylem** altında **Erişimi Engelle'yi** tıklatın.
- 6 **Tamam'ı** tıklatın.

Yeni bir programın erişimini engelleme

Yeni bir programın gelen ve giden Internet erişimini engelleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ'ı**, ardından **Yapılandır'ı** tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş'i** tıklatın.
- 3 Güvenlik Duvarı bölümünde **Program İzinleri'ni** tıklatın.
- 4 **Program İzinleri** altında **Engellenen Program Ekle'yi** tıklatın.
- 5 Program Ekle iletişim kutusunda, eklemek istediğiniz programa gidip seçin ve sonra **Aç'ı** tıklatın.

Not: Yeni eklenen programın izinlerini değiştirebilirsiniz; bunun için programı seçin ve sonra **Eylem** altında **Yalnızca Giden Erişimine İzin Ver'i** veya **Erişime İzin Ver'i** tıklatın.

Son Olaylar günlüğünden erişimi engelleme

Son Olaylar günlüğünde görüntülenen bir programın gelen ve giden Internet erişimini engelleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Gelişmiş Menü'yü** tıklatın.
- 2 **Raporlar ve Günlükler'i** tıklatın.
- 3 **Son Olaylar** altında olay açıklamasını seçin ve sonra **Erişimi Engelle'yi** tıklatın.
- 4 Onaylamak için Program İzinleri iletişim kutusunda **Evet'i** tıklatın.

Programların erişim izinlerini kaldırma

Bir program iznini kaldırmadan önce, izin kaldırılınca bilgisayarınızın işlevlerinin veya ağ bağlantınızın etkilenmeyeceğinden emin olun.

Program iznini kaldırma

Bir programın gelen ve giden Internet erişimini kaldırabilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ'ı**, ardından **Yapılandır'ı** tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş'i** tıklatın.
- 3 Güvenlik Duvarı bölümünde **Program İzinleri'ni** tıklatın.
- 4 **Program İzinleri** altında bir program seçin.
- 5 **Eylem** altında **Program İznini Kaldır'ı** tıklatın.
- 6 **Tamam'ı** tıklatın.

Not: Firewall, belirli eylemleri karartarak veya devre dışı bırakarak, bazı programları değiştirmenizi önler.

Programlar hakkında bilgi alma

Hangi program iznini uygulamanız gerektiğinden emin olamıyorsanız, McAfee'nin HackerWatch Web sitesinden programla ilgili bilgi alabilirsiniz.

Program bilgilerini alma

Gelen ve giden Internet erişimine izin verme veya engelleme kararı verebilmek için McAfee'nin HackerWatch Web sitesinden program bilgileri alabilirsiniz.

Not: Tarayıcınızın, McAfee'nin programlar, Internet erişimi gereksinimleri ve güvenlik tehditleri hakkında güncel bilgiler sunan HackerWatch Web sitesini açabilmesi için Internet'e bağlandığınızdan emin olun.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ'ı**, ardından **Yapılandır'ı** tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş'i** tıklatın.
- 3 Güvenlik Duvarı bölümünde **Program İzinleri'ni** tıklatın.
- 4 **Program İzinleri** altında bir program seçin.
- 5 **Eylem** altında **Ek Bilgi'yi** tıklatın.

Giden Olaylar günlüğünden program bilgilerini alma

Giden Olaylar günlüğünde, hangi programların gelen ve giden Internet erişimine izin vereceğinize karar verebilmek için McAfee'nin HackerWatch Web sitesinden program bilgileri alabilirsiniz.

Not: Tarayıcınızın, McAfee'nin programlar, Internet erişimi gereksinimleri ve güvenlik tehditleri hakkında güncel bilgiler sunan HackerWatch Web sitesini açabilmesi için Internet'e bağlandığınızdan emin olun.

- 1 McAfee SecurityCenter bölümünde **Gelişmiş Menü'yü** tıklatın.
- 2 **Raporlar ve Günlükler'i** tıklatın.
- 3 Son Olaylar altında bir olay seçin ve sonra **Günlüğü Görüntüle'yi** tıklatın.
- 4 **Internet ve Ağ'ı** tıklatın ve sonra **Giden Olaylar'ı** tıklatın.
- 5 Bir IP adresi seçin ve sonra **Ek bilgi'yi** tıklatın.

B Ö L Ü M 19

Bilgisayar bağlantılarını yönetme

Uzak bilgisayarlarla ilişkili Internet Protokolü (IP) adreslerini temel alan kurallar oluşturarak, bilgisayarınıza yapılan belirli uzak bağlantıları yönetmek üzere Firewall'u yapılandırabilirsiniz. Güvenilen IP adresleriyle ilişkili bilgisayarların bilgisayarınıza bağlanmasına izin verilirken; bilinmeyen, şüpheli veya güvenilmeyen IP'lerin bilgisayarınıza bağlanması yasaklanabilir.

Bir bağlantıya izin verirken, güvendiğiniz bilgisayarın güvenli olduğundan emin olun. Güvenilen bir bilgisayara solucan veya başka bir mekanizma bulaşmışsa, bilgisayarınız etkilere açık olabilir. Ayrıca, McAfee güvendiğiniz bilgisayarın güvenlik duvarının yanı sıra güncel bir antivirüs programıyla korunmasını önerir. Firewall, Ağlar listesinde bulunan güvenilen IP adreslerinin trafiğini günlüğe kaydetmez veya bunlardan olay uyarıları üretmez.

Bilinmeyen, şüpheli veya güvenilmeyen IP adresleriyle ilişkili bilgisayarların, bilgisayarınıza bağlanmasını yasaklayabilirsiniz.

Firewall tüm istenmeyen trafiği engellediği için, genellikle bir IP adresini yasaklamanız gerekmez. Bir IP adresini ancak Internet bağlantısının belirli bir tehdit olduğundan eminseniz yasaklamalısınız. DNS veya DHCP sunucunuz ya da diğer ISS ile ilişkili sunucular gibi önemli IP adreslerini engellemediğinizden emin olun.

Bu bölümde

Bilgisayar bağlantıları hakkında	86
Bilgisayar bağlantılarını yasaklama	89

Bilgisayar bağlantıları hakkında

Bilgisayar bağlantıları, herhangi bir ağ ile kendi ağınız üzerindeki bilgisayarlar arasında oluşturduğunuz bağlantılardır. **Ağlar** listesinde IP adresleri ekleyebilir, düzenleyebilir ve kaldırabilirsiniz. Bu IP adresleri, bilgisayarınıza bağlanırken bir güvenlik düzeyi atamak istediğiniz ağlarla ilişkilidir: Güvenilen, Standart ve Kamu.

Düzye	Açıklama
Güvenilen	Firewall, bir IP'den gelen trafiğin herhangi bir port aracılığıyla bilgisayarınıza erişmesine izin verir. Güvenilen bir IP adresiyle ilişkili bilgisayar ve sizin bilgisayarınız arasındaki etkinlik, Firewall tarafından filtrelenmez veya analiz edilmez. Varsayılan olarak, Firewall'un bulunduğu ilk özel ağ, Ağlar listesinde Güvenilen olarak listelenir. Yerel veya ev ağınızdaki bilgisayar veya bilgisayarlar, Güvenilen ağa örnek olarak verilebilir.
Standart	Firewall, bilgisayarınıza bağlandığında IP'den (ancak bu ağdaki herhangi bir bilgisayardan değil) gelen trafiği denetler ve Sistem Hizmetleri listesindeki kurallara göre buna izin verir veya engeller. Firewall, trafiği günlüğe kaydeder ve Standart IP adreslerinden olay uyarıları üretir. Şirket ağınızdaki bilgisayar veya bilgisayarlar, Standart ağa örnek olarak verilebilir.
Kamu	Firewall, Sistem Hizmetleri listesindeki kurallara göre kamu ağından gelen trafiği denetler. Bir kafede, otelde veya havaalanında bulunan Internet ağı Kamu ağına örnek olarak verilebilir.

Bir bağlantıya izin verirken, güvendiğiniz bilgisayarın güvenli olduğundan emin olun. Güvenilen bir bilgisayara solucan veya başka bir mekanizma bulaşmışsa, bilgisayarınız etkilere açık olabilir. Ayrıca, McAfee güvendiğiniz bilgisayarın güvenlik duvarının yanı sıra güncel bir antivirüs programıyla korunmasını önerir.

Bilgisayar bağlantısı ekleme

Güvenilen, standart veya kamu bilgisayar bağlantısı ve bununla ilişkili IP adresi ekleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ'ı**, ardından **Yapılandır'ı** tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş'i** tıklatın.
- 3 Güvenlik Duvarı bölümünde **Ağlar'ı** tıklatın.
- 4 Ağlar bölümünde **Ekle'yi** tıklatın.
- 5 Bilgisayar bağlantısı IPv6 ağı üzerindeyse, **IPv6 onay** kutusunu seçin.

- 6 Kural Ekle** altında aşağıdakilerden birini gerçekleştirin:
- **Tek**'i seçin ve sonra IP adresini **IP Adresi** kutusuna girin.
 - **Aralık**'i seçin ve sonra **IP Adreslerinden** ve **IP Adreslerine** kutularına başlangıç ve bitiş IP adreslerini girin. Bilgisayar bağlantınız bir IPv6 ağı üzerindeyse, **IP Adreslerinden** ve **Önek Uzunluğu** kutularına başlangıç IP adresini ve önek uzunluğunu girin.
- 7 Tür** altında aşağıdakilerden birini gerçekleştirin:
- Bu bilgisayar bağlantısına güvenildiğini belirtmek için **Güvenilen**'i seçin (örneğin ev ağındaki bir bilgisayar).
 - Bu bilgisayar bağlantısına (ağıdaki bilgisayarlara değil) güvenildiğini belirtmek için **Standart**'i seçin (örneğin şirket ağındaki bir bilgisayar).
 - Bu bilgisayar bağlantısının kamu olduğunu belirtmek için **Kamu**'yu seçin (örneğin Internet kafedeki, oteldeki veya havaalanındaki bir bilgisayar).
- 8** Sistem hizmeti Internet Bağlantısı Paylaşımı (ICS) kullanıyorsa, şu IP adresi aralığını ekleyebilirsiniz: 192.168.0.1 - 192.168.0.255.
- 9** İsterseniz, **Kuralın geçerlilik süresi**'ni seçip, kuralın geçerli olacağı gün sayısını girebilirsiniz.
- 10** Ayrıca, kural için bir açıklama da yazabilirsiniz.
- 11 Tamam**'ı tıklatın.

Not: Internet Bağlantısı Paylaşımı (ICS) hakkında ayrıntılı bilgi için bkz. Yeni bir sistem hizmeti yapılandırma.

Gelen Olaylar günlüğünden bir bilgisayarı ekleme

Gelen Olaylar günlüğünden güvenilen veya standart bir bilgisayar bağlantısını ve onunla ilişkili IP adresini ekleyebilirsiniz.

- 1** McAfee SecurityCenter bölmesinde, Ortak Görevler bölümünde **Gelişmiş Menü**'yü tıklatın.
- 2** **Raporlar ve Günlükler**'i tıklatın.
- 3** **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklatın.
- 4** **Internet ve Ağ**'i tıklatın ve sonra **Gelen Olaylar**'i tıklatın.
- 5** Bir kaynak IP adresi seçin ve **Şunu yapmak istiyorum** altında aşağıdakilerden birini gerçekleştirin:
 - Bu bilgisayarı **Ağlar** listenize Güvenilen olarak eklemek için **Bu IP'yi Güvenilen olarak ekle**'yi tıklatın.
 - Bu bilgisayar bağlantısını **Ağlar** listenize Standart olarak eklemek için **Bu IP'yi Standart olarak ekle**'yi tıklatın.
- 6** Onaylamak için **Evet**'i tıklatın.

Bilgisayar bağlantısını düzenleme

Güvenilen, standart veya kamu bilgisayar bağlantısını ve bununla ilişkili IP adresini düzenleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Duvarı bölümünde **Ağlar**'ı tıklatın.
- 4 Ağlar bölümünde bir IP adresi seçin ve ardından **Düzenle**'yi tıklatın.
- 5 Bilgisayar bağlantısı IPv6 ağı üzerindeyse, **IPv6** onay kutusunu seçin.
- 6 **Kuralı Düzenle** altında aşağıdakilerden birini gerçekleştirin:
 - **Tek**'i seçin ve sonra IP adresini **IP Adresi** kutusuna girin.
 - **Aralık**'i seçin ve sonra **IP Adreslerinden** ve **IP Adreslerine** kutularına başlangıç ve bitiş IP adreslerini girin. Bilgisayar bağlantınız bir IPv6 ağı üzerindeyse, **IP Adreslerinden** ve **Önek Uzunluğu** kutularına başlangıç IP adresini ve önek uzunluğunu girin.
- 7 **Tür** altında aşağıdakilerden birini gerçekleştirin:
 - Bu bilgisayar bağlantısına güvenildiğini belirtmek için **Güvenilen**'i seçin (örneğin ev ağındaki bir bilgisayar).
 - Bu bilgisayar bağlantısına (ağıdaki bilgisayarlara değil) güvenildiğini belirtmek için **Standart**'i seçin (örneğin şirket ağındaki bir bilgisayar).
 - Bu bilgisayar bağlantısının kamu olduğunu belirtmek için **Kamu**'yu seçin (örneğin Internet kafedeki, oteldeki veya havaalanındaki bir bilgisayar).
- 8 İsterseniz **Kuralın geçerlilik süresi**'ni işaretleyip, kuralın geçerli olacağı gün sayısını girebilirsiniz.
- 9 Ayrıca, kural için bir açıklama da yazabilirsiniz.
- 10 **Tamam**'ı tıklatın.

Not: Firewall'un güvenilen özel ağdan otomatik olarak eklediği varsayılan bilgisayar bağlantısını düzenleyemezsiniz.

Bilgisayar bağlantısını kaldırma

Güvenilen, standart veya kamu bilgisayar bağlantısını ve bununla ilişkili IP adresini kaldırabilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Duvarı bölümünde **Ağlar**'ı tıklatın.
- 4 Ağlar bölümünde bir IP adresi seçin ve ardından **Kaldır**'i tıklatın.
- 5 Onaylamak için **Evet**'i tıklatın.

Bilgisayar bağlantılarını yasaklama

Yasaklı IP'ler bölümünde, yasaklanan IP adresleri ekleyebilir, düzenleyebilir ve kaldırabilirsiniz.

Bilinmeyen, şüpheli veya güvenilmeyen IP adresleriyle ilişkili bilgisayarların, bilgisayarınıza bağlanmasını yasaklayabilirsiniz.

Firewall tüm istenmeyen trafiği engellediği için, genellikle bir IP adresini yasaklamanız gerekmez. Bir IP adresini ancak Internet bağlantısının belirli bir tehdit olduğundan eminseniz yasaklamalısınız. DNS veya DHCP sunucunuz ya da diğer ISS ile ilişkili sunucular gibi önemli IP adreslerini engellemediğinizden emin olun.

Yasaklanan bilgisayar bağlantısı ekleme

Yasaklanan bir bilgisayar bağlantısı ve bununla ilişkili IP adresi ekleyebilirsiniz.

Not: DNS veya DHCP sunucunuz ya da diğer ISS ile ilişkili sunucular gibi önemli IP adreslerini engellemediğinizden emin olun.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'i tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Duvarı bölümünde, **Yasaklı IP'ler** seçeneğini tıklatın.
- 4 Yasaklı IP'ler bölümünde, **Ekle**'yi tıklatın.
- 5 Bilgisayar bağlantısı IPv6 ağı üzerindeyse, **IPv6** onay kutusunu seçin.

- 6 **Kural Ekle** altında aşağıdakilerden birini gerçekleştirin:
 - **Tek**'i seçin ve sonra IP adresini **IP Adresi** kutusuna girin.
 - **Aralık**'i seçin ve sonra **IP Adreslerinden** ve **IP Adreslerine** kutularına başlangıç ve bitiş IP adreslerini girin. Bilgisayar bağlantınız bir IPv6 ağı üzerindeyse, **IP Adreslerinden** ve **Önek Uzunluğu** kutularına başlangıç IP adresini ve önek uzunluğunu girin.
- 7 İsterseniz, **Kuralın geçerlilik süresi**'ni seçip, kuralın geçerli olacağı gün sayısını girebilirsiniz.
- 8 Ayrıca, kural için bir açıklama da yazabilirsiniz.
- 9 **Tamam**'ı tıklatın.
- 10 Onaylamak için **Evet**'i tıklatın.

Yasaklanan bilgisayar bağlantısını düzenleme

Yasaklanan bir bilgisayar bağlantısını ve bununla ilişkili IP adresini düzenleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde **İnternet ve Ağ**'ı, ardından **Yapılandır**'i tıklatın.
- 2 İnternet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Duvarı bölümünde, **Yasaklı IP'ler** seçeneğini tıklatın.
- 4 Yasaklı IP'ler bölümünde, **Düzenle**'yi tıklatın.
- 5 Bilgisayar bağlantısı IPv6 ağı üzerindeyse, **IPv6 onay** kutusunu seçin.
- 6 **Kuralı Düzenle** altında aşağıdakilerden birini gerçekleştirin:
 - **Tek**'i seçin ve sonra IP adresini **IP Adresi** kutusuna girin.
 - **Aralık**'i seçin ve sonra **IP Adreslerinden** ve **IP Adreslerine** kutularına başlangıç ve bitiş IP adreslerini girin. Bilgisayar bağlantınız bir IPv6 ağı üzerindeyse, **IP Adreslerinden** ve **Önek Uzunluğu** kutularına başlangıç IP adresini ve önek uzunluğunu girin.
- 7 İsterseniz, **Kuralın geçerlilik süresi**'ni seçip, kuralın geçerli olacağı gün sayısını girebilirsiniz.
- 8 Ayrıca, kural için bir açıklama da yazabilirsiniz.
- 9 **Tamam**'ı tıklatın.

Yasaklanan bilgisayar bağlantısını kaldırma

Yasaklanan bir bilgisayar bağlantısını ve bununla ilişkili IP adresini kaldırabilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Duvarı bölümünde, **Yasaklı IP'ler** seçeneğini tıklatın.
- 4 Yasaklı IP'ler bölümünde bir IP adresi seçin ve sonra **Kaldır**'ı tıklatın.
- 5 Onaylamak için **Evet**'i tıklatın.

Gelen Olaylar günlüğünden bir bilgisayarı yasaklama

Gelen Olaylar günlüğünden bir bilgisayar bağlantısını ve onunla ilişkili IP adresini yasaklayabilirsiniz. Şüpheli veya istenmeyen Internet etkinliğinin kaynağı olduğundan şüphelendiğiniz bir IP adresini yasaklamak için tüm gelen Internet trafiğinin IP adreslerini listeleyen bu günlüğü kullanın.

Sistem Hizmetleri portlarınızın açık veya kapalı olmasına bakılmaksızın bir IP adresinden gelen tüm Internet trafiğini engellemek için **Yasaklı IP'ler** listenize bir IP adresi ekleyin.

- 1 McAfee SecurityCenter bölümünde, **Ortak Görevler** altında, **Gelişmiş Menü**'yü tıklatın.
- 2 **Raporlar ve Günlükler**'i tıklatın.
- 3 **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklatın.
- 4 **Internet ve Ağ**'ı tıklatın ve sonra **Gelen Olaylar**'ı tıklatın.
- 5 Kaynak IP adresini seçin ve **Şunu yapmak istiyorum** altında **Bu IP'yi Yasakla** seçeneğini tıklatın.
- 6 Onaylamak için **Evet**'i tıklatın.

İzinsiz Giriş Tespiti Olayları günlüğünden bir bilgisayarı yasaklama

İzinsiz Giriş Tespiti Olayları günlüğünden, bir bilgisayar bağlantısını ve onunla ilişkili IP adresini yasaklayabilirsiniz.

- 1** McAfee SecurityCenter bölmesinde, **Ortak Görevler** altında, **Gelişmiş Menü**'yü tıklatın.
- 2** **Raporlar ve Günlükler**'i tıklatın.
- 3** **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklatın.
- 4** **Internet ve Ağ**'ı tıklatın ve ardından **İzinsiz Giriş Tespiti Olayları**'nı tıklatın.
- 5** Kaynak IP adresini seçin ve **Şunu yapmak istiyorum** altında **Bu IP'yi Yasakla** seçeneğini tıklatın.
- 6** Onaylamak için **Evet**'i tıklatın.

B Ö L Ü M 2 0

Sistem hizmetlerini yönetme

Düzenli çalışabilmeleri için, bazı programların (web sunucuları ve dosya paylaşımı sunucu programları dahil) atanmış sistem hizmeti portları aracılığıyla, başka bilgisayarlardan istenmeyen bağlantıları kabul etmeleri gerekir. Sisteminizde güvenli olmama olasılığı bulunan kaynakları temsil ettikleri için, Firewall genellikle bu sistem hizmeti portlarını kapatır. Ancak uzak bilgisayarlardan bağlantıları kabul etmek için, sistem hizmeti portları açık olmalıdır.

Bu bölümde

Sistem hizmeti portlarını yapılandırma 94

Sistem hizmeti portlarını yapılandırma

Sistem hizmeti portları, bilgisayarınızda bir hizmete uzak ağ erişimi izni verecek veya engelleyecek şekilde yapılandırılabilir. Bu sistem hizmeti portları, **Ağlar** listenizde Güvenilen, Standart veya Kamu olarak listelenen bilgisayarlar için açılabilir veya kapatılabilir.

Aşağıdaki listede, yaygın sistem hizmetleri ve ilişkili portları gösterilmektedir:

- Ortak İşletim Sistemi Portu 5357
- Dosya Aktarım Protokolü (FTP) Portları 20-21
- Posta Sunucusu (IMAP) Portu 143
- Posta Sunucusu (POP3) Portu 110
- Posta Sunucusu (SMTP) Portu 25
- Microsoft Directory Server (MSFT DS) Portu 445
- Microsoft SQL Server (MSFT SQL) Portu 1433
- Ağ Saati Protokolü Portu 123
- Uzak Masaüstü / Uzaktan Yardım / Terminal Server (RDP) Portu 3389
- Uzaktan Yordam Çağruları (RPC) Portu 135
- Güvenli Web Sunucusu (HTTPS) Portu 443
- Evrensel Tak ve Kullan (UPNP) Portu 5000
- Web Sunucusu (HTTP) Portu 80
- Windows Dosya Paylaşımı (NETBIOS) Portları 137-139

Sistem hizmeti portları, bilgisayarın Internet bağlantısını aynı ağ aracılığıyla kendisine bağlı başka bilgisayarlarla paylaşmasına izin verecek şekilde de yapılandırılabilir. Internet Bağlantısı Paylaşımı (ICS) olarak adlandırılan bu bağlantı, bağlantıyı paylaşan bilgisayarın ağ üzerindeki diğer bilgisayarlar için Internet'e açılan bir ağ geçidi görevi görmesine olanak verir.

Not: Bilgisayarınızda web veya FTP sunucusu bağlantılarını kabul eden bir uygulama varsa, bağlantıyı paylaşan bilgisayarın ilişkili sistem hizmeti portunu açması ve bu portlar için gelen bağlantıların iletilmesine izin vermesi gerekebilir.

Mevcut sistem hizmeti portuna erişim izni verme

Mevcut bir portu, bilgisayarınızda bir sistem hizmetine uzak ağ erişimi izni vermesi için açabilirsiniz.

Not: Açık sistem hizmeti portu, bilgisayarınızı Internet güvenliği tehditlerine açabilir; bu nedenle yalnızca gerekli olursa bir port açın.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ'ı**, ardından **Yapılandır**'i tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Duvarı bölümünde **Sistem Hizmetleri**'ni tıklatın.
- 4 **Sistem Hizmeti Portu Aç** altında portunu açmak için bir sistem hizmeti seçin.
- 5 **Düzenle**'yi tıklatın.
- 6 Aşağıdakilerden birini gerçekleştirin:
 - Portu güvenilen, standart veya kamu ağı üzerinde herhangi bir bilgisayara açmak için (örneğin ev ağında, şirket ağında veya Internet ağında) **Güvenilen, Standart ve Kamu**'yu seçin.
 - Portu standart ağ üzerinde herhangi bir bilgisayara açmak için (örneğin şirket ağında) **Standart (Güvenilen dahil)** seçeneğini belirleyin.
- 7 **Tamam**'i tıklatın.

Mevcut sistem hizmeti portuna erişimi engelleme

Mevcut bir portu, bilgisayarınızda bir sistem hizmetine uzak ağ erişimini engellemesi için kapatabilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ'ı**, ardından **Yapılandır**'i tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Duvarı bölümünde **Sistem Hizmetleri**'ni tıklatın.
- 4 **Sistem Hizmeti Portu Aç** altında, kapatmak istediğiniz sistem hizmeti portunun yanındaki onay kutusunun işaretini kaldırın.
- 5 **Tamam**'i tıklatın.

Yeni bir sistem hizmeti portunu yapılandırma

Bilgisayarınızda, bilgisayarınızdan uzaktan erişime izin vermeyi veya engellemeyi açıp kapatabileceğiniz yeni bir ağ hizmet portu yapılandırabilirsiniz.

- 1 McAfee SecurityCenter bölümünde **Internet ve Ağ'ı**, ardından **Yapılandır**'i tıklatın.
- 2 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3 Güvenlik Duvarı bölümünde **Sistem Hizmetleri**'ni tıklatın.
- 4 **Ekle**'yi tıklatın.
- 5 Sistem Hizmetleri bölümünde, **Sistem Hizmeti Kuralı Ekle** altında şunları girin:
 - Sistem Hizmeti adı
 - Sistem Hizmeti kategorisi
 - Yerel TCP/IP portları
 - Yerel UDP portları
- 6 Aşağıdakilerden birini gerçekleştirin:
 - Portu güvenilen, standart veya kamu ağı üzerinde herhangi bir bilgisayara açmak için (örneğin ev ağında, şirket ağında veya Internet ağında) **Güvenilen, Standart ve Kamu**'yu seçin.
 - Portu standart ağ üzerinde herhangi bir bilgisayara açmak için (örneğin şirket ağında) **Standart (Güvenilen dahil)** seçeneğini belirleyin.
- 7 Bu portun etkinlik bilgilerini, Internet bağlantınızı paylaşan başka bir Windows ağ bilgisayarına göndermek isterseniz, **Bu portun ağ etkinliğini, Internet Bağlantısı Paylaşımı kullanan ağ bilgisayarlarına iletin** seçeneğini belirleyin.
- 8 İsterseniz, yeni yapılandırmaya açıklama ekleyebilirsiniz.
- 9 **Tamam**'i tıklatın.

Not: Bilgisayarınızda web veya FTP sunucusu bağlantılarını kabul eden bir program varsa, bağlantıyı paylaşan bilgisayarın ilişkili sistem hizmeti portunu açması ve bu portlar için gelen bağlantıların iletilmesine izin vermesi gerekebilir. Internet Bağlantısı Paylaşımı (ICS) özelliğini kullanıyorsanız, **Ağlar** listesine güvenilen bilgisayar bağlantısı da eklemeniz gerekebilir. Ayrıntılı bilgi için bkz. Bilgisayar bağlantısı ekleme

Sistem hizmeti portunu deęiřtirme

Mevcut sistem hizmeti portuyla ilgili gelen ve giden aę eriřimi bilgilerini deęiřtirebilirsiniz.

Not: Port bilgisi yanlış girilirse, sistem hizmeti başarısız olur.

- 1 McAfee SecurityCenter bölmesinde **Internet ve Aęı**, ardından **Yapılandır**'i tıklatın.
- 2 Internet ve Aę Yapılandırması bölmesinde, **Güvenlik Duvarı koruma etkin** altında **Geliřmiř**'i tıklatın.
- 3 Güvenlik Duvarı bölmesinde **Sistem Hizmetleri**'ni tıklatın.
- 4 Bir sistem hizmetinin yanındaki onay kutusunu tıklatın ve sonra **Düzenle**'yi tıklatın.
- 5 Sistem Hizmetleri bölmesinde, **Sistem Hizmeti Kuralı Ekle** altında şunları deęiřtirin:
 - Sistem hizmeti adı
 - Yerel TCP/IP portları
 - Yerel UDP portları
- 6 Ařaęıdakilerden birini gerekleřtirin:
 - Portu güvenli, standart veya kamu aęı üzerinde herhangi bir bilgisayara açmak için (örneğin ev aęında, řirket aęında veya Internet aęında) **Güvenilen, Standart ve Kamu**'yu seçin.
 - Portu standart aę üzerinde herhangi bir bilgisayara açmak için (örneğin řirket aęında) **Standart (Güvenilen dahil)** seçeneęini belirleyin.
- 7 Bu portun etkinlik bilgilerini, Internet bağlantınızı paylařan başka bir Windows aę bilgisayarına göndermek isterseniz, **Bu portun aę etkinlięini, Internet Bağlantısı Paylařımı kullanan aę bilgisayarlarına iletin** seçeneęini belirleyin.
- 8 İsterseniz, deęiřtirilen yapılandırmaya açıklama ekleyebilirsiniz.
- 9 **Tamam**'i tıklatın.

Sistem hizmeti portunu kaldırma

Mevcut bir sistem hizmeti portunu bilgisayarınızdan kaldırabilirsiniz. Kaldırdıktan sonra, uzak bilgisayarlar artık bilgisayarınızdaki ağ hizmetine erişemez.

- 1** McAfee SecurityCenter bölümünde **Internet ve Ağ**'ı, ardından **Yapılandır**'ı tıklatın.
- 2** Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 3** Güvenlik Duvarı bölümünde **Sistem Hizmetleri**'ni tıklatın.
- 4** Bir sistem hizmeti seçin ve **Kaldır**'ı tıklatın.
- 5** Onaylamak için açılan sorgu penceresinde **Evet**'i tıklatın.

B Ö L Ü M 2 1

Günlüğe kaydetme, izleme ve analiz

Firewall, İnternet olayları ve trafiğinin kapsamlı ve okunması kolay bir biçimde günlüğe kaydedilmesini, izlenmesini ve analizini sağlar. İnternet trafiğini ve olayları anlamak, İnternet bağlantılarınızı yönetmenize yardımcı olur.

Bu bölümde

Olay Günlüğü Kaydetme.....	100
İstatistiklerle Çalışma.....	102
İnternet trafiğini izleme.....	102
İnternet trafiğini izleme.....	105

Olay Günlüğü Kaydetme

Firewall, olay günlüğü kaydetmeyi etkinleştirmenize veya devre dışı bırakmanıza ve etkinleştirildiğinde hangi olay türlerinin günlüğe kaydedileceğini belirlemenize olanak verir. Olay günlüğüne kaydetme, en son gelen ve giden olayları görüntülemenizi sağlar.

Olay günlüğü ayarlarını yapılandırma

Günlüğe kaydedilecek Firewall olaylarının türlerini belirtebilir ve bunları yapılandırabilirsiniz. Varsayılan olarak, olay günlüğü kaydetme tüm olaylar ve etkinlikler için etkindir.

- 1 Internet ve Ağ Yapılandırması bölümünde, **Güvenlik Duvarı koruma etkin** altında **Gelişmiş**'i tıklatın.
- 2 Güvenlik Duvarı bölümünde **Olay Günlüğü Ayarları**'ni tıklatın.
- 3 Zaten seçili değilse, **Olay Günlüğü Kaydetmeyi Etkinleştir**'i seçin.
- 4 **Olay Günlüğü Kaydetmeyi Etkinleştir** altında günlüğe kaydedilmesini istediğiniz veya istemediğiniz olay türlerini seçin veya seçimini kaldırın. Olay türleri aşağıdakileri içerir:
 - Engellenen Programlar
 - ICMP Pingleri
 - Yasaklı IP Adreslerinden Gelen Trafik
 - Sistem Hizmet Portları İle İlgili Olaylar
 - Bilinmeyen Portları İle İlgili Olaylar
 - İzinsiz Giriş Tespiti (IDS) olayları
- 5 Belirli portlarda günlük kaydını engellemek için, **Aşağıdaki portlarla ilgili olayları günlüğe kaydetme**'yi seçin ve ardından tek port numaralarını virgüllerle, port aralıklarını tirelerle ayırarak girin. Örnek: 137-139, 445, 400-5000.
- 6 **Tamam**'i tıklatın.

Son olayları görüntüleme

Günlük kaydı etkinse, son olayları görüntüleyebilirsiniz. Son Olaylar bölümünde, olayın tarihi ve açıklaması görüntülenir. Bu bölme, Internet erişimi açıkça engellenmiş olan programların etkinliğini görüntüler.

- **Gelişmiş Menü**'de, Ortak Görevler bölümünde **Raporlar ve Günlükler**'i veya **Son Olayları Görüntüle**'yi tıklatın. İsterseniz Temel Menü'de, Ortak Görevler bölümünde **Son Olayları Görüntüle**'yi tıklatabilirsiniz.

Gelen olayları görüntüleme

Günlük kaydı etkinse, gelen olayları görüntüleyebilirsiniz. Gelen Olaylar; tarih ve saati, kaynak IP adresini, ana bilgisayar adını, bilgi ve olay türünü içerir.

- 1 Gelişmiş menünün etkin olduğundan emin olun. Ortak Görevler bölümünde **Raporlar ve Günlükler**'i tıklayın.
- 2 **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklayın.
- 3 **Internet ve Ağ**'ı tıklayın ve sonra **Gelen Olaylar**'ı tıklayın.

Not: Gelen Olay günlüğünde bir IP adresini güvenilen, yasaklanan veya izlenen olarak belirleyebilirsiniz.

Giden olayları görüntüleme

Günlük kaydı etkinse, giden olayları görüntüleyebilirsiniz. Giden Olaylar, giden erişim sağlamaya çalışan programın adını, olay tarihi ve saatini, programın bilgisayarınızdaki konumunu içerir.

- 1 Ortak Görevler bölümünde **Raporlar ve Günlükler**'i tıklayın.
- 2 **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklayın.
- 3 **Internet ve Ağ**'ı tıklayın ve sonra **Giden Olaylar**'ı tıklayın.

Not: Giden Olaylar günlüğünden, bir programa tam erişim veya yalnızca giden erişim izni verebilirsiniz. Ayrıca, programla ilgili ek bilgiler de bulabilirsiniz.

İzinsiz giriş tespiti olaylarını görüntüleme

Günlük kaydı etkinse, gelen izinsiz giriş olaylarını görüntüleyebilirsiniz. İzinsiz Giriş Tespiti olayları; olayın tarih ve saatini, kaynak IP'sini, ana bilgisayar adını ve türünü görüntüler.

- 1 Ortak Görevler bölümünde **Raporlar ve Günlükler**'i tıklayın.
- 2 **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklayın.
- 3 **Internet ve Ağ**'ı ve sonra **İzinsiz Giriş Tespiti Olayları**'nı tıklayın.

Not: İzinsiz Giriş Tespiti Olayları günlüğünde, bir IP adresini yasaklanan ve izlenen olarak belirleyebilirsiniz.

İstatistiklerle Çalışma

Firewall, size genel İnternet güvenliği olayları ve port etkinliği hakkında istatistikler sunmak için, McAfee'nin HackerWatch güvenlik Web sitesini destekler.

Genel güvenlik olayı istatistiklerini görüntüleme

HackerWatch, SecurityCenter'da görüntüleyebileceğiniz dünya çapındaki İnternet güvenliği olaylarını izler. İzleme bilgilerinde son 24 saat, 7 gün ve 30 gün içinde HackerWatch'a raporlanan olaylar listelenir.

- 1 Gelişmiş Menü'nün etkin olduğundan emin olun ve ardından **Araçlar**'ı tıklatın.
- 2 Araçlar bölümünde **HackerWatch**'u tıklatın.
- 3 Olay İzleme altında güvenlik olayı istatistiklerini görüntüleyin.

Genel İnternet port etkinliğini görüntüleme

HackerWatch, SecurityCenter'da görüntüleyebileceğiniz dünya çapındaki İnternet güvenliği olaylarını izler. Görüntülenen bilgiler, son yedi gün içinde HackerWatch'a rapor edilen en son olay portlarını içerir. Genellikle HTTP, TCP ve UDP port bilgileri görüntülenir.

- 1 Gelişmiş Menü'nün etkin olduğundan emin olun ve ardından **Araçlar**'ı tıklatın.
- 2 Araçlar bölümünde **HackerWatch**'u tıklatın.
- 3 **En Son Port Etkinliği** altında en son olay portlarını görüntüleyin.

İnternet trafiğini izleme

Firewall, İnternet trafiğini izlemek için çeşitli seçenekler sunar. Bu seçenekler, bir ağ bilgisayarının coğrafi konumunu izlemenize, etki alanı ve ağ bilgilerini elde etmenize, Gelen Olaylar ve İzinsiz Giriş Tespiti Olayları günlüklerinden bilgisayarları izlemenize olanak verir.

Bir ağ bilgisayarının coğrafi konumunu izleme

Görsel İzleyici kullanarak, bilgisayarınıza bağlanan veya bağlanmaya çalışan bir bilgisayarın coğrafi konumunu, adı veya IP adresi ile bulabilirsiniz. Ayrıca, Görsel İzleyici ile ağ ve kayıt bilgilerine de erişebilirsiniz. Görsel İzleyici çalıştırıldığında, kaynak bilgisayardan sizin bilgisayarınıza alınan veriler için en olası yolu gösteren bir dünya haritası görüntülenir.

- 1 Gelişmiş Menü'nün etkin olduğundan emin olun ve ardından **Araçlar**'ı tıklatın.
- 2 Araçlar bölümünde **Görsel İzleyici**'yi tıklatın.
- 3 Bilgisayarın IP adresini yazın ve **İzle**'yi tıklatın.
- 4 **Görsel İzleyici** altında **Harita Görünümü**'nü seçin.

Not: Döngüsel, özel veya geçersiz IP adresi olaylarını izleyemezsiniz.

Bilgisayar kayıt bilgilerini elde etme

Visual Trace kullanarak, SecurityCenter'dan bir bilgisayarın kayıt bilgilerini elde edebilirsiniz. Bu bilgiler etki alanı adını, kayıt adı ve adresini, yönetici iletişim bilgilerini içerir.

- 1 Gelişmiş Menü'nün etkin olduğundan emin olun ve ardından **Araçlar**'ı tıklatın.
- 2 Araçlar bölümünde **Görsel İzleyici**'yi tıklatın.
- 3 Bilgisayarın IP adresini yazın ve ardından **İzle**'yi tıklatın.
- 4 **Görsel İzleyici** altında **Kayıt Görünümü**'nü seçin.

Bilgisayar ağ bilgilerini elde etme

Visual Trace kullanarak, SecurityCenter'dan bir bilgisayarın ağ bilgilerini elde edebilirsiniz. Ağ bilgileri, etki alanının bulunduğu ağ ile ilgili ayrıntıları içerir.

- 1 Gelişmiş Menü'nün etkin olduğundan emin olun ve ardından **Araçlar**'ı tıklatın.
- 2 Araçlar bölümünde **Görsel İzleyici**'yi tıklatın.
- 3 Bilgisayarın IP adresini yazın ve ardından **İzle**'yi tıklatın.
- 4 **Görsel İzleyici** altında **Ağ Görünümü**'nü seçin.

Gelen Olaylar günlüğünden bir bilgisayarı izleme

Gelen Olaylar bölümünden, Gelen Olaylar günlüğünde görüntülenen bir IP adresini izleyebilirsiniz.

- 1 Gelişmiş menünün etkin olduğundan emin olun. Ortak Görevler bölümünde **Raporlar ve Günlükler**'i tıklayın.
- 2 **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklayın.
- 3 **Internet ve Ağ**'ı tıklayın ve sonra **Gelen Olaylar**'ı tıklayın.
- 4 Gelen Olaylar bölümünde, bir kaynak IP adresi seçin ve ardından **Bu IP'yi izle** seçeneğini tıklayın.
- 5 Görsel İzleyici bölümünde, aşağıdakilerden birini tıklayın:
 - **Harita Görünümü**: Seçili IP adresini kullanarak bilgisayarın coğrafi konumunu bulun.
 - **Kayıt Görünümü**: Seçili IP adresini kullanarak etki alanı bilgilerini bulun.
 - **Ağ Görünümü**: Seçili IP adresini kullanarak ağ bilgilerini bulun.
- 6 **Bitti**'yi tıklayın.

İzinsiz Giriş Tespiti Olayları günlüğünden bir bilgisayarı izleme

İzinsiz Giriş Tespiti Olayları bölümünden, İzinsiz Giriş Tespiti Olayları günlüğünde görüntülenen bir IP adresini izleyebilirsiniz.

- 1 Ortak Görevler bölümünde **Raporlar ve Günlükler**'i tıklayın.
- 2 **Son Olaylar** bölümünde, **Günlüğü Görüntüle**'yi tıklayın.
- 3 **Internet ve Ağ**'ı ve sonra **İzinsiz Giriş Tespiti Olayları**'nı tıklayın. İzinsiz Giriş Tespiti Olayları bölümünde, bir kaynak IP adresi seçin ve sonra **Bu IP'yi izle** seçeneğini tıklayın.
- 4 Görsel İzleyici bölümünde, aşağıdakilerden birini tıklayın:
 - **Harita Görünümü**: Seçili IP adresini kullanarak bilgisayarın coğrafi konumunu bulun.
 - **Kayıt Görünümü**: Seçili IP adresini kullanarak etki alanı bilgilerini bulun.
 - **Ağ Görünümü**: Seçili IP adresini kullanarak ağ bilgilerini bulun.
- 5 **Bitti**'yi tıklayın.

İzlenen bir IP adresini izleme

Kaynak bilgisayardan sizin bilgisayarınıza alınan veriler için en olası yolu gösteren coğrafi görünümü elde etmek üzere, izlenen bir IP adresini izleyebilirsiniz. Ayrıca, IP adresiyle ilgili kayıt ve ağ bilgilerini de elde edebilirsiniz.

- 1 Gelişmiş Menü'nün etkin olduğundan emin olun ve **Araçlar**'ı tıklayın.
- 2 Araçlar bölümünde **Trafik Monitörü**'nü tıklayın.
- 3 **Trafik Monitörü** altında **Etkin Programlar**'ı tıklayın.
- 4 Bir program seçin ve ardından program adının altında görüntülenen IP adresini belirleyin.
- 5 **Program Etkinliği** altında **Bu IP'yi izle** seçeneğini tıklayın.
- 6 **Görsel İzleyici** altında, kaynak bilgisayardan sizin bilgisayarınıza alınan veriler için en olası yolu gösteren bir harita görüntüleyebilirsiniz. Ayrıca, IP adresiyle ilgili kayıt ve ağ bilgilerini de elde edebilirsiniz.

Not: En güncel istatistikleri görüntülemek için, **Görsel İzleyici** altında **Yenile**'yi tıklayın.

İnternet trafiğini izleme

Firewall, aşağıdakileri içeren İnternet trafiğinizi izlemek için çeşitli yöntemler sunar:

- **Trafik Analizi grafiği:** En son gelen ve giden İnternet trafiğini görüntüler.
- **Trafik Kullanımı grafiği:** Son 24 saatte en etkin programlar tarafından kullanılan bant genişliği yüzdesini görüntüler.
- **Etkin Programlar:** Bilgisayarınızda ağ bağlantılarının büyük bir bölümünü kullanan programları ve bu programların eriştikleri IP adreslerini görüntüler.

Trafik Analizi grafiđi hakkında

Trafik Analizi grafiđi, gelen ve giden Internet trafiđinin sayısal ve grafiksel anlatımıdır. Ayrıca Trafik Monitörü, ađ bađlantılarının büyük bir bölümünü kullanan programları ve bu programların eriştikleri IP adreslerini görüntüler.

Trafik Analizi bölümünde, en son gelen ve giden Internet trafiđinin yanı sıra geçerli, ortalama ve en yüksek aktarım hızlarını görüntüleyebilirsiniz. Ayrıca, Firewall'u başlattıktan sonra gerçekleşen trafiđin miktarını içeren trafik hacmini, geçerli ve önceki aylara ait toplam trafiđi de görüntüleyebilirsiniz.

Trafik Analizi bölümü, bilgisayarınızda son gelen ve giden Internet trafiđinin hacmi ve hızı, bađlantı hızı ve Internet üzerinden aktarılan toplam baytı içeren bilgisayarınızın gerçek zamanlı Internet etkinliđini görüntüler.

Düz yeşil çizgi, gelen trafiđin geçerli aktarım hızını temsil eder. Kesik yeşil çizgi, gelen trafiđin ortalama aktarım hızını temsil eder. Geçerli aktarım hızı ve ortalama aktarım hızı aynıysa, grafikte kesik çizgi görüntülenmez. Bu durumda, düz çizgi hem ortalama hem de geçerli aktarım hızını temsil eder.

Düz kırmızı çizgi, giden trafiđin geçerli aktarım hızını temsil eder. Kesik kırmızı çizgi, giden trafiđin ortalama aktarım hızını temsil eder. Geçerli aktarım hızı ve ortalama aktarım hızı aynıysa, grafikte kesik çizgi görüntülenmez. Bu durumda, düz çizgi hem ortalama hem de geçerli aktarım hızını temsil eder.

Gelen ve giden trafiđi analiz etme

Trafik Analizi grafiđi, gelen ve giden Internet trafiđinin sayısal ve grafiksel anlatımıdır. Ayrıca Trafik Monitörü, ađ bađlantılarının büyük bir bölümünü kullanan programları ve bu programların eriştikleri IP adreslerini görüntüler.

- 1 Gelişmiş Menü'nün etkin olduğundan emin olun ve ardından **Araçlar**'ı tıkladın.
- 2 Araçlar bölümünde **Trafik Monitörü**'nü tıkladın.
- 3 **Trafik Monitörü** altında **Trafik Analizi**'ni tıkladın.

İpucu: En güncel istatistikleri görüntülemek için, **Trafik Analizi** altında **Yenile**'yi tıkladın.

Program bant genişliğini izleme

Son yirmi dört saat içinde bilgisayarınızdaki en etkin programlar tarafından kullanılan bant genişliğinin yaklaşık yüzdesini gösteren pasta grafiği görüntüleyebilirsiniz. Pasta grafik, programlar tarafından kullanılan göreceli bant genişliği miktarlarının görsel anlatımını sunar.

- 1 Gelişmiş Menü'nün etkin olduğundan emin olun ve ardından **Araçlar**'ı tıklatın.
- 2 Araçlar bölümünde **Trafik Monitörü**'nü tıklatın.
- 3 **Trafik Monitörü** altında **Trafik Kullanımı**'ni tıklatın.

İpucu: En güncel istatistikleri görüntülemek için, **Trafik Kullanımı** altında **Yenile**'yi tıklatın.

Program etkinliğini izleme

Uzak bilgisayar bağlantılarını ve portları gösteren, gelen ve giden program etkinliğini görüntüleyebilirsiniz.

- 1 Gelişmiş Menü'nün etkin olduğundan emin olun ve ardından **Araçlar**'ı tıklatın.
- 2 Araçlar bölümünde **Trafik Monitörü**'nü tıklatın.
- 3 **Trafik Monitörü** altında **Etkin Programlar**'ı tıklatın.
- 4 Aşağıdaki bilgileri görüntüleyebilirsiniz:
 - Program Etkinliği grafiği: Etkinlik grafiğini görüntüleyeceğiniz programı seçin.
 - Dinleme bağlantısı: Program adı altında bir Dinleme ögesi seçin.
 - Bilgisayar bağlantısı: Program adı, sistem işlemi veya hizmet altında bir IP adresi seçin.

Not: En güncel istatistikleri görüntülemek için, **Etkin Programlar** altında **Yenile**'yi tıklatın.

B Ö L Ü M 2 2

Internet güvenliđi hakkında bilgi alma

Firewall, size programlar ve genel Internet etkinliđi hakkında güncel bilgiler sunmak için McAfee'nin güvenlik Web sitesi HackerWatch'u destekler. HackerWatch, Firewall hakkında bir HTML dersi de sağlar.

Bu bölümde

HackerWatch dersini başlatma..... 110

HackerWatch dersini başlatma

Firewall hakkında bilgi almak için, SecurityCenter'dan HackerWatch dersine erişebilirsiniz.

- 1** Gelişmiş Menü'nün etkin olduğundan emin olun ve ardından **Araçlar**'ı tıklatın.
- 2** Araçlar bölümünde **HackerWatch**'u tıklatın.
- 3** **HackerWatch Kaynakları** altında **Dersi Görüntüle**'yi tıklatın.

B Ö L Ü M 2 3

McAfee Anti-Spam

Anti-Spam (eski adıyla SpamKiller), gelen e-postalarınızı inceleyip, istenmeyen e-postaları spam (sizin bir şey satın almanıza yetki veren e-posta) veya phishing (kişisel bilgilerinizi hileli olma olasılığı bulunan Web sitelerine sağlamanıza yetki veren e-posta) olarak işaretler ve böylece bunların Gelen Kutusu'na girişini durdurur. Anti-Spam, daha sonra spam e-postaları filtreler ve McAfee Anti-Spam klasörüne taşır.

Arkadaşlarınız bazen size spam gibi görünen yasal e-postalar gönderirlerse, bu adresleri Anti-Spam'in arkadaş listesine ekleyerek bunların filtrelenmemesini sağlayabilirsiniz. Ayrıca, spam iletilerin algılanma biçimini de özelleştirebilirsiniz. Örneğin, iletileri daha kararlı bir şekilde filtreleyebilir, ileti içinde nelerin aranacağını belirtebilir ve kendi filtrelerinizi oluşturabilirsiniz.

E-posta iletilerinin içindeki bir bağlantı aracılığıyla hileli olma olasılığı bulunan bir Web sitesine erişmeye çalıştığınızda da Anti-Spam sizi korur. Hileli olma olasılığı bulunan bir Web sitesinin bağlantısını tıklattığınızda, Phishing filtresinin güvenli sayfasına yönlendirilirsiniz. Filtrelenmesini istemediğiniz Web siteleri varsa, bunları beyaz listeye ekleyebilirsiniz (bu listedeki Web siteleri filtrelenmez).

Anti-Spam; Yahoo®, MSN®/Hotmail®, Windows® Mail ve Live™ Mail, Microsoft® Outlook® ve Outlook Express ve Mozilla Thunderbird™ gibi çeşitli e-posta programlarının yanı sıra POP3, POP3 Web postası ve MAPI (Microsoft Exchange Server) gibi çeşitli e-posta hesaplarıyla çalışır. E-postanızı okumak için tarayıcı kullanıyorsanız, Web posta hesabınızı Anti-Spam'e eklemeniz gerekir. Diğer tüm hesaplar otomatik olarak yapılandırılır ve bunları Anti-Spam'e eklemeniz gerekmez.

Anti-Spam'i yükledikten sonra yapılandırmanız gerekmez, ancak deneyimli bir kullanıcıysanız, programın gelişmiş spam ve phish koruma özelliklerinde tercihlerinize göre ince ayar yapmak isteyebilirsiniz.

Not: SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde

Anti-Spam özellikleri.....	112
Spam algılamayı yapılandırma.....	113
E-posta filtreleme.....	121
Arkadaşları ayarlama.....	123
Web posta hesaplarınızı ayarlama.....	127
Filtrelenen e-posta ile çalışma.....	131
Phishing korumasını yapılandırma.....	133

Anti-Spam özellikleri

Spam filtreleme	İstenmeyen e-postanın Gelen Kutusu'na girmesini engelleyin. Anti-Spam'in gelişmiş filtreleri, tüm e-posta hesaplarınız için otomatik olarak güncelleştirilir. Ayrıca, tüm spam iletilerin filtrelendiğinden emin olmak için özel filtreler oluşturabilir ve spam iletileri analiz için McAfee'ye bildirebilirsiniz.
Phishing filtreleme	Kişisel bilgileri ele geçiren olası phishing (hileli) web sitelerini tanımlayın.
Özelleştirilmiş spam ileti işleme	İstenmeyen e-postaları spam olarak işaretleyip McAfee Anti-Spam klasörünüze taşıyın veya yasal e-postaları spam değil olarak işaretleyip Gelen Kutusu'na taşıyın.
Arkadaşlar	Arkadaşlarınızdan gelen e-postaların filtrelenmemesi için e-posta adreslerini Arkadaş listesine alın.

B Ö L Ü M 2 4

Spam algılamayı yapılandırma

Anti-Spam, spam iletilerin algılanma biçimini özelleştirmenize olanak verir. İletileri daha kararlı bir şekilde filtreleyebilir, ileti içinde nelerin aranacağını belirtebilir ve spam'i analiz ederken özel karakter kümeleri arayabilirsiniz. Ayrıca, Anti-Spam'in hangi iletileri spam olarak tanımlayacağını ayarlamak için kişisel filtreler oluşturabilirsiniz. Örneğin, ipotek sözcüğünü içeren istenmeyen e-posta filtrelenmiyorsa, ipotek sözcüğünü içeren bir filtre ekleyebilirsiniz.

E-postanızla ilgili sorunlar yaşıyorsanız, sorun giderme stratejiniz kapsamında spam korumasını devre dışı bırakabilirsiniz.

Bu bölümde

Filtreleme seçeneklerini ayarlama.....	114
Kişisel filtreleri kullanma.....	117
Spam korumasını devre dışı bırakma	119

Filtreleme seçeneklerini ayarlama

İletileri daha kararlı bir şekilde filtrelemek, spam'i nasıl işlemek istediğinizi belirtmek ve spam'i analiz ederken özel karakter kümeleri aramak isterseniz, Anti-Spam'in filtreleme seçeneklerini ayarlayın.

Filtreleme düzeyi

Filtreleme düzeyi, e-postanızın ne kadar kararlı bir düzeyde filtreleneceğini belirler. Örneğin, spam filtrelenmezse ve filtreleme düzeyiniz Orta seçeneğine ayarlıysa, bunu Orta-Yüksek veya Yüksek olarak değiştirebilirsiniz. Ancak, filtreleme düzeyiniz Yüksek olarak ayarlıysa, yalnızca arkadaş listenizdeki göndericilerden gelen e-posta iletileri kabul edilir: Diğer tüm iletiler filtrelenir.

Spam işleme

Anti-Spam, çeşitli spam işleme seçeneklerini özelleştirmenize olanak verir. Örneğin, spam ve phishing e-postayı özel klasörlere yerleştirebilir, spam ve phishing e-postanın konu satırında görüntülenen etiketin adını değiştirebilir, filtre için bir maksimum boyut belirleyebilir ve spam kurallarının güncelleştirilme sıklığını belirtebilirsiniz.

Karakter kümeleri

Anti-Spam, spam analizi yaparken özel karakter kümelerini arayabilir. Karakter kümeleri; dilin alfabesi, rakamlar ve diğer simgeleri de kapsayan bir dili temsil etmek üzere kullanılır. Yunanca spam alıyorsanız, Yunanca karakter kümesi içeren tüm iletileri filtreleyebilirsiniz.

Yasal e-posta aldığınız dillerin karakter kümelerini filtrelememeye dikkat edin. Örneğin, yalnızca İtalyanca iletileri filtrelemek istiyorsanız, İtalya Batı Avrupa'da olduğu için Batı Avrupa'yı seçebilirsiniz. Ancak İngilizce yasal e-posta alıyorsanız, Batı Avrupa'yı seçtiğinizde, İngilizce iletiler ve Batı Avrupa karakter kümesindeki diğer diller de filtrelenir. Bu durumda, yalnızca İtalyanca iletileri filtreleyemezsiniz.

Not: Karakter kümesi filtresi belirtmek, deneyimli kullanıcılara yönelik bir işlemdir.

Filtreleme düzeyini deęiřtirme

E-postanızı filtrelemek istedięiniz etkinlik düzeyini deęiřtirebilirsiniz. Örneęin, yasal iletiler filtreleniyorsa, filtreleme düzeyini düşürebilirsiniz.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriř bölümünde **E-posta ve Anlık İleti**'yi tıkladın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıkladın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Geliřmiş**'i tıkladın.

2 Spam'den Korunma bölümünde **Filtreleme Seçenekleri**'ni tıkladın.

3 Spam filtresi düzeyi belirtin listesinde, uygun düzeyi seçin ve sonra **Tamam**'ı tıkladın.

Düzyey	Açıklama
Düşük	Çoęu e-posta kabul edilir.
Orta-Düşük	Yalnızca spam olduęu belli olan iletiler filtrelenir.
Orta (Önerilen)	E-posta önerilen düzeyde filtrelenir.
Orta-Yüksek	Spam'e benzeyen tüm e-postalar filtrelenir.
Yüksek	Yalnızca arkadaş listenizdeki gönderenlerden iletiler kabul edilir.

Spam işleme ve işaretleme biçimini deęiřtirme

Spam ve phishing e-postayı özel yerleřtirmek için bir klasör belirtebilir, e-posta konu satırında görüntülenen [SPAM] veya [PHISH] etiketini deęiřtirebilir, filtre için bir maksimum boyut belirleyebilir ve spam kurallarının ne sıklıkla güncelleřtirileceęini belirtebilirsiniz.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriř bölümünde **E-posta ve Anlık İleti**'yi tıkladın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıkladın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Geliřmiş**'i tıkladın.

2 Spam'den Korunma bölümünde **Filtreleme Seçenekleri**'ni tıkladın.

3 Ařaęıdaki uygun seçenekleri deęiřtirin veya belirleyin ve sonra **Tamam**'ı tıkladın.

Bunu yapmak için...	Bunu yapın...
Spam ve phish e-postanın yerleştirileceği konumu belirtmek	Spam e-postaları bu klasöre koy listesinde bir klasör seçin. Varsayılan olarak McAfee Anti-Spam klasörü ayarlıdır.
Spam e-postanın konu satırını değiştirmek	Spam e-postanın konusunu işaret le altında spam e-postanın konu satırına eklemek için bir etiket belirtin. Varsayılan olarak [SPAM] etiketi ayarlıdır.
Phish e-postanın konu satırını değiştirmek	Phish e-postanın konusunu işaret le altında phish e-postanın konu satırına eklemek için bir etiket belirtin. Varsayılan olarak [PHISH] etiketi ayarlıdır.
Filtrelenecek en büyük e-postayı belirtmek	Filtrelenecek en büyük e-postayı belirtin (KB olarak boyut) altında, filtrelemek istediğiniz en büyük e-posta boyutunu girin.
Spam kurallarını güncelleştirmek	Spam kurallarını güncelleştir (dakika olarak) seçeneğini belirleyin ve sonra spam kurallarınızın güncelleştirilme sıklığını girin. Önerilen sıklık 30 dakikadır. Hızlı ağ bağlantınız varsa, daha iyi sonuçlar elde etmek için 5 dakika gibi daha sık bir ayar yapılandırabilirsiniz.
Spam kurallarını güncelleştirmemek	Spam kurallarını güncelleştirme 'yi seçin.

Karakter kümesi filtrelerini uygulama

Not: Belirli bir karakter kümesinden karakterler içeren iletileri filtrelemek, deneyimli kullanıcılara yönelik bir işlemdir.

Belirli dillerin karakter kümelerini filtreleyebilirsiniz; ancak yasal e-posta aldığınız dillerin karakter kümelerini filtrelemeyin.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölmesinde **E-posta ve Anlık İleti**'yi tıklatın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklatın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklatın.

2 Spam'den Korunma bölümünde **Karakter Kümeleri**'ni tıklatın.

3 Filtrelemek istediğiniz karakter kümelerinin yanındaki onay kutularını seçin.

4 **Tamam**'ı tıklatın.

Kişisel filtreleri kullanma

Kişisel filtre, belirli sözcüklere veya tümceciklere göre e-posta iletilerine izin verme veya engelleme ayarını belirtir. Bir e-posta iletisi, filtrenin engellemek üzere ayarlandığı bir sözcük veya tümcecik içeriyorsa, ileti spam olarak işaretlenir ve Gelen Kutusu'nda bırakılır veya McAfee Anti-Spam klasörüne taşınır. Spam'in işleme biçimi hakkında ayrıntılı bilgi için bkz. İletinin işleme ve işaretlenme biçimini değiştirme (sayfa 115).

Anti-Spam, yetkisiz e-posta iletilerinin Gelen Kutusu'na girmesini önleyen gelişmiş bir filtre içerir, ancak Anti-Spam'in spam olarak tanımlayacağı iletilere ince ayar yapmak isterseniz, bir kişisel filtre oluşturabilirsiniz. Örneğin, ipotek sözcüğünü içeren bir filtre eklerseniz, Anti-Spam ipotek sözcüğünü içeren iletileri filtreler. Yasal e-posta iletilerinde yaygın olarak bulunan sözcükler için filtreler oluşturmayın çünkü bu durumda spam olmayan e-postalar da filtrelenir. Bir filtre oluşturduktan sonra, filtrenin bazı spam iletileri algılamadığını fark ederseniz bunu düzenleyebilirsiniz. Örneğin, iletinin konusunda viagra sözcüğünü arayacak bir filtre oluşturduysanız ancak iletinin gövdesinde geçtiği için viagra sözcüğünü içeren iletileri almaya devam ediyorsanız, filtreyi ileti konusu yerine ileti gövdesinde viagra sözcüğünü arayacak şekilde değiştirin.

Düzenli ifadeler (RegEx) de kişisel filtrelerde kullanılabilen özel karakterler ve sıralardır; ancak McAfee, düzenli ifadelerin yalnızca deneyimli kullanıcılar tarafından kullanılmasını önerir. Düzenli ifadeleri tanıımıyorsanız veya bunların kullanımı hakkında ayrıntılı bilgi almak isterseniz, Web'de düzenli ifadelerle ilgili araştırma yapabilirsiniz (örneğin, http://en.wikipedia.org/wiki/Regular_expression adresine gidin).

Kişisel filtre ekleme

Anti-Spam'in hangi iletileri spam olarak tanımlayacağını ayarlamak için filtreler ekleyebilirsiniz.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölmesinde **E-posta ve Anlık İleti**'yi tıklatın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'i tıklatın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklatın.

2 Spam'den Korunma bölümünde **Kişisel Filtreler**'i tıklatın.

3 **Ekle**'yi tıklatın.

4 E-posta iletisinde kişisel filtrenin neyi arayacağını belirtin (sayfa 119).

5 **Tamam**'i tıklatın.

Kişisel filtreyi düzenleme

Hangi iletilerin spam olarak tanımlanacağını ayarlamak için mevcut filtreleri düzenleyin.

1 Spam'den Korunma bölümünü açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklayın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklayın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklayın.

2 Spam'den Korunma bölümünde **Kişisel Filtreler**'i tıklayın.

3 Düzenlemek istediğiniz filtreyi seçin ve ardından **Düzenle**'yi tıklayın.

4 E-posta iletilerinde kişisel filtrenin neyi arayacağını belirtin (sayfa 119).

5 **Tamam**'ı tıklayın.

Kişisel filtreyi kaldırma

Artık kullanmak istemediğiniz filtreleri kalıcı olarak kaldırabilirsiniz.

1 Spam'den Korunma bölümünü açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklayın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklayın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklayın.

2 Spam'den Korunma bölümünde **Kişisel Filtreler**'i tıklayın.

3 Kaldırmak istediğiniz filtreyi seçin ve ardından **Kaldır**'ı tıklayın.

4 **Tamam**'ı tıklayın.

Kişisel filtre belirtme

Bu tabloda, e-postada kişisel filtrenin neyi arayacağı açıklanmaktadır.

Bunu yapmak için...	Bunu yapın...
Filtrelenecek e-posta bölümünü belirtmek	Filtrenin sözcükleri veya tümcecikleri e-posta konusu, gövde, gönderen, başlık veya alıcı seçeneklerinde arayıp aramayacağını belirlemek için E-posta parçası listesinde bir girişi tıklatın. Filtrenin belirlediğiniz sözcükleri veya tümcecikleri içeren ya da içermeyen bir e-postayı arayıp aramayacağını belirlemek için E-posta parçası listesinde bir girişi tıklatın.
Filtrenizdeki sözcükleri veya tümcecikleri belirtmek	Sözcük veya tümcecik alanına e-postada nelerin aranacağını yazın. Örneğin <i>ipotek</i> sözcüğünü belirtirseniz, bu sözcüğü içeren tüm e-postalar filtrelenir.
Filtrenin düzenli ifadeler kullandığını belirtmek	Bu filtre düzenli ifadeleri kullanır 'ı seçin.
Filtrenizdeki sözcüklere veya tümceciklere göre e-postaları engellemeyi veya bunlara izin vermeyi seçmek	Filtrenizdeki sözcükleri veya tümcecikleri içeren e-postaları engellemek veya bunlara izin vermek için Bu eylemi gerçekleştir altında Engelle veya İzin Ver 'i seçin.

Spam korumasını devre dışı bırakma

Anti-Spam'in e-postaları filtrelemesini önlemek için spam korumasını devre dışı bırakabilirsiniz.

- 1 Gelişmiş Menü'de **Yapılandır**'ı tıklatın.
- 2 Yapılandır bölmesinde **E-posta ve Anlık İleti**'yi tıklatın.
- 3 **Spam'den koruma etkin** altında **Kapalı**'yı tıklatın.

İpucu: Spam'den korunmak için **Spam'den koruma devre dışı** altında **Açık**'ı tıklatmayı unutmayın.

B Ö L Ü M 2 5

E-posta filtreleme

Anti-Spam gelen e-postanızı inceler ve bunu spam (sizden bir şey satın almanızı isteyen e-postalar) veya phishing (olası bir hileli Web sitesine kişisel bilgi sağlamanızı isteyen e-postalar) olarak sınıflandırır.

Varsayılan olarak, Anti-Spam daha sonra tüm istenmeyen e-posta iletilerini spam veya phishing (iletinin konu satırında [SPAM] veya [PHISH] etiketi görüntülenir) olarak işaretler ve iletileri McAfee Anti-Spam klasörüne taşır.

Anti-Spam araç çubuğundan e-postayı spam olarak veya spam değil olarak işaretleyebilir, spam iletilerin taşındığı konumu değiştirebilir ve konu satırında görüntülenen etiketi değiştirebilirsiniz.

E-posta programınızla ilgili sorunlar yaşarsanız, sorun giderme stratejiniz kapsamında Anti-Spam araç çubuklarını da devre dışı bırakabilirsiniz.

Bu bölümde

Anti-Spam araç çubuğundan bir iletiyi işaretleme	121
Anti-Spam araç çubuğunu devre dışı bırakma	122

Anti-Spam araç çubuğundan bir iletiyi işaretleme

Bir iletiyi spam olarak işaretlediğinizde, iletinin konusuna [SPAM] etiketi veya sizin seçtiğiniz bir etiket eklenir ve Gelen Kutusu'nda, McAfee Anti-Spam klasörünüzde (Outlook, Outlook Express, Windows Mail, Thunderbird) veya Önemsiz Posta klasörünüzde (Eudora®) bırakılır. Bir iletiyi spam değil olarak işaretlediğinizde, ileti etiketi kaldırılır ve ileti Gelen Kutusu'na taşınır.

Bu programda bir iletiyi işaretlemek için...	Bir iletiyi seçin ve sonra...
Outlook, Outlook Express, Windows Mail	Spam Olarak İşaretle 'yi veya Spam Değil Olarak İşaretle 'yi tıklatın.
Eudora	Anti-Spam menüsünde Spam Olarak İşaretle 'yi veya Spam Değil Olarak İşaretle 'yi tıklatın.
Thunderbird	Anti-Spam araç çubuğunda M simgesine gidin, İşaretlenme Biçimi 'ne gidin ve sonra Spam 'i veya Spam Değil 'i tıklatın.

Anti-Spam araç çubuğunu devre dışı bırakma

Outlook, Outlook Express, Windows Mail, Eudora veya Thunderbird kullanıyorsanız, Anti-Spam araç çubuğunu devre dışı bırakabilirsiniz.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklatın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklatın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklatın.

2 Spam'den Korunma bölümünde **E-Posta Araç Çubukları**'nı tıklatın.

3 Devre dışı bırakmak istediğiniz araç çubuğunun yanındaki onay kutusunu temizleyin.

4 **Tamam**'ı tıklatın.

İpucu: İsteddiğiniz zaman onay kutularını işaretleyerek Anti-Spam araç çubuklarınızı yeniden etkinleştirebilirsiniz.

B Ö L Ü M 26

Arkadaşları ayarlama

Anti-Spam'in yasal e-posta iletilerini tanıyarak bunlara izin veren gelişmiş filtresi nedeniyle, arkadaşlarınızın e-posta adreslerini nadiren arkadaş listenize eklemeniz gerekir (bunları ister el ile ekliyor isterse adres defterlerine alıyor olun). Buna rağmen bir arkadaşınızın e-posta adresini eklerseniz ve birisi bu adresi hileli şekilde ele geçirirse, Anti-Spam bu e-posta adresinden gelen iletilerin Gelen Kutusu'na girmesine izin verir.

Yine de adres defterlerinizi almak istiyorsanız ve bunlarda değişiklik olursa, Anti-Spam arkadaş listenizi otomatik olarak güncelleştirmediği için bunları yeniden almanız gerekir.

Anti-Spam'in arkadaş listesini el ile de güncelleştirebilirsiniz veya etki alanı üzerindeki tüm kullanıcıların arkadaş listenize eklenmesini istiyorsanız tüm etki alanını ekleyebilirsiniz. Örneğin, şirket.com etki alanını eklerseniz, bu kuruluştan gelen hiçbir e-posta filtrelenmez.

Bu bölümde

Adres defteri alma	123
Arkadaşları el ile ayarlama.....	124

Adres defteri alma

Anti-Spam'in arkadaşlarınızın e-posta adreslerini arkadaş listenize eklemesini istiyorsanız, adres defterlerinizi alın.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklatın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklatın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklatın.

2 Spam'den Korunma bölümünde **Arkadaşlar**'ı tıklatın.

3 Arkadaşlar bölümünde **Al**'ı tıklatın.

4 **Alınacak adres defterini seçin** listesinde almak istediğiniz adres defteri türünü tıklatın.

5 **Şimdi Al**'ı tıklatın.

Arkadaşları el ile ayarlama

Girişleri tek tek düzenleyerek arkadaş listenizi el ile güncelleştirirsiniz. Örneğin, adresi adres defterinizde olmayan bir arkadaşınızdan e-posta alırsanız, e-posta adresini hemen el ile ekleyebilirsiniz. Bunu yapmanın en kolay yolu, Anti-Spam araç çubuğunu kullanmaktır. Anti-Spam araç çubuğunu kullanmazsanız, arkadaşınızın bilgilerini belirtmeniz gerekir.

Anti-Spam araç çubuğundan arkadaş ekleme

Outlook, Outlook Express, Windows Mail, Eudora™ veya Thunderbird e-posta programlarını kullanıyorsanız, doğrudan Anti-Spam araç çubuğunu kullanarak arkadaşlarınızı ekleyebilirsiniz.

Bu programa arkadaş eklemek için...	Bir iletiyi seçin ve sonra...
Outlook, Outlook Express, Windows Mail	Arkadaş Ekle'yi tıklatın.
Eudora	Anti-Spam menüsünde Arkadaş Ekle'yi tıklatın.
Thunderbird	Anti-Spam araç çubuğunda M simgesine gidin, İşaretlenme Biçimi 'ne gidin ve sonra Arkadaş'ı tıklatın.

Arkadaşınızı el ile ekleme

Arkadaşınızı doğrudan araç çubuğundan eklemek istemiyorsanız veya e-posta iletisini aldığınızda bunu yapmayı unuttuysanız, arkadaşınızı arkadaş listesine ekleyebilirsiniz.

1 Spam'den Korunma bölmesini açın.

Nasıl?

- SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklatın.
- E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklatın.
- E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklatın.

2 Spam'den Korunma bölümünde **Arkadaşlar**'ı tıklatın.

3 Arkadaşlar bölümünde **Ekle**'yi tıklatın.

4 **Ad** kutusuna arkadaşınızın adını yazın.

5 **Tür** listesinde **Tek e-posta adresi**'ni seçin.

6 Arkadaşınızın e-posta adresini **E-posta Adresi** kutusuna yazın.

7 **Tamam**'ı tıklatın.

Etki alanı ekleme

Bir etki alanı üzerindeki tüm kullanıcıları arkadaş listenize eklemek istiyorsanız tüm etki alanını ekleyin. Örneğin, şirket.com etki alanını eklerseniz, bu kuruluştan gelen hiçbir e-posta filtrelenmez.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklatın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklatın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklatın.

2 Spam'den Korunma bölümünde **Arkadaşlar**'ı tıklatın.

3 Arkadaşlar bölümünde **Ekle**'yi tıklatın.

4 **Ad** kutusuna kuruluşun veya grubun adını yazın.

5 **Tür** listesinde **Tüm etki alanı**'nı seçin.

6 Etki alanı adını **E-posta Adresi** kutusuna yazın.

7 **Tamam**'ı tıklatın.

Arkadaşınızı düzenleme

Bir arkadaşınızın bilgileri değişirse, Anti-Spam'in ondan gelen iletileri spam olarak işaretlememesi için arkadaş listenizi güncelleştirebilirsiniz.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklatın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklatın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklatın.

2 Spam'den Korunma bölümünde **Arkadaşlar**'ı tıklatın.

3 Düzenlemek istediğiniz arkadaşınızı seçin ve ardından **Düzenle**'yi tıklatın.

4 **Ad** kutusunda arkadaşınızın adını değiştirin.

5 Arkadaşınızın e-posta adresini **E-posta Adresi** kutusunda değiştirin.

6 **Tamam**'ı tıklatın.

Etki alanını düzenleme

Bir etki alanının bilgileri deęişirse, Anti-Spam'in bu etki alanından gelen iletileri spam olarak iřaretlememesi için arkadaş listenizi gncelleřtirebilirsiniz.

1 Spam'den Korunma blmesini aın.

Nasıl?

1. SecurityCenter Giriř blmesinde **E-posta ve Anlık İleti**'yi tıklatın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklatın.
3. E-posta ve Anlık İleti blmesinde, **Spam'den korunma** altında **Geliřmiř**'i tıklatın.

2 Spam'den Korunma blmesinde **Arkadařlar**'ı tıklatın.

3 Arkadařlar blmesinde **Ekle**'yi tıklatın.

4 **Ad** kutusunda kuruluřun veya grubun adını deęiřtirin.

5 **Tr** listesinde **Tm etki alanı**'nı sein.

6 Etki alanı adını **E-posta Adresi** kutusunda deęiřtirin.

7 **Tamam**'ı tıklatın.

Arkadařınızı kaldırma

Arkadař listenizdeki bir kiři veya etki alanı size spam gnderirse, bunu Anti-Spam'in arkadaş listesinden kaldırarak, buradan gelen e-posta iletilerinin yeniden filtrelenmesini saęlayın.

1 Spam'den Korunma blmesini aın.

Nasıl?

1. SecurityCenter Giriř blmesinde **E-posta ve Anlık İleti**'yi tıklatın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklatın.
3. E-posta ve Anlık İleti blmesinde, **Spam'den korunma** altında **Geliřmiř**'i tıklatın.

2 Spam'den Korunma blmesinde **Arkadařlar**'ı tıklatın.

3 Kaldırmak istedięiniz arkadaşınızı sein ve ardından **Kaldır**'ı tıklatın.

B Ö L Ü M 27

Web posta hesaplarınızı ayarlama

E-posta iletilerinizi okumak için tarayıcı kullanıyorsanız, hesabınıza bağlanması ve iletilerinizi filtrelemesi için Anti-Spam'i yapılandırmanız gerekir. Web posta hesabınızı Anti-Spam'e eklemek için e-posta sağlayıcınız tarafından verilen hesap bilgilerinizi eklemeniz yeterlidir.

Web posta hesabını ekledikten sonra, hesap bilgilerinizi düzenleyebilir ve filtrelenen Web postası hakkında ayrıntılı bilgi alabilirsiniz. Artık Web posta hesabı kullanmıyorsanız veya hesabın filtrelenmesini istemiyorsanız, bunu kaldırabilirsiniz.

Anti-Spam; Yahoo!®, MSN®/Hotmail®, Windows® Mail and Live™ Mail, Microsoft® Outlook® ve Outlook Express ve Mozilla Thunderbird™ gibi çeşitli e-posta programlarının yanı sıra POP3, POP3 Web postası ve MAPI (Microsoft Exchange Server) gibi çeşitli e-posta hesaplarıyla çalışır. POP3, en yaygın hesap türüdür ve Internet e-postasında standarttır. POP3 hesabınız varsa, Anti-Spam doğrudan e-posta sunucusuna bağlanır ve iletileri Web posta hesabınız tarafından alınmadan önce filtreler. POP3 Web postası, Yahoo!, MSN/Hotmail ve Windows Mail hesapları Web tabanlıdır. POP3 Web posta hesaplarını filtrelemek, POP3 hesaplarını filtrelemeye benzer.

Bu bölümde

Web posta hesabı ekleme	128
Web posta hesabını düzenleme	128
Web posta hesabını kaldırma	129
Web posta hesabı bilgilerinizi anlama	129

Web posta hesabı ekleme

Hesabınızdaki iletilere spam filtresi uygulamak istiyorsanız, bir POP3 (örneğin Yahoo), MSN/Hotmail veya Windows Mail (yalnızca ücretli sürümler tam olarak desteklenir) Web posta hesabı ekleyin.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklatın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklatın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklatın.

2 Spam'den Korunma bölümünde **Web Posta Hesapları**'ni tıklatın.

3 Web Posta Hesapları bölümünde **Ekle**'yi tıklatın.

4 Hesap bilgileri (sayfa 129)'ni belirtin ve sonra **İleri**'yi tıklatın.

5 **Denetleme Seçenekleri** altında Anti-Spam'in hesabınızda spam denetleyeceği zamanı (sayfa 129) belirtin.

6 Çevirmeli bağlantı kullanıyorsanız, Anti-Spam'in Internet'e nasıl bağlanacağını (sayfa 129) belirtin.

7 **Son**'u tıklatın.

Web posta hesabını düzenleme

Hesabınızda değişiklikler olduğu zaman Web posta hesabınızı düzenlemeniz gerekir. Örneğin, parolanızı değiştirirseniz veya Anti-Spam'in daha sık spam denetimi yapmasını isterseniz, Web posta hesabınızı düzenleyin.

1 Spam'den Korunma bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklatın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'ı tıklatın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklatın.

2 Spam'den Korunma bölümünde **Web Posta Hesapları**'ni tıklatın.

3 Değiştirmek istediğiniz hesabı seçin ve ardından **Düzenle**'yi tıklatın.

4 Hesap bilgileri (sayfa 129)'ni belirtin ve sonra **İleri**'yi tıklatın.

5 **Denetleme Seçenekleri** altında Anti-Spam'in hesabınızda spam denetleyeceği zamanı (sayfa 129) belirtin.

6 Çevirmeli bağlantı kullanıyorsanız, Anti-Spam'in Internet'e nasıl bağlanacağını (sayfa 129) belirtin.

7 **Son**'u tıklatın.

Web posta hesabını kaldırma

Artık e-postalarına spam filtresi uygulamak istemediğiniz Web posta hesabını kaldırın. Örneğin, hesabınız artık etkin değilse veya sorun yaşıyorsanız, sorunu giderirken hesabı kaldırabilirsiniz.

1 Spam'den Korunma bölümünü açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklayın.
2. E-posta ve Anlık İleti alanında **Yapılandır**'i tıklayın.
3. E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklayın.

2 Spam'den Korunma bölümünde **Web Posta Hesapları**'nı tıklayın.

3 Kaldırmak istediğiniz hesabı seçin ve ardından **Kaldır**'i tıklayın.

Web posta hesabı bilgilerini anlama

Aşağıdaki tabloda, Web posta hesabı eklerken veya düzenlerken belirtmeniz gereken bilgiler açıklanmaktadır.

Hesap bilgisi

Bilgi	Açıklama
Açıklama	Kendiniz başvurmak üzere hesaba açıklama ekleyin. Bu kutuya her türde bilgiyi yazabilirsiniz.
E-posta Adresi	Bu e-posta hesabıyla ilişkili e-posta adresini belirtin.
Hesap Türü	Eklemekte olduğunuz e-posta hesabının türünü belirtin. (Örneğin, POP3 Web postası veya MSN/Hotmail).
Sunucu	Bu hesabı barındıran posta sunucusunun adını belirtin. Sunucunuzun adını bilmiyorsanız, Internet Servis Sağlayıcınız (ISS) tarafından verilen bilgilere bakın.
Kullanıcı Adı	Bu e-posta hesabının kullanıcı adını belirtin. Örneğin, e-posta adresiniz <i>kullanıcıadı@hotmail.com</i> ise, kullanıcı adınız büyük olasılıkla <i>kullanıcıadı</i> 'dir.
Parola	Bu e-posta hesabının parolasını belirtin.
Parolayı Onayla	Bu e-posta hesabının parolasını doğrulayın.

Denetleme seçenekleri

Seçenek	Açıklama
Her	Anti-Spam, belirttiğiniz sıklıkta (dakika) bu hesapta spam denetler. Aralık 5-3600 dakika arasında olmalıdır.
Başlangıçta denetle	Anti-Spam, bilgisayarı her başlattığınızda bu hesabı denetler.

Bağlantı seçenekleri

Seçenek	Açıklama
Asla bağlantı numarası çevirme	Anti-Spam sizin için otomatik olarak bağlantı numarası çevirmez. Çevirmeli bağlantınızı el ile başlatmanız gerekir.
Bağlantı yoksa bağlantı numarası çevir	İnternet bağlantısı yoksa, Anti-Spam sizin belirttiğiniz çevirmeli bağlantıyı kullanarak bağlanmaya çalışır.
Her zaman belirtilen bağlantıyı çevir	Anti-Spam, sizin belirttiğiniz çevirmeli bağlantıyı kullanarak bağlanmaya çalışır. Belirttiğiniz çevirmeli bağlantıdan farklı bir bağlantıyla bağlı olduğunuzda, bağlantınız kesilir.
Bu bağlantıyı çevir	Anti-Spam'ın İnternet'e bağlanmak için kullandığı çevirmeli bağlantıyı belirtin.
Filtreleme tamamlandıktan sonra bağlı kal	Filtreleme tamamlandıktan sonra, bilgisayarınız İnternet'e bağlı kalır.

B Ö L Ü M 2 8

Filtrelenen e-posta ile çalışma

Bazen bazı spam iletiler algılanmayabilir. Bu durumda, McAfee'ye spam raporlayabilirsiniz; bunlar filtre güncelleştirmeleri oluşturmak üzere analiz edilir.

Web posta hesabı kullanıyorsanız, filtrelenen e-posta iletilerinizi görüntüleyebilir, verebilir ve silebilirsiniz. Yasal bir iletinin filtrelenip filtrelenmediğinden emin olamıyorsanız veya iletinin ne zaman filtrelendiğini bilmek istiyorsanız bu kullanışlı bir özelliktir.

Bu bölümde

E-posta iletilerini McAfee'ye raporlama	131
Filtrelenen Web postasını görüntüleme, verme veya silme	132
Filtrelenen Web postasında olay görüntüleme	132

E-posta iletilerini McAfee'ye raporlama

E-posta iletilerini spam veya spam değil olarak işaretlediğinizde McAfee'ye raporlayabilirsiniz; böylece bunları analiz edip filtre güncelleştirmeleri oluşturabiliriz.

- Spam'den Korunma bölmesini açın.
Nasıl?
 - SecurityCenter Giriş bölümünde **E-posta ve Anlık İleti**'yi tıklatın.
 - E-posta ve Anlık İleti alanında **Yapılandır**'i tıklatın.
 - E-posta ve Anlık İleti bölümünde, **Spam'den korunma** altında **Gelişmiş**'i tıklatın.
- Spam'den Korunma bölümünde **E-Posta Araç Çubukları**'ni tıklatın.
- Anti-Spam'i Geliştirmeye Yardımcı Ol** altında uygun onay kutularını işaretleyin ve sonra **Tamam**'i tıklatın.

Bunu yapmak için...	Bunu yapın...
Spam olarak işaretlediğiniz her e-postayı McAfee'ye raporlamak	E-postayı spam olarak işaretlersiniz 'i seçin.
Spam değil olarak işaretlediğiniz her e-postayı McAfee'ye raporlamak	E-postayı spam olarak işaretlemezsiz 'i seçin.

Bunu yapmak için...	Bunu yapın...
Bir e-postayı spam değil olarak raporladığınızda McAfee'ye yalnızca başlığı değil e-postanın tamamını göndermek	Tüm e-postayı gönder (yalnızca başlığı değil) seçeneğini belirleyin.

Not: Bir e-postayı spam değil olarak raporladığınızda ve McAfee'ye e-postanın tamamını gönderdiğinizde, e-posta iletisi şifrelenmez.

Filtrelenen Web postasını görüntüleme, verme veya silme

Web posta hesabınızda filtrelenen iletleri görüntüleyebilir, verebilir veya silebilirsiniz.

- 1 **Ortak Görevler** altında **Raporlar ve Günlükler**'i tıklatın.
- 2 Raporlar ve Günlükler bölümünde **Filtrelenmiş Web Postası**'nı tıklatın.
- 3 Bir ileti seçin.
- 4 **Şunu yapmak istiyorum** altında, aşağıdakilerden birini gerçekleştirin:
 - İletiyi varsayılan e-posta programınızda görüntülemek için **Görüntüle**'yi tıklatın.
 - İletiyi bilgisayarınıza kopyalamak için **Ver**'i tıklatın.
 - İletiyi silmek için **Sil**'i tıklatın.

Filtrelenen Web postasında olay görüntüleme

E-posta iletilerinin filtrelendiği tarih ve saati ve bunları alan hesabı görüntüleyebilirsiniz.

- 1 **Ortak Görevler** altında **Son Olayları Görüntüle**'yi tıklatın.
- 2 Son Olaylar bölümünde **Günlüğü Görüntüle**'yi tıklatın.
- 3 Soldaki bölmede **E-posta ve Anlık İleti** listesini genişletin ve sonra **Web Postası Filtreleme Olayları**'nı tıklatın.
- 4 Görüntülemek istediğiniz günlüğü seçin.

B Ö L Ü M 29

Phishing korumasını yapılandırma

Anti-Spam, istenmeyen e-postaları, spam (sizden bir şey satın almanızı isteyen e-postalar) veya phishing (bilinen veya olası bir hileli Web sitesine kişisel bilgi sağlamanızı isteyen e-postalar) olarak sınıflandırır. Phishing koruması, sizi hileli Web sitelerine erişmekten korur. Bir e-posta iletilirken hileli olduğu bilinen veya olma olasılığı bulunan bir Web sitesinin bağlantısını tıklatırsanız, Anti-Spam sizi Phishing filtresinin güvenli sayfasına yönlendirir.

Filtrelemek istemediğiniz Web siteleri varsa, bunları Phishing beyaz listesine ekleyin. Ayrıca beyaz listedeki Web sitelerini düzenleyebilir ve kaldırabilirsiniz. Google®, Yahoo veya McAfee gibi siteleri eklemenize gerek yoktur çünkü bu Web siteleri hileli olarak değerlendirilmez.

Not: Bilgisayarınızda SiteAdvisor yüklüyse, SiteAdvisor'da Anti-Spam'in phishing korumasına benzer bir koruma olduğu için Anti-Spam'in phishing korumasını almazsınız.

Bu bölümde

Beyaz listeye Web sitesi ekleme	133
Beyaz listenizdeki siteleri düzenleme	134
Beyaz listeden Web sitesini kaldırma	134
Phishing korumasını devre dışı bırakma	134

Beyaz listeye Web sitesi ekleme

Filtrelemek istemediğiniz Web siteleri varsa, bunları beyaz listeye ekleyin.

1 Phishing Koruması bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **İnternet ve Ağ**'ı tıklatın.
2. İnternet ve Ağ bilgi alanında **Yapılandır**'ı tıklatın.

2 Phishing Koruması bölümünde **Gelişmiş**'i tıklatın.

3 **Beyaz Liste** altında **Ekle**'yi tıklatın.

4 Web sitesinin adresini yazın ve sonra **Tamam**'i tıklatın.

Beyaz listenizdeki siteleri düzenleme

Bir Web sitesini beyaz listeye eklediyseniz ve Web sitesinin adresi deđiřtiyse, her zaman bunu g¼ncelleřtirebilirsiniz.

1 Phishing Koruması b¼lmesini aın.

Nasıl?

1. SecurityCenter Giriř b¼lmesinde **Internet ve Ađ**'i tıkladın.
2. Internet ve Ađ bilgi alanında **Yapılandır**'i tıkladın.

2 Phishing Koruması b¼lmesinde **Geliřmiř**'i tıkladın.

3 **Beyaz Liste** altında g¼ncelleřtirmek istediđiniz Web sitesini sein ve sonra **D¼zenle**'yi tıkladın.

4 Web sitesinin adresini d¼zenleyin ve sonra **Tamam**'i tıkladın.

Beyaz listeden Web sitesini kaldırma

Eriřmek istediđiniz bir Web sitesini beyaz listeye eklediyseniz ancak artık siteyi filtrelemek istiyorsanız, bunu beyaz listeden kaldırın.

1 Phishing Koruması b¼lmesini aın.

Nasıl?

1. SecurityCenter Giriř b¼lmesinde **Internet ve Ađ**'i tıkladın.
2. Internet ve Ađ bilgi alanında **Yapılandır**'i tıkladın.

2 Phishing Koruması b¼lmesinde **Geliřmiř**'i tıkladın.

3 **Beyaz Liste** altında kaldırmak istediđiniz Web sitesini sein ve sonra **Kaldır**'i tıkladın.

Phishing korumasını devre dıřı bırakma

McAfee olmayan bir phishing yazılımınız varsa ve bunlar akıřıyorsa, Anti-Spam phishing korumasını devre dıřı bırakabilirsiniz.

1 SecurityCenter Giriř b¼lmesinde **Internet ve Ađ**'i tıkladın.

2 Internet ve Ađ bilgi alanında **Yapılandır**'i tıkladın.

3 **Phishing koruması etkin** altında **Kapalı**'yi tıkladın.

İpucu: İřiniz bitince, hileli Web sitelerinden korunmak iin **Phishing koruması devre dıřı** altında **Aık**'i tıkladmayı unutmayın.

B Ö L Ü M 3 0

McAfee Parental Controls

Ebeveyn Denetimleri, siz, aileniz, kişisel dosyalarınız ve bilgisayarınız için gelişmiş koruma sunar. Çevrimiçi kimlik hırsızlığından korunmanıza, kişisel bilgilerin iletilmesini engelleme, olası zararlı çevrimiçi içeriği (görüntüler dahil) filtrelemenize yardımcı olur. Yetkisiz Web'de gezinme alışkanlıklarını izlemenize, denetlemenize ve kaydetmenize olanak verir ve kişisel parolalar için güvenli bir saklama alanı sağlar.

Ebeveyn Denetimleri'ni kullanmaya başlamadan önce, en popüler özelliklerden bazıları hakkında bilgi edinebilirsiniz. Bu özelliklerin yapılandırılması ve kullanımıyla ilgili ayrıntılar, Ebeveyn Denetimleri yardımında sunulmaktadır.

Not: SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde

Ebeveyn Denetimleri özellikleri	136
Çevrimiçi ortamda çocuklarınızı koruma.....	137
Web'de bilgileri koruma	153
Parolaları koruma	155

Ebeveyn Denetimleri özellikleri

Ebeveyn Denetimleri

SecurityCenter kullanıcıları olası uygunsuz görüntüleri filtreleyebilir, yaşa uygun arama yapabilir, içerik derecelendirme gruplarını (kullanıcının görüntüleyebileceği web sitelerini ve içeriği kısıtlamak için kullanılan yaş grupları) yapılandırabilir ve web'de gezinme saat sınırlamalarını (kullanıcının web'e erişebileceği zaman aralığı ve süre) ayarlayabilirler. Ebeveyn Denetimleri, belirli web sitelerine erişimi genel olarak kısıtlamanızı ve ilişkili anahtar sözcüklere göre erişime izin vermenizi veya engellemenizi de sağlar.

Kişisel Bilgi Koruması

Hassas veya gizli bilgilerin (örneğin kredi kartı numaraları, banka hesap numaraları, adresler gibi) web üzerinden iletilmesini engelleyin.

Parola Kasası

Kişisel parolalarınızı başka hiçbir kullanıcının (hatta yöneticinin) erişmeyeceği şekilde güvenle saklayın.

B Ö L Ü M 3 1

Çevrimiçi ortamda çocuklarınızı koruma

Çocuklarınız bilgisayar kullanıyorsa, her çocuğun neleri görebileceğini ve Web'de gezinirken neler yapabileceğini düzenlemeye yardımcı olması için Ebeveyn Denetimleri'ni kullanabilirsiniz. Örneğin, yaşa uygun arama ve görüntü filtrelemeyi etkinleştirebilir veya devre dışı bırakabilir, içerik derecelendirme grubu seçebilir ve Web'de gezinme saat sınırlamalarını ayarlayabilirsiniz.

Yaşa uygun arama, bazı popüler arama motorlarının güvenlik filtrelerinin, olası uygunsuz öğeleri çocuğunuzun arama sonuçlarının otomatik olarak dışında tutacak şekilde etkinleştirilmesini sağlar; görüntü filtreleme, çocuğunuz Web'de gezinirken olası uygunsuz görüntülerin gösterilmesini engeller; içerik derecelendirme grubu, çocuğunuzun yaş grubuna göre erişebileceği Web içeriğinin türünü belirler; Web'de gezinme saat sınırlamaları, çocuğunuzun Web'e erişebileceği günleri ve saatleri tanımlar. Ayrıca tüm çocuklar için belirli Web sitelerini filtreleyebilirsiniz (engelleyebilir veya izin verebilirsiniz).

Not: Ebeveyn Denetimleri'ni çocuklarınızı koruyacak şekilde yapılandırmak için bilgisayarınızda Windows Yöneticisi olarak oturum açmanız gerekir. Bu McAfee ürününün daha önceki bir sürümünden yükseltme yaptıysanız ve hâlâ McAfee kullanıcılarını kullanıyorsanız, aynı zamanda McAfee yöneticisi olarak da oturum açtığınızdan emin olun.

Bu bölümde

Anahtar sözcükler kullanarak Web sitelerini filtreleme.....	138
Filtrelenen Web siteleri.....	139
Web'de gezinme saat sınırlarını ayarlama.....	142
içerik derecelendirme grubunu ayarlama.....	143
Olası uygunsuz Web resimlerini filtreleme.....	144
Yaşa uygun aramayı etkinleştirme.....	145
Kullanıcıları yapılandırma.....	147

Anahtar sözcükler kullanarak Web sitelerini filtreleme

Anahtar sözcük filtreleme, Yetişkin olmayan kullanıcıların olası uygunsuz sözcükler içeren Web sitelerine girmelerini engellemeye olanak verir. Anahtar sözcük filtreleme özelliği etkinleştirildiğinde, içerik derecelendirme grubuna göre kullanıcıların görebilecekleri içeriği derecelendirmek için varsayılan anahtar sözcük listesi ve ilişkili kurallar kullanılır. Kullanıcılar, bazı anahtar sözcükleri içeren Web sitelerine erişmek için belirli bir yaş grubuna ait olmalıdır. Örneğin, *porno* sözcüğünü içeren Web sitelerine yalnızca Yetişkin grubunun üyeleri girebilirken, *ilaçlar* sözcüğünü içeren Web sitelerine yalnızca Çocuk grubunun (ve daha büyük grupların) üyeleri girebilir.

Bu varsayılan listeye kendi anahtar sözcüklerinizi de ekleyebilir ve bunları belirli içerik derecelendirme gruplarıyla ilişkilendirebilirsiniz. Eklediğiniz anahtar sözcük kuralları, varsayılan listede eşleşen bir anahtar sözcükle önceden ilişkilendirilmiş kuralı geçersiz kılar.

Web sitelerini anahtar sözcüklere göre engelleme

Web sitelerini uygunsuz bir içeriğe göre engellemek istiyor ancak site adreslerini tam olarak bilemiyorsanız, siteleri anahtar sözcüklerine göre engelleyebilirsiniz. Bunun için bir anahtar sözcük girip, daha sonra bu anahtar sözcüğü içeren Web sitelerinin hangi içerik derecelendirme grupları tarafından görüntülenebileceğini belirlemeniz yeterlidir.

1 Ebeveyn Denetimleri bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
2. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklatın.
3. Ebeveyn Denetimleri Yapılandırma bölümünde, Ebeveyn Denetimleri'nin etkin olduğundan emin olun ve ardından **Gelişmiş**'i tıklatın.

2 Ebeveyn Denetimleri bölümünde **Anahtar Sözcükler**'i tıklatın ve anahtar sözcük filtrelemenin etkin olduğundan emin olun.

3 **Anahtar Sözcük Listesi** altında **Aranan** kutusuna bir anahtar sözcük yazın.

4 Minimum yaş grubunu belirtmek için **Minimum Yaş** kaydırma çubuğunu hareket ettirin.

Bu yaş grubunda ve daha büyük gruplardaki kullanıcılar, bu anahtar sözcüğü içeren Web sitelerine girebilirler.

5 **Tamam**'ı tıklatın.

Anahtar sözcük filtrelemeyi devre dışı bırakma

Varsayılan olarak anahtar sözcük filtreleme özelliği etkindir; böylece, içerik derecelendirme grubuna göre kullanıcıların görebilecekleri içeriği derecelendirmek için varsayılan anahtar sözcük listesi ve ilişkili kurallar kullanılır. McAfee tarafından önerilmemesine karşın, istediğiniz zaman anahtar sözcük filtrelemeyi devre dışı bırakabilirsiniz.

1 Ebeveyn Denetimleri bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
2. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklatın.
3. Ebeveyn Denetimleri Yapılandırma bölümünde, Ebeveyn Denetimleri'nin etkin olduğundan emin olun ve ardından **Gelişmiş**'i tıklatın.

2 Ebeveyn Denetimleri bölümünde **Anahtar Sözcükler**'i tıklatın.

3 Anahtar Sözcükler bölümünde **Kapalı**'yı tıklatın.

4 **Tamam**'ı tıklatın.

Filtrelenen Web siteleri

Yetişkin grubuna ait kullanıcılar dışında tüm kullanıcılar için Web sitelerini filtreleyebilirsiniz (engellenebilir veya izin verebilirsiniz). Çocuğunuzun Web'de gezinirken bir Web sitesine erişmesini önlemek için bu siteyi engellersiniz. Çocuğunuz engellenen Web sitesine erişmeye çalışırsa, bir iletiyle McAfee tarafından engellendiği için siteye erişilemeyeceği bildirilir.

Varsayılan olarak McAfee tarafından engellenen bir Web sitesine çocuklarınızın erişmesini isterseniz siteye izin verirsiniz. McAfee tarafından varsayılan olarak engellenen Web siteleri hakkında ayrıntılı bilgi için bkz. Anahtar sözcükler kullanarak Web sitelerini filtreleme (sayfa 138). Ayrıca filtrelenen bir Web sitesini istediğiniz zaman güncelleştirebilir veya kaldırabilirsiniz.

Not: Yetişkin yaş grubuna ait kullanıcılar (Yöneticiler dahil), engellenenler dahil olmak üzere tüm Web sitelerine erişebilirler. Engellenen Web sitelerini test etmek için Yetişkin olmayan kullanıcı olarak oturum açmanız gerekir, ancak testi tamamladığınızda Web tarayıcısının gezinme geçmişini temizlemeyi unutmayın.

Filtrelenen bir Web sitesini kaldırma

Artık engellemek veya izin vermek istemediğiniz filtrelenen Web sitesini kaldırabilirsiniz.

1 Ebeveyn Denetimleri bölümünü açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
2. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklatın.
3. Ebeveyn Denetimleri Yapılandırma bölümünde, Ebeveyn Denetimleri'nin etkin olduğundan emin olun ve ardından **Gelişmiş**'i tıklatın.

2 Ebeveyn Denetimleri bölümünde **Filtrelenen Web Siteleri**'ni tıklatın.

3 Filtrelenen Web Siteleri bölümünde, **Filtrelenen Verilen Web Siteleri** listesinden bir girişi tıklatın ve sonra **Kaldır**'ı tıklatın.

4 **Tamam**'ı tıklatın.

Filtrelenen bir Web sitesini güncelleştirme

Bir Web sitesinin adresi değişirse ya da onu engellerken veya izin verirken adresi yanlış girdiyse güncelleştirebilirsiniz.

1 Ebeveyn Denetimleri bölümünü açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
2. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklatın.
3. Ebeveyn Denetimleri Yapılandırma bölümünde, Ebeveyn Denetimleri'nin etkin olduğundan emin olun ve ardından **Gelişmiş**'i tıklatın.

2 Ebeveyn Denetimleri bölümünde **Filtrelenen Web Siteleri**'ni tıklatın.

3 Filtrelenen Web Siteleri bölümünde, **Filtrelenen Web Siteleri** listesinden bir girişi tıklatın, **http://** kutusunda Web sitesinin adresini değiştirin ve sonra **Güncelleştir**'i tıklatın.

4 **Tamam**'ı tıklatın.

Bir Web sitesine izin verme

Hiçbir kullanıcı erişiminin engellenmediğinden emin olmak için Web sitesine izin verirsiniz. Varsayılan olarak McAfee tarafından engellenen bir Web sitesine izin verirseniz, varsayılan ayarı geçersiz kılarırsınız.

1 Ebeveyn Denetimleri bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
2. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklatın.
3. Ebeveyn Denetimleri Yapılandırma bölümünde, Ebeveyn Denetimleri'nin etkin olduğundan emin olun ve ardından **Gelişmiş**'i tıklatın.

2 Ebeveyn Denetimleri bölümünde **Filtrelenen Web Siteleri**'ni tıklatın.

3 Filtrelenen Web Siteleri bölümünde **http://** kutusuna bir Web sitesinin adresini yazın ve sonra **İzin Ver**'i tıklatın.

4 **Tamam**'ı tıklatın.

İpucu: Web sitesinin adresini **Filtrelenen Web Siteleri** listesinde tıklatıp ardından **İzin Ver**'i tıklatarak, daha önceden engellenen bir Web sitesine izin verebilirsiniz.

Bir Web sitesini engelleme

Çocuğunuzun Web'de gezinirken bir Web sitesine erişmesini önlemek için bu siteyi engellersiniz. Çocuğunuz engellenen Web sitesine erişmeye çalışırsa, McAfee tarafından engellendiği için siteye erişilemediğini bildiren bir ileti görüntülenir.

1 Ebeveyn Denetimleri bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
2. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklatın.
3. Ebeveyn Denetimleri Yapılandırma bölümünde, Ebeveyn Denetimleri'nin etkin olduğundan emin olun ve ardından **Gelişmiş**'i tıklatın.

- 2 Ebeveyn Denetimleri bölümünde **Filtrelenen Web Siteleri**'ni tıklatın.
- 3 Filtrelenen Web Siteleri bölümünde **http://** kutusuna bir Web sitesinin adresini yazın ve sonra **Engelle**'yi tıklatın.
- 4 **Tamam**'ı tıklatın.

İpucu: Web sitesinin adresini **Filtrelenen Web Siteleri** listesinde tıklatıp ardından **Engelle**'yi tıklatarak, daha önceden izin verilen bir Web sitesini engelleyebilirsiniz.

Web'de gezinme saat sınırlarını ayarlama

Sorumsuz veya aşırı Internet kullanımı hakkında endişeleriniz varsa, çocuğunuzun Web'de gezinmesi için uygun saat sınırlamaları ayarlayabilirsiniz. Çocuğunuzun Web'de gezinmesini belirli saatlerle kısıtladığınızda, siz evde olmasanız bile SecurityCenter'ın bu kısıtlamaları uygulayacağından emin olabilirsiniz.

Varsayılan olarak, çocukların haftada yedi gün, gece ve gündüz her saat Web'de gezinmelerine izin verilir; ancak Web'de gezinmeyi belirli saatlerle veya günlerle sınırlayabilir ya da Web'de gezinmeyi tamamen yasaklayabilirsiniz. Bir çocuk yasaklanan zamanda Web'de gezinmeye çalışırsa, McAfee çocuğa bunu yapamayacağını bildirir. Web'de gezinmeyi tamamen yasaklarsanız, çocuk oturum açıp bilgisayarını ve e-posta, anlık ileti programları, ftp, oyunlar gibi diğer Internet programlarını kullanabilir ancak Web'de gezinemez.

Web'de gezinme saat sınırlarını ayarlama

Çocuğunuzun Web'de gezinmesini belirli günler ve saatlerle kısıtlamak için Web'de gezinme saat sınırlamaları kılavuzunu kullanabilirsiniz.

- 1 Kullanıcı Ayarları bölümünü açın.
Nasıl?
 1. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
 2. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklatın.
 3. Ebeveyn Denetimleri Yapılandırma bölümünde **Gelişmiş**'i tıklatın.
 4. Ebeveyn Denetimleri bölümünde **Kullanıcı Ayarları**'nı tıklatın.
- 2 Kullanıcı Ayarları bölümünde bir kullanıcı adını tıklatın ve sonra **Düzenle**'yi tıklatın.
- 3 Kullanıcı Hesabını Düzenle penceresinde, **Web'de Gezinme Saat Sınırları** altında fareni sürükleyerek bu kullanıcının Web'de gezinemeyeceği günleri ve saatleri belirtin.
- 4 **Tamam**'ı tıklatın.

İçerik derecelendirme grubunu ayarlama

Kullanıcı aşağıdaki içerik derecelendirme gruplarından birine ait olabilir:

- Küçük çocuk
- Çocuk
- Büyük çocuk
- Genç
- Yetişkin

Ebeveyn Denetimleri, kullanıcının ait olduğu gruba göre Web içeriğini derecelendirir (engeller veya izin verir). Bu, evinizdeki bazı kullanıcılar için belirli Web sitelerini engelleme veya izin vermenizi sağlar. Örneğin, bazı Web içeriklerini Küçük çocuk grubundan kullanıcılar için engelleyebilir, ancak Genç grubundan kullanıcılar için bu içeriklere izin verebilirsiniz. Bir kullanıcı için içeriği daha kısıtlı şekilde derecelendirmek isterseniz, kullanıcının yalnızca **Filtrelenen Web Siteleri** listesinde izin verilen Web sitelerini görüntülemesine izin verebilirsiniz. Ayrıntılı bilgi için bkz. Web sitelerini filtreleme (sayfa 139).

Kullanıcının içerik derecelendirme grubunu ayarlama

Varsayılan olarak, yeni bir kullanıcı Yetişkin grubuna eklenir ve bu kullanıcının tüm Web içeriğine erişmesine izin verilir. Daha sonra yaşına ve olgunluk düzeyine göre kullanıcının içerik derecelendirme grubunu ayarlayabilirsiniz.

1 Kullanıcı Ayarları bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
2. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'i tıklatın.
3. Ebeveyn Denetimleri Yapılandırma bölümünde **Gelişmiş**'i tıklatın.
4. Ebeveyn Denetimleri bölümünde **Kullanıcı Ayarları**'ni tıklatın.

2 Kullanıcı Ayarları bölümünde bir kullanıcı adını tıklatın ve sonra **Düzenle**'yi tıklatın.

3 Kullanıcı Hesabını Düzenle penceresinde, **İçerik Derecelendirmesi** altında kullanıcıya atamak istediğiniz yaş grubunu tıklatın.

Kullanıcının **Filtrelenen Verilen Web Siteleri** listesinde engellenen Web sitelerine girmesini önlemek için **Bu kullanıcı yalnızca İzin Verilen Web Siteleri** listesindeki sitelere erişebilir onay kutusunu işaretleyin.

4 **Tamam**'i tıklatın.

Olası uygunsuz Web resimlerini filtreleme

Kullanıcının yaşına ve olgunluk düzeyine göre, kullanıcı Web'de gezinirken olası uygunsuz resimleri filtreleyebilirsiniz (engelleyebilir veya izin verebilirsiniz). Örneğin, küçük çocuğunuz Web'de gezinirken olası uygunsuz resimlerin görüntülenmesini engelleyebilir, ancak bunların evinizdeki gençler ve yetişkinler için görüntülenmesine izin verebilirsiniz. Varsayılan olarak, resim filtreleme özelliği Yetişkin grubunun tüm üyeleri için devre dışıdır; bu kullanıcılar Web'de gezinirken olası uygunsuz resimleri görebilirler. Kullanıcının yaş grubunu ayarlama hakkında ayrıntılı bilgi için bkz. İçerik derecelendirme grubunu ayarlama (sayfa 143).

Olası uygunsuz Web resimlerini filtreleme

Varsayılan olarak, yeni kullanıcılar Yetişkin grubuna eklenir ve görüntü filtreleme devre dışı bırakılır. Belirli bir kullanıcı Web'de gezinirken olası uygunsuz resimlerin görüntülenmesini engellemek isterseniz, görüntü filtrelemeyi etkinleştirebilirsiniz. Olası uygunsuz Web resimlerinin yerine otomatik olarak sabit bir McAfee görüntüsü gösterilir.

1 Kullanıcı Ayarları bölmesini açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
2. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklatın.
3. Ebeveyn Denetimleri Yapılandırma bölümünde **Gelişmiş**'i tıklatın.
4. Ebeveyn Denetimleri bölümünde **Kullanıcı Ayarları**'nı tıklatın.

2 Kullanıcı Ayarları bölümünde bir kullanıcı adını tıklatın ve sonra **Düzenle**'yi tıklatın.

3 Kullanıcı Hesabını Düzenle penceresinde, **Görüntü Filtreleme** altında **Açık**'i tıklatın.

4 **Tamam**'i tıklatın.

Yaşa uygun aramayı etkinleştirme

Bazı popüler arama motorları (Yahoo! ve Google gibi), uygunsuz olabilecek arama sonuçlarının sonuç listelerinde görüntülenmesini engelleyen bir arama ayarı olan "güvenli arama" özelliğini sunar. Bu arama motorları, genellikle güvenli arama filtresinin ne kadar kısıtlayıcı olmasını istediğinizi belirlemenize olanak tanır, ancak aynı zamanda bunun siz veya herhangi bir kullanıcı tarafından kapatılmasına da izin verir.

Ebeveyn Denetimleri'nin yaşa uygun arama özelliği, şu arama motorlarından birini veya birkaçını kullanırken, "güvenli arama"nın bir kullanıcıda her zaman açık olmasını sağlamak için kullanışlı bir yöntemdir:

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

Yaşa uygun aramayı etkinleştirirseniz, arama motorunun güvenli arama filtresinin bu kullanıcıda açık ve en kısıtlayıcı ayarda olmasını sağlarız ve kullanıcı bunu kapatmaya çalışırsa (arama motorunun tercihlerinde veya gelişmiş ayarlarında) bunu otomatik olarak yeniden açarız.

Varsayılan olarak, yaşa uygun arama yöneticiler ve Yetişkin yaş grubundakiler dışında tüm kullanıcılar için etkindir. Kullanıcının yaş grubunu ayarlama hakkında ayrıntılı bilgi için bkz. İçerik derecelendirme grubunu ayarlama (sayfa 143).

Yaşaya uygun aramayı etkinleştirme

Varsayılan olarak, yeni kullanıcılar Yetişkin grubuna eklenir ve yaşaya uygun arama devre dışı bırakılır. Bazı popüler arama motorları tarafından sunulan güvenli arama filtrelemesinin bir Yetişkin kullanıcı için açık olmasını istiyorsanız, yaşaya uygun aramayı etkinleştirebilirsiniz.

1 Kullanıcı Ayarları bölümünü açın.

Nasıl?

1. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
 2. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'ı tıklatın.
 3. Ebeveyn Denetimleri Yapılandırma bölümünde **Gelişmiş**'i tıklatın.
 4. Ebeveyn Denetimleri bölümünde **Kullanıcı Ayarları**'nı tıklatın.
- 2** Kullanıcı Ayarları bölümünde bir kullanıcı adını tıklatın ve sonra **Düzenle**'yi tıklatın.
- 3** Kullanıcı Hesabını Düzenle penceresinde, **Yaşaya Uygun Arama** altında **Açık**'ı tıklatın.
- 4** **Tamam**'ı tıklatın.

B Ö L Ü M 3 2

Kullanıcıları yapılandırma

Ebeveyn Denetimleri'ni çocuklarınızı koruyacak şekilde yapılandırmak için SecurityCenter'da onlara belirli izinler atarsınız. Bu izinler, her çocuğun Web'de neler görebileceğini ve yapabileceğini belirler.

Varsayılan olarak, SecurityCenter kullanıcıları, bilgisayarınızda ayarladığınız Windows kullanıcılarına karşılık gelir. Ancak McAfee kullanıcılarını kullanan önceki bir SecurityCenter sürümünden yükseltme yaptıysanız, McAfee kullanıcılarınız ve izinleri geçerlidir.

Not: Kullanıcıları yapılandırmak için bilgisayarınızda Windows yöneticisi olarak oturum açmanız gerekir. Bu McAfee ürününün daha önceki bir sürümünden yükseltme yaptıysanız ve hâlâ McAfee kullanıcılarını kullanıyorsanız, aynı zamanda McAfee yöneticisi olarak da oturum açtığınızdan emin olun.

Bu bölümde

McAfee kullanıcılarıyla çalışma	148
Windows kullanıcılarıyla çalışma	151


McAfee kullanıcılarıyla çalışma

McAfee kullanıcılarını kullanan önceki bir SecurityCenter sürümünden yükseltme yaptıysanız, McAfee kullanıcılarınız ve izinleri otomatik olarak geçerlidir. McAfee kullanıcılarını yapılandırmaya ve yönetmeye devam edebilirsiniz; ancak McAfee, Windows kullanıcılarına geçmenizi önerir. Windows kullanıcılarına geçtikten sonra, hiçbir zaman yeniden McAfee kullanıcılarına dönemezsiniz.

McAfee kullanıcılarını kullanmaya devam ederseniz, kullanıcı ekleyebilir, düzenleyebilir veya kaldırabilir ve McAfee yönetici parolasını değiştirebilir veya alabilirsiniz.

McAfee yönetici parolasını alma

Yönetici parolasını unutursanız, bunu alabilirsiniz.

- 1 SecurityCenter simgesini  sağ tıklatın ve sonra **Kullanıcı Değiştir'i** tıklatın.
- 2 **Kullanıcı Adı** listesinde **Yönetici**'yi seçin ve sonra **Parolayı mı Unuttunuz?**'u tıklatın.
- 3 **Yanıt** kutusuna gizli sorunuzun yanıtını yazın.
- 4 **Gönder**'i tıklatın.

McAfee yönetici parolasını değiştirme

McAfee yönetici parolasını anımsamakta zorlanıyor veya parolanın ele geçirildiğinden şüpheleniyorsanız, onu değiştirebilirsiniz.

- 1 SecurityCenter'da Yönetici olarak oturum açın.
- 2 Kullanıcı Ayarları bölmesini açın.
Nasıl?
 1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
 3. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'i tıklatın.
 4. Ebeveyn Denetimleri Yapılandırma bölümünde **Gelişmiş**'i tıklatın.
- 3 Kullanıcı Ayarları bölümünde, **McAfee Kullanıcı Hesapları** altında **Yönetici**'yi seçin ve sonra **Düzenle**'yi tıklatın.
- 4 Kullanıcı Hesabını Düzenle iletişim kutusunda, **Yeni Parola** kutusuna yeni parolanızı yazın ve sonra **Parolayı Yeniden Girin** kutusuna parolanızı yeniden yazın.
- 5 **Tamam**'i tıklatın.

Bir McAfee kullanıcıını kaldırma

İstedığınız zaman bir McAfee kullanıcıını kaldırabilirsiniz.

McAfee kullanıcıını kaldırmak için:

- 1** SecurityCenter'da Yönetici olarak oturum açın.
- 2** Kullanıcı Ayarları bölmesini açın.
Nasıl?
 1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
 3. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'i tıklatın.
 4. Ebeveyn Denetimleri Yapılandırma bölümünde **Gelişmiş**'i tıklatın.
- 3** Kullanıcı Ayarları bölümünde, **McAfee Kullanıcı Hesapları** altında bir kullanıcı adı seçin ve sonra **Kaldır**'i tıklatın.

Bir McAfee kullanıcıının hesap bilgilerini düzenleme

Bir McAfee kullanıcıının parolasını, hesap türünü veya otomatik oturum açma özelliğini değiştirebilirsiniz.

- 1** SecurityCenter'da Yönetici olarak oturum açın.
- 2** Kullanıcı Ayarları bölümünü açın.
Nasıl?
 1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
 3. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'i tıklatın.
 4. Ebeveyn Denetimleri Yapılandırma bölümünde **Gelişmiş**'i tıklatın.
- 3** Kullanıcı Ayarları bölümünde bir kullanıcı adını tıklatın ve sonra **Düzenle**'yi tıklatın.
- 4** Kullanıcının parolasını, hesap türünü veya Ebeveyn Denetimleri korumasını düzenlemek için ekran yönergelerini izleyin.
- 5** **Tamam**'i tıklatın.

McAfee kullanıcısı ekleme

McAfee kullanıcısı oluşturduktan sonra, bu kullanıcı için Ebeveyn Denetimleri korumasını yapılandırabilirsiniz. Ayrıntılı bilgi için Ebeveyn Denetimleri yardımına bakın.

- 1 SecurityCenter'da Yönetici olarak oturum açın.
- 2 Kullanıcı Ayarları bölmesini açın.
Nasıl?
 1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
 3. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'i tıklatın.
 4. Ebeveyn Denetimleri Yapılandırma bölümünde **Gelişmiş**'i tıklatın.
- 3 Kullanıcı Ayarları bölümünde **Ekle**'yi tıklatın.
- 4 Kullanıcı adı, parola, hesap türü ve Ebeveyn Denetimleri korumasını ayarlamak için ekran yönergelerini uygulayın.
- 5 **Oluştur**'u tıklatın.

Windows kullanıcılarına geçme

İşlem kolaylığı için McAfee Windows kullanıcılarına geçmenizi önerir, ancak bunu yaparsanız hiçbir zaman yeniden McAfee kullanıcılarına dönemezsiniz.

- 1 Kullanıcı Ayarları bölmesini açın.
Nasıl?
 1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
 2. SecurityCenter Giriş bölümünde **Ebeveyn Denetimleri**'ni tıklatın.
 3. Ebeveyn Denetimleri bilgi bölümünde **Yapılandır**'i tıklatın.
 4. Ebeveyn Denetimleri Yapılandırma bölümünde **Gelişmiş**'i tıklatın.
- 2 Kullanıcı Ayarları bölümünde **Değiştir**'i tıklatın.
- 3 İşlemi onaylayın.

Windows kullanıcılarıyla çalışma

Varsayılan olarak, SecurityCenter kullanıcıları, bilgisayarınızda ayarladığımız Windows kullanıcılarına karşılık gelir. Windows'ta Bilgisayar Yönetimi altında kullanıcı ekleyebilir, bir kullanıcının hesap bilgilerini düzenleyebilir ve kullanıcı kaldırabilirsiniz. Daha sonra SecurityCenter'da bu kullanıcılar için Ebeveyn Denetimleri koruması ayarlayabilirsiniz.

Ancak McAfee kullanıcılarını kullanan önceki bir SecurityCenter sürümünden yükseltme yaptıysanız bkz. McAfee kullanıcılarıyla çalışma (sayfa 148).

B Ö L Ü M 3 3

Web'de bilgileri koruma

Korunan bilgi alanına ekleyerek, kişisel bilgilerinizin (ad, adres, kredi kartı numaraları ve banka hesap numaraları gibi) Web üzerinden iletilmesini engelleyebilirsiniz.

Not: Ebeveyn Denetimleri, kişisel bilgilerin iletilmesini, banka siteleri gibi güvenli Web siteleriyle (https:// protokolünü kullanan Web siteleri) engellemez.

Bu bölümde

Kişisel bilgileri koruma..... 154

Kişisel bilgileri koruma

Engelleyerek, kişisel bilgilerinizin (ad, adres, kredi kartı numaraları ve banka hesap numaraları gibi) Web üzerinden iletilmesini engelleyin. McAfee Web üzerinden gönderilmek üzere olan bir şeyde (örneğin form alanı veya dosya) kişisel bilgiler algılırsa şunlar gerçekleşir:

- Yöneticiyseniz, bilgi gönderme işlemi onaylamanız gerekir.
- Yönetici değilseniz, engellenen bölümün yerine yıldız işaretleri (*) yerleştirilir. Örneğin, kötü niyetli bir Web sitesi kredi kartı numaranızı başka bir bilgisayara göndermeye çalışırsa, numaranın yerine yıldız işaretleri yerleştirilir.

Kişisel bilgileri koruma

Şu türde kişisel bilgileri engelleyebilirsiniz: ad, adres, posta kodu, sosyal sigorta numarası, telefon numarası, kredi kartı numaraları, banka hesapları, komisyonculuk hesapları ve telefon kartları. Farklı türde kişisel bilgileri engellemek istiyorsanız, bilgi türünü **diğer** olarak ayarlayabilirsiniz.

1 Korunan Bilgiler bölümünü açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
2. SecurityCenter Giriş bölümünde **Internet** ve **Ağ**'i tıklatın.
3. Internet ve Ağ bilgi bölümünde **Yapılandır**'i tıklatın.
4. Internet ve Ağ Yapılandırması bölümünde, **Kişisel bilgi** korumanın etkin olduğundan emin olun ve ardından **Gelişmiş**'i tıklatın.

2 Korunan Bilgiler bölümünde **Ekle**'yi tıklatın.

3 Listedeki engellemek istediğiniz bilgi türünü seçin.

4 Kişisel bilgilerinizi girin ve ardından **Tamam**'i tıklatın.

B Ö L Ü M 3 4

Parolaları koruma

Parola Mahzeni, kişisel parolalarınız için güvenli bir saklama alanıdır. Parolalarınızı başka hiçbir kullanıcının (hatta Yöneticinin) erişemeyeceği şekilde güvenle saklamanıza olanak verir.

Bu bölümde

Parola Kasası'nı ayarlama 156

Parola Kasası'nı ayarlama

Parola Kasası'nı kullanmaya başlamadan önce, Parola Kasası parolasını ayarlamanız gerekir. Yalnızca bu parolayı bilen kullanıcılar Parola Kasası'na erişebilirler. Parola Kasası parolanızı unutursanız, onu sıfırlayabilirsiniz; ancak bu durumda Parola Kasası'nda daha önceden saklanan tüm parolalar silinir.

Parola Kasası parolasını ayarladıktan sonra, kasanızda parolalar ekleyebilir, silebilir veya kaldırabilirsiniz. İsteddiğiniz zaman Parola Kasası parolanızı da değiştirebilirsiniz.

Parola Kasası parolanızı sıfırlama

Parola Kasası parolanızı unutursanız, onu sıfırlayabilirsiniz; ancak bu durumda daha önceden girmiş olduğunuz tüm parolalar silinir.

1 Parola Kasası bölmesini açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
2. SecurityCenter Giriş bölümünde **Internet ve Ağ**'ı tıklatın.
3. Internet ve Ağ bilgi bölümünde **Yapılandır**'i tıklatın.
4. Internet ve Ağ Yapılandırması bölümünde, **Parola Mahzeni** altında **Gelişmiş**'i tıklatın.

2 Parolanızı unuttunuz mu? seçeneğini tıklatın.

3 Parola Kasasını Sıfırla iletişim kutusunda, **Parola** kutusuna yeni bir parola yazın ve sonra **Parolayı Yeniden Girin** kutusuna parolayı yeniden yazın.

4 Sıfırla'yı tıklatın.

5 Parola Onayını Sıfırla iletişim kutusunda **Evet**'i tıklatın.

Parola Mahzeni parolanızı deęiřtirme

İstedięiniz zaman Parola Mahzeni parolanızı deęiřtirebilirsiniz.

- 1** Parola Mahzeni bۆlmesini aın.
Nasıl?
 1. **Ortak Gۆrevler** bۆlümünde **Giriř**'i tıklatın.
 2. SecurityCenter Giriř bۆlmesinde **Internet ve Aę**'i tıklatın.
 3. Internet ve Aę bilgi bۆlümünde **Yapılandır**'i tıklatın.
 4. Internet ve Aę Yapılandırması bۆlmesinde, **Parola Mahzeni** altında **Geliřmiř**'i tıklatın.
- 2** Parolayı Mahzeni bۆlmesinde, **Parola** kutusuna geerli parolanızı yazın ve sonra **A**'i tıklatın.
- 3** Parola Mahzenini Yۆnet bۆlmesinde **Parolayı Deęiřtir**'i tıklatın.
- 4** **Parola Sein** kutusuna yeni bir parola yazın ve sonra **Parolayı Yeniden Girin** kutusuna parolanızı yeniden yazın.
- 5** **Tamam**'i tıklatın.
- 6** Parola Mahzeni Parolası Deęiřtirildi iletiřim kutusunda **Tamam**'i tıklatın.

Parolayı kaldırma

İstedięiniz zaman Parola Mahzeni'nden bir parolayı kaldırabilirsiniz. Mahzenden kaldırdıęınız parolayı hibir řekilde kurtaramazsınız.

- 1** Parola Mahzeni bۆlmesini aın.
Nasıl?
 1. **Ortak Gۆrevler** bۆlümünde **Giriř**'i tıklatın.
 2. SecurityCenter Giriř bۆlmesinde **Internet ve Aę**'i tıklatın.
 3. Internet ve Aę bilgi bۆlümünde **Yapılandır**'i tıklatın.
 4. Internet ve Aę Yapılandırması bۆlmesinde, **Parola Mahzeni** altında **Geliřmiř**'i tıklatın.
- 2** Parola Mahzeni parolanızı **Parola** kutusuna yazın.
- 3** **A**'i tıklatın.
- 4** Parola Mahzenini Y�net bۆlmesinde bir parola giriřini tıklatın ve sonra **Kaldır**'i tıklatın.
- 5** Kaldırma Onayı iletiřim kutusunda **Evet**'i tıklatın.

Parolayı deęiřtirme

Parola Mahzeni'ndeki giriřlerin her zaman doęru ve güvenilir olmasını saęlamak için, parolalar deęiřtięinde bunları g¼ncelleřtirmeniz gerekir.

1 Parola Mahzeni b¼lmesini aın.

Nasıl?

1. **Ortak G¼revler** b¼l¼m¼nde **Giriř**'i tıkladın.
2. SecurityCenter Giriř b¼lmesinde **Internet** ve **Aę**'i tıkladın.
3. Internet ve Aę bilgi b¼l¼m¼nde **Yapılandır**'i tıkladın.
4. Internet ve Aę Yapılandırması b¼lmesinde, **Parola Mahzeni** altında **Geliřmiř**'i tıkladın.

2 Parola Mahzeni parolanızı **Parola** kutusuna yazın.

3 **A**'i tıkladın.

4 Parola Mahzenini Y¼net b¼lmesinde bir parola giriřini tıkladın ve sonra **D¼zenle**'yi tıkladın.

5 **Aıklama** kutusundaki parola aıklamasını (¼rneęin parolanın neyle ilgili olduęu) deęiřtirin ve ardından **Parola** kutusundaki parolayı deęiřtirin.

6 **Tamam**'i tıkladın.

Parola ekleme

Parolalarınızı anımsamakta zorlanıyorsanız, bunları Parola Kasası'na ekleyebilirsiniz. Parola Kasası, yalnızca Parola Kasası parolasını bilen kullanıcılar tarafından eriřilebilen güvenli bir konumdur.

1 Parola Kasası b¼lmesini aın.

Nasıl?

1. **Ortak G¼revler** b¼l¼m¼nde **Giriř**'i tıkladın.
2. SecurityCenter Giriř b¼lmesinde **Internet** ve **Aę**'i tıkladın.
3. Internet ve Aę bilgi b¼l¼m¼nde **Yapılandır**'i tıkladın.
4. Internet ve Aę Yapılandırması b¼lmesinde, **Parola Mahzeni** altında **Geliřmiř**'i tıkladın.

2 Parola Kasası parolanızı **Parola** kutusuna yazın.

3 **A**'i tıkladın.

4 Parola Kasasını Y¼net b¼lmesinde **Ekle**'yi tıkladın.

5 **Aıklama** kutusuna parola aıklamasını (¼rneęin parolanın neyle ilgili olduęu) yazın ve ardından **Parola** kutusuna parolayı yazın.

6 **Tamam**'i tıkladın.

B Ö L Ü M 3 5

McAfee Yedekleme ve Geri Yükleme

Dosyalarınızı CD, DVD, USB sürücüye, harici sabit diske veya ağ sürücüsüne arşivleyerek verilerinizin yanlışlıkla kaybolmasını engellemek için McAfee® Backup and Restore kullanın. Yerel arşivleme, kişisel verilerinizi CD, DVD, USB sürücüye, harici sabit diske veya ağ sürücüsüne arşivlemenize (yedeklemenize) olanak verir. Bu özellik, yanlışlıkla kaybettiğiniz kayıtlarınızın, belgelerinizin ve kişisel olarak ilgilendiğiniz diğer malzemelerin yerel kopyasını sağlar.

Backup and Restore'u kullanmaya başlamadan önce, en popüler özelliklerden bazıları hakkında bilgi edinebilirsiniz. Bu özelliklerin yapılandırılması ve kullanımıyla ilgili ayrıntılar, Backup and Restore yardımında sunulmaktadır. Program özelliklerine göz attıktan sonra, yerel arşivler gerçekleştirmek için yeterli kullanılabilir arşiv ortamının bulunduğundan emin olmalısınız.

Not: SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde

Backup and Restore özellikleri	160
Dosyaları arşivleme.....	161
Arşivlenen dosyalarla çalışma.....	171

Backup and Restore özellikleri

Yerel zamanlanan arşivleme

Dosyaları ve klasörleri CD, DVD, USB sürücüsüne, harici sabit diske veya ağ sürücüsüne arşivleyerek verilerinizi koruyun. Siz ilk arşivlemeyi başlattıktan sonra, artımlı arşivler otomatik olarak gerçekleşir.

Tek tıklatmayla geri yükleme

Dosyalar ve klasörler bilgisayarınızda yanlışlıkla silinir veya bozulursa, en son arşivlenen sürümleri kullanılan arşiv ortamından geri yükleyebilirsiniz.

Sıkıştırma ve şifreleme

Varsayılan olarak, arşivlenen dosyalarınız sıkıştırılır ve bu şekilde arşiv ortamınızda alan kazanılır. Ek güvenlik önlemi için, arşivleriniz varsayılan olarak şifrelenir.

B Ö L Ü M 3 6

Dosyaları arşivleme

McAfee Backup and Restore'u kullanarak, bilgisayarınızdaki dosyaların kopyasını CD, DVD, USB sürücüye, harici sabit diske veya ağ aygıtına arşivleyebilirsiniz. Dosyalarınızı bu şekilde arşivlemek, yanlışlıkla kaybolan veya zarar gören verileri geri almanızı kolaylaştırır.

Dosyaları arşivlemeye başlamadan önce, varsayılan arşiv konumunuzu (CD, DVD, USB sürücü, harici sabit disk veya ağ sürücüsü) seçmeniz gerekir. McAfee, örneğin arşivlemek istediğiniz klasörler ve dosya türleri gibi bazı ayarları önceden yapmıştır, ancak bu ayarları değiştirebilirsiniz.

Yerel arşiv seçeneklerini ayarladıktan sonra, Backup and Restore'un tam veya hızlı arşivlemeleri çalıştırma sıklığı ile ilgili varsayılan ayarları değiştirebilirsiniz. İstedığınız zaman el ile arşivlemeleri çalıştırabilirsiniz.

Bu bölümde

Yerel arşivi etkinleştirme ve devre dışı bırakma.....	162
Arşiv seçeneklerini ayarlama	163
Tam ve hızlı arşivlemeleri çalıştırma	167

Yerel arşivi etkinleştirme ve devre dışı bırakma

Backup and Restore'u ilk açtığımızda, Backup and Restore'u nasıl kullanmak istediğinize bağlı olarak, yerel arşivi etkinleştirmeye veya devre dışı bırakmaya karar verirsiniz. Backup and Restore'da oturum açıp kullanmaya başladıktan sonra, istediğiniz zaman yerel arşivlemeyi etkinleştirebilir veya devre dışı bırakabilirsiniz.

Bilgisayarınızdaki dosyaların kopyasını CD, DVD, USB sürücüye, harici sabit diske veya ağ aygıtına arşivlemek istemiyorsanız, yerel arşivi devre dışı bırakabilirsiniz.

Yerel arşivi etkinleştirme

Bilgisayarınızdaki dosyaların kopyasını CD, DVD, USB sürücüye, harici sabit diske veya ağ aygıtına arşivlemek istiyorsanız, yerel arşivi etkinleştirebilirsiniz.

- 1 SecurityCenter'da **Gelişmiş Menü'de Yapılandır**'ı tıklatın.
- 2 Yapılandır bölümünde **Bilgisayar ve Dosyalar**'ı tıklatın.
- 3 Bilgisayar ve Dosyalar Yapılandırma bölümünde, **Yerel Arşiv devre dışı** altında **Açık**'ı tıklatın.

Yerel arşivi devre dışı bırakma

Bilgisayarınızdaki dosyaların kopyasını CD, DVD, USB sürücüye, harici sabit diske veya ağ aygıtına arşivlemek istemiyorsanız, yerel arşivi devre dışı bırakabilirsiniz.

- 1 SecurityCenter'da **Gelişmiş Menü'de Yapılandır**'ı tıklatın.
- 2 Yapılandır bölümünde **Bilgisayar ve Dosyalar**'ı tıklatın.
- 3 Bilgisayar ve Dosyalar Yapılandırma bölümünde, **Yerel Arşiv etkin** altında **Kapalı**'yı tıklatın.

Arşiv seçeneklerini ayarlama

Dosyalarınızı arşivlemeye başlamadan önce, bazı yerel arşiv seçeneklerini ayarlamalısınız. Örneğin, izleme konumlarını ve izlenen dosya türlerini ayarlamanız gereklidir. İzleme konumları, Backup and Restore'un bilgisayarınızda yeni dosyaları veya dosya değişikliklerini izlediği klasörlerdir. İzlenen dosya türleri, Backup and Restore'un izleme konumlarında arşivlediği dosya türleridir (örn., .doc, .xls gibi). Varsayılan olarak, aşağıdaki dosya türleri arşivlenir; ancak başka dosya türlerini de arşivleyebilirsiniz.

- Microsoft® Word belgeleri (.doc, .docx)
- Microsoft Excel® elektronik tabloları (.xls, .xlsx)
- Microsoft PowerPoint® sunuları (.ppt, .pptx)
- Microsoft Project® dosyaları (.mpp)
- Adobe® PDF dosyaları (.pdf)
- Düz metin dosyaları (.txt)
- HTML dosyaları (.html)
- JPEG dosyaları (.jpg, .jpeg)
- TIFF dosyaları (.tif)
- MPEG Ses Akışı III dosyaları (.mp3)
- Video dosyaları (.vdo)

Not: Şu dosya türlerini arşivleyemezsiniz: .ost ve .pst.

İki tür izleme konumu ayarlayabilirsiniz: üst düzey klasörler ve alt klasörler ve yalnızca üst düzey klasörler. Üst düzey klasörler ve alt klasörler konumu ayarlarsanız, Backup and Restore bu klasörün ve alt klasörlerinin içindeki izlenen dosya türlerini arşivler. Üst düzey klasörler konumu ayarlarsanız, Backup and Restore yalnızca bu klasörün (alt klasörlerinin değil) içindeki izlenen dosya türlerini arşivler. Ayrıca, yerel arşivin dışında tutmak istediğiniz konumları da tanımlayabilirsiniz. Varsayılan olarak, Windows Masaüstü ve Belgelerim konumları üst düzey klasörler ve alt klasörler izleme konumları olarak ayarlıdır.

İzlenen dosya türlerini ve konumları ayarladıktan sonra, arşiv konumunu (arşivlenen verilerin depolanacağı CD, DVD, USB sürücü, harici sabit disk veya ağ sürücüsü) ayarlamanız gerekir. Arşiv konumunu istediğiniz zaman değiştirebilirsiniz.

Güvenlik nedenleri veya boyut sorunlarından ötürü, arşivlenen dosyalarınızda varsayılan olarak şifreleme veya sıkıştırma etkindir. Bilgileri şifrenin nasıl çözüleceğini bilmeyen kişiler tarafından okunamayacak şekilde gizleyerek, şifrelenen dosyaların içeriği metinden şifreye dönüştürülür. Sıkıştırılan dosyalar, onları depolamak veya iletmek için gereken alanı en aza indirecek şekilde sıkıştırılır. McAfee tarafından önerilmemesine karşın, istediğiniz zaman şifreleme veya sıkıştırmayı devre dışı bırakabilirsiniz.

Arşivlemeye konum ekleme

Arşivleme için iki tür izleme konumu ayarlayabilirsiniz: üst düzey klasörler ve alt klasörler ve yalnızca üst düzey klasörler. Üst düzey klasörler ve alt klasörler konumu ayarlarsanız, Backup and Restore klasörün ve alt klasörlerinin içeriklerindeki değişiklikleri izler. Üst düzey klasörler konumu ayarlarsanız, Backup and Restore yalnızca klasörün (alt klasörlerinin değil) içeriklerini izler.

1 Yerel Arşiv Ayarları iletişim kutusunu açın.

Nasıl?

1. **Yerel Arşiv** sekmesini tıklatın.
2. Soldaki bölmede **Ayarlar**'ı tıklatın.

2 **İzleme Konumları**'nı tıklatın.

3 Aşağıdakilerden birini gerçekleştirin:

- Alt klasörlerinin içerikleri dahil olmak üzere bir klasörün içeriklerini arşivlemek için **Arşivleme Üst Düzey Klasörleri ve Alt Klasörleri** altında **Klasör Ekle**'yi tıklatın.
- Alt klasörlerinin içerikleri hariç bir klasörün içeriklerini arşivlemek için **Arşivleme Üst Düzey Klasörleri** altında **Klasör Ekle**'yi tıklatın.
- Bir dosyanın tamamını arşivlemek için **Arşivleme Üst Düzey Klasörleri** altında **Dosya Ekle**'yi tıklatın.

4 Klasöre Gözet (veya Aç) iletişim kutusunda, izlemek istediğiniz klasöre (veya dosyaya) gidin ve ardından **Tamam**'ı tıklatın.

5 **Tamam**'ı tıklatın.

İpucu: Backup and Restore'un henüz oluşturmadığınız bir klasörü izlemesini istiyorsanız, bir klasör eklemek ve aynı zamanda bunu izleme konumu olarak ayarlamak için, Klasöre Gözet iletişim kutusunda **Yeni Klasör Oluştur**'u tıklatabilirsiniz.

Arşivleme dosyası türlerini ayarlama

Üst düzey klasörler ve alt klasörler veya üst düzey klasörler konularınızda hangi dosya türlerinin arşivleneceğini belirleyebilirsiniz. Bunları mevcut bir dosya türleri listesinden seçebilir veya listeye yeni bir tür ekleyebilirsiniz.

- 1 Yerel Arşiv Ayarları iletişim kutusunu açın.
Nasıl?
 1. **Yerel Arşiv** sekmesini tıklatın.
 2. Soldaki bölmede **Ayarlar**'ı tıklatın.
- 2 **Dosya Türleri**'ni tıklatın.
- 3 Dosya türleri listesini genişletin ve arşivlemek istediğiniz dosya türlerinin yanındaki onay kutularını seçin.
- 4 **Tamam**'ı tıklatın.

İpucu: **Seçili Dosya Türleri** listesine yeni bir dosya türü eklemek için dosya uzantısını **Özel dosya türünü Diğer'e Ekle** kutusuna, ardından **Ekle**'yi ve **Tamam**'ı tıklatın. Yeni dosya türü, otomatik olarak izlenen dosya türü olur.

Bir konumu arşivlemenin dışında tutma

Bir konumun (klasör) ve içeriklerinin çevrimiçi olarak arşivlenmesini engellemek isterseniz, o konumu arşivlemenin dışında tutarsınız.

- 1 Yerel Arşiv Ayarları iletişim kutusunu açın.
Nasıl?
 1. **Yerel Arşiv** sekmesini tıklatın.
 2. Soldaki bölmede **Ayarlar**'ı tıklatın.
- 2 **İzleme Konuları**'ni tıklatın.
- 3 **Yedeklemeden Dışlanan Klasörler** altında **Klasör Ekle**'yi tıklatın.
- 4 Klasöre Gözet iletişim kutusunda, dışarıda tutmak istediğiniz klasöre gidip seçin ve ardından **Tamam**'ı tıklatın.
- 5 **Tamam**'ı tıklatın.

İpucu: Backup and Restore'un henüz oluşturmadığınız bir klasörü dışarıda tutmasını istiyorsanız, bir klasör eklemek ve aynı zamanda bunu dışarıda tutmak için, Klasöre Gözet iletişim kutusunda **Yeni Klasör Oluştur**'u tıklatabilirsiniz.

Arşiv konumunu değiştirme

Arşiv konumunu değiştirdiğinizde, farklı bir konumda daha önceden arşivlenen dosyalar *Hiç Arşivlenmemiş* olarak listelenir.

1 Yerel Arşiv Ayarları iletişim kutusunu açın.

Nasıl?

1. **Yerel Arşiv** sekmesini tıklatın.
2. Soldaki bölmede **Ayarlar**'ı tıklatın.

2 **Arşiv Konumunu Değiştir**'i tıklatın.

3 Arşiv Konumu iletişim kutusunda, aşağıdakilerden birini gerçekleştirin:

- **CD/DVD Yazıcı Seç**'i tıklatın, **Yazıcı** listesinde bilgisayarınızın CD veya DVD sürücüsünü tıklatın ve ardından **Tamam**'ı tıklatın.
- **Sürücü Konumunu Seç**'i tıklatın; bir USB sürücüye, yerel sürücüye veya harici sabit diske gidip seçin ve ardından **Tamam**'ı tıklatın.
- **Ağ Konumunu Seç**'i tıklatın, ağ klasörüne gidip seçin ve ardından **Tamam**'ı tıklatın.

4 **Seçili Arşiv Konumu** bölümünde yeni arşiv konumunu doğrulayın ve ardından **Tamam**'ı tıklatın.

5 Onay iletişim kutusunda **Tamam**'ı tıklatın.

6 **Tamam**'ı tıklatın.

Not: Arşiv konumunu değiştirdiğinizde, daha önceden arşivlenen dosyalar **Durum** sütununda **Arşivlenmeyen** olarak listelenir.

Arşiv şifreleme ve sıkıştırma devre dışı bırakma

Arşivlenen dosyaları şifrelemek, dosyaların içeriklerinin okunmasını engelleyerek verilerinizin gizliliğini korur. Arşivlenen dosyaları sıkıştırmak, dosya boyutlarının en az indirilmesine yardımcı olur. Varsayılan olarak, şifreleme ve sıkıştırma etkindir; ancak bu seçenekleri istediğiniz zaman devre dışı bırakabilirsiniz.

1 Yerel Arşiv Ayarları iletişim kutusunu açın.

Nasıl?

1. **Yerel Arşiv** sekmesini tıklatın.
2. Soldaki bölmede **Ayarlar**'ı tıklatın.

- 2 **Gelişmiş Ayarlar**'ı tıklatın.
- 3 **Güvenliği artırmak için şifrelemeyi etkinleştir** onay kutusunu temizleyin.
- 4 **Depolama yerini azaltmak için sıkıştırmayı etkinleştir** onay kutusunu temizleyin.
- 5 **Tamam**'ı tıklatın.

Not: McAfee, dosyalarınızı arşivlerken şifreleme ve sıkıştırmayı devre dışı bırakmamanızı önerir.

Tam ve hızlı arşivlemeleri çalıştırma

İki tür arşivleme çalıştırabilirsiniz: tam veya hızlı. Tam arşivlemeyi çalıştırdığınızda, ayarladığımız izlenen dosya türleri ve konumlarını temel alan tam bir veri setini arşivlersiniz. Hızlı arşivlemeyi çalıştırdığınızda, yalnızca en son tam veya hızlı arşivleme işleminden sonra değiştirilmiş olan izlenen dosyaları arşivlersiniz.

Varsayılan olarak, Backup and Restore izleme konumlarınızda izlenen dosya türleri için her Pazartesi günü saat 09:00'da tam arşivlemeyi ve en son tam veya hızlı arşivlemeden sonra her 48 saatte bir hızlı arşivlemeyi çalıştırmaya zamanlanmıştır. Bu zamanlama, dosyalarınızın varolan arşivinin her zaman sürdürülmesini sağlar. Ancak 48 saatte bir arşivlemek istemiyorsanız, zamanlamayı gereksinimlerinize uygun şekilde ayarlayabilirsiniz.

İzleme konumlarınızın içeriklerini istek üzerine arşivlemek istiyorsanız, bunu istediğiniz zaman yapabilirsiniz. Örneğin, bir dosyada değişiklik yaptıysanız ve onu arşivlemek istiyorsanız ancak Backup and Restore tam veya hızlı arşivlemeyi birkaç saat sonra çalıştıracak şekilde zamanlanmışsa, dosyaları el ile arşivleyebilirsiniz. Dosyaları el ile arşivlediğinizde, otomatik arşivlemeler için ayarladığınız aralık sıfırlanır.

Ayrıca, uygun olmayan bir zamanda gerçekleşen otomatik veya el ile arşivlemeyi de kesebilirsiniz. Örneğin, kaynak ağırlıklı bir görev gerçekleştirdiğiniz sırada otomatik arşivleme başlarsa, onu durdurabilirsiniz. Otomatik arşivlemeyi durdurduğunuzda, otomatik arşivlemeler için ayarladığınız aralık sıfırlanır.

Otomatik arşivlemeleri zamanlama

Verilerinizin her zaman korunmasını sağlamak için, tam ve hızlı arşivlemelerin sıklığını ayarlayabilirsiniz.

- 1 Yerel Arşiv Ayarları iletişim kutusunu açın.
Nasıl?
 1. **Yerel Arşiv** sekmesini tıklatın.
 2. Soldaki bölmede **Ayarlar**'ı tıklatın.

- 2 Genel'i tıktatın.
- 3 Tam arşivlemeyi her gün, her hafta veya her ay çalıştırmak için **Tam Arşivleme Sıklığı** bölümünde şu seçeneklerden birini tıktatın:
 - **Gün**
 - **Hafta**
 - **Ay**
- 4 Tam arşivlemeyi çalıştırmak istediğiniz günün yanındaki onay kutusunu seçin.
- 5 Tam arşivlemeyi çalıştırmak istediğiniz zamanı belirtmek için **Saat** listesinde bir değeri tıktatın.
- 6 Günlük veya saatlik olarak hızlı arşivlemeyi çalıştırmak için, **Hızlı Arşiv** bölümünde şu seçeneklerden birini tıktatın:
 - **Saat**
 - **Gün**
- 7 **Hızlı Arşivleme Sıklığı** kutusuna sıklığı temsil eden bir sayı yazın.
- 8 **Tamam**'ı tıktatın.

Not: **Tam Arşivleme Sıklığı** altında **El İle**'yi seçerek zamanlanan arşivi devre dışı bırakabilirsiniz.

Otomatik arşivlemeyi kesme

Backup and Restore, izleme konumlarındaki dosyaları ve klasörleri, tanımladığımız zamanlamaya göre otomatik olarak arşivler. Ancak otomatik arşivlemeyi çalışırken kesmek isterseniz, bunu istediğiniz zaman yapabilirsiniz.

- 1 Soldaki bölmede **Arşivlemeyi Durdur**'u tıktatın.
- 2 Onay iletişim kutusunda **Evet**'i tıktatın.

Not: **Arşivlemeyi Durdur** bağlantısı, yalnızca arşivleme çalışırken görüntülenir.

Arşivlemeleri el ile çalıştırma

Otomatik arşivlemelerin önceden tanımlı zamanlamaya göre çalışmasına karşın, istediğiniz zaman el ile hızlı veya tam arşivlemeyi de çalıştırabilirsiniz. Hızlı arşivleme, yalnızca en son tam veya hızlı arşivlemeden sonra değiştirilen dosyaları arşivler. Tam arşivleme, tüm izleme konumlarındaki izlenen dosya türlerini arşivler.

- 1 Yerel Arşiv** sekmesini tıklatın.
- 2** Aşağıdakilerden birini gerçekleştirin:
 - Hızlı arşivlemeyi çalıştırmak için, sol bölmede **Hızlı Arşiv'i** tıklatın.
 - Tam arşivlemeyi çalıştırmak için, sol bölmede **Tam Arşiv'i** tıklatın.
- 3** Arşivlemeyi Başlat iletişim kutusunda, depolama alanınızı ve ayarlarınızı doğrulayın ve ardından **Devam Et'i** tıklatın.

B Ö L Ü M 3 7

Arşivlenen dosyalarla çalışma

Bazı dosyaları arşivledikten sonra, bunlarla çalışmak için Backup and Restore'u kullanabilirsiniz. Arşivlenen dosyalarınız, onları kolayca bulmanıza olanak veren geleneksel gezgin görünümünde sunulur. Arşiviniz genişledikçe, dosyaları sıralamak veya aramak isteyebilirsiniz. Ayrıca, dosyaları almaya gerek kalmadan incelemek için, onları doğrudan gezgin görünümünde açabilirsiniz.

Dosyanızın yerel kopyası eskirse, eksikse veya bozulmuşsa, dosyaları arşivden alırsınız. Backup and Restore, çevrimiçi arşivlerinizi ve depolama ortamınızı yönetmek için gerek duyduğunuz bilgileri de sağlar.

Bu bölümde

Yerel arşivleme gezginini kullanma.....	172
Arşivlenen dosyaları geri yükleme.....	173
Arşivleri yönetme.....	175

Yerel arşivleme gezginini kullanma

Yerel arşivleme gezgini, yerel olarak arşivlediğiniz dosyaları görüntülemenize ve yönetmenize olanak verir. Her dosyanın adını, konumunu, boyutunu, durumunu (arşivlenmiş, arşivlenmemiş veya arşivleniyor) ve her dosyanın en son arşivlendiği tarihi görüntüleyebilirsiniz. Ayrıca dosyaları bu ölçütlerden birine göre sıralayabilirsiniz.

Geniş bir arşiviniz varsa, arama yaparak bir dosyayı hızla bulabilirsiniz. Dosya adının veya yolunun tamamı veya bir kısmı ile arama yapılabilir ve daha sonra yaklaşık dosya boyutunu ve en son arşivleme tarihini belirterek aramanızın kapsamını daraltabilirsiniz.

Dosyayı bulduktan sonra, onu doğrudan yerel arşivleme gezgininden açabilirsiniz. Backup and Restore, dosyayı kendi programında açarak, yerel arşivleme gezgininden çıkmadan değişiklikler yapmanıza olanak verir. Dosya, bilgisayarınızda özgün izleme konumuna kaydedilir ve tanımladığınız arşivleme zamanlamasına göre otomatik olarak arşivlenir.

Arşivlenen dosyaları sıralama

Arşivlenen dosyalarınızla klasörlerinizi şu ölçütlere göre sıralayabilirsiniz: ad, dosya türü, boyut, durum (arşivlenmiş, arşivlenmemiş veya arşivleniyor), dosyaların en son arşivlendiği tarih veya dosyaların bilgisayarınızdaki konumu (yolu).

Arşivlenen dosyaları sıralamak için:

- 1 Yerel Arşiv sekmesini tıklatın.
- 2 Sağ bölmede bir sütun adını tıklatın.

Arşivlenen bir dosyayı arama

Geniş bir arşivlenmiş dosya havuzunuz varsa, arama yaparak bir dosyayı hızla bulabilirsiniz. Dosya adının veya yolunun tamamı veya bir kısmı ile arama yapılabilir ve daha sonra yaklaşık dosya boyutunu ve en son arşivleme tarihini belirterek aramanızın kapsamını daraltabilirsiniz.

- 1 Dosya adının tamamını veya bir kısmını ekranın üst bölümündeki **Ara** kutusuna yazın ve ardından ENTER tuşuna basın.
- 2 **Yolun tamamı veya bir kısmı** kutusuna yolun tamamını veya bir kısmını yazın.
- 3 Aşağıdakilerden birini yaparak, aradığınız dosyanın yaklaşık boyutunu belirtin:
 - **100 KB'den küçük, 1 MB'den küçük veya 1 MB'den büyük** seçeneğini tıklatın.
 - **Boyut (KB)'u** tıklatın ve ardından kutularda uygun boyut değerlerini belirtin.

- 4 Aşağıdakilerden birini gerçekleştirerek, dosyanın en son yaklaşık arşivleme tarihini belirtin:
 - **Bu Hafta, Bu Ay veya Bu Yıl'**ı tıklattın.
 - **Tarihleri Belirt'**i tıklattın, listede **Arşivlendi'**yi tıklattın ve ardından tarih listelerinde uygun tarih değerlerini tıklattın.
- 5 **Ara'yı** tıklattın.

Not: En son arşivlemenin yaklaşık boyutunu veya tarihini bilmiyorsanız, **Bilinmiyor'**u tıklattın.

Arşivlenen bir dosyayı açma

Arşivlenen bir dosyayı doğrudan yerel arşivleme gezgininde açarak içeriğini inceleyebilirsiniz.

Arşivlenen dosyaları açmak için:

- 1 **Yerel Arşiv** sekmesini tıklattın.
- 2 Sağ bölmede, bir dosya adını tıklattın ve ardından **Aç'**ı tıklattın.

İpucu: Ayrıca, dosya adını çift tıklatarak da arşivlenen bir dosyayı açabilirsiniz.

Arşivlenen dosyaları geri yükleme

İzlenen bir dosya bozulur, kaybolur veya yanlışlıkla silinirse, dosyanın kopyasını yerel arşivden geri yükleyebilirsiniz. Bu nedenle, dosyalarınızı düzenli olarak arşivlemeniz önemlidir. Ayrıca, yerel arşivden dosyaların eski sürümlerini de geri yükleyebilirsiniz. Örneğin, bir dosyayı düzenli olarak arşivlemenize karşın dosyanın daha önceki bir sürümüne dönmek isterseniz, dosyayı arşiv konumunda bularak bunu gerçekleştirebilirsiniz. Arşiv konumu bir yerel sürücü veya ağ sürücüsü ise, dosyaya göz atabilirsiniz. Arşiv konumu bir harici sabit disk veya USB sürücü ise, dosyaya göz atmak için sürücüyü bilgisayara bağlamanız gerekir. Arşiv konumu CD veya DVD ise, dosyaya göz atmak için CD veya DVD'yi bilgisayara takmanız gerekir.

Ayrıca, bir bilgisayardan başka bir bilgisayara arşivlediğiniz dosyaları da geri yükleyebilirsiniz. Örneğin, bir dosya grubunu A bilgisayarındaki bir harici sabit diske arşivlediyseniz, bu dosyaları B bilgisayarına geri yükleyebilirsiniz. Bunun için, B bilgisayarına Backup and Restore yüklemeniz ve harici sabit diski bağlamanız gerekir. Daha sonra, Backup and Restore'da dosyalara göz attığınızda, dosyalar geri yükleme için **Eksik Dosyalar** listesine eklenir.

Dosyaları arşivleme hakkında ayrıntılı bilgi için bkz. Dosyaları arşivleme. İzlenen bir dosyayı bilerek arşivinizden silerseniz, **Eksik Dosyalar** listesinden girişi de silebilirsiniz.

Eksik dosyaları yerel arşivden geri yükleme

Backup and Restore'un yerel arşivi, yerel bilgisayarınızda izlenen bir klasördeki eksik verileri kurtarmanıza olanak verir. Örneğin, bir dosya izlenen klasörden taşınmış veya silinmişse ve önceden arşivlenmişse, onu yerel arşivden geri yükleyebilirsiniz.

- 1 **Yerel Arşiv** sekmesini tıklatın.
- 2 Ekranın altında bulunan **Eksik Dosyalar** sekmesinde, geri yüklemek istediğiniz dosya adının yanındaki onay kutusunu seçin.
- 3 **Geri Yükle**'yi tıklatın.

İpucu: **Tümünü Geri Yükle**'yi tıklatarak, **Eksik Dosyalar** listesindeki tüm dosyaları geri yükleyebilirsiniz.

Yerel arşivden bir dosyanın eski sürümünü geri yükleme

Arşivlenen bir dosyanın eski sürümünü geri yüklemek isterseniz, onu bulup **Eksik Dosyalar** listesine ekleyebilirsiniz. Daha sonra, bu dosyayı **Eksik Dosyalar** listesindeki herhangi bir dosya için yapacağımız gibi geri yükleyebilirsiniz.

- 1 **Yerel Arşiv** sekmesini tıklatın.
- 2 Ekranın altında bulunan **Eksik Dosyalar** sekmesinde, **Gözet**'i tıklatın ve ardından arşivin depolandığı konuma gidin.

Arşivlenen dosya adları şu biçimde olur: `cre ggaayy_ss-dd-ss_***`; burada `ggaayy` dosyaların arşivlendiği tarihtir, `ss-dd-ss` dosyaların arşivlendiği saattir ve `***` gerçekleştirilen arşivlemenin tam veya hızlı arşivleme olmasına göre **Tam** veya **Kapsam**'dir.

- 3 Konumu seçin ve ardından **Tamam**'i tıklatın.

Seçili konumda bulunan dosyalar **Eksik Dosyalar** listesinde görüntülenir ve geri yüklenmeye hazırdır. Ayrıntılı bilgi için, bkz. Eksik dosyaları yerel arşivden geri yükleme (sayfa 174).

Dosyaları eksik dosyalar listesinden kaldırma

Arşivlenen bir dosya izlenen klasörden taşındığında veya silindiğinde, otomatik olarak **Eksik Dosyalar** listesinde görüntülenir. Bu, arşivlenen dosyalarla izlenen klasörlerde bulunan dosyalar arasında tutarsızlık olduğunu size bildirir. Dosya bilerek izlenen klasörden kaldırılmışsa veya silinmişse, dosyayı **Eksik Dosyalar** listesinden silebilirsiniz.

Eksik Dosyalar listesinden dosya kaldırmak için:

- 1 **Yerel Arşiv** sekmesini tıklatın.
- 2 Ekranın altında bulunan **Eksik Dosyalar** sekmesinde, kaldırmak istediğiniz dosya adının yanındaki onay kutusunu seçin.
- 3 **Sil**'i tıklatın.

İpucu: **Tümünü Sil**'i tıklatarak, **Eksik Dosyalar** listesindeki tüm dosyaları kaldırabilirsiniz.

Arşivleri yönetme

Tam ve hızlı arşivlemelerinizle ilgili bilgilerin özetini istediğiniz zaman görüntüleyebilirsiniz. Örneğin izlenen verilerin miktarı, arşivlenmiş verilerin miktarı ve izlenen ancak henüz arşivlenmemiş verilerin miktarı hakkında bilgiler görüntüleyebilirsiniz. Ayrıca, en son ve bir sonraki arşivlemelerin gerçekleşme tarihi gibi arşivleme zamanlamanızla ilgili bilgileri de görüntüleyebilirsiniz.

Arşivleme etkinliğinizin özetini görüntüleme

İstediğiniz zaman arşivleme etkinliğinizle ilgili bilgiler görüntüleyebilirsiniz. Örneğin, arşivlenmiş dosyaların yüzdesini, izlenen verilerin boyutunu, arşivlenmiş verilerin boyutunu ve izlenen ancak henüz arşivlenmemiş verilerin boyutunu görüntüleyebilirsiniz. Ayrıca, en son ve bir sonraki arşivlemelerin gerçekleşme tarihlerini de görüntüleyebilirsiniz.

- 1 Yerel Arşiv** sekmesini tıklatın.
- Ekranın üst bölümündeki **Hesap Özeti**'ni tıklatın.

B Ö L Ü M 3 8

McAfee QuickClean

QuickClean, bilgisayarınızda dağınıklığa neden olabilecek dosyaları silerek bilgisayarınızın performansını geliştirir. Geri Dönüşüm Kutusu'nu boşaltır ve geçici dosyaları, kısayolları, kayıp dosya parçalarını, kayıt defteri dosyalarını, önbellek dosyalarını, tanımlama bilgilerini, tarayıcı geçmiş dosyalarını, gönderilen ve silinen e-postaları, en son kullanılan dosyaları, Active-X dosyalarını ve sistem geri yükleme noktası dosyalarını siler. QuickClean, adınız ve adresiniz gibi hassas ve kişisel bilgiler içerebilen öğeleri güvenli ve kalıcı şekilde silmek için McAfee Shredder bileşenini kullanarak gizliliğinizi de korur. Dosyaları parçalama hakkında bilgi için bkz. McAfee Shredder.

Disk Birleştirici, bilgisayarınızdaki dosya ve klasörleri düzenleyerek, bilgisayarınızın sabit diskine kaydedildiklerinde bunların dağılmamalarını (parçalanmamalarını) sağlar. Sabit diskinizi düzenli olarak birleştirdiğinizde, bu parçalanmış dosya ve klasörleri daha sonra hızla çağrılacak şekilde bir araya getirirsiniz.

Bilgisayarınıza el ile bakım yapmak istemiyorsanız, hem QuickClean hem de Disk Birleştirici uygulamalarını, istediğiniz sıklıkta bağımsız görevler halinde otomatik olarak çalışacak şekilde zamanlayabilirsiniz.

Not: SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde

QuickClean özellikleri	178
Bilgisayarınızı temizleme.....	179
Bilgisayarınızı birleştirme	183
Görev zamanlama.....	185

QuickClean özellikleri

Dosya Temizleyici

Çeşitli temizleyiciler kullanarak gereksiz dosyaları güvenli ve etkili bir biçimde silin. Bu dosyaları sildiğinizde, bilgisayarınızın sabit diskinde alan kazanır ve performansını geliştirirsiniz.

B Ö L Ü M 3 9

Bilgisayarınızı temizleme

QuickClean, bilgisayarınızda dağınıklığa neden olabilecek dosyaları siler. Geri Dönüşüm Kutusu'nu boşaltır ve geçici dosyaları, kısayolları, kayıp dosya parçalarını, kayıt defteri dosyalarını, önbellek dosyalarını, tanımlama bilgilerini, tarayıcı geçmişi dosyalarını, gönderilen ve silinen e-postaları, en son kullanılan dosyaları, Active-X dosyalarını ve sistem geri yükleme noktası dosyalarını siler. QuickClean, bu öğeleri diğer gerekli bilgileri etkilemeden siler.

Bilgisayarınızdan gereksiz dosyaları silmek için QuickClean'in temizleyicilerinden herhangi birini kullanabilirsiniz. Aşağıdaki tabloda QuickClean temizleyicileri açıklanmaktadır:

Ad	İşlev
Geri Dönüşüm Kutusu Temizleyicisi	Geri Dönüşüm Kutusu'ndaki dosyaları siler.
Geçici Dosya Temizleyicisi	Geçici klasörlerinizde saklanan dosyaları siler.
Kısayol Temizleyicisi	Bozuk kısayolları ve herhangi bir programla ilişkili olmayan kısayolları siler.
Kayıp Dosya Parçası Temizleyicisi	Bilgisayarınızda kaybolan dosya parçalarını siler.
Kayıt Defteri Temizleyicisi	Bilgisayarınızda artık bulunmayan programların Windows® kayıt defteri bilgilerini siler. Kayıt defteri, Windows'un yapılandırma bilgilerini depoladığı bir veritabanıdır. Kayıt defteri, tüm bilgisayar kullanıcılarının profillerini ve sistem donanımı, yüklenen programlar ve özellik ayarları hakkındaki bilgileri içerir. Windows çalışırken sürekli bu bilgilere başvurur.
Önbellek Temizleyicisi	Siz web sayfalarında gezinirken biriken önbellek dosyalarını siler. Bu dosyalar, genellikle önbellek klasöründe geçici dosyalar halinde depolanır. Önbellek klasörü, bilgisayarınızda geçici bir depolama alanıdır. Web'de gezinme hızını ve etkinliğini artırmak için tarayıcınız, daha önce görüntülediğiniz bir web sayfasını önbellekten (uzak sunucu yerine) çağırabilir.

Ad	İşlev
Tanımlama Bilgisi Temizleyicisi	<p>Tanımlama bilgilerini siler. Bu dosyalar, genellikle geçici dosyalar halinde depolanır.</p> <p>Tanımlama bilgisi, genellikle web'de gezinen kişinin bilgisayarında depolanan ve kullanıcı adı ve geçerli tarih ve saat gibi bilgiler içeren küçük bir dosyadır. Tanımlama bilgileri, web siteleri tarafından genellikle siteye önceden kaydolun veya siteyi ziyaret eden kullanıcıları tanımlamak için kullanılır; ancak bunlar, korsanlar için bilgi kaynağı da olabilir.</p>
Tarayıcı Geçmişini Temizleyicisi	Web tarayıcısı geçmişinizi siler.
Outlook Express ve Outlook E-posta Temizleyicisi (gönderilmiş ve silinmiş öğeler)	Outlook® ve Outlook Express'ten gönderilmiş ve silinmiş e-postaları siler.
Son Kullanılanlar Temizleyicisi	<p>Şu programlardan herhangi birinde oluşturulan son kullanılan dosyaları siler:</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 Temizleyicisi	<p>ActiveX denetimlerini siler.</p> <p>ActiveX, programla veya web sayfasıyla bütünleşip onun doğal bir parçası gibi görünen, programlar veya web sayfaları tarafından işlevsellik eklemek üzere kullanılan bir yazılım bileşenidir. Çoğu ActiveX denetimi zararsızdır; ancak bazıları bilgisayarınızdan bilgiler yakalayabilir.</p>
Sistem Geri Yükleme Noktası Temizleyicisi	<p>Eski sistem geri yükleme noktalarını (en sonuncusu dışında) bilgisayarınızdan siler.</p> <p>Sistem geri yükleme noktaları, herhangi bir sorun ortaya çıkarsa önceki duruma geri dönebilmeniz için bilgisayarınızda yapılan değişiklikleri işaretlemek üzere Windows tarafından oluşturulur.</p>

Bu bölümde

Bilgisayarınızı temizleme..... 181

Bilgisayarınızı temizleme

Bilgisayarınızdan gereksiz dosyaları silmek için QuickClean'in temizleyicilerinden herhangi birini kullanabilirsiniz. İşlemi tamamladığınızda, **QuickClean Özeti** altında, temizlik işleminden sonra kazanılan disk alanı miktarını, silinen dosyaların sayısını, bilgisayarınızda en son çalıştırılan QuickClean işleminin tarih ve saatini görüntüleyebilirsiniz.

- 1 McAfee SecurityCenter bölümünde, **Ortak Görevler** altında, **Bilgisayar Bakımı**'ni tıklatın.
- 2 **McAfee QuickClean** altında **Başlat**'ı tıklatın.
- 3 Aşağıdakilerden birini gerçekleştirin:
 - Listedeki varsayılan temizleyicileri kabul etmek için **İleri**'yi tıklatın.
 - Uygun temizleyicileri seçin veya işaretini kaldırın ve ardından **İleri**'yi tıklatın. Son Kullanılanlar Temizleyicisi'ni seçerseniz, listedeki programlarla en son oluşturulan dosyaları seçmek veya işaretini kaldırmak için **Özellikler** seçeneğini belirleyin ve sonra **Tamam**'ı tıklatın.
 - Varsayılan temizleyicileri geri yüklemek için **Varsayılanları Geri Yükle**'yi ve ardından **İleri**'yi tıklatın.
- 4 Analizi gerçekleştirdikten sonra **İleri**'yi tıklatın.
- 5 Dosya silme işlemi onaylamak için **İleri**'yi tıklatın.
- 6 Aşağıdakilerden birini gerçekleştirin:
 - Varsayılan **Hayır, dosyalarımı standart Windows silme işlemi kullanarak silmek istiyorum**'u kabul etmek için **İleri**'yi tıklatın.
 - **Evet, Shredder kullanarak dosyalarımı güvenli bir şekilde silmek istiyorum**'u tıklatın, geçiş sayısını (en çok 10) belirtin ve sonra **İleri**'yi tıklatın. Büyük miktarda silinecek bilgi varsa, dosya parçalama işlemi uzun sürebilir.

7 Temizleme işlemi sırasında herhangi bir dosya veya öge kilitlenirse, bilgisayarınızı yeniden başlatmanız istenebilir. Pencereyi kapatmak için **Tamam**'ı tıkladın.

8 **Son**'u tıkladın.

Not: Shredder ile silinen dosyalar kurtarılamaz. Dosyaları parçalama hakkında bilgi için bkz. McAfee Shredder.

B Ö L Ü M 4 0

Bilgisayarınızı birleştirme

Disk Birleştirici, bilgisayarınızdaki dosya ve klasörleri düzenleyerek, bilgisayarınızın sabit diskine kaydedildiklerinde bunların dağılmalarını (parçalanmalarını) sağlar. Sabit diskinizi düzenli olarak birleştirdiğinizde, bu parçalanmış dosya ve klasörleri daha sonra hızla çağrılacak şekilde bir araya getirirsiniz.

Bilgisayarınızı birleştirme

Dosya ve klasörlere daha kolay erişmek ve bunları çağırmak için bilgisayarınızı birleştirebilirsiniz.

- 1 McAfee SecurityCenter bölmesinde, **Ortak Görevler** altında, **Bilgisayar Bakımı**'ni tıklatın.
- 2 **Disk Birleştirici** altında **Analiz**'i tıklatın.
- 3 Ekran yönergelerini izleyin.

Not: Disk Birleştirici hakkında ayrıntılı bilgi için Windows Yardımı'na bakın.

B Ö L Ü M 4 1

Görev zamanlama

Görev Zamanlayıcı, QuickClean veya Disk Birleştirici uygulamasının bilgisayarınızdaki çalışma sıklığını otomatikleştirir. Örneğin, QuickClean'i her Pazar günü saat 21:00 'de Geri Dönüşüm Kutusu'nu boşaltması veya Disk Birleştirici'yi her ayın son gününde bilgisayarınızın sabit diskini birleştirmesi için zamanlayabilirsiniz. İstedığınız zaman bir görev oluşturabilir, bunu değiştirebilir veya silebilirsiniz. Zamanlanan görevin çalışabilmesi için bilgisayarınızda oturum açmış olmanız gerekir. Görev herhangi bir nedenle çalışmazsa, bir sonraki oturum açışınızdan beş dakika sonrası için yeniden zamanlanır.

QuickClean görevi zamanlama

Bir veya birkaç temizleyici kullanarak bilgisayarınızı otomatik olarak temizlemek için QuickClean görevi zamanlayabilirsiniz. İşlem tamamlandığında, **QuickClean Özeti** altında, görevin bir daha çalışmak üzere zamanlandığı tarih ve saati görüntüleyebilirsiniz.

1 Görev Zamanlayıcı bölmesini açın.

Nasıl?

1. McAfee SecurityCenter'da, **Ortak Görevler** altında, **Bilgisayar Bakımı**'ni tıklatın.
2. **Görev Zamanlayıcı** altında **Başlat**'ı tıklatın.

2 Zamanlanacak işlemi seçin listesinde, McAfee QuickClean'i tıklatın.

3 Görev adını Görev adı kutusuna yazın ve sonra **Oluştur**'u tıklatın.

4 Aşağıdakilerden birini gerçekleştirin:

- Listedeki temizleyicileri kabul etmek için **İleri**'yi tıklatın.
- Uygun temizleyicileri seçin veya işaretini kaldırın ve sonra **İleri**'yi tıklatın. Son Kullanılanlar Temizleyicisi'ni seçerseniz, listedeki programlarla en son oluşturulan dosyaları seçmek veya işaretini kaldırmak için **Özellikler** seçeneğini belirleyin ve sonra **Tamam**'ı tıklatın.
- Varsayılan temizleyicileri geri yüklemek için **Varsayılanları Geri Yükle**'yi ve sonra **İleri**'yi tıklatın.

5 Aşağıdakilerden birini gerçekleştirin:

- Varsayılan **Hayır, dosyalarımı standart Windows silme işlemi kullanarak silmek istiyorum**'u kabul etmek için **Zamanlama**'yı tıklatın.
- **Evet, Shredder kullanarak dosyalarımı güvenli bir şekilde silmek istiyorum**'u tıklatın, geçiş sayısını (en çok 10) belirtin ve sonra **Zamanlama**'yı tıklatın.

- 6 **Zamanlama** iletişim kutusunda, görevin çalışmasını istediğiniz sıklığı seçin ve sonra **Tamam**'ı tıklatın.
- 7 Son Kullanılanlar Temizleyicisi özelliklerinde değişiklik yaptıysanız, bilgisayarınızı yeniden başlatmanız istenebilir. Pencereyi kapatmak için **Tamam**'ı tıklatın.
- 8 **Son**'u tıklatın.

Not: Shredder ile silinen dosyalar kurtarılamaz. Dosyaları parçalama hakkında bilgi için bkz. McAfee Shredder.

QuickClean görevini değiştirme

Programın kullandığı temizleyicileri veya bilgisayarınızda otomatik olarak çalışma sıklığını değiştirmek için zamanlanan bir QuickClean görevinde değişiklik yapabilirsiniz. İşlem tamamlandığında, **QuickClean Özeti** altında, görevin bir daha çalışmak üzere zamanlandığı tarih ve saati görüntüleyebilirsiniz.

- 1 Görev Zamanlayıcı bölmesini açın.
Nasıl?
 1. McAfee SecurityCenter'da, **Ortak Görevler** altında, **Bilgisayar Bakımı**'ni tıklatın.
 2. **Görev Zamanlayıcı** altında **Başlat**'i tıklatın.
- 2 **Zamanlanacak işlemi seçin** listesinde, **McAfee QuickClean**'i tıklatın.
- 3 **Varolan bir görev seçin** listesinden görevi seçin ve sonra **Değiştir**'i tıklatın.
- 4 Aşağıdakilerden birini gerçekleştirin:
 - Görevle ilgili seçilen temizleyicileri kabul etmek için **İleri**'yi tıklatın.
 - Uygun temizleyicileri seçin veya işaretini kaldırın ve sonra **İleri**'yi tıklatın. Son Kullanılanlar Temizleyicisi'ni seçerseniz, listedeki programlarla en son oluşturulan dosyaları seçmek veya işaretini kaldırmak için **Özellikler** seçeneğini belirleyin ve sonra **Tamam**'ı tıklatın.
 - Varsayılan temizleyicileri geri yüklemek için **Varsayılanları Geri Yükle**'yi ve ardından **İleri**'yi tıklatın.
- 5 Aşağıdakilerden birini gerçekleştirin:
 - Varsayılan **Hayır, dosyalarımı standart Windows silme işlemi kullanarak silmek istiyorum**'u kabul etmek için **Zamanlama**'yı tıklatın.
 - **Evet, Shredder kullanarak dosyalarımı güvenli bir şekilde silmek istiyorum**'u tıklatın, geçiş sayısını (en çok 10) belirtin ve sonra **Zamanlama**'yı tıklatın.

- 6 **Zamanlama** iletişim kutusunda, görevin çalışmasını istediğiniz sıklığı seçin ve sonra **Tamam**'ı tıklatın.
- 7 Son Kullanılanlar Temizleyicisi özelliklerinde değişiklik yaptıysanız, bilgisayarınızı yeniden başlatmanız istenebilir. Pencereyi kapatmak için **Tamam**'ı tıklatın.
- 8 **Son**'u tıklatın.

Not: Shredder ile silinen dosyalar kurtarılamaz. Dosyaları parçalama hakkında bilgi için bkz. McAfee Shredder.

QuickClean görevini silme

Otomatik olarak çalışmasını istemediğiniz zamanlanan bir QuickClean görevini silebilirsiniz.

- 1 Görev Zamanlayıcı bölmesini açın.
Nasıl?
 1. McAfee SecurityCenter'da, **Ortak Görevler** altında, **Bilgisayar Bakımı**'ni tıklatın.
 2. **Görev Zamanlayıcı** altında **Başlat**'ı tıklatın.
- 2 **Zamanlanacak işlemi seçin** listesinde, **McAfee QuickClean**'i tıklatın.
- 3 **Varolan bir görev seçin** listesinden görevi seçin.
- 4 **Sil**'i ve sonra silme işlemi onaylamak için **Evet**'i tıklatın.
- 5 **Son**'u tıklatın.

Disk Birleştirici görevi zamanlama

Bilgisayarınızın sabit diskinin otomatik olarak birleştirilme sıklığını zamanlamak için bir Disk Birleştirici görevi zamanlayabilirsiniz. İşlem tamamlandığında, **Disk Birleştirici** altında, görevin bir daha çalışmak üzere zamanlandığı tarih ve saati görüntüleyebilirsiniz.

- 1 Görev Zamanlayıcı bölmesini açın.
Nasıl?
 1. McAfee SecurityCenter'da, **Ortak Görevler** altında, **Bilgisayar Bakımı**'ni tıklatın.
 2. **Görev Zamanlayıcı** altında **Başlat**'ı tıklatın.
- 2 **Zamanlanacak işlemi seçin** listesinde, **Disk Birleştirici**'yi tıklatın.
- 3 Görev adını **Görev adı** kutusuna yazın ve sonra **Oluştur**'u tıklatın.

- 4 Aşağıdakilerden birini gerçekleştirin:
 - Varsayılan **Boş alan az olsa da birleştirmeyi gerçekleştir** seçeneğini kabul etmek için **Zamanlama**'yı tıklatın.
 - **Boş alan az olsa da birleştirmeyi gerçekleştir** seçeneğinin işaretini kaldırın ve sonra **Zamanlama**'yı tıklatın.
- 5 **Zamanlama** iletişim kutusunda, görevin çalışmasını istediğiniz sıklığı seçin ve sonra **Tamam**'ı tıklatın.
- 6 **Son**'u tıklatın.

Disk Birleştirici görevini değiştirme

Programın bilgisayarınızda otomatik olarak çalışma sıklığını değiştirmek için zamanlanan bir Disk Birleştirici görevinde değişiklik yapabilirsiniz. İşlem tamamlandığında, **Disk Birleştirici** altında, görevin bir daha çalışmak üzere zamanlandığı tarih ve saati görüntüleyebilirsiniz.

- 1 Görev Zamanlayıcı bölmesini açın.

Nasıl?

 1. McAfee SecurityCenter'da, **Ortak Görevler** altında, **Bilgisayar Bakımı**'nı tıklatın.
 2. **Görev Zamanlayıcı** altında **Başlat**'ı tıklatın.
- 2 Zamanlanacak işlemi seçin listesinde, **Disk Birleştirici**'yi tıklatın.
- 3 **Varolan bir görev seçin** listesinden görevi seçin ve sonra **Değiştir**'i tıklatın.
- 4 Aşağıdakilerden birini gerçekleştirin:
 - Varsayılan **Boş alan az olsa da birleştirmeyi gerçekleştir** seçeneğini kabul etmek için **Zamanlama**'yı tıklatın.
 - **Boş alan az olsa da birleştirmeyi gerçekleştir** seçeneğinin işaretini kaldırın ve sonra **Zamanlama**'yı tıklatın.
- 5 **Zamanlama** iletişim kutusunda, görevin çalışmasını istediğiniz sıklığı seçin ve sonra **Tamam**'ı tıklatın.
- 6 **Son**'u tıklatın.

Disk Birleřtirici görevini silme

Otomatik olarak çalışmasını istemediđiniz zamanlanan bir Disk Birleřtirici görevini silebilirsiniz.

1 Görev Zamanlayıcı bölmesini açın.

Nasıl?

1. McAfee SecurityCenter'da, **Ortak Görevler** altında, **Bilgisayar Bakımı'nı** tıkladın.
2. **Görev Zamanlayıcı** altında **Başlat'**ı tıkladın.

2 Zamanlanacak işlemi seçin listesinde, **Disk Birleřtirici'yi** tıkladın.

3 Varolan bir görev seçin listesinden görevi seçin.

4 Sil'i ve sonra silme işlemi onaylamak için **Evet'i** tıkladın.

5 Son'u tıkladın.

B Ö L Ü M 4 2

McAfee Shredder

McAfee Shredder, öğeleri bilgisayarınızın sabit diskinden kalıcı olarak siler (veya parçalar). Bu dosyaları ve klasörleri el ile sildiğinizde, Geri Dönüşüm Kutusu'nu boşalttığınızda veya Temporary Internet Files klasörünü sildiğinizde bile, bilgisayarın teknik araçlarını kullanarak bu bilgileri kurtarabilirsiniz. Bunun yanı sıra, bazı programlar dosyaların geçici, gizli kopyalarını çıkardığı için silinen bir dosya kurtarılabilir. Shredder, bu istenmeyen dosyaları güvenli ve kalıcı bir şekilde silerek gizliliğinizi korur. Parçalanmış dosyaların geri yüklenemediğini unutmayın.

Not: SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde

Shredder özellikleri	192
Dosyaları, klasörleri ve diskleri parçalama	192

Shredder özellikleri

Dosya ve klasörleri kalıcı olarak silme

Bilgisayarınızın sabit diskindeki öğeleri, ilişkili bilgilerin kurtarılamayacağı şekilde kaldırın. Bu program, dosyaları ve klasörleri, Geri Dönüşüm Kutusu ve Temporary Internet Files klasöründeki öğeleri ve yeniden yazılabilir CD'ler, harici sabit diskler ve disketler gibi bilgisayar disklerinin tüm içeriklerini güvenli ve kalıcı şekilde silerek gizliliğinizi korur.

Dosyaları, klasörleri ve diskleri parçalama

Shredder, Geri Dönüşüm Kutusu ve Temporary Internet Files klasöründeki silinen dosya ve klasörlerde bulunan bilgilerin, özel araçlarla bile kurtarılamamasını güvence altına alır. Shredder ile bir öğenin kaç kez (en çok 10) parçalanmasını istediğinizi belirtebilirsiniz. Parçalama sayısı arttıkça, güvenli dosya silme düzeyi de artar.

Dosya ve klasörleri parçalama

Geri Dönüşüm Kutusu ve Temporary Internet Files klasöründe bulunan öğeler dahil olmak üzere, bilgisayarınızın sabit diskindeki dosya ve klasörleri parçalayabilirsiniz.

1 Shredder'ı açın.

Nasıl?

1. McAfee SecurityCenter bölmesinde, **Ortak Görevler** altında, **Gelişmiş Menü**'yü tıklatın.
2. Soldaki bölmede **Araçlar**'ı tıklatın.
3. **Shredder**'ı tıklatın.

2 Dosya ve klasörleri parçala bölümünde, **Şunu yapmak istiyorum** altında, **Dosya ve klasörleri silmek** seçeneğini tıklatın.

3 **Parçalama Düzeyi** altında, aşağıdaki parçalama düzeylerinden birini tıklatın:

- **Hızlı:** Seçilen öğeleri bir kez parçalar.
- **Kapsamlı:** Seçilen öğeleri 7 kez parçalar.
- **Özel:** Seçilen öğeleri en fazla 10 kez parçalar.

4 **İleri**'yi tıklatın.

5 Aşağıdakilerden birini gerçekleştirin:

- **Parçalanacak dosyaları seçin** listesinde, **Geri Dönüşüm Kutusu içeriği** veya **Geçici Internet dosyaları** seçeneğini tıklatın.
- **Gözet**'i tıklatın, parçalamak istediğiniz dosyaya gidip seçin ve sonra **Aç**'i tıklatın.

- 6 İleri'yi tıklatın.
- 7 Başlat'ı tıklatın.
- 8 Shredder işlemi tamamlayınca Bitti'yi tıklatın.

Not: Shredder görevi tamamlayıncaya dek lütfen hiçbir dosyayla çalışmayın.

Tüm diski parçalama

Bir diskin tüm içeriğini aynı anda silebilirsiniz. Yalnızca harici sabit diskler, yazılabilir CD'ler ve disketler gibi çıkarılabilir sürücüler parçalanabilir.

- 1 Shredder'ı açın.
Nasıl?
 1. McAfee SecurityCenter bölümünde, **Ortak Görevler** altında, **Gelişmiş Menü**'yü tıklatın.
 2. Soldaki bölmede **Araçlar**'ı tıklatın.
 3. **Shredder**'ı tıklatın.
- 2 Dosya ve klasörleri parçala bölümünde, **Şunu yapmak istiyorum** altında, **Tüm diski silmek** seçeneğini tıklatın.
- 3 **Parçalama Düzeyi** altında, aşağıdaki parçalama düzeylerinden birini tıklatın:
 - **Hızlı:** Seçilen sürücüyü bir kez parçalar.
 - **Kapsamlı:** Seçilen sürücüyü 7 kez parçalar.
 - **Özel:** Seçilen sürücüyü en fazla 10 kez parçalar.
- 4 İleri'yi tıklatın.
- 5 **Diski seçin** listesinde, parçalamak istediğiniz sürücüyü tıklatın.
- 6 İleri'yi ve sonra seçiminizi onaylamak için **Evet**'i tıklatın.
- 7 **Başlat**'ı tıklatın.
- 8 Shredder işlemi tamamlayınca **Bitti**'yi tıklatın.

Not: Shredder görevi tamamlayıncaya dek lütfen hiçbir dosyayla çalışmayın.

B Ö L Ü M 4 3

McAfee Network Manager

Network Manager, ev ađınızı oluřturan bilgisayarların ve diđer aygıtların grafiksel görünümünü sunar. Network Manager'ı kullanarak, ađınızda yönetilen tüm bilgisayarların koruma durumunu uzaktan yönetebilir ve bu bilgisayarlarla ilgili raporlanan güvenlik açıklarını uzaktan düzeltebilirsiniz. McAfee Total Protection yüklediyseniz, Network Manager ađınızda bağlanmaya çalışan Saldırganları (tanımadığınız veya güvenmediğiniz bilgisayarlar veya aygıtlar) da izleyebilir.

Network Manager'ı kullanmadan önce, bu özelliklerden bazıları hakkında bilgi edinebilirsiniz. Bu özelliklerin yapılandırılması ve kullanımıyla ilgili ayrıntılar, Network Manager yardımında sunulmaktadır.

Not: SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde














Network Manager özellikleri	196
Network Manager simgeleri hakkında bilgi	197
Yönetilen bir ađ kurma	199
Ađı uzaktan yönetme	205
Ađlarınızı izleme	211

Network Manager özellikleri

- Grafiksel ağ haritası** Ev ağını oluşturulan bilgisayarların ve aygıtların koruma durumuna ilişkin grafiksel görünümü görüntüleyin. Ağınızda değişiklikler yaptığınızda (örneğin bilgisayar eklediğinizde), ağ haritası bu değişiklikleri tanır. Ağ haritasını yenileyebilir, ağın adını değiştirebilir ve görünümü özelleştirmek için ağ haritasının bileşenlerini gösterebilir veya gizleyebilirsiniz. Ayrıca, ağ haritasında gösterilen herhangi bir aygıtla ilgili ayrıntıları da görüntüleyebilirsiniz.
- Uzaktan yönetme** Ev ağını oluşturulan bilgisayarların koruma durumunu yönetin. Yönetilen ağa katılması için bir bilgisayarı davet edebilir, yönetilen bilgisayarın koruma durumunu izleyebilir ve ağdaki uzak bir bilgisayarın bilinen güvenlik açıklarını düzeltebilirsiniz.
- Ağ izleme** Kullanılıyorsa, Ağ Yöneticisi'nin ağlarınızı izlemesine ve Arkadaşlar veya Saldırganlar bağlandığında size bildirmesine izin verin. Ağ izleme, yalnızca McAfee Total Protection satın aldıysanız kullanılabilir.

Network Manager simgeleri hakkında bilgi

Aşağıdaki tabloda, Network Manager ağ haritasında yaygın olarak kullanılan simgeler açıklanmaktadır.

Simge	Açıklama
	Çevrimiçi ve yönetilen bir bilgisayarı temsil eder
	Çevrimdışı ve yönetilen bir bilgisayarı temsil eder
	SecurityCenter yüklenmiş yönetilmeyen bir bilgisayarı temsil eder
	Çevrimdışı ve yönetilmeyen bir bilgisayarı temsil eder
	SecurityCenter yüklenmemiş çevrimiçi bir bilgisayarı veya bilinmeyen bir ağ aygıtını temsil eder
	SecurityCenter yüklenmemiş çevrimdışı bir bilgisayarı veya bilinmeyen çevrimdışı bir ağ aygıtını temsil eder
	Karşılık gelen ögenin korunduğunu ve bağlı olduğunu gösterir
	Karşılık gelen öğeyle ilgilenmeniz gerekebileceğini gösterir
	Karşılık gelen öğeyle hemen ilgilenmeniz gerektiğini gösterir
	Kablosuz ev yönlendiricisini temsil eder
	Standart ev yönlendiricisini temsil eder
	İnternet'in bağlı olduğunu gösterir
	İnternet bağlantısının kesildiğini gösterir

B Ö L Ü M 4 4

Yönetilen bir ağ kurma

Yönetilen bir ağ kurmak için ağa güvenin (henüz güvenmediyseniz) ve ağa üyeler (bilgisayarlar) ekleyin. Bir bilgisayarın uzaktan yönetilebilmesi veya ağdaki diğer bilgisayarları uzaktan yönetme izni alabilmesi için ağın güvenilen bir üyesi olması gerekir. Ağ üyeliği, yeni bilgisayarlara yönetici izinlerine sahip mevcut ağ üyeleri (bilgisayarlar) tarafından sağlanır.

Ağınızda değişiklik yaparsanız (örneğin bilgisayar ekleseniz) bile, ağ haritasında gösterilen herhangi bir öğeyle ilgili ayrıntıları görüntüleyebilirsiniz.

Bu bölümde

Ağ haritasıyla çalışma	200
Yönetilen ağa katılma	201

Ağ haritasıyla çalışma

Ağa bilgisayar bağladığınızda, Network Manager yönetilen veya yönetilmeyen herhangi bir üye olup olmadığını, yönlendirici özniteliklerini ve Internet durumunu belirlemek için ağı analiz eder. Herhangi bir üye bulunamazsa, Network Manager bağlı olan bu bilgisayarın ağıdaki ilk bilgisayar olduğunu varsayar ve bu bilgisayarı yönetici izinlerine sahip yönetilen bir üye yapar. Varsayılan olarak, ağ adı SecurityCenter yüklenmiş ağa bağlanan ilk bilgisayarın adını içerir; ancak istediğiniz zaman ağın adını değiştirebilirsiniz.

Ağınızda değişiklikler yaptığınızda (örneğin bilgisayar eklediğinizde), ağ haritasını özelleştirebilirsiniz. Örneğin, ağ haritasını yenileyebilir, ağın adını değiştirebilir ve görünümü özelleştirmek için ağ haritasının öğelerini gösterebilir veya gizleyebilirsiniz. Ayrıca, ağ haritasında gösterilen herhangi bir öğeyle ilgili ayrıntıları da görüntüleyebilirsiniz.

Ağ haritasına erişme

Ağ haritası, ev ağınıza oluşturan bilgisayarları ve aygıtları grafiksel olarak gösterir.

- Temel veya Gelişmiş Menü'de **Ağı Yönet**'i tıklatın.

Not: Ağa henüz güvenmediyseniz (McAfee Personal Firewall kullanarak), ağ haritasına ilk eriştiğinizde sizden bunu yapmanız istenir.

Ağ haritasını yenileme

Ağ haritasını istediğiniz zaman, örneğin yönetilen ağa başka bir bilgisayar katıldıktan sonra yenileyebilirsiniz.

- 1 Temel veya Gelişmiş Menü'de **Ağı Yönet**'i tıklatın.
- 2 **Şunu yapmak istiyorum** altında **Ağ haritasını yenile**'yi tıklatın.

Not: **Ağ haritasını yenile** bağlantısı, yalnızca ağ haritasında hiç seçili öğe yoksa kullanılabilir. Bir öğenin seçimini kaldırmak için seçili öğeyi tıklatın veya ağ haritası üzerinde beyaz bir alanı tıklatın.

Ağın adını değiştirme

Varsayılan olarak, ağ adı SecurityCenter yüklü olan ve ağa bağlanan ilk bilgisayarın adını içerir. Farklı bir ad kullanmayı tercih ederseniz bunu değiştirebilirsiniz.

- 1 Temel veya Gelişmiş Menü'de **Ağı Yönet**'i tıklatın.
- 2 **Şunu yapmak istiyorum** altında **Ağın adını değiştir**'i tıklatın.
- 3 **Ağ Adı** kutusuna ağın adını yazın.
- 4 **Tamam**'i tıklatın.

Not: **Ağın adını değiştir** bağlantısı, yalnızca ağ haritasında hiç seçili öğe yoksa kullanılabilir. Bir öğenin seçimini kaldırmak için seçili öğeyi tıklatın veya ağ haritası üzerinde beyaz bir alanı tıklatın.

Ağ haritasında öğeyi gösterme veya gizleme

Varsayılan olarak, ev ağınızdaki tüm bilgisayarlar ve aygıtlar ağ haritasında görüntülenir. Ancak öğeleri gizlediyseniz, bunları istediğiniz zaman yeniden gösterebilirsiniz. Yalnızca yönetilmeyen öğeler gizlenebilir; yönetilen bilgisayarlar gizlenemez.

Bunu yapmak için...	Temel veya Gelişmiş Menü'de Ağ Yönet'i tıklatın ve ardından bunu yapın...
Ağ haritasında bir öğeyi gizlemek	Ağ haritasında bir öğeyi tıklatın ve ardından Şunu yapmak istiyorum bölümünde Bu öğeyi gizle 'yi tıklatın. Onay iletişim kutusunda Evet 'i tıklatın.
Ağ haritasında öğeleri göstermek	Şunu yapmak istiyorum bölümünde Gizli öğeleri göster 'i tıklatın.

Öğenin ayrıntılarını görüntüleme

Ağ haritasında seçerek, ağınızdaki herhangi bir öğeyle ilgili ayrıntılı bilgi görüntüleyebilirsiniz. Bu bilgiler öğe adını, koruma durumunu ve öğeyi yönetmek için gerekli diğer bilgileri içerir.

- 1 Ağ haritasında öğenin simgesini tıklatın.
- 2 **Ayrıntılar** bölümünde, öğe hakkındaki bilgileri görüntüleyin.

Yönetilen ağa katılma

Bir bilgisayarın uzaktan yönetilebilmesi veya ağdaki diğer bilgisayarları uzaktan yönetme izni alabilmesi için bu bilgisayar ağın güvenilen bir üyesi olmalıdır. Ağ üyeliği, yeni bilgisayarlara yönetici izinlerine sahip mevcut ağ üyeleri (bilgisayarlar) tarafından sağlanır. Yalnızca güvenilen bilgisayarların ağa bağlanmasını sağlamak için, ağa katılan ve üyeliği veren bilgisayarlar birbirlerinin kimliğini doğrulamalıdır.

Bir bilgisayar ağa katıldığında, ondan McAfee koruma durumunu ağdaki diğer bilgisayarlara göstermesi istenir. Bilgisayar koruma durumunu göstermeyi kabul ederse, ağın yönetilen bir üyesi olur. Bilgisayar koruma durumunu göstermeyi kabul etmezse, ağın yönetilmeyen bir üyesi olur. Ağın yönetilmeyen üyeleri, genellikle başka ağ özelliklerine erişmek (örneğin, dosyalar göndermek veya yazıcıları paylaşmak) isteyen konuk bilgisayarlardır.

Not: Ağa katıldıktan sonra, başka McAfee ağ programları yüklenmişse (örneğin EasyNetwork), bilgisayarınız bu programlar tarafından da yönetilen bir bilgisayar olarak tanınır. Network Manager'da bir bilgisayara atanan izin düzeyi, tüm McAfee ağ programlarında geçerlidir. Diğer McAfee ağ programlarında konuk, tam veya yönetici izinlerinin anlamları hakkında ayrıntılı bilgi için o programlarla birlikte sağlanan belgelere bakın.

Yönetilen bir ağa katılma

Yönetilen bir ağa katılmak için davet aldığımızda, bunu kabul edebilir veya reddedebilirsiniz. Ayrıca ağ üzerindeki diğer bilgisayarların bu bilgisayarın güvenlik ayarlarını yönetmesini isteyip istemediğinizi belirleyebilirsiniz.

- 1 Yönetilen Ağ iletişim kutusunda, **Bu ağdaki her bilgisayarın güvenlik ayarlarını yönetmesine izin ver** onay kutusunun işaretli olduğundan emin olun.
- 2 **Katıl**'ı tıklatın.
Daveti kabul ettiğinizde, iki oyun kartı görüntülenir.
- 3 Oyun kartlarının, sizi yönetilen ağa katılmak üzere davet eden bilgisayarda görüntülenen kartlarla aynı olduğunu doğrulayın.
- 4 **Tamam**'ı tıklatın.

Not: Sizi yönetilen ağa katılmak üzere davet eden bilgisayar, güvenlik onayı iletişim kutusunda görüntülenen oyun kartlarıyla aynı kartları görüntülemese, yönetilen ağ üzerinde bir güvenlik ihlali olmuştur. Ağa katılırsanız bilgisayarınız risk altına girebilir; bu nedenle, Yönetilen Ağ iletişim kutusunda **İptal**'i tıklatın.

Bir bilgisayarı yönetilen ağa katılmaya davet etme

Yönetilen ağa bir bilgisayar eklenirse veya ağ üzerinde başka bir yönetilmeyen bilgisayar varsa, bu bilgisayarı yönetilen ağa katılmak üzere davet edebilirsiniz. Yalnızca ağ üzerinde yönetici izinlerine sahip bilgisayarlar diğer bilgisayarları katılmaya davet edebilir. Daveti gönderdiğinizde, katılacak olan bilgisayara atamak istediğiniz izin düzeyini de belirtebilirsiniz.

- 1 Ağ haritasında yönetilmeyen bilgisayarın simgesini tıklatın.
- 2 **Şunu yapmak istiyorum** altında **Bu bilgisayarı yönet**'i tıklatın.
- 3 Bir bilgisayarı yönetilen ağa katılmaya davet et iletişim kutusunda, aşağıdakilerden birini yapın:
 - Bilgisayarın ağa erişmesine izin vermek için **Yönetilen ağ programlarına konuk erişim izni ver**'i tıklatın (bu seçeneği, evinizdeki geçici kullanıcılar için kullanabilirsiniz).
 - Bilgisayarın ağa erişmesine izin vermek için **Yönetilen ağ programlarına tam erişim izni ver**'i tıklatın.
 - Bilgisayarın ağa yönetici haklarıyla erişmesine izin vermek için **Yönetilen ağ programlarına yönetici erişim izni ver**'i tıklatın. Bu, bilgisayarın yönetilen ağa katılmak isteyen diğer bilgisayarlara erişim sağlamasına da olanak verir.

- 4 Tamam'ı tıkladın.**
Bilgisayara, yönetilen ağa katılması için davet gönderilir. Bilgisayar daveti kabul ettiğinde, iki oyun kartı görüntülenir.
- 5 Oyun kartlarının, yönetilen ağa katılmak üzere davet ettiğiniz bilgisayarda görüntülenen kartlarla aynı olduğunu doğrulayın.**
- 6 Erişim İzni Ver'i tıkladın.**

Not: Yönetilen ağa katılmak üzere davet ettiğiniz bilgisayar, güvenlik onayı iletişim kutusunda görüntülenen oyun kartlarıyla aynı kartları görüntüleme, yönetilen ağ üzerinde bir güvenlik ihlali olmuştur. Bilgisayarın ağa katılmasına izin verirseniz diğer bilgisayarlar risk altına girebilir; bu nedenle, güvenlik onayı iletişim kutusunda **Erişimi Reddet'i** tıkladın.

Ağdaki bilgisayarlara güvenmeyi durdurma

Ağdaki diğer bilgisayarlara yanlışlıkla güvendiyseniz, bunlara güvenmeyi durdurabilirsiniz.

- **Şunu yapmak istiyorum altında Bu ağdaki bilgisayarlara güvenmeyi durdur'u tıkladın.**

Not: Yönetici izinleriniz varsa ve ağda başka yönetilen bilgisayarlar bulunuyorsa, **Bu ağdaki bilgisayarlara güvenmeyi durdur** bağlantısı kullanılamaz.

B Ö L Ü M 4 5

Ağı uzaktan yönetme

Yönetilen ağınızdı kurduktan sonra, ağınızdı oluşturan bilgisayarları ve aygıtları uzaktan yönetebilirsiniz. Bilgisayarların ve aygıtların durumunu ve izin düzeylerini yönetebilir; güvenlik açıklarının çoğunu uzaktan düzeltebilirsiniz.

Bu bölümde

Durum ve izinleri yönetme.....	206
Güvenlik açıklarını düzeltme	208

Durum ve izinleri yönetme

Yönetilen bir ağın yönetilen ve yönetilmeyen üyeleri vardır. Yönetilen üyeler, McAfee koruma durumlarının ağdaki diğer bilgisayarlar tarafından yönetilmesine izin verirler; yönetilmeyen üyeler buna izin vermezler. Yönetilmeyen üyeler, genellikle başka ağ özelliklerine erişmek (örneğin, dosya göndermek veya yazıcıları paylaşmak) isteyen konuk bilgisayarlardır. Yönetilmeyen bir bilgisayar, herhangi bir zamanda ağ üzerinde yönetici izinlerine sahip başka bir yönetilen bilgisayar tarafından yönetilen üye olmak üzere davet edilebilir. Benzer şekilde, yönetici izinlerine sahip yönetilen bir bilgisayar, başka bir yönetilen bilgisayarı herhangi bir zamanda yönetilmeyen bilgisayar yapabilir.

Yönetilen bilgisayarlar yönetici, tam veya konuk izinlerine sahiptir. Yönetici izinleri, yönetilen bilgisayarın ağdaki diğer tüm bilgisayarların koruma durumunu yönetmesine ve diğer bilgisayarlara ağ üzerinde üyelik sağlamasına olanak verir. Tam ve konuk izinleri, bilgisayarın yalnızca ağa erişmesine olanak verir. Bir bilgisayarın izin düzeyini istediğiniz zaman değiştirebilirsiniz.

Yönetilen bir ağda aygıtlar da (örneğin yönlendiriciler) olabileceği için bunları yönetmek için Network Manager'ı kullanabilirsiniz. Ayrıca, bir aygıtın görüntü özelliklerini ağ haritasında yapılandırabilir veya değiştirebilirsiniz.

Bir bilgisayarın koruma durumunu yönetme

Bir bilgisayarın koruma durumu ağ üzerinde yönetilmiyorsa (bilgisayar ağın üyesi değilse veya ağın yönetilmeyen bir üyesiyse), onu yönetmek için istekte bulunabilirsiniz.

- 1 Ağ haritasında yönetilmeyen bilgisayarın simgesini tıklatın.
- 2 **Şunu yapmak istiyorum** altında **Bu bilgisayarı yönet**'i tıklatın.

Bir bilgisayarın koruma durumunu yönetmeyi durdurma

Ağınızda yönetilen bir bilgisayarın koruma durumunu yönetmeyi durdurabilirsiniz; ancak bu durumda bilgisayar yönetilmeyen üye olur ve koruma durumunu uzaktan yönetemezsiniz.

- 1 Ağ haritasında yönetilen bilgisayarın simgesini tıklatın.
- 2 **Şunu yapmak istiyorum** altında **Bu bilgisayarı yönetmeyi durdur**'u tıklatın.
- 3 Onay iletişim kutusunda **Evet**'i tıklatın.

Yönetilen bir bilgisayarın izinlerini değiştirme

Yönetilen bir bilgisayarın izinlerini herhangi bir zamanda değiştirebilirsiniz. Bu, ağdaki diğer bilgisayarların koruma durumunu yönetebilen bilgisayarları değiştirmenize olanak verir.

- 1 Ağ haritasında yönetilen bilgisayarın simgesini tıklatın.
- 2 **Şunu yapmak istiyorum** altında **Bu bilgisayardaki izinleri değiştir**'i tıklatın.
- 3 İzinleri değiştirme iletişim kutusunda, bu bilgisayarla yönetilen ağdaki diğer bilgisayarların birbirlerinin koruma durumunu yönetip yönetmeyeceklerini belirlemek için onay kutusunu seçin veya işaretini kaldırın.
- 4 **Tamam**'i tıklatın.

Bir aygıtı yönetme

Ağ haritasından yönetici Web sayfasına erişerek, bir aygıtı yönetebilirsiniz.

- 1 Ağ haritasında aygıtın simgesini tıklatın.
- 2 **Şunu yapmak istiyorum** altında **Bu aygıtı yönet**'i tıklatın. Bir Web tarayıcısı açılır ve aygıtın yönetici Web sayfasını görüntüler.
- 3 Web tarayıcınızda oturum açma bilgilerini sağlayın ve aygıtın güvenlik ayarlarını yapılandırın.

Not: Aygıt McAfee Wireless Network Security tarafından korunan bir kablosuz yönlendirici veya erişim noktasıysa, aygıtın güvenlik ayarlarını yapılandırmak için Wireless Network Security kullanmanız gerekir.

Bir aygıtın görüntü özelliklerini değiştirme

Bir aygıtın görüntü özelliklerini değiştirdiğinizde, ağ haritasında aygıtın görüntü adını değiştirebilir ve aygıtın kablosuz yönlendirici olup olmadığını belirtebilirsiniz.

- 1 Ağ haritasında aygıtın simgesini tıklatın.
- 2 **Şunu yapmak istiyorum** bölümünde **Aygıt özelliklerini değiştir**'i tıklatın.
- 3 Aygıtın görüntü adını belirtmek için, **Ad** kutusuna bir ad yazın.
- 4 Aygıtın türünü belirtirken, aygıt kablosuz yönlendirici değilse **Standart Yönlendirici**'yi, kablosuzsa **Kablosuz Yönlendirici**'yi tıklatın.
- 5 **Tamam**'i tıklatın.

Güvenlik açıklarını düzeltme

Yönetici izinlerine sahip yönetilen bilgisayarlar, ağdaki diğer yönetilen bilgisayarların McAfee koruma durumunu yönetebilir ve raporlanan güvenlik açıklarını uzaktan düzeltebilir. Örneğin, yönetilen bir bilgisayarın McAfee koruma durumu VirusScan'ın devre dışı olduğunu gösteriyorsa, yönetici izinlerine sahip başka bir yönetilen bilgisayar VirusScan'ı uzaktan etkinleştirebilir.

Güvenlik açıklarını uzaktan düzelttiğinizde, Network Manager en çok raporlanan sorunları onarır. Ancak bazı güvenlik açıkları, yerel bilgisayarda el ile müdahale gerektirebilir. Bu durumda, Network Manager uzaktan onarılabilen sorunları düzeltir ve daha sonra geri kalan sorunları, tehditlere açık bilgisayarda SecurityCenter oturumu açıp size sağlanan önerileri izleyerek düzeltmenizi ister. Bazen çözüm olarak, uzak bilgisayara veya ağınızdaki bilgisayarlara SecurityCenter'ın en son sürümünü yüklemeniz önerilebilir.

Güvenlik açıklarını düzeltme

Network Manager'ı kullanarak, yönetilen uzak bilgisayarlarda pek çok güvenlik açıklığını düzeltebilirsiniz. Örneğin, uzak bilgisayarda VirusScan devre dışıysa bunu etkinleştirebilirsiniz.

- 1 Ağ haritasında ögenin simgesini tıklatın.
- 2 **Ayrıntılar** bölümünde, ögenin koruma durumunu görüntüleyin.
- 3 **Şunu yapmak istiyorum** bölümünde **Güvenlik açıklarını düzelt**'i tıklatın.
- 4 Güvenlik açıkları düzeltilince, **Tamam**'ı tıklatın.

Not: Network Manager pek çok güvenlik açıklığını otomatik olarak düzeltir, ancak bazı onarımlarda tehditlere açık bilgisayarda SecurityCenter'ı açıp size sağlanan önerileri izlemeniz gerekebilir.

Uzak bilgisayarlara McAfee güvenlik yazılımını yükleme

Ağınızdaki bir veya daha fazla bilgisayar SecurityCenter'ın en son sürümlerinden birini kullanmıyorsa, bunların koruma durumu uzaktan yönetilemez. Bu bilgisayarları uzaktan yönetmek istiyorsanız, her bilgisayara tek tek SecurityCenter'ın en son sürümlerinden birini yüklemeniz gerekir.

- 1 Uzaktan yönetmek istediğiniz bilgisayarda bu yönergeleri uyguladığınızdan emin olun.
- 2 McAfee oturum açma bilgilerinizi hazır bulundurun: Bu, McAfee yazılımı ilk etkinleştirilirken kullanılan e-posta adresi ve paroladır.
- 3 Tarayıcıda, McAfee Web sitesine gidin, oturum açın ve **Hesabım'ı** tıklatın.
- 4 Yükleme istediğiniz ürünü bulun, **Yükle** düğmesini tıklatın ve sonra ekran yönergelerini uygulayın.

İpucu: Ayrıca ağ haritasını açıp **Şunu yapmak istiyorum** altında **PC'lerimi koru**'yu tıklatarak uzak bilgisayarlara McAfee güvenlik yazılımını nasıl yükleyeceğinizi öğrenebilirsiniz.

B Ö L Ü M 4 6

Ağlarınızı izleme

McAfee Total Protection yüklediyseniz, Network Manager da ağlarınızda saldırganları izler. Bilinmeyen bir bilgisayar veya aygıt ağınıza her bağlandığında bu size bildirilir; böylece bu bilgisayarın veya aygıtın Arkadaş mı yoksa Saldırgan mı olduğuna karar verebilirsiniz. Arkadaş tanıdığınız ve güvendiğiniz bir bilgisayar veya aygıt, Saldırgan ise tanımadığınız veya güvenmediğiniz bir bilgisayar veya aygıttır. Bir bilgisayarı veya aygıtı Arkadaş olarak işaretlerseniz, bu Arkadaş ağa her bağlandığında size bildirilmesini isteyip istemediğinize karar verebilirsiniz. Bir bilgisayarı veya aygıtı Saldırgan olarak işaretlerseniz, ağınıza her bağlandığında bunu size otomatik olarak bildiririz.

Bu Total Protection sürümünü yükledikten veya bu sürüme yükseltme yaptıktan sonra ağa ilk bağlandığınızda, her bilgisayarı veya aygıtı Arkadaş olarak otomatik işaretleriz ve ileride ağa bağlandıkları zaman bunu size bildirmeyiz. Üç gün sonra, bilinmeyen her bilgisayarı veya aygıtı size bildirmeye başlarız; böylece bunları kendiniz işaretleyebilirsiniz.

Not: Ağ izleme, Network Manager'ın yalnızca McAfee Total Protection ile kullanılabilen bir özelliğidir. Total Protection hakkında daha fazla bilgi için Web sitemizi ziyaret edin.

Bu bölümde

Ağları izlemeyi durdurma	211
Ağ izleme bildirimlerini yeniden etkinleştirme	212
Saldırgan olarak işaretleme	212
Arkadaş olarak işaretleme	213
Yeni Arkadaşlar algılamayı durdurma	213

Ağları izlemeyi durdurma

Ağ izlemeyi devre dışı bırakırsanız, ev ağınıza veya bağlandığınız başka herhangi bir ağa saldırganların bağlandığını artık size bildiremeyiz.

1 İnternet ve Ağ Yapılandırma bölmesini açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
2. SecurityCenter Giriş bölümünde **İnternet ve Ağ**'i tıklatın.
3. İnternet ve Ağ bilgi bölümünde **Yapılandır**'i tıklatın.

2 Ağ izleme altında **Kapalı**'yı tıklatın.

Ağ izleme bildirimlerini yeniden etkinleştirme

Ağ izleme bildirimlerini devre dışı bırakabilirsiniz, ancak bunu önermiyoruz. Bunu yaparsanız, ağınıza bağlanan bilinmeyen bilgisayarları veya Saldırganları artık size bildiremeyebiliriz. Bu bildirimleri yanlışlıkla devre dışı bırakırsanız (örneğin bir uyarıda **Bu uyarıyı bir daha gösterme** onay kutusunu seçerseniz), bunları istediğiniz zaman yeniden etkinleştirebilirsiniz.

1 Uyarı Seçenekleri bölmesini açın.

Nasıl?

1. **Ortak Görevler** bölümünde **Giriş**'i tıklatın.
2. Sağdaki bölmede, **SecurityCenter Bilgisi** altında **Yapılandır**'ı tıklatın.
3. **Uyarılar** altında **Gelişmiş**'i tıklatın.

2 SecurityCenter Yapılandırma bölümünde **Bilgi Uyarıları**'ni tıklatın.

3 Bilgi Uyarıları bölümünde şu onay kutularının işaretlenmediğinden emin olun:

- **Yeni bilgisayarlar veya aygıtlar ağa bağlanınca uyarı gösterme**
- **Saldırganlar ağa bağlanınca uyarı gösterme**
- **Genellikle bana bildirilmesini istediğim Arkadaşlar için uyarı gösterme**
- **Bilinmeyen bilgisayarlar veya aygıtlar algılanınca bana anımsatma**
- **McAfee yeni Arkadaşlar algılamayı bitirdiğinde bana haber verme**

4 **Tamam**'ı tıklatın.

Saldırgan olarak işaretleme

Ağınızda bir bilgisayarı veya aygıtı, onu tanımiyorsanız ve güvenmiyorsanız Saldırgan olarak işaretleyin. Ağınıza her bağlandığında bunu size otomatik olarak bildiririz.

1 Temel veya Gelişmiş Menü'de **Ağı Yönet**'i tıklatın.

2 Ağ haritasında bir öğeyi tıklatın.

3 **Şunu yapmak istiyorum** altında **Arkadaş veya Saldırgan Olarak İşaretle**'yi tıklatın.

4 İletişim kutusunda **Saldırgan**'i tıklatın.

Arkadaş olarak işaretleme

Ağınızda bir bilgisayarı veya aygıtı, yalnızca onu tanıyorsanız ve güveniyorsanız Arkadaş olarak işaretle. Bir bilgisayarı veya aygıtı Arkadaş olarak işaretlediğinizde, ağa her bağlandığında size bildirilmesini isteyip istemediğinize de karar verebilirsiniz.

- 1 Temel veya Gelişmiş Menü'de **Ağı Yönet**'i tıklatın.
- 2 Ağ haritasında bir öğeyi tıklatın.
- 3 **Şunu yapmak istiyorum** altında **Arkadaş veya Saldırgan Olarak İşaretle**'yi tıklatın.
- 4 İletişim kutusunda **Arkadaş**'i tıklatın.
- 5 Bu Arkadaş ağa her bağlandığında size bildirilmesi için **Bu bilgisayar veya aygıt ağa bağlandığında bana bildir** onay kutusunu seçin.

Yeni Arkadaşlar algılamayı durdurma

Bu Total Protection sürümünü yükleyip ağa ilk kez bağlandıktan üç gün sonra, hakkında bildirim almak istemediğiniz her bilgisayarı veya aygıtı Arkadaş olarak otomatik işaretleriz. Bu üç gün içinde otomatik işaretleme istediğiniz zaman durdurabilirsiniz, ancak sonra yeniden başlatamazsınız.

- 1 Temel veya Gelişmiş Menü'de **Ağı Yönet**'i tıklatın.
- 2 **Şunu yapmak istiyorum** altında **Yeni Arkadaşlar algılamayı durdur**'u tıklatın.

B Ö L Ü M 4 7

McAfee EasyNetwork

EasyNetwork, dosyaları güvenli şekilde paylaşmanıza, dosya aktarımlarını basitleştirmenize ve ev ağınızdaki bilgisayarlar arasında yazıcıları paylaşmanıza olanak verir. Ancak program özelliklerine erişebilmeniz için ağınızdaki bilgisayarlarda EasyNetwork yüklü olmalıdır.

EasyNetwork'ü kullanmadan önce, bu özelliklerden bazıları hakkında bilgi edinebilirsiniz. Bu özelliklerin yapılandırılması ve kullanımıyla ilgili ayrıntılar, EasyNetwork yardımında sunulmaktadır.

Not: SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz.

Bu bölümde

EasyNetwork özellikleri.....	216
EasyNetwork'ü ayarlama.....	217
Dosyaları paylaşma ve gönderme	221
Yazıcıları paylaşma.....	227

EasyNetwork özellikleri

EasyNetwork aşağıdaki özellikleri sunar.

Dosya paylaşımı

EasyNetwork, dosyaları ağınızdaki diğer bilgisayarlarla paylaşmanızı kolaylaştırır. Dosyaları paylaşırken, diğer bilgisayarlara bu dosyalar için salt okunur erişim izni verirsiniz. Yalnızca yönetilen ağınızda tam veya yönetici erişimine sahip bilgisayarlar (üyeler), diğer üyeler tarafından paylaşılan dosyaları paylaşabilir veya bunlara erişebilirler.

Dosya aktarımı

Yönetilen ağınızda tam veya yönetici erişimine sahip diğer bilgisayarlara (üyelere) dosyalar gönderebilirsiniz. Bir dosya aldığımızda, bu EasyNetwork gelen kutusunda görüntülenir. Gelen kutusu, ağdaki diğer bilgisayarların size gönderdiği tüm dosyalar için geçici bir depolama konumudur.

Otomatik yazıcı paylaşımı

Yönetilen bir ağa katıldığımızda, varsa bilgisayarınıza bağlı yerel yazıcıları, paylaşılan yazıcı adı için yazıcının geçerli adını kullanarak diğer üyelerle paylaşabilirsiniz. Ayrıca, ağınızdaki diğer bilgisayarlar tarafından paylaşılan yazıcıları algılar; bu yazıcıları yapılandırmanıza ve kullanmanıza olanak verir.

B Ö L Ü M 4 8

EasyNetwork'ü ayarlama

EasyNetwork'ü kullanabilmek için önce programı açıp yönetilen ağa katılmanız gerekir. Yönetilen ağa katıldıktan sonra, dosyaları ağdaki diğer bilgisayarlarla paylaşabilir, arayabilir ve bunlara gönderebilirsiniz. Yazıcıları da paylaşabilirsiniz. Ağı terk etmeye karar vererseniz, bunu istediğiniz zaman yapabilirsiniz.

Bu bölümde

EasyNetwork'ü açma.....	217
Yönetilen bir ağa katılma	218
Yönetilen ağı terk etme	220

EasyNetwork'ü açma

EasyNetwork'ü Windows Başlat menüsünden veya masaüstü simgesini tıklatarak açabilirsiniz.

- **Başlat** menüsünde **Programlar**'a gelin, **McAfee**'ye gelin ve ardından **McAfee EasyNetwork'ü** tıklatın.

İpucu: EasyNetwork'ü masaüstünüzdeki McAfee EasyNetwork simgesini çift tıklatarak da açabilirsiniz.

Yönetilen bir ağa katılma

Bağlı olduğunuz ağdaki hiçbir bilgisayarda SecurityCenter yoksa, ağa üye olursunuz ve sizden bu ağın güvenilen bir ağ olup olmadığı tanımlamanız istenir. Ağa katılan ilk bilgisayar olduğu için bilgisayarınızın adı ağ adına eklenir; ancak istediğiniz zaman ağın adını değiştirebilirsiniz.

Ağa bir bilgisayar bağlandığında, ağ üzerindeki diğer tüm bilgisayarlara bir katılma isteği gönderir. Bu katılma isteğini, ağ üzerinde yönetim izinlerine sahip herhangi bir bilgisayar kabul edebilir. Katılma izni veren bilgisayar, ağa katılan bilgisayarın izin düzeyini de belirleyebilir: örneğin konuk (yalnızca dosya aktarımı) veya tam/yönetici (dosya aktarımı ve dosya paylaşımı). EasyNetwork'te yönetici erişimine sahip bilgisayarlar, diğer bilgisayarlara erişim izni verebilir ve izinleri yönetebilir (bilgisayarların izinlerini yükseltebilir veya düşürebilir); tam erişime sahip bilgisayarlar bu yönetici görevlerini gerçekleştiremez.

Not: Ağa katıldıktan sonra, başka McAfee ağ programları yüklenmişse (örneğin Network Manager), bilgisayarınız bu programlar tarafından da yönetilen bir bilgisayar olarak tanınır. EasyNetwork'te bilgisayara atanan izin düzeyi, tüm McAfee ağ programlarında geçerlidir. Diğer McAfee ağ programlarında konuk, tam veya yönetici izinlerinin anlamları hakkında ayrıntılı bilgi için o programlarla birlikte sağlanan belgelere bakın.

Ağa katılma

EasyNetwork yüklendikten sonra bilgisayar güvenilen ağa ilk kez bağlandığında, yönetilen ağa katılıp katılmayacağını soran bir ileti görüntülenir. Bilgisayar katılmayı kabul ederse, ağ üzerinde yönetici erişimine sahip diğer tüm bilgisayarlara bir istek gönderilir. Bilgisayarın yazıcıları veya dosyaları paylaşabilmesi ya da ağ üzerinde dosyalar gönderebilmesi ve kopyalayabilmesi için, bu isteğin kabul edilmesi gerekir. Ağ üzerindeki ilk bilgisayara, otomatik olarak yönetici izinleri verilir.

- 1 Paylaşılan Dosyalar penceresinde **Bu ağa katıl**'ı tıklatın. Ağdaki yönetici bilgisayar isteğinizi kabul ederse, bu bilgisayar ve ağ üzerindeki diğer bilgisayarlar tarafından güvenlik ayarlarının karşılıklı yönetilmesine izin verip vermediğinizi soran bir ileti görüntülenir.
- 2 Bu bilgisayar ve ağ üzerindeki diğer bilgisayarlar tarafından karşılıklı güvenlik ayarlarının yönetilmesine izin vermek için **Tamam**'ı, reddetmek içinse **İptal**'i tıklatın.
- 3 Ağa katılma izni veren bilgisayarda görüntülenen oyun kartlarıyla, güvenlik onayı iletişim kutusunda görüntülenen kartların aynı olduğunu doğrulayın ve sonra **Tamam**'ı tıklatın.

Not: Sizi yönetilen ağa katılmak üzere davet eden bilgisayar, güvenlik onayı iletişim kutusunda görüntülenen oyun kartlarıyla aynı kartları görüntülemeyse, yönetilen ağ üzerinde bir güvenlik ihlali olmuştur. Ağa katılırsanız bilgisayarınız risk altına girebilir; bu nedenle, güvenlik onayı iletişim kutusunda **İptal**'i tıklayın.

Ağa erişim izni verme

Bir bilgisayar yönetilen ağa katılmak istediğinde, ağ üzerinde yönetici erişimine sahip diğer bilgisayarlara bir ileti gönderilir. İlk yanıt veren bilgisayar, katılma iznini veren bilgisayardır. Katılma iznini siz veriyorsanız, bilgisayara şu erişim izinlerinden hangisinin verileceğine karar verme sorumluluğu size aittir: konuk, tam veya yönetici.

- 1 Uyarıda, uygun erişim düzeyini tıklayın.
- 2 Bir bilgisayarı yönetilen ağa katılmaya davet et iletişim kutusunda, aşağıdakilerden birini yapın:
 - Bilgisayarın ağa erişmesine izin vermek için **Yönetilen ağ programlarına konuk erişim izni ver**'i tıklayın (bu seçeneği, evinizdeki geçici kullanıcılar için kullanabilirsiniz).
 - Bilgisayarın ağa erişmesine izin vermek için **Yönetilen ağ programlarına tam erişim izni ver**'i tıklayın.
 - Bilgisayarın ağa yönetici haklarıyla erişmesine izin vermek için **Yönetilen ağ programlarına yönetici erişim izni ver**'i tıklayın. Bu, bilgisayarın yönetilen ağa katılmak isteyen diğer bilgisayarlara erişim sağlamasına da olanak verir.
- 3 **Tamam**'i tıklayın.
- 4 Bilgisayarın, güvenlik onayı iletişim kutusunda gösterilen oyun kartlarını görüntülediğini doğrulayın ve sonra **Erişim İzni Ver**'i tıklayın.

Not: Bilgisayarda görüntülenen oyun kartlarıyla güvenlik onayı iletişim kutusunda görüntülenen kartlar aynı değilse, yönetilen ağ üzerinde bir güvenlik ihlali olmuştur. Bu bilgisayara ağa erişim izni verirseniz bilgisayarınız risk altına girebilir; bu nedenle, güvenlik onayı iletişim kutusunda **Erişimi Reddet**'i tıklayın.

Ağın adını deęiřtirme

Varsayılan olarak, ağın adı ilk katılan bilgisayarın adını içerir; ancak istediđiniz zaman ağın adını deęiřtirebilirsiniz. Ağın adını deęiřtirdiđinizde, EasyNetwork'te grntlenen ađ aıklamasını da deęiřtirirsiniz.

- 1** Seenekler mensnde **Yapılandır**'i tıklatın.
- 2** Yapılandır iletiřim kutusunda, **Ađ Adı** kutusuna ağın adını yazın.
- 3** **Tamam**'i tıklatın.

Ynetilen ađı terk etme

Ynetilen bir ađa katıldıktan sonra ađın yesi olmak istemediđinize karar verirseniz, ađı terk edebilirsiniz. Ynetilen ađı terk ettikten sonra, her zaman yeniden katılabilirsiniz; ancak size yeniden izin verilmesi gerekir. Ađa katılma hakkında ayrıntılı bilgi iin bkz. Ynetilen bir ađa katılma (sayfa 218).

Ynetilen ađı terk etme

Daha nceden katılmıř olduđunuz ynetilen ađı terk edebilirsiniz.

- 1** Bilgisayarınızın ađ ile bađlantısını kesin.
- 2** EasyNetwork'te **Aralar** mensnde **Ađı Terket**'i tıklatın.
- 3** Ađı Terket iletiřim kutusunda, terk etmek istediđiniz ađın adını sein.
- 4** **Ađı Terket**'i tıklatın.

B Ö L Ü M 4 9

Dosyaları paylaşma ve gönderme

EasyNetwork, dosyaları ağdaki diğer bilgisayarlarla paylaşmanızı ve onlara göndermenizi kolaylaştırır. Dosyaları paylaşırken, diğer bilgisayarlara bunlar için salt okunur erişim izni verirsiniz. Yalnızca yönetilen ağın üyesi olan (tam veya yönetici erişimiyle) bilgisayarlar, dosyalar paylaşabilir veya diğer üye bilgisayarlar tarafından paylaşılan dosyalara erişebilir.

Not: Çok sayıda dosya paylaşıyorsanız, bilgisayarınızın kaynakları etkilenebilir.

Bu bölümde

Dosyaları paylaşma	222
Dosyaları diğer bilgisayarlara gönderme	224

Dosyaları paylaşma

Yalnızca yönetilen ağın üyesi olan (tam veya yönetici erişimiyle) bilgisayarlar, dosyalar paylaşabilir veya diğer üye bilgisayarlar tarafından paylaşılan dosyalara erişebilir. Bir klasörü paylaşıyorsanız, bu klasörde bulunan tüm dosyalar ve alt klasörler paylaşılır; ancak klasöre sonradan eklenen dosyalar otomatik olarak paylaşılmaz. Paylaşılan bir dosya veya klasör silinirse, Paylaşılan Dosyalar penceresinden kaldırılır. İstedığınız zaman dosya paylaşımını durdurabilirsiniz.

Paylaşılan bir dosyaya erişmek için dosyayı doğrudan EasyNetwork'ten açın veya bilgisayarınıza kopyalayıp daha sonra buradan açın. Paylaşılan dosyalar listeniz büyükse ve dosyanın nerede olduğunu görmek güçse, bunu arayabilirsiniz.

Not: EasyNetwork ile paylaşılan dosyalara, diğer bilgisayarlardan Windows Gezgini kullanılarak erişilemez, çünkü EasyNetwork dosya paylaşımı güvenli bağlantılar üzerinden gerçekleştirilmelidir.

Dosya paylaşma

Bir dosyayı paylaştığınızda, yönetilen ağ üzerinde tam veya yönetici erişimine sahip tüm üyeler dosyayı kullanabilir.

- 1 Windows Gezgini'nde, paylaşmak istediğiniz dosyayı bulun.
- 2 Dosyayı Windows Gezgini'ndeki konumundan, EasyNetwork'teki Paylaşılan Dosyalar penceresine sürükleyin.

İpucu: Ayrıca **Araçlar** menüsünde **Dosyaları Paylaş**'ı tıklattıysanız da dosyayı paylaşabilirsiniz. Paylaş iletişim kutusunda, paylaşmak istediğiniz dosyanın depolandığı klasöre gidin, onu seçin ve sonra **Paylaş**'ı tıklatın.

Dosya paylaşmayı durdurma

Yönetilen ağ üzerinde bir dosyayı paylaşıyorsanız, istediğiniz zaman paylaşımı durdurabilirsiniz. Dosya paylaşımını durdurduğunuzda, yönetilen ağın diğer üyeleri bu dosyaya erişemez.

- 1 **Araçlar** menüsünde **Dosyaları Paylaştırmayı Durdur**'u tıklatın.
- 2 **Dosyaları Paylaştırmayı Durdur** iletişim kutusunda, artık paylaşmak istemediğiniz dosyayı seçin.
- 3 **Tamam**'ı tıklatın.

Paylaşılan dosyayı kopyalama

Paylaşılan dosyayı kopyaladığınızda, artık paylaşılmasa bile ona sahip olabilirsiniz. Yönetilen ağınızdaki herhangi bir bilgisayardan, paylaşılan bir dosyayı kopyalayabilirsiniz.

- EasyNetwork'te Paylaşılan Dosyalar penceresinden bir dosyayı, Windows Gezgini'ndeki bir konuma veya Windows masaüstüne sürükleyin.

İpucu: Ayrıca, EasyNetwork'te paylaşılan bir dosya seçip **Araçlar** menüsünde **Kopyala**'yı tıklarsanız da dosyayı kopyalayabilirsiniz. Klasöre kopyala iletişim kutusunda, dosyayı kopyalamak istediğiniz klasöre gidip seçin ve ardından **Kaydet**'i tıklatın.

Paylaşılan bir dosyayı arama

Siz veya ağın başka bir üyesi tarafından paylaşılan bir dosyayı arayabilirsiniz. Arama ölçütlerinizi yazdığınızda, EasyNetwork ilişkili sonuçları Paylaşılan Dosyalar penceresinde görüntüler.

- 1 Paylaşılan Dosyalar penceresinde **Ara**'yı tıklatın.
- 2 **İçeriği** listesinde uygun seçeneği (sayfa 223) tıklatın.
- 3 **Dosya veya Yol Adı** listesine, dosya adının veya yolun bir bölümünü ya da tamamını yazın.
- 4 **Tür** listesinde uygun dosya türünü (sayfa 223) tıklatın.
- 5 **Başlangıç** ve **Bitiş** listelerinde, dosyanın oluşturulduğu tarih aralığını temsil eden tarihleri tıklatın.

Arama ölçütleri

Aşağıdaki tabloda, paylaşılan dosyaları ararken belirtebileceğiniz arama ölçütleri açıklanmaktadır.

Dosya adı veya yolu

İçeriği	Açıklama
Tüm sözcükleri içerir	Dosya veya Yol Adı listesinde, herhangi bir sırayla belirttiğiniz tüm sözcükleri içeren dosya veya yol adını arayın.
Herhangi bir sözcüğü içerir	Dosya veya Yol Adı listesinde, belirttiğiniz sözcüklerden herhangi birini içeren dosya veya yol adını arayın.
Tam dizeyi içerir	Dosya veya Yol Adı listesinde, belirttiğiniz tam tümceciği içeren dosya veya yol adını arayın.

Dosya türü

Tür	Açıklama
Herhangi	Tüm paylaşılan dosya türlerini arayın.
Belge	Tüm paylaşılan belgeleri arayın.
Resim	Tüm paylaşılan resim dosyalarını arayın.
Video	Tüm paylaşılan video dosyalarını arayın.
Ses	Tüm paylaşılan ses dosyalarını arayın.
Sıkıştırılmış	Tüm sıkıştırılmış dosyaları arayın (örneğin .zip dosyaları).

Dosyaları diğer bilgisayarlara gönderme

Yönetilen ağın üyesi olan diğer bilgisayarlara dosyalar gönderebilirsiniz. Bir dosya göndermeden önce, EasyNetwork dosyayı alan bilgisayarın yeterli kullanılabilir disk alanı olduğunu doğrular.

Bir dosya aldığınızda, bu EasyNetwork gelen kutusunda görüntülenir. Gelen kutusu, ağdaki diğer bilgisayarların size gönderdiği dosyalar için geçici bir depolama konumudur. Dosyayı aldığınızda EasyNetwork açıksa, dosya anında gelen kutunuzda görüntülenir; açık değilse, görev çubuğunuzun sağ ucundaki bildirim alanında bir ileti görüntülenir. Bildirim iletilerini almak istemiyorsanız (örneğin yaptığınız işe müdahale ettikleri için), bu özelliği kapatabilirsiniz. Gelen kutunuzda önceden aynı ada sahip bir dosya varsa, yeni dosya sayısal bir son eklenerek yeniden adlandırılır. Siz onları kabul edene (bilgisayarınıza kopyalayana) kadar, dosyalar gelen kutunuzda kalır.

Başka bir bilgisayara dosya gönderme

Bir dosyayı paylaşmadan, yönetilen ağdaki başka bir bilgisayara gönderebilirsiniz. Alıcı bilgisayardaki kullanıcının dosyayı görüntüleyebilmesi için dosyanın yerel bir konuma kaydedilmesi gerekir. Ayrıntılı bilgi için, bkz. Başka bir bilgisayardan dosya kabul etme (sayfa 225).

- 1 Windows Gezgini'nde, göndermek istediğiniz dosyayı bulun.
- 2 Dosyayı Windows Gezgini'ndeki konumundan, EasyNetwork'teki etkin bilgisayar simgesine sürükleyin.

İpucu: Bilgisayara birden fazla dosya göndermek için dosyaları seçerken CTRL tuşuna basın. Ayrıca, **Araçlar** menüsünde **Gönder**'i tıklar, dosyaları seçer ve sonra **Gönder**'i tıklarsanız da dosyaları gönderebilirsiniz.

Başka bir bilgisayardan dosya kabul etme

Yönetilen ağdaki başka bir bilgisayar size dosya gönderirse, bunu bilgisayarınıza kaydederek kabul etmeniz gerekir. Bilgisayarınıza dosya gönderildiği sırada EasyNetwork çalışmıyorsa, görev çubuğunuzun sağ ucundaki bildirim alanında bir bildirim iletisi görüntülenir.

EasyNetwork'ü açıp dosyaya erişmek için bu bildirim iletisini tıklayın.

- **Alınma tarihi**'ni tıklayın ve sonra dosyayı, EasyNetwork gelen kutunuzdan Windows Gezgininde bir klasöre sürükleyin.

İpucu: Ayrıca, EasyNetwork gelen kutunuzdan bir dosya seçer ve sonra **Araçlar** menüsünde **Kabul Et**'i tıklarsanız da başka bir bilgisayardan dosya alabilirsiniz. Klasöre kabul et iletişim kutusunda, aldığınız dosyaları kaydetmek istediğiniz klasöre gidip seçin ve ardından **Kaydet**'i tıklayın.

Dosya gönderildiğinde bildirim alma

Yönetilen ağdaki başka bir bilgisayar size dosya gönderdiğinde bildirim iletisi alabilirsiniz. EasyNetwork çalışmıyorsa, görev çubuğunuzun sağ ucundaki bildirim alanında bildirim iletisi görüntülenir.

- 1 **Seçenekler** menüsünde **Yapılandır**'i tıklayın.
- 2 Yapılandır iletişim kutusunda, **Başka bilgisayar bana dosya gönderdiğinde bildir** onay kutusunu işaretleyin.
- 3 **Tamam**'i tıklayın.

B Ö L Ü M 5 0

Yazıcıları paylaşma

Yönetilen bir ağa katıldığınızda, EasyNetwork bilgisayarınıza bağlı yerel yazıcıları paylaşır ve paylaşılan yazıcı adı için yazıcının adını kullanır. EasyNetwork, ağınızdaki diğer bilgisayarlar tarafından paylaşılan yazıcıları da algılar, bunları yapılandırmanıza ve kullanmanıza olanak verir.

Bir yazıcı sürücüsünü ağ yazıcı sunucusu (örneğin kablosuz USB yazdırma sunucusu) aracılığıyla yazdıracak şekilde yapılandırdıysanız, EasyNetwork bu yazıcıyı yerel yazıcı olarak görür ve ağ üzerinde paylaşır. Ayrıca, istediğiniz zaman yazıcı paylaşımını durdurabilirsiniz.

Bu bölümde

Paylaşılan yazıcılarla çalışma 228

Paylaşılan yazıcılarla çalışma

EasyNetwork, ağdaki bilgisayarlar tarafından paylaşılan yazıcıları algılar. EasyNetwork bilgisayarınıza bağlı olmayan bir uzak yazıcı algılsa, EasyNetwork'ü ilk kez açtığınızda, Paylaşılan Dosyalar penceresinde **Kullanılabilir ağ yazıcıları** bağlantısı görüntülenir. Daha sonra, kullanılabilir yazıcıları yükleyebilir veya zaten bilgisayarınıza bağlı olan yazıcıları kaldırabilirsiniz. Ayrıca, görüntülediğiniz bilgilerin güncel olduğundan emin olmak için yazıcı listesini yenileyebilirsiniz.

Yönetilen ağa bağlı olmanıza karşın ağa katılmadıysanız, paylaşılan yazıcılara Windows yazıcı denetim masasından erişebilirsiniz.

Yazıcı paylaşmayı durdurma

Yazıcı paylaşımını durdurduğunuzda, üyeler bunu kullanamaz.

- 1 Araçlar** menüsünde **Yazıcılar**'ı tıklatın.
- Ağ Yazıcılarını Yönet iletişim kutusunda, artık paylaşmak istemediğiniz yazıcının adını tıklatın.
- 3 Paylaştırma**'yı tıklatın.

Kullanılabilir ağ yazıcısı yükleme

Yönetilen ağın üyesiyseniz, paylaşılan yazıcılara erişebilirsiniz; ancak yazıcı tarafından kullanılan yazıcı sürücüsünü yüklemeniz gerekir. Yazıcının sahibi yazıcı paylaşımını durdurursa, bunu kullanamazsınız.

- 1 Araçlar** menüsünde **Yazıcılar**'ı tıklatın.
- Kullanılabilir Ağ Yazıcıları iletişim kutusunda, bir yazıcı adını tıklatın.
- 3 Yükle**'yi tıklatın.

Başvuru

Bu Terimler Sözlüğü'nde, McAfee ürünlerinde bulunan ve en sık kullanılan güvenlik terminolojisi listelenmekte ve tanımlanmaktadır.

Sözlük

8

802.11

Kablosuz yerel ağ üzerinde veri iletmek için standartlar grubu. 802.11 genellikle Wi-Fi olarak bilinir.

802.11a

5 GHz bantta 54 Mb/sn'ye kadar veri gönderen 802.11 uzantısı. İletim hızının 802.11b'den daha yüksek olmasına karşın, kapsanan uzaklık daha kısadır.

802.11b

2,4 GHz bantta 11 Mb/sn'ye kadar veri gönderen 802.11 uzantısı. İletim hızının 802.11a'dan daha düşük olmasına karşın, kapsanan uzaklık daha uzundur.

802.1x

Kablolu ve kablosuz ağlarda kimlik doğrulama için bir standart. 802.1x genellikle 802.11 kablosuz ağ ile kullanılır. Ayrıca bkz. kimlik doğrulama (sayfa 234).

A

ActiveX denetimi

Programlar veya web sayfaları tarafından programın veya web sayfasının doğal bir parçası gibi görünen işlevsellik eklemek üzere kullanılan bir yazılım bileşeni. Çoğu ActiveX denetimi zararsızdır; ancak bazıları bilgisayarınızdan bilgiler yakalayabilir.

açılan pencereler

Bilgisayar ekranınızda diğer pencerelerin üzerinde beliren küçük pencereler. Açılan pencereler, reklamlar görüntülemek üzere web tarayıcılarında sıklıkla kullanılır.

ağ

Mantıksal bir birim olarak bir araya getirilen IP tabanlı sistemler (yönlendiriciler, anahtarlar, sunucular ve güvenlik duvarları) grubu. Örneğin, “Finans Ağı” finans departmanına hizmet veren tüm sunucuları, yönlendiricileri ve sistemleri içerebilir. Ayrıca bkz. ev ağı (sayfa 232).

ağ haritası

Ev ağınıza oluşturan bilgisayarların ve bileşenlerin grafiksel anlatımı.

ağ sürücüsü

Çok sayıda kullanıcı tarafından paylaşılan ağ üzerinde bir sunucuya bağlı disk veya teyp sürücüsü. Ağ sürücülerini bazen “uzak sürücüler” olarak adlandırılır.

akıllı sürücü

Bkz. USB sürücüsü (sayfa 240).

anahtar

İki aygıt tarafından aralarındaki iletişimin kimliğini doğrulamak için kullanılan harfler ve sayılar dizisi. Her iki aygıtın da anahtarı olmalıdır. Ayrıca bkz. WEP (sayfa 240), WPA (sayfa 241), WPA2 (sayfa 241), WPA2-PSK (sayfa 241), WPA-PSK (sayfa 241).

arabellek taşması

Şüpheli programlar veya işlemler, arabelleğe (geçici depolama alanı) saklayabileceğinden daha fazla veri depolamaya çalıştığında işletim sisteminde veya uygulamada ortaya çıkan durum. Arabellek taşması, belleği bozar veya komşu arabelleklerdeki verilerin üzerine yazar.

arşivleme

CD, DVD, USB sürücüsü, harici sabit disk veya ağ sürücüsü üzerinde önemli dosyaların yerel kopyasını oluşturmak. Karşılaştırın: yedekleme (sayfa 241).

B

bant genişliği

Belirli bir süre içinde iletilebilen veri miktarı.

beyaz liste

Güvenli olduğu düşünülen web sitelerinin veya e-posta adreslerinin listesi. Beyaz listedeki web siteleri, kullanıcılar tarafından erişim izni verilen sitelerdir. Beyaz listedeki e-posta adresleri, gönderdikleri iletileri almak istediğiniz güvenilen kaynakların adresleridir. Karşılaştırın: kara liste (sayfa 234).

D

DAT

Virüsler, Truva atları, casus yazılımlar, reklam yazılımlar ve diğer olası istenmeyen programları (PUP) saptayan, algılayan ve onaran tanımlar içeren, aynı zamanda imza dosyaları olarak da bilinen algılama tanım dosyaları.

DNS

Etki Alanı Sistemi. 11.2.3.44 gibi bir IP adresini www.mcafee.com gibi bir etki alanı adına dönüştüren veritabanı sistemi.

dolaşım

Hizmette kesinti veya bağlantı kaybı olmaksızın, bir erişim noktası (AP) kapsama alanından diğerine hareket etme.

dosya parçaları

Bir dosyanın disk üzerine dağılmış kalıntıları. Dosya parçalanması, dosyalar eklenip silindikçe oluşur ve bilgisayarınızın performansını düşürebilir.

düğüm

Bir ağa bağlı olan tek bir bilgisayar.

düz metin

Şifreli olmayan metin. Ayrıca bkz. şifreleme (sayfa 238).

E

e-posta

Elektronik posta. Bilgisayar ağında elektronik olarak gönderilen ve alınan iletiler. Ayrıca bkz. web postası (sayfa 240).

e-posta istemcisi

Bilgisayarınızda e-posta gönderip almak için çalıştırdığınız program (örneğin Microsoft Outlook).

eklenti

Büyük bir yazılıma özellikler ekleyen veya bunu geliştiren küçük bir yazılım programı. Örneğin eklentiler, HTML belgelerine gömülen ve tarayıcının normalde fark etmeyeceği biçimlerdeki animasyon, video ve ses dosyaları gibi dosyalara web tarayıcısının erişmesine ve bunları yürütmesine izin verir.

erişim noktası (AP)

Kablosuz kullanıcının fiziksel hizmet kapsamını genişletmek için Ethernet merkezine veya anahtarına takılan ağ aygıtı (genellikle kablosuz yönlendirici olarak adlandırılır). Kablosuz kullanıcılar mobil cihazlarıyla dolaşıma girdiklerinde, bağlantıyı korumak için iletim bir erişim noktasından (AP) başka bir erişim noktasına geçer.

ESS

Uzatılmış hizmet seti. Tek bir alt ağ oluşturan iki veya daha fazla ağ.

etki alanı

İnternet üzerindeki siteler için bir yerel alt ağ veya tanımlayıcı. Etki alanı, yerel ağ (LAN) üzerinde tek güvenlik veritabanı tarafından kontrol edilen istemci ve sunucu bilgisayarlardan oluşan bir alt ağdır. İnternet üzerinde etki alanı, her web adresinin bir parçasını oluşturur. Örneğin www.mcafee.com adresinde mcafee etki alanıdır.

etkin nokta

Wi-Fi (802.11) erişim noktası (AP) kapsamındaki coğrafi sınır. Etkin nokta “yayın yapıyorsa” (varlığını duyuruyorsa) ve kimlik doğrulaması gerekmiyorsa, kablosuz dizüstü bilgisayarla etkin noktaya giren kullanıcılar İnternet'e bağlanabilirler. Etkin noktalar genellikle havaalanları gibi kalabalık yerlerde bulunur.

ev ağı

Evde dosya ve İnternet erişimini paylaşmak üzere birbirine bağlanan iki veya daha çok bilgisayar. Ayrıca bkz. LAN (sayfa 235).

G

geçici dosya

İşletim sistemi veya başka bir program tarafından, bir oturum sırasında kullanılıp daha sonra silinmek üzere bellekte veya diskte oluşturulan dosya.

gerçek zamanlı tarama

Siz veya bilgisayarınız tarafından erişilen dosya ve klasörlerde virüsleri ve diğer etkinliği tarama işlemi.

Geri Dönüşüm Kutusu

Windows'ta silinen dosyalar ve klasörler için sanal bir çöp kutusu.

güvenilenler listesi

Güvendiğiniz ve algılanmayan öğelerin listesi. Bir öğeye (örneğin olası istenmeyen programa veya kayıt defteri değişikliğine) yanlışlıkla güvenerseniz veya öğenin yeniden algılanmasını isterseniz, onu bu listeden kaldırmanız gerekir.

güvenlik duvarı

Özel bir ağa veya ağdan yetkisiz erişimi engellemek için tasarlanan sistem (donanım, yazılım veya her ikisi birden). Güvenlik duvarları, yetkisiz Internet kullanıcılarının Internet'e ve özellikle bir intranete bağlanan özel ağlara erişmelerini engellemek için sıklıkla kullanılır. İnanete giren veya çıkan tüm iletiler güvenlik duvarından geçer; güvenlik duvarı, tüm iletileri inceler ve belirtilen güvenlik ölçütlerini karşılamayanları engeller.

H

harici sabit disk

Bilgisayar kasasının dışında saklanan harici sürücü.

hileli erişim noktası

Yetkisiz erişim noktası. Hileli erişim noktaları, yetkisiz taraflara ağ erişimi sağlamak için güvenli şirket ağına yüklenebilir. Bunlar, saldırganın ortadaki adam saldırısı gerçekleştirmesini sağlamak için de oluşturulabilir.

hizmet reddi (DOS) saldırısı

Bilgisayara, sunucuya veya ağa karşı düzenlenen ve ağ üzerinde trafiği yavaşlatan veya durduran bir saldırı türü. Ağ düzenli trafiği yavaşlatacak veya tamamen kesecek kadar çok istekle dolduğunda gerçekleşir. Hizmet reddi saldırısı, hedefini sahte bağlantı isteklerine boğar ve böylece hedef yasal istekleri yok sayar.

I

içerik derecelendirme grubu

Ebeveyn Denetimleri'nde, bir kullanıcının ait olduğu yaş grubu. İçerik, kullanıcının ait olduğu içerik derecelendirme grubuna göre kullanıma açılır. İçerik derecelendirme grupları şunları kapsar: Küçük Çocuk, Çocuk, Büyük Çocuk, Genç ve Yetişkin.

ileti kimlik doğrulama kodu (MAC)

Bilgisayarlar arasında gönderilen iletileri şifrelemek için kullanılan güvenlik kodu. Bilgisayar şifresi çözülen kodun geçerli olduğunu anlarsa ileti kabul edilir.

intranet

Genellikle bir kuruluşun içinde bulunan ve yalnızca yetkili kullanıcılar tarafından erişilebilen özel bilgisayar ağı.

IP adresi

Internet Protokolü adresi. TCP/IP ağı üzerinde bir bilgisayarı veya aygıtı tanımlamak için kullanılan adres. IP adresi, noktalarla birbirinden ayrılan dört sayı şeklinde yazılan 32 bitlik sayısal bir adrestir. Her sayı 0 ile 255 arasında olabilir (örneğin, 192.168.1.100).

IP hilesi

Bir IP paketi içindeki IP adreslerinin sahtelerini yapmak. Bu, oturum soymak dahil, çok çeşitli saldırı türlerinde kullanılır. Genellikle tam olarak izlenememeleri için SPAM e-posta başlıklarının sahtelerini yapmada kullanılır.

isteğe bağlı tarama

Tehdit, açık veya başka olası istenmeyen kod bulmak için seçili dosyalara, uygulamalara veya ağ aygıtlarına uygulanan zamanlanmış inceleme. Anında, daha sonra zamanlanan bir saatte veya zamanlanmış düzenli aralıklarla gerçekleşebilir. Erişim üzerine tarama ile karşılaştırın. Ayrıca bkz. açık.

istemci

Bilgisayar veya iş istasyonu üzerinde çalışan ve bazı işlemleri gerçekleştirmek için sunucuya gerek duyan bir program. Örneğin e-posta istemcisi, e-posta gönderip almanıza olanak veren bir uygulamadır.

izleme konumları

Backup and Restore'un bilgisayarınızda izlediği klasörler.

izlenen dosya türleri

Backup and Restore'un izleme konumlarında arşivlediği veya yedeklediği dosya türleri (örn., .doc, .xls).

K

kaba kuvvet saldırısı

Şifreyi kırana kadar olası tüm karakter birleşimlerini deneyerek parolaları veya şifre anahtarlarını bulmak için kullanılan bir korsanlık yöntemi.

kablosuz bağdaştırıcı

Bilgisayara veya PDA'ya kablosuz özelliği ekleyen aygıt. USB port, PC kartı (CardBus) yuvası, bellek kartı yuvası üzerinden veya dahili olarak PCI veri yoluna takılır.

kara liste

Anti-Spam'de, iletilerin spam olduğunu düşündüğünüz için gönderdiği iletileri almak istemediğiniz e-posta adreslerinin listesi. Phishing korumasında, hileli oldukları düşünülen web sitelerinin listesi. Karşılaştırın: beyaz liste (sayfa 231).

karantina

Virüs, spam, şüpheli içerik veya olası istenmeyen programlar (PUP) içerdiğinden şüphelenilen bir dosyaya veya klasöre, dosyanın veya klasörün açılmasını veya yürütülmesini engelleyecek şekilde uygulanan yalıtım.

kayıt defteri

Windows tarafından her bilgisayar kullanıcısı, sistem donanımı, yüklenen programlar ve özellik ayarları hakkında yapılandırma bilgilerini depolamak için kullanılan veritabanı. Bu veritabanı anahtarlara ayrılır ve bunlar için değerler ayarlanır. İstenmeyen programlar, zararlı kodu yürütmek için kayıt defteri anahtarlarının değerini değiştirebilir veya yenilerini oluşturabilir.

kimlik doğrulama

Bir elektronik belgeyi gönderen kişinin dijital kimliğini doğrulama işlemi.

kısayol

Bilgisayarınızda başka bir dosyanın yalnızca konumunu içeren bir dosya.

komut dosyası

Otomatik olarak yürütülebilen (kullanıcı etkileşimi olmadan) komut listesi. Programların aksine komut dosyaları, genellikle düz metin biçiminde depolanır ve çalıştırıldıkları her seferde derlenir. Makrolar ve toplu iş dosyaları da komut dosyaları olarak adlandırılır.

köke inme

Bir bilgisayarda veya bilgisayar ağında kullanıcıya yönetici düzeyinde erişim sağlayan araçlar grubu (programlar). Köke inme programları, bilgisayarınızdaki veriler veya kişisel bilgileriniz için ek güvenlik veya gizlilik riskleri oluşturabilen casus yazılımları ve diğer olası istenmeyen programları içerebilir.

L

LAN

Yerel Ağ. Göreceli olarak küçük bir alanı (örneğin bir tek bina) kapsayan bilgisayar ağı. Yerel ağ üzerindeki bilgisayarlar, birbirleriyle iletişim kurabilir, yazıcı ve dosya gibi kaynakları paylaşabilir.

launchpad

U3 USB programlarını başlatmak ve yönetmek için başlangıç noktası görevi gören bir U3 arabirim bileşeni.

M

MAC adresi

Ortam Erişim Denetimi adresi. Ağa erişen fiziksel ayağa (NIC, ağ arabirim kartı) atanan benzersiz bir seri numarası.

MAPI

İleti Uygulaması Programlama Arabirimi. Farklı ileti ve çalışma grubu programlarının (e-posta, sesli posta ve faks dahil) Exchange istemcisi gibi tek bir istemci aracılığıyla çalışmasına izin veren Microsoft arabirimi belirtimi.

MSN

Microsoft Ağı. Microsoft Corporation tarafından sunulan arama motoru, e-posta, anlık ileti ve portal gibi web tabanlı hizmetler grubu.

N

NIC

Ağ Arabirim Kartı. Dizüstü bilgisayara veya başka bir ayağa takılan ve ayağı yerel ağa bağlayan kart.

numara çeviriciler

Bir içerik sağlayıcı, satıcı veya başka herhangi bir üçüncü tarafın ek bağlantı ücretleri alması için Internet bağlantılarını kullanıcının varsayılan ISS'sinden (Internet servis sağlayıcısı) başka bir tarafa yönlendiren yazılım.

O

olası istenmeyen program (PUP)

Kullanıcılar karşıdan yüklenmesine izin vermiş olsalar bile, istenmeyebilecek bir yazılım programı. Yüklendiği bilgisayarda güvenlik veya gizlilik ayarlarını değiştirebilir. PUP'ler, her zaman olmasa da casus yazılımlar, reklam yazılımlar ve numara çeviriciler içerebilir ve kullanıcının istediği bir programla birlikte karşıdan yüklenebilir.

olay

Bilgisayar sisteminde veya programında, önceden tanımlı ölçütlere göre güvenlik yazılımı tarafından algılanabilen durum. Olay, genellikle bildirim göndermek veya olay günlüğüne giriş eklemek gibi bir eylemi tetikler.

ortadaki adam saldırısı

İletişim bağlantısının ihlal edildiğini bilmeyen iki taraf arasındaki iletileri ele geçirmek ve büyük olasılıkla değiştirmek için bir yöntem.

Ö

önbellek

Bilgisayarınızda sık sık veya yakın zamanda erişilen veriler için geçici bir depolama alanı. Örneğin, web'de gezinme hızını ve etkinliğini artırmak için tarayıcınız, daha önce görüntülediğiniz bir web sayfasını uzak sunucu yerine önbellekten çağırabilir.

P

parola

Bilgisayarınıza, bir programa veya web sitesine erişim sağlamak için kullandığınız kod (genellikle harfler ve sayılardan oluşur).

parola kasası

Kişisel parolalarınız için güvenli bir saklama alanı. Parolalarınızı başka hiçbir kullanıcının (hatta yöneticinin) erişemeyeceği şekilde güvenle saklamanıza olanak verir.

paylaşılan şifre

İletişim başlamadan önce iletişim kuran iki taraf arasında paylaşılan bir dize veya anahtar (genellikle parola). RADIUS iletilerinin hassas bölümlerini korumak için kullanılır. Ayrıca bkz. RADIUS (sayfa 237).

paylaştırma

E-posta alıcılarının sınırlı bir süre için seçili yedeklenen dosyalara erişmelerine izin verme. Bir dosyayı paylaştığınızda, dosyanın yedeklenen kopyasını belirlediğiniz e-posta alıcılarına gönderirsiniz. Alıcılar Backup and Restore'dan dosyaların kendileriyle paylaşıldığını gösteren bir e-posta iletileri alırlar. E-posta, paylaşılan dosyalara bağlantı da içerir.

PCI kablosuz bağdaştırıcı kartı

Çevre Birim Bileşeni Bağlantısı. Bilgisayarın içindeki PCI genişletme yuvasına takılan kablosuz bağdaştırıcı kartı.

phishing

Bankalar veya yasal şirketler gibi güvenilir kaynaklardan geliyormuş gibi görünen hileli e-postalar göndererek, hileli yollardan parolalar, sosyal sigorta numaraları, kredi kartı bilgileri vb. kişisel bilgileri elde etme yöntemi. Phishing e-postalarda, genellikle alıcılardan iletişim bilgilerini veya kredi kartı bilgilerini doğrulamak veya güncelleştirmek için e-postanın içindeki bağlantıyı tıklatmaları istenir.

POP3

Posta Ofis Protokolü 3. E-posta istemci programı ve e-posta sunucusu arasındaki arabirim. Ev kullanıcılarının çoğu, standart e-posta hesabı olarak da bilinen bu hesap türüne sahiptir.

port

Bilgisayara veri gönderip almak için kullanılan bir donanım konumu. Kişisel bilgisayarlarda; disk sürücülerini, monitörleri ve tüm klavyeleri bağlamak için dahili portların yanı sıra modemler, yazıcılar, fareler ve diğer çevre birimleri bağlamak için harici portları da içeren çok çeşitli port türleri vardır.

PPPoE

Ethernet Üzerinden Noktalar Arası Protokol. Aktarım olarak Ethernet'le Noktalar Arası Protokol (PPP) çevirmeli protokolünü kullanma yöntemi.

protokol

Bilgisayarlar veya aygıtlar arasında veri alışverişi sağlayan bir kurallar kümesi. Katmanlı ağ mimarisinde (Açık Sistemler Bağlantı modeli), her katmanın o düzeyde iletişimin nasıl gerçekleştiğini belirten kendi protokolleri vardır. Diğer bilgisayarlarla iletişim kurmak için bilgisayarınız veya aygıtınız doğru protokolü desteklemelidir. Ayrıca bkz. Açık Sistem Bağlantısı (OSI).

proxy

Harici sitelere yalnızca tek bir ağ adresi vererek, ağ ile Internet arasında engel görevi gören bilgisayar (veya bilgisayarda çalışan yazılım). Proxy, tüm dahili bilgisayarları temsil ederek, bir yandan Internet'e erişim sağlarken diğer yandan da ağ kimliklerini korur. Ayrıca bkz. proxy sunucusu (sayfa 237).

proxy sunucusu

Yerel ağa (LAN) girip çıkan Internet trafiğini yöneten bir güvenlik duvarı bileşeni. Proxy sunucusu, popüler bir web sayfası gibi sık sık istenen verileri sağlayarak performansı geliştirebilir ve özel dosyalara yetkisiz erişim gibi kullanıcının uygun görmediği istekleri filtreleyip silebilir.

R

RADIUS

Uzaktan Erişim Çevirme Kullanıcı Hizmeti. Genellikle uzaktan erişimde, kullanıcı kimlik doğrulamasına olanak veren bir protokol. İlk başlarda çevirmeli uzaktan erişim sunucularıyla kullanılmak üzere tanımlanan bu protokol, artık kablosuz yerel ağ kullanıcısının paylaşılan şifresinin 802.1x kimlik doğrulaması dahil, çok çeşitli kimlik doğrulama ortamlarında kullanılmaktadır. Ayrıca bkz. paylaşılan şifre.

S

savaş sürücüsü

Wi-Fi bilgisayar ve birtakım özel donanımlar veya yazılımlarla şehirde dolaşarak Wi-Fi (802.11) ağları arayan kişi.

senkronize etme

Yedeklenen dosyalarla yerel bilgisayarınızda saklanan dosyalar arasındaki tutarsızlıkları çözme. Çevrimiçi yedekleme havuzundaki dosya sürümü diğer bilgisayarlardaki dosya sürümünden daha yeniyse dosyaları senkronize edersiniz.

sıkıştırma

Dosyaları, onları depolamak veya iletmek için gereken alanı en aza indirecek şekilde sıkıştıran bir işlem.

sistem geri yükleme noktası

Bilgisayar belleğinin veya bir veritabanının içeriklerinin anlık görüntüsü. Windows, düzenli olarak ve örneğin bir programın veya sürücünün yüklenmesi gibi önemli sistem olayları gerçekleştiğinde geri yükleme noktaları oluşturur. İstedığınız zaman kendi geri yükleme noktalarınızı da oluşturup adlandırabilirsiniz.

Sistem Koruması

Bilgisayarınızdaki yetkisiz değişiklikleri algılayan ve bunlar oluştuğunda size bildiren McAfee uyarıları.

SMTP

Basit Dosya Paylaşım Protokolü. Bir ağ üzerinde bir bilgisayardan diğerine iletiler göndermeyi sağlayan TCP/IP protokolüdür. Bu protokol, Internet üzerinde e-posta yönlendirmek için kullanılır.

solucan

Diğer sürücülerde, sistemlerde veya ağlarda kendi kopyalarını oluşturarak yayılan bir virüs. Toplu postayla gelen solucan, yayılmak için kullanıcının müdahalesine (örneğin bir eki açmak veya karşıdan yüklenen bir dosyayı yürütmek) gereksinim duyar. Bugün e-posta virüslerinin çoğu solucandır. Kendi kendine yayılan solucan, yayılmak için kullanıcının müdahalesine gereksinim duymaz. Blaster ve Sasser, kendi kendine yayılan solucanlara örnek olarak verilebilir.

sözlük saldırısı

Parolayı bulmak için yaygın sözcükleri kullanan bir tür kaba kuvvet saldırısı.

SSID

Hizmet Seti Tanımlayıcısı. Wi-Fi (802.11) ağını tanımlayan belirteç (gizli anahtar). SSID, ağ yöneticisi tarafından ayarlanır ve ağa katılmak isteyen kullanıcılar tarafından sağlanmalıdır.

SSL

Güvenli Yuva Katmanı. Netscape tarafından Internet'te özel belgeleri iletmek üzere geliştirilen bir protokol. SSL, SSL bağlantısı üzerinden aktarılan verileri şifrelemek için ortak bir anahtar kullanarak çalışır. SSL bağlantısı gerektiren URL'ler HTTP yerine HTTPS ile başlar.

standart e-posta hesabı

Bkz. POP3 (sayfa 237).

sunucu

Diğer bilgisayarlardan veya programlardan bağlantılar kabul eden ve uygun yanıtları veren bir bilgisayar veya program. Örneğin, her e-posta iletisi gönderip aldığınızda, e-posta programınız bir e-posta sunucusuna bağlanır.

Ş

şifreleme

Yetkisiz kişilerin erişimini engellemek için bir bilgi kodlama yöntemi. Veriler kodlanınca, işlem bir “anahtar” ve matematik algoritmaları kullanır. Şifrelenen bilgilerin şifresi doğru anahtar olmadan çözülemez. Bazen virüsler algılanmamak için şifreleme kullanır.

şifreli metin

Şifrelenmiş metin. Şifreli metin, düz metne dönüştürülene (şifresi çözülene) kadar okunamaz. Ayrıca bkz. şifreleme (sayfa 238).

T

tanımlama bilgisi

Pek çok web sitesi tarafından ziyaret edilen sayfalarla ilgili bilgileri depolamak için kullanılan ve web'de gezinen kişinin bilgisayarında depolanan küçük bir metin dosyası. Oturum açma veya kayıt bilgilerini, alışveriş sepeti bilgilerini veya kullanıcı tercihlerini içerebilir. Tanımlama bilgileri, web siteleri tarafından genellikle web sitesine önceden kaydolun veya web sitesini ziyaret eden kullanıcıları tanımlamak için kullanılır; ancak bunlar, korsanlar için bilgi kaynağı da olabilir.

tarayıcı

İnternet'te web sayfalarını görüntülemek için kullanılan program. Popüler web tarayıcıları arasında Microsoft Internet Explorer ve Mozilla Firefox sayılabilir.

TKIP

Geçici Anahtar Bütünlüğü Protokolü. Kablosuz yerel ağlar için 802.11i şifreleme standardının bir parçası. TKIP, 802.11 kablosuz yerel ağları korumak için kullanılan yeni nesil WEP'tir. TKIP, bir ileti bütünlüğü denetimi ve yeniden anahtarlama mekanizması olan pakette anahtar karıştırma özelliği sağlar ve böylece WEP kusurlarını giderir.

Truva, Truva atı

Çoğalmayan ancak bilgisayara zarar veren veya güvenliğini tehlikeye atan bir program. Genellikle birisi size Truva atı içeren e-posta gönderir; kendi kendisini e-posta ile göndermez. Truva atını, bir web sitesinden veya eşler arası ağ kurma programıyla da farkında olmadan karşıdan yükleyebilirsiniz.

tümleşik ağ geçidi

Erişim noktası (AP), yönlendirici ve güvenlik duvarı işlevlerini birleştiren bir aygıt. Bazı aygıtlar, güvenlik geliştirmeleri ve köprü kurma özellikleri de içerir.

U

U3

Siz: Basitleştirilmiş, Daha Akıllı, Mobil. Windows 2000 veya Windows XP programlarını doğrudan USB sürücüsünden çalıştırmak için bir platform. U3 girişimi, 2004 yılında M-Systems ve SanDisk tarafından gerçekleştirilmiştir ve kullanıcıların U3 programlarını bilgisayara veriler veya ayarlar yüklemeyen veya depolamadan bir Windows bilgisayarda çalıştırmalarına olanak verir.

URL

Birörnek Kaynak Konumlayıcı. İnternet adresleri için standart biçim.

USB

Evrensel Seri Veri Yolu. Modern bilgisayarlarda klavyeler ve farelerden web kameralarına, tarayıcılara ve yazıcılara kadar çok çeşitli aygıtları bağlayan sektör standardında bir bağdaştırıcı.

USB kablosuz bağdaştırıcı kartı

Bilgisayardaki USB portuna takılan kablosuz bağdaştırıcı kartı.

USB sürücüsü

Bilgisayarın USB portuna takılan küçük bellek sürücüsü. USB sürücüsü, küçük bir sabit disk gibi hareket ederek, bir bilgisayardan diğerine dosyalar aktarmayı kolaylaştırır.

V

virüs

Kendisini kopyalayabilen ve kullanıcının izni veya bilgisi olmadan bilgisayara bulaşabilen bir bilgisayar programı.

VPN

Sanal Özel Ağ. İnternet gibi bir ana bilgisayar sunucusuyla yapılandırılan özel iletişim ağı. VPN bağlantısıyla gönderilip alınan veriler şifrenir ve güçlü güvenlik özelliklerine sahiptir.

W

web bug'ları

Kendilerini HTML sayfalarına gömebilen ve yetkisiz bir kaynağın bilgisayarınızda tanımlama bilgileri ayarlamasına izin veren küçük grafik dosyaları. Bu tanımlama bilgileri, daha sonra yetkisiz kaynağa bilgi iletebilir. Web bug'ları, "web işaretleri", "piksel etiketleri", "net GIF'ler" veya "görünmez GIF'ler" olarak da adlandırılır.

web postası

Web tabanlı posta. Genellikle Microsoft Outlook gibi bilgisayar tabanlı bir e-posta istemcisiyle web tarayıcısı üzerinden erişilen elektronik posta hizmeti. Ayrıca bkz. e-posta (sayfa 231).

WEP

Kablolu Eşdeğeri Gizlilik. Wi-Fi (802.11) standardının bir parçası olarak tanımlanan şifreleme ve kimlik doğrulama protokolü. Başlangıç sürümleri, RC4 şifrelerini temel alır ve önemli açıkları vardır. WEP, bir uçtan diğerine iletilirken korunması için, telsiz dalgaları üzerinden verileri şifreleyerek güvenliği sağlamaya çalışır. Ancak WEP'in eskiden zannedildiği kadar güvenli olmadığı görülmüştür.

Wi-Fi

Kablosuz Sadakat. Wi-Fi Alliance tarafından 802.11 türünde ağlardan söz ederken kullanılan terim.

Wi-Fi Alliance

Lider kablosuz donanım ve yazılım sağlayıcılardan oluşan bir kuruluş. Wi-Fi Alliance, tüm 802.11 tabanlı ürünlerin birlikte çalışabilirliğini doğrulamayı ve Wi-Fi teriminin tüm pazarlarda bütün 802.11 tabanlı kablosuz yerel ağ ürünleri için genel marka adı olmasını teşvik etmeyi amaçlar. Bu kuruluş, sektör büyümesini teşvik etmek isteyen satıcılar için bir konsorsiyum, test laboratuvarı ve takas odası görevi görür.

Wi-Fi Certified

Wi-Fi Alliance tarafından test edilmiş ve onaylanmış olmak. Wi-Fi onaylı ürünlerin, farklı üreticilere ait olsalar bile birbirleriyle çalışabilirliği onaylanmıştır. Wi-Fi onaylı ürünü bulunan bir kullanıcı, herhangi bir markaya ait erişim noktasını (AP), başka herhangi bir markaya ait onaylı istemci donanımlarıyla birlikte kullanabilir.

WLAN

Kablosuz Yerel Ağ. Kablosuz bağlantı kullanan yerel ağ (LAN). Kablosuz yerel ağ, bilgisayarların birbirleriyle iletişim kurmasına olanak vermek için kablolar yerine yüksek frekanslı telsiz dalgaları kullanır.

WPA

Wi-Fi Korunmalı Erişim. Mevcut ve gelecekteki kablosuz yerel ağ sistemleri için veri korumasının ve erişim denetiminin düzeyini önemli ölçüde artıran bir belirtim standardı. Yazılım yükseltmesi olarak mevcut donanımın üzerinde çalışmak için tasarlanan WPA, 802.11i standardından türetilmiştir ve bununla uyumludur. Doğru şekilde yüklendiğinde, kablosuz yerel ağ kullanıcılarına verilerinin korunmaya devam edeceği ve yalnızca yetkili kullanıcıların ağa erişebilecekleri yönünde üst düzey güvence sağlar.

WPA-PSK

Güçlü şirket sınıfı güvenliğe ihtiyaç duymayan ve kimlik doğrulama sunucularına erişmeleri gerekmeyen ev kullanıcıları için tasarlanan özel WPA modu. Bu modda, ev kullanıcısı Önceden Paylaşılan Anahtar modunda Wi-Fi Korunmalı Erişim'i etkinleştirmek için, başlangıç parolasını el ile girer ve her kablosuz bilgisayardaki geçiş sözcüğünü ve erişim noktasını düzenli olarak değiştirmesi gerekir. Ayrıca bkz. WPA2-PSK (sayfa 241), TKIP (sayfa 239).

WPA2

WPA güvenlik standardının 802.11i standardını temel alan güncelleştirmesi.

WPA2-PSK

WPA-PSK'ye benzeyen ve WPA2 standardını temel alan özel WPA modu. Daha eski aygıtlar genelde her seferinde yalnızca tek bir şifreleme modunu desteklerken (tüm istemcilerin aynı şifreleme modunu kullanmaları gerekiyordu), WPA2-PSK'nin genel özelliği aygıtların çoğunlukla eşzamanlı olarak çoklu şifreleme modlarını (örneğin AES, TKIP) desteklemesidir.

Y

yayımlama

Yedeklenen bir dosyayı Internet üzerinde kullanıma açma işlemi. Yayımlanan dosyalara, Backup and Restore kitaplığında arama yaparak erişebilirsiniz.

yedekleme

Genellikle güvenli bir çevrimiçi sunucuda önemli dosyaların kopyasını oluşturmak. Karşılaştırın: arşivleme (sayfa 231).

yönlendirici

Bir ağdan diğerine veri paketleri ileten ağ aygıtı. Yönlendiriciler, gelen her paketi okur; kaynak ve hedef adreslere ve geçerli trafik koşullarına göre bunun nasıl iletileceğine karar verir. Yönlendirici bazen erişim noktası (AP) olarak da adlandırılır.

McAfee Hakkında

Merkezi Santa Clara, California'da bulunan ve İzinsiz Girişleri Engelleme ve Güvenlik Risk Yönetimi alanında dünya lideri olan McAfee, Inc., tüm dünyada sistemleri ve ağları güvence altına alan etkin ve kanıtlanmış çözümler ve hizmetler sunar. McAfee, güvenlik alanında sahip olduğu eşsiz uzmanlığı ve yeniliğe olan bağlılığıyla, ev kullanıcılarını, şirketleri, devlet sektörünü ve hizmet sağlayıcıları, saldırıları engelleme, aksaklıkları önleme, güvenliği sürekli izleme ve geliştirme olanağıyla güçlendirir.

Lisans

TÜM KULLANICILAR İÇİN BİLDİRİM: LİSANSLI YAZILIMIN KULLANIMINA YÖNELİK GENEL KOŞULLAR VE HÜKÜMLERİ ORTAYA KOYAN, SATIN ALDIĞINIZ LİSANSLA İLİŞKİLİ UYGUN YASAL ANLAŞMAYI DİKKATLE OKUYUN. LİSANSINIZIN TÜRÜNÜ BİLMİYORSANIZ, LÜTFEN YAZILIM PAKETİYLE BİRLİKTE SAĞLANAN VEYA SATIN ALMA SIRASINDA AYRICA ALDIĞINIZ SATIŞ VEYA DİĞER İLGİLİ LİSANS BELGELERİNE YA DA SİPARİŞ BELGELERİNE (KİTAPÇIK, ÜRÜN CD'SİNDEKİ DOSYA VEYA YAZILIM PAKETİNİ YÜKLEDİĞİNİZ WEB SİTESİNDEKİ DOSYA) BAŞVURUN. ANLAŞMADA YER ALAN BÜTÜN KOŞULLARI KABUL ETMİYORSANIZ, YAZILIMI YÜKLEMİYİN: UYGUNSA, ÜRÜNÜ MCAFEE, INC.'YE VEYA SATIN ALDIĞINIZ YERE İADE EDEREK PARANIZIN TAMAMINI GERİ ALABİLİRSİNİZ.

Telif Hakkı

Telif Hakkı © 2008 McAfee, Inc. Tüm Hakları Saklıdır. McAfee, Inc.'nin yazılı izni olmaksızın, bu yayımın hiçbir bölümü çoğaltılamaz, aktarılamaz, uyarlanamaz, bir çağırma sisteminde saklanamaz veya hiçbir şekilde ya da hiçbir yolla herhangi bir dile çevirisi yapılamaz. McAfee ve burada belirtilen diğer ticari markalar, ABD ve/veya diğer ülkelerde McAfee, Inc. ve/veya bağlı kuruluşlarına ait tescilli ticari markalar veya ticari markalardır. Güvenlikle bağlantılı olarak McAfee Red, McAfee markalı ürünlerden farklıdır. Burada yer alan diğer tüm tescilli veya tescilsiz ticari markalar ve telif hakkı korumalı materyal, yalnızca ilgili sahiplerinin mülkiyetindedir.

TİCARİ MARKA ÖZELLİKLERİ

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.

B Ö L Ü M 5 1

Müşteri Desteği ve Teknik Destek

SecurityCenter, kritik ve kritik olmayan korunma sorunlarını algıladığı anda bildirir. Kritik sorunlarla hemen ilgilenilmesi gerekir ve bunlar koruma durumunuzu tehlikeye atar (rengi kırmızıya döner). Kritik olmayan sorunlarla hemen ilgilenilmesi gerekmez ve bunlar koruma durumunuzu tehlikeye atabilir veya atmayabilir (sorunun türüne göre). Yeşil koruma durumuna ulaşmak için tüm kritik sorunları düzeltmeniz ve tüm kritik olmayan sorunları düzeltmeniz veya yok saymanız gerekir. Korunma sorunlarınızı belirleme konusunda yardıma ihtiyaç duyarsanız, McAfee Virtual Technician'ı çalıştırabilirsiniz. McAfee Virtual Technician hakkında ayrıntılı bilgi için McAfee Virtual Technician yardımına bakın.

Güvenlik yazılımınızı McAfee dışındaki bir ortaktan veya sağlayıcıdan satın aldıysanız, bir Web tarayıcı açın ve www.mcafeehelp.com adresine gidin. Sonra Ortak Bağlantıları altında, McAfee Virtual Technician'a erişmek için ortağınızı veya sağlayıcınızı seçin.

Not: McAfee Virtual Technician'ı yükleyip çalıştırmak için bilgisayarınızda Windows Yöneticisi olarak oturum açmanız gerekir. Aksi halde, MVT sorunlarınızı çözemeyebilir. Windows Yöneticisi olarak oturum açma hakkında ayrıntılı bilgi için Windows Yardımı'na bakın. Windows Vista™'da MVT'yi çalıştırdığınızda bir sorgu penceresi açılır. Bu durumda **Kabul Et**'i tıklatın. Virtual Technician Mozilla® Firefox ile çalışmaz.

Bu bölümde

McAfee Virtual Technician'ı kullanma 246

McAfee Virtual Technician'ı kullanma

Virtual Technician, kişisel teknik destek temsilciniz gibi çalışarak, SecurityCenter programlarınız hakkında bilgi toplar ve bilgisayarınızın korunma sorunlarını çözenize yardımcı olur. Virtual Technician'ı çalıştırdığınızda, SecurityCenter programlarınızın doğru şekilde çalıştığından emin olmak için denetim yapar. Sorunlar bulursa, Virtual Technician bunları sizin için düzeltmeyi önerir veya size bunlarla ilgili ayrıntılı bilgi verir. İşlem tamamlanınca, Virtual Technician analizinin sonuçlarını görüntüler ve gerekirse McAfee'den ek teknik destek istemenize olanak verir.

Virtual Technician, bilgisayarınızın ve dosyalarınızın güvenliğini ve bütünlüğünü korumak için kişisel ve tanımlayıcı bilgiler toplamaz.

Not: Virtual Technician hakkında ayrıntılı bilgi için Virtual Technician'da **Yardım** simgesini tıklatın.

Virtual Technician'ı başlatma

Virtual Technician, SecurityCenter programlarınız hakkında bilgi toplar ve bilgisayarınızın korunma sorunlarını çözenize yardımcı olur. Gizliliğinizi korumak için bu bilgilere kişisel ve tanımlayıcı bilgiler eklenmez.

- 1 **Ortak Görevler** altında **McAfee Virtual Technician'ı** tıklatın.
- 2 Virtual Technician'ı yüklemek ve çalıştırmak için ekran yönergelerini izleyin.

Kullanıcı Kılavuzlarını içeren ülkenize veya bölgeniz özel McAfee Destek ve Yükleme siteleri için aşağıdaki tablolara başvurun.

Destek ve Yüklemeler

Ülke/Bölge	McAfee Destek	McAfee Yüklemeler
Avustralya	www.mcafeehelp.com	au.mcafee.com/root/downloadads.asp
Brezilya	www.mcafeeajuda.com	br.mcafee.com/root/downloadads.asp
Kanada (İngilizce)	www.mcafeehelp.com	ca.mcafee.com/root/downloadads.asp
Kanada (Fransızca)	www.mcafeehelp.com	ca.mcafee.com/root/downloadads.asp?langid=48
Çin (Basitleştirilmiş Çince)	www.mcafeehelp.com	cn.mcafee.com/root/downloadads.asp
Çek Cumhuriyeti	www.mcafeenapoveda.com	cz.mcafee.com/root/downloadads.asp
Danimarka	www.mcafeehjaelp.com	dk.mcafee.com/root/downloadads.asp

Finlandiya	www.mcafeehelp.com	fi.mcafee.com/root/downlo ads.asp
Fransa	www.mcafeeaide.com	fr.mcafee.com/root/downlo ads.asp
Almanya	www.mcafeehilfe.com	de.mcafee.com/root/downlo ads.asp
Yunanistan	www.mcafeehelp.com	el.mcafee.com/root/downlo ads.asp
Macaristan	www.mcafeehelp.com	hu.mcafee.com/root/downlo ads.asp
İtalya	www.mcafeeaiuto.com	it.mcafee.com/root/downlo ads.asp
Japonya	www.mcafeehelp.jp	jp.mcafee.com/root/downlo ads.asp
Kore	www.mcafeehelp.com	kr.mcafee.com/root/downlo ads.asp
Meksika	www.mcafeehelp.com	mx.mcafee.com/root/downl oads.asp
Norveç	www.mcafeehjelp.com	no.mcafee.com/root/downlo ads.asp
Polonya	www.mcafeepomoc.com	pl.mcafee.com/root/downlo ads.asp
Portekiz	www.mcafeeajuda.com	pt.mcafee.com/root/downlo ads.asp
Rusya	www.mcafeehelp.com	ru.mcafee.com/root/downlo ads.asp
Slovakya	www.mcafeehelp.com	sk.mcafee.com/root/downlo ads.asp
İspanya	www.mcafeeayuda.com	es.mcafee.com/root/downlo ads.asp
İsveç	www.mcafeehjalp.com	se.mcafee.com/root/downlo ads.asp
Tayvan	www.mcafeehelp.com	tw.mcafee.com/root/downlo ads.asp
Türkiye	www.mcafeehelpturkey.com	tr.mcafee.com/root/downlo ads.asp
İngiltere	www.mcafeehelp.com	uk.mcafee.com/root/downlo ads.asp
Birleşik Devletler	www.mcafeehelp.com	us.mcafee.com/root/downlo ads.asp

McAfee Total Protection Kullanıcı Kılavuzları

Ülke/Bölge	McAfee Kullanıcı Kılavuzları
Avustralya	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brezilya	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Kanada (İngilizce)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Kanada (Fransızca)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
Çin (Basitleştirilmiş Çince)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
Çek Cumhuriyeti	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Danimarka	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Finlandiya	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
Fransa	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Almanya	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Yunanistan	download.mcafee.com/products/manuals/el/MTP_userguide_2008.pdf
Macaristan	download.mcafee.com/products/manuals/hu/MTP_userguide_2008.pdf
İtalya	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
Japonya	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf
Kore	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Meksika	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Hollanda	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Norveç	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Polonya	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
Portekiz	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Rusya	download.mcafee.com/products/manuals/ru/MTP_userguide_2008.pdf

Slovakya	download.mcafee.com/products/manuals/sk/MTP_userguide_2008.pdf
İspanya	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
İsveç	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Tayvan	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Türkiye	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
İngiltere	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Birleşik Devletler	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

McAfee Internet Security Kullanıcı Kılavuzları

Ülke/Bölge	McAfee Kullanıcı Kılavuzları
Avustralya	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brezilya	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Kanada (İngilizce)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Kanada (Fransızca)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
Çin (Basitleştirilmiş Çince)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
Çek Cumhuriyeti	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Danimarka	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Finlandiya	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
Fransa	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Almanya	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf
Yunanistan	download.mcafee.com/products/manuals/el/MIS_userguide_2008.pdf
Macaristan	download.mcafee.com/products/manuals/hu/MIS_userguide_2008.pdf
İtalya	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf

Japonya	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
Kore	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Meksika	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Hollanda	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Norveç	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Polonya	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portekiz	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
Rusya	download.mcafee.com/products/manuals/ru/MIS_userguide_2008.pdf
Slovakya	download.mcafee.com/products/manuals/sk/MIS_userguide_2008.pdf
İspanya	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
İsveç	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Tayvan	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Türkiye	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
İngiltere	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Birleşik Devletler	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

McAfee VirusScan Plus Kullanıcı Kılavuzları

Ülke/Bölge	McAfee Kullanıcı Kılavuzları
Avustralya	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brezilya	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Kanada (İngilizce)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Kanada (Fransızca)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
Çin (Basitleştirilmiş Çince)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
Çek Cumhuriyeti	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf

Danimarka	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Finlandiya	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
Fransa	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Almanya	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Yunanistan	download.mcafee.com/products/manuals/el/VSP_userguide_2008.pdf
Macaristan	download.mcafee.com/products/manuals/hu/VSP_userguide_2008.pdf
İtalya	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japonya	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Kore	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Meksika	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Hollanda	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Norveç	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Polonya	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Portekiz	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
Rusya	download.mcafee.com/products/manuals/ru/VSP_userguide_2008.pdf
Slovakya	download.mcafee.com/products/manuals/sk/VSP_userguide_2008.pdf
İspanya	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
İsveç	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Tayvan	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Türkiye	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
İngiltere	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Birleşik Devletler	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

McAfee VirusScan Kullanıcı Kılavuzları

Ülke/Bölge	McAfee Kullanıcı Kılavuzları
Avustralya	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brezilya	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Kanada (İngilizce)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf
Kanada (Fransızca)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
Çin (Basitleştirilmiş Çince)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
Çek Cumhuriyeti	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Danimarka	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Finlandiya	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
Fransa	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Almanya	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Yunanistan	download.mcafee.com/products/manuals/el/VS_userguide.2008.pdf
Macaristan	download.mcafee.com/products/manuals/hu/VS_userguide.2008.pdf
İtalya	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japonya	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Kore	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Meksika	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Hollanda	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Norveç	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
Polonya	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portekiz	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
Rusya	download.mcafee.com/products/manuals/ru/VS_userguide_2008.pdf

Slovakya	download.mcafee.com/products/manuals/sk/VS_userguide_2008.pdf
İspanya	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
İsveç	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Tayvan	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Türkiye	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
İngiltere	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Birleşik Devletler	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

Ülkenize veya bölgenize özel McAfee Threat Center ve Virüs Bilgisi siteleri için aşağıdaki tabloya başvurun.

Ülke/Bölge	Güvenlik Merkezi	Virüs Bilgisi
Avustralya	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brezilya	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Kanada (İngilizce)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Kanada (Fransızca)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Çin (Basitleştirilmiş Çince)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
Çek Cumhuriyeti	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Danimarka	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Finlandiya	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
Fransa	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Almanya	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Yunanistan	www.mcafee.com/us/threat_center	gr.mcafee.com/virusInfo
Macaristan	www.mcafee.com/us/threat_center	hu.mcafee.com/virusInfo
İtalya	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japonya	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Kore	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Meksika	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo

Hollanda	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Norveç	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
Polonya	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
Portekiz	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
Rusya	www.mcafee.com/us/threat_center	ru.mcafee.com/virusInfo
Slovakya	www.mcafee.com/us/threat_center	sk.mcafee.com/virusInfo
İspanya	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
İsveç	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Tayvan	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Türkiye	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
İngiltere	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Birleşik Devletler	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

Ülkenize veya bölgenize özel HackerWatch ve Virüs Bilgisi siteleri için aşağıdaki tabloya başvurun.

Ülke/Bölge	HackerWatch
Avustralya	www.hackerwatch.org
Brezilya	www.hackerwatch.org/?lang=pt-br
Kanada (İngilizce)	www.hackerwatch.org
Kanada (Fransızca)	www.hackerwatch.org/?lang=fr-ca
Çin (Basitleştirilmiş Çince)	www.hackerwatch.org/?lang=zh-cn
Çek Cumhuriyeti	www.hackerwatch.org/?lang=cs
Danimarka	www.hackerwatch.org/?lang=da
Finlandiya	www.hackerwatch.org/?lang=fi
Fransa	www.hackerwatch.org/?lang=fr
Almanya	www.hackerwatch.org/?lang=de
Yunanistan	www.hackerwatch.org/?lang=el
Macaristan	www.hackerwatch.org/?lang=hu
İtalya	www.hackerwatch.org/?lang=it
Japonya	www.hackerwatch.org/?lang=jp
Kore	www.hackerwatch.org/?lang=ko
Meksika	www.hackerwatch.org/?lang=es-mx
Hollanda	www.hackerwatch.org/?lang=nl
Norveç	www.hackerwatch.org/?lang=no
Polonya	www.hackerwatch.org/?lang=pl
Portekiz	www.hackerwatch.org/?lang=pt-pt

Rusya	www.hackerwatch.org/?lang=ru
Slovakya	www.hackerwatch.org/?lang=sk
İspanya	www.hackerwatch.org/?lang=es
İsveç	www.hackerwatch.org/?lang=sv
Tayvan	www.hackerwatch.org/?lang=zh-tw
Türkiye	www.hackerwatch.org/?lang=tr
İngiltere	www.hackerwatch.org
Birleşik Devletler	www.hackerwatch.org

Dizin

8

802.11	230
802.11a	230
802.11b	230
802.1x	230

A

Aboneliđinizi dođrulama	11
Aboneliđinizi yenileme	12
Aboneliklerinizi ynetme	11, 18
ActiveX denetimi	230
aılan pencereler	230
Adres defteri alma	123
ađ	230
ađ haritası	230
Ađ haritasına eriřme	200
Ađ haritasında ođeyi gsterme veya gizleme	201
Ađ haritasını yenileme	200
Ađ haritasıyla alıřma	200
Ađ izleme bildirimlerini yeniden etkinleřtirme	212
ađ srcs	230
Ađa eriřim izni verme	219
Ađa katılma	218
Ađdaki bilgisayarlara gvenmeyi durdurma	203
Ađı uzaktan ynetme	205
Ađın adını deđiřtirme	200, 220
Ađları izlemeyi durdurma	211
Ađlarınızı izleme	211
Akıllı nerileri devre dıřı bırakma	73
Akıllı nerileri etkinleřtirme	73
Akıllı nerileri grntleme	73
Akıllı nerileri uyarılar iin yapılandırma	72
akıllı src	230
anahtar	231
Anahtar szck filtrelemeyi devre dıřı bırakma	139
Anahtar szckler kullanarak Web sitelerini filtreleme	138, 139
Anlık ileti korumasını bařlatma	43
Anti-Spam ara ubuđundan arkadař ekleme	124
Anti-Spam ara ubuđundan bir iletiyi iřaretleme	121

Anti-Spam ara ubuđunu devre dıřı bırakma	122
Anti-Spam zellikleri	112
arabellek tařması	231
Arama ltleri	223
Arkadař olarak iřaretleme	213
Arkadařınızı dzenleme	125
Arkadařınızı el ile ekleme	124
Arkadařınızı kaldırma	126
Arkadařları ayarlama	123
Arkadařları el ile ayarlama	124
Arřiv konumunu deđiřtirme	166
Arřiv seeneklerini ayarlama	163
Arřiv Őifreleme ve sıkıřtırmayı devre dıřı bırakma	166
arřivleme	231, 241
Arřivleme dosyası trlerini ayarlama	165
Arřivleme etkinliđinizin zetini grntleme	175
Arřivlemeleri el ile alıřtırma	169
Arřivlemeye konum ekleme	164
Arřivlenen bir dosyayı ama	173
Arřivlenen bir dosyayı arama	172
Arřivlenen dosyaları geri ykleme	173
Arřivlenen dosyaları sıralama	172
Arřivlenen dosyalarla alıřma	171
Arřivleri ynetme	175

B

Backup and Restore zellikleri	160
bant geniřliđi	231
Bařka bir bilgisayara dosya gnderme	224
Bařka bir bilgisayardan dosya kabul etme	224, 225
Bařlangıta giriř ekranını gizleme	24
Bařlatma sırasında bilgisayarınızı koruma	74
Bařvuru	229
beyaz liste	231, 234
Beyaz listeden Web sitesini kaldırma	134
Beyaz listenizdeki siteleri dzenleme	134
Beyaz listeye Web sitesi ekleme	133
Bilgi uyarılarını gizleme	67
Bilgi uyarılarını gsterme ve gizleme	22
Bilgi uyarılarını gsterme veya gizleme	22
Bilgi uyarılarını ynetme	67
Bilgisayar ađ bilgilerini elde etme	103
Bilgisayar bađlantıları hakkında	86

Bilgisayar bağlantılarını yasaklama	89
Bilgisayar bağlantılarını yönetme	85
Bilgisayar bağlantısını ekleme	86
Bilgisayar bağlantısını düzenleme.....	88
Bilgisayar bağlantısını kaldırma.....	89
Bilgisayar kayıt bilgilerini elde etme	103
Bilgisayarınızı birleştirme	183
Bilgisayarınızı tarama.....	31
Bilgisayarınızı temizleme.....	179, 181
Bir ağ bilgisayarının coğrafi konumunu izleme	102
Bir aygıtı yönetme.....	207
Bir aygıtın görüntü özelliklerini değiştirme	207
Bir bilgisayarı yönetilen ağa katılmaya davet etme	202
Bir bilgisayarın koruma durumunu yönetme	206
Bir bilgisayarın koruma durumunu yönetmeyi durdurma.....	206
Bir konumu arşivlemenin dışında tutma.....	165
Bir McAfee kullanıcıasını kaldırma.....	149
Bir McAfee kullanıcıasının hesap bilgilerini düzenleme	149
Bir programa tam erişim izni verme.....	80
Bir programa yalnızca giden erişim izni verme	81
Bir programın erişimini engelleme.....	82
Bir Web sitesine izin verme	141
Bir Web sitesini engelleme.....	141
C	
Casus yazılım korumasını başlatma	42
Ç	
Çevrimiçi ortamda çocuklarınızı koruma....	137
D	
DAT.....	231
Disk Birleştirici görevi zamanlama.....	187
Disk Birleştirici görevini değiştirme	188
Disk Birleştirici görevini silme	189
DNS	231
dolaşım	231
Dosya gönderildiğinde bildirim alma.....	225
dosya parçaları.....	231
Dosya paylaşma.....	222
Dosya paylaşmayı durdurma	222
Dosya ve klasörleri parçalama	192
Dosyaları arşivleme.....	161
Dosyaları diğer bilgisayarlara gönderme.....	224
Dosyaları eksik dosyalar listesinden kaldırma	174
Dosyaları paylaşma	222

Dosyaları paylaşma ve gönderme.....	221
Dosyaları, klasörleri ve diskleri parçalama.	192
Durum ve izinleri yönetme	206
düğüm	231
düz metin	231

E

EasyNetwork özellikleri	216
EasyNetwork'ü açma	217
EasyNetwork'ü ayarlama	217
Ebeveyn Denetimleri özellikleri.....	136
Ek koruma kullanma.....	41
eklenti	232
Eksik dosyaları yerel arşivden geri yükleme	174
e-posta.....	232, 240
E-posta filtreleme	121
E-posta iletilerini McAfee'ye raporlama.....	131
e-posta istemcisi	232
E-posta korumasını başlatma.....	43
erişim noktası (AP).....	232
ESS	232
etki alanı	232
Etki alanı ekleme	125
Etki alanını düzenleme	126
etkin nokta	232
ev ağı	230, 232

F

Filtreleme düzeyini değiştirme	115
Filtreleme seçeneklerini ayarlama	114
Filtrelenen bir Web sitesini güncelleştirme	140
Filtrelenen bir Web sitesini kaldırma	140
Filtrelenen e-posta ile çalışma	131
Filtrelenen Web postasında olay görüntüleme	132
Filtrelenen Web postasını görüntüleme, verme veya silme	132
Filtrelenen Web siteleri	139, 143
Firewall ayarlarını geri yükleme.....	78
Firewall güvenliğini iyileştirme.....	74
Firewall güvenlik düzeylerini yönetme	70
Firewall Koruma Durumu ayarlarını yapılandırma.....	76
Firewall korumasını yapılandırma	69
Firewall'u anında kilitleme	77
Firewall'u Başlatma	63
Firewall'u kilitleme ve geri yükleme	77
Firewall'un kilidini anında açma.....	77

G

geçici dosya	232
--------------------	-----

Gelen Olaylar günlüğünden bir bilgisayarı ekleme.....	87
Gelen Olaylar günlüğünden bir bilgisayarı izleme.....	104
Gelen Olaylar günlüğünden bir bilgisayarı yasaklama	91
Gelen olayları görüntüleme	101
Gelen ve giden trafiği analiz etme.....	106
Genel güvenlik olayı istatistiklerini görüntüleme	102
Genel Internet port etkinliğini görüntüleme	102
gerçek zamanlı tarama.....	232
Gerçek zamanlı tarama seçeneklerini ayarlama	38, 46
Gerçek zamanlı virüsten korumayı durdurma	47
Geri Dönüşüm Kutusu.....	233
Giden Olaylar günlüğünden program bilgilerini alma.....	84
Giden Olaylar günlüğünden tam erişim izni verme	81
Giden Olaylar günlüğünden yalnızca giden erişim izni verme	82
Giden olayları görüntüleme.....	81, 101
Görev zamanlama.....	185
Güncelleştirmeleri denetleme.....	13, 15
Günlüğe kaydetme, izleme ve analiz.....	99
Güvenilenler listelerini kullanma	57
Güvenilenler listelerini yönetme	57
güvenilenler listesi.....	233
Güvenilenler listesi türleri hakkında	58, 59
Güvenlik açıklarını düzeltme	208
güvenlik duvarı.....	233
Güvenlik duvarı korumasını başlatma.....	63
Güvenlik duvarı korumasını durdurma	64
Güvenlik düzeyini Görünmez seçeneğine ayarlama.....	71
Güvenlik düzeyini Otomatik seçeneğine ayarlama.....	72
Güvenlik düzeyini Standart seçeneğine ayarlama.....	71
Güvenlik iletilerini gizleme.....	25
H	
HackerWatch dersini başlatma	110
harici sabit disk.....	233
hileli erişim noktası	233
hizmet reddi (DOS) saldırısı.....	233
I	
Internet güvenliği hakkında bilgi alma.....	109
Internet trafiğini izleme	102, 105
IP adresi.....	233

IP hilesi	234
-----------------	-----

i

içerik derecelendirme grubu	233
içerik derecelendirme grubunu ayarlama... 143, 144, 145	
ileti kimlik doğrulama kodu (MAC).....	233
intranet	233
İstatistiklerle Çalışma	102
isteğe bağlı tarama	234
istemci.....	234
İzinsiz Giriş Tespiti Olayları günlüğünden bir bilgisayarı izleme	104
İzinsiz Giriş Tespiti Olayları günlüğünden bir bilgisayarı yasaklama	92
İzinsiz giriş tespiti olaylarını görüntüleme .	101
İzinsiz giriş tespitini yapılandırma.....	76
izleme konumları	234
İzlenen bir IP adresini izleme	105
izlenen dosya türleri.....	234

K

kaba kuvvet saldırısı	234
kablosuz bağdaştırıcı	234
kara liste.....	231, 234
Karakter kümesi filtrelerini uygulama.....	116
karantina	234
Karantinadaki dosyalarla çalışma	36, 37
Karantinadaki programlar ve tanımlama bilgileriyle çalışma.....	37
kayıt defteri.....	234
kısayol.....	235
kimlik doğrulama.....	230, 235
Kişisel bilgileri koruma	154
Kişisel filtre belirtme	117, 118, 119
Kişisel filtre ekleme.....	117
Kişisel filtreleri kullanma	117
Kişisel filtreyi düzenleme	118
Kişisel filtreyi kaldırma	118
komut dosyası.....	235
Komut dosyası tarama korumasını başlatma	42
Koruma durumu hakkında bilgi.....	7, 8, 9
Koruma hizmetleri hakkında bilgi	10
Koruma kategorileri hakkında bilgi.....	7, 9, 27
Koruma sorunlarını el ile onarma	18
Koruma sorunlarını onarma.....	8, 18
Koruma sorunlarını onarma veya yok sayma 8, 17	
Koruma sorunlarını otomatik olarak onarma	18
Koruma sorunlarını yok sayma.....	19
Koruma sorununu yok sayma	19
köke inme	235
Kullanıcıları yapılandırma	147

Kullanıcının içerik derecelendirme grubunu ayarlama.....	143
Kullanılabilir ağ yazıcısı yükleme.....	228

L

LAN.....	232, 235
launchpad	235
Lisans	243

M

MAC adresi	235
MAPI.....	235
McAfee Anti-Spam	111
McAfee EasyNetwork	215
McAfee Hakkında	243
McAfee hesabınıza erişme	11
McAfee kullanıcılarıyla çalışma	148, 151
McAfee kullanıcısı ekleme.....	150
McAfee Network Manager.....	195
McAfee Parental Controls.....	135
McAfee Personal Firewall.....	61
McAfee QuickClean.....	177
McAfee SecurityCenter.....	5
McAfee Shredder	191
McAfee Total Protection.....	3
McAfee Virtual Technician'ı kullanma	246
McAfee VirusScan	29
McAfee Yedekleme ve Geri Yükleme.....	159
McAfee yönetici parolasını alma	148
McAfee yönetici parolasını değiştirme	148
Mevcut sistem hizmeti portuna erişim izni verme	95
Mevcut sistem hizmeti portuna erişimi engelleme.....	95
MSN	235
Müşteri Desteği ve Teknik Destek	245

N

Network Manager özellikleri.....	196
Network Manager simgeleri hakkında bilgi	197
NIC	235
numara çeviriciler.....	235

O

olası istenmeyen program (PUP).....	236
Olası istenmeyen programlarla çalışma	36
Olası uygunsuz Web resimlerini filtreleme	144
olay	236
Olay günlüğü ayarlarını yapılandırma.....	100
Olay Günlüğü Kaydetme.....	100
Olayları görüntüleme.....	18, 27
ortadaki adam saldırısı.....	236
Otomatik arşivlemeleri zamanlama.....	167

Otomatik arşivlemeyi kesme	168
Otomatik güncelleştirmeleri devre dışı bırakma	15
Otomatik güncelleştirmeleri yapılandırma ...	14
Oyun oynarken bilgi uyarılarını gösterme veya gizleme	23
Oyun sırasında uyarıları görüntüleme	67

Ö

Öğenin ayrıntılarını görüntüleme	201
önbellek	236
Özel tarama seçeneklerini ayarlama .	39, 48, 49

P

parola	236
Parola ekleme	158
parola kasası	236
Parola Kasası parolanızı sıfırlama	156
Parola Kasası'nı ayarlama.....	156
Parola Mahzeni parolanızı değiştirme	157
Parolaları koruma	155
Parolayı değiştirme	158
Parolayı kaldırma.....	157
Paylaşılan bir dosyayı arama	223
Paylaşılan dosyayı kopyalama.....	223
paylaşılan şifre	236
Paylaşılan yazıcılarla çalışma.....	228
paylaştırma.....	236
PCI kablosuz bağdaştırıcı kartı.....	236
PC'nizi tarama.....	32, 39
Personal Firewall özellikleri.....	62
phishing	237
Phishing korumasını devre dışı bırakma....	134
Phishing korumasını yapılandırma	133
Ping isteği ayarlarını yapılandırma	75
POP3	237, 238
port.....	237
PPPoE	237
Program bant genişliğini izleme	107
Program bilgilerini alma	84
Program etkinliğini izleme	107
Program iznini kaldırma	83
Programlar hakkında bilgi alma.....	84
Programlara İnternet erişim izni verme	80
Programlara yalnızca giden erişim izni verme	81
Programları ve izinleri yönetme	79
Programların erişim izinlerini kaldırma.....	83
Programların İnternet erişimini engelleme ...	82
protokol.....	237
proxy	237
proxy sunucusu	237

Q

QuickClean görevi zamanlama	185
QuickClean görevini deęiřtirme.....	186
QuickClean görevini silme.....	187
QuickClean özellikleri.....	178

R

RADIUS	236, 237
--------------	----------

S

Saldırılan olarak iřaretleme	212
savaş sürücüsü.....	237
SecurityCenter özellikleri.....	6
SecurityCenter'ı güncelleřtirme.....	13
SecurityCenter'ı kullanma	7
senkronize etme.....	238
Shredder özellikleri	192
sıkıřtırma	238
sistem geri yükleme noktası	238
Sistem hizmeti portlarını yapılandırma	94
Sistem hizmeti portunu deęiřtirme.....	97
Sistem hizmeti portunu kaldırma	98
Sistem hizmetlerini yönetme	93
Sistem Koruması	238
Sistem Koruması seçeneklerini kullanma	51
Sistem Koruması seçeneklerini yapılandırma.....	53
Sistem Koruması türleri hakkında.....	54
Sistem Koruması'nı etkinleřtirme.....	53
SMTP	238
solucan.....	238
Son Olaylar günlüğünden eriřimi engelleme	83
Son Olaylar günlüğünden tam eriřim izni verme	81
Son Olaylar günlüğünden yalnızca giden eriřim izni verme	82
Son olayları görüntüleme	27, 100
sözlük saldırısı.....	238
Spam algılamayı yapılandırma	113
Spam iřleme ve iřaretleme biçimini deęiřtirme	115, 117
Spam korumasını devre dıřı bırakma	119
SSID	238
SSL.....	238
standart e-posta hesabı.....	238
sunucu.....	238

ř

řifreleme	231, 239
řifreli metin	239

T

Tam ve hızlı arřivlemeleri çalıştırma	167
---	-----

tanımlama bilgisi	239
Tarama sonuçlarını görüntüleme	34
Tarama sonuçlarıyla çalışma	35
Tarama türleri	33, 38
Tarama zamanlama.....	39, 50
tarayıcı	239
Telif Hakkı.....	244
TKIP	239, 241
Trafik Analizi grafięi hakkında	106
Truva, Truva atı	239
Tüm diski parçalama	193
Tüm olayları görüntüleme	27
tümleřik aę geçidi	239

U

U3	239
UDP ayarlarını yapılandırma	75
URL	239
USB	240
USB kablosuz baędařtırıcı kartı	240
USB sürücüsü	230, 240
Uyarı seçeneklerini yapılandırma	23
Uyarılar hakkında	66
Uyarılarla birlikte sesi açma	23
Uyarılarla çalışma.....	14, 21, 65
Uzak bilgisayarlara McAfee güvenlik yazılımı yükleme.....	209

Ü

Ürününüzü etkinleřtirme	11
-------------------------------	----

V

Virtual Technician'ı başlatma	246
VirusScan özellikleri	30
virüs	240
Virüs saldırısı uyarılarını gizleme	24
Virüsler ve Truva atlarıyla çalışma.....	36
Virüsten korumayı ayarlama.....	31, 45
VPN	240

W

web bug'ları	240
Web posta hesabı bilgilerini anlama... ..	128, 129
Web posta hesabı ekleme	128
Web posta hesabını düzenleme.....	128
Web posta hesabını kaldırma.....	129
Web posta hesaplarınızı ayarlama	127
web postası	232, 240
Web sitelerini anahtar sözcüklere göre engelleme	138
Web'de bilgileri koruma	153
Web'de gezinme saat sınırlarını ayarlama ..	142
WEP.....	231, 240

Wi-Fi	240
Wi-Fi Alliance	240
Wi-Fi Certified	241
Windows kullanıcılarına geçme	150
Windows kullanıcılarıyla çalışma	151
WLAN	241
WPA	231, 241
WPA2	231, 241
WPA2-PSK	231, 241
WPA-PSK	231, 241

Y

Yasaklanan bilgisayar bağlantısı ekleme	89
Yasaklanan bilgisayar bağlantısını düzenleme	90
Yasaklanan bilgisayar bağlantısını kaldırma	91
Yaşa uygun aramayı etkinleştirme	145, 146
yayımlama	241
Yazıcı paylaşmayı durdurma	228
Yazıcıları paylaşma	227
yedekleme	231, 241
Yeni Arkadaşlar algılamayı durdurma	213
Yeni bir programa tam erişim izni verme	80
Yeni bir programın erişimini engelleme	83
Yeni bir sistem hizmeti portunu yapılandırma	96
Yerel arşivden bir dosyanın eski sürümünü geri yükleme	174
Yerel arşivi devre dışı bırakma	162
Yerel arşivi etkinleştirme	162
Yerel arşivi etkinleştirme ve devre dışı bırakma	162
Yerel arşivleme gezginini kullanma	172
Yok sayılan sorunları gösterme veya gizleme	19
Yönetilen ağa katılma	201
Yönetilen ağı terk etme	220
Yönetilen bir ağ kurma	199
Yönetilen bir ağa katılma	202, 218, 220
Yönetilen bir bilgisayarın izinlerini değiştirme	207
yönlendirici	241