Avira

Professional Security

Kullanıcı Kılavuzu

Ticari Markalar ve Telif Hakkı

Ticari Markalar

Windows, Microsoft Corporation'ın ABD ve diğer ülkelerdeki tescilli ticari markasıdır.
Diğer tüm marka ve ürün adları, ilgili sahiplerinin ticari markaları veya tescilli ticari markalarıdır.
Korumalı ticari markalar bu kılavuzda bu şekilde işaretlenmemiştir. Ancak bu, söz konusu markaların serbestçe kullanılabileceği anlamına gelmez.

Telif hakkı bilgileri

Avira Professional Security için üçüncü taraf sağlayıcıların sunduğu kod kullanılmıştır. Kodu kullanımımıza sundukları için telif hakkı sahiplerine teşekkür ederiz.
Telif hakkıyla ilgili ayrıntılı bilgi için lütfen Avira Professional Security ürününün program yardımı'nda Üçüncü Taraf Lisansları.

Son Kullanıcı Lisans Sözleşmesi - EULA

http://www.avira.com/tr/license-agreement

Gizlilik İlkesi

http://www.avira.com/tr/general-privacy

İçindekiler

1. Giriş

Avira ürününüz, bilgisayarınızı virüslere, solucanlara, Truva atlarına, reklam yazılımlarına, casus yazılımlara ve diğer risklere karşı korur. Bu kılavuzda tüm bunlar, virüsler veya zararlı yazılımlar ve istenmeyen programlar olarak anılır.

Kılavuzda, programın kurulumu ve çalışması açıklanmaktadır.

Daha fazla seçenek ve bilgi için lütfen web sitemizi ziyaret edin:
http://www.avira.com/tr

Avira web sitesi şunları yapmanıza olanak sağlar:

- diğer Avira masaüstü programlarıyla ilgili bilgilere erişme
- en son Avira masaüstü programlarını karşıdan yükleme
- en son ürün kılavuzlarını PDF biçiminde karşıdan yükleme
- ücretsiz destek ve onarım araçlarını karşıdan yükleme
- sorun giderme için kapsamlı bilgi bankamıza ve SSS'lere erişme
- ülkeye özel destek adreslerine erişme.

Avira Ekibiniz

1.1 Simgeler ve vurgular

Aşağıdaki simgeler kullanılır:

Simge / gösterge	Açıklama
✓	Bir eylem yürütülmeden önce yerine getirilmesi gereken bir koşulun önüne yerleştirilir.
▸	Uyguladığınız bir eylem adımının önüne yerleştirilir.
↪	Önceki eylemi takip eden bir olayın önüne yerleştirilir.
Uyarı	Kritik veri kaybı olabileceği durumlara ilişkin bir uyarının önüne yerleştirilir.

Not	Özellikle önemli bir bilgi bağlantısının veya Avira ürününüzün kullanımını kolaylaştıran bir ipucunun önüne yerleştirilir.

Aşağıdaki vurgular kullanılır:

Vurgu	Açıklama
İtalik	Dosya adı veya yol verileri.
	Görüntülenen yazılım arabirimi öğeleri (örn. pencere bölümü veya hata mesajı).
Kalın	Tıklatılabilir yazılım arabirimi öğeleri (örn. menü öğesi, gezinti alanı, seçenek kutusu veya düğme).

2. Ürün bilgileri

Bu bölümde, Avira ürününüzün satın alınması ve kullanımıyla ilgili tüm bilgiler bulunur:

- bkz. Bölüm: Teslim kapsamı
- bkz. Bölüm: Sistem gereksinimleri
- bkz. Bölüm: Lisanslama ve Yükseltme
- bkz. Bölüm: Lisans Yöneticisi

Avira ürünleri, bilgisayarınızı virüslere, zararlı yazılımlara, istenmeyen programlara ve diğer tehlikelere karşı korumak için güvenebileceğiniz kapsamlı ve esnek araçlardır.

▸ Lütfen şu bilgileri unutmayın:

Uyarı
Değerli verilerin kaybedilmesi genellikle ciddi sonuçlara yol açar. En iyi virüs koruma programı bile veri kaybına karşı yüzde yüz koruma sağlayamaz. Güvenlik amacıyla verilerinizin düzenli olarak kopyalarını (Yedeklerini) oluşturun.

Not
Bir program yalnızca güncelse virüslere, zararlı yazılımlara, istenmeyen programlara ve diğer tehlikelere karşı güvenilir ve etkili koruma sağlayabilir. Avira ürününüzün otomatik güncellemelerle güncel olduğundan emin olun. Programı uygun şekilde yapılandırın.

2.1 Teslim kapsamı

Avira ürününüz şu işlevlere sahiptir:

- Programın tamamının izlenmesi, yönetilmesi ve denetlenmesi için Kontrol Merkezi
- Kullanıcı dostu standart ve gelişmiş seçenekler ve bağlama duyarlı yardım ile merkezi yapılandırma
- Tüm bilinen virüs ve zararlı yazılım türleri için profil denetimli ve yapılandırılabilir tarama ile Sistem Tarayıcı (istek üzerine tarama)
- Windows Kullanıcı Hesabı Denetimi ile tümleştirme, yönetici hakları gerektiren görevler yürütmenize olanak tanır.
- Tüm dosya erişimi girişimlerinin sürekli izlenmesi için Gerçek Zamanlı Koruma (erişim taraması)

- Program eylemlerinin kalıcı olarak izlenmesi için Proaktif bileşeni (yalnızca 32 bit sistemler için)
- E-posta eklerinin kontrolü de dahil olmak üzere e-postaların virüs ve zararlı yazılımlara karşı kalıcı olarak denetlenmesi için EPosta Koruması (POP3 Tarayıcı, IMAP Tarayıcı ve SMTP Tarayıcı)
- HTTP protokolü (80, 8080, 3128 numaralı bağlantı noktalarının izlenmesi) kullanarak Internet'ten aktarılan veri ve dosyaların izlenmesi için Web Koruması
- Şüpheli dosyaları yalıtmak ve işlemek için tümleşik karantina yönetimi
- Bilgisayar sisteminize kurulu gizli zararlı yazılımları algılamak için Kök kullanıcı takımı koruması (kök kullanıcı takımları)
  (Windows XP 64 bit ile birlikte kullanılamaz)
- Algılanan virüs ve zararlı yazılımlarla ilgili ayrıntılı bilgilere Internet aracılığıyla doğrudan erişim
- Internet veya intranet üzerinde web sunucusu aracılığıyla Tekli Dosya Güncellemesi ve artımlı VDF güncellemeleri yoluyla program, virüs tanımları ve arama motoruna yönelik basit ve hızlı güncellemeler
- Lisans Yöneticisi'nde kullanıcı dostu lisanslama
- Güncelleme veya tarama gibi bir defalık ya da yinelenen işleri planlamak için Tümleşik Zamanlayıcı
- Buluşsal yöntem tarama yöntemini içeren yenilikçi tarama teknolojisi (tarama motoru) aracılığıyla son derece yüksek virüs ve zararlı yazılım algılaması
- İç içe geçmiş arşivlerin algılanması ve akıllı uzantı algılaması gibi tüm geleneksel arşiv türlerinin algılanması
- Yüksek performanslı çoklu kullanım işlevi (birden çok dosyanın eşzamanlı yüksek hızlı taraması)
- Bilgisayarınızı Internet'ten veya başka bir ağdan gelebilecek yetkisiz erişime ve yetkisiz kullanıcıların Internet'e/ağa yetkisiz erişimine karşı korumaya yönelik Güvenlik Duvarı

2.2 Sistem gereksinimleri

2.2.1 Sistem gereksinimleri Avira Professional Security

Avira Professional Security, sistemin başarıyla kullanılması için aşağıdaki gereksinimlere sahiptir.

İşletim sistemi

- Windows 8, en yeni SP (32 veya 64 bit) veya
- Windows 7, en yeni SP (32 veya 64 bit) veya
- Windows XP, en yeni SP (32 veya 64 bit)

Donanım

- Pentium işlemcili veya sonraki sürümlere sahip bilgisayar, en az 1 GHz
- En az 150 MB boş sabit disk bellek alanı (geçici depolama için karantina kullanılıyorsa daha fazla)
- Windows 8, Windows 7 en az 1024 MB RAM
- Windows XP'de en az 512 MB RAM

Diğer gereksinimler

- Program kurulumu için: Yönetici hakları
- Tüm kurulumlar için: Windows Internet Explorer 6.0 veya sonraki sürümler
- Gerekli olduğunda İnternet bağlantısı (bkz. Kurulum için hazırlık)

2.2.2 Yönetici hakları (Windows Vista'dan itibaren)

Windows XP'de birçok kullanıcı, yönetici haklarıyla çalışır. Ancak virüslerin ve istenmeyen programların bilgisayarlara sızması kolay olduğundan, güvenlik açısından bakıldığında bu önerilmez.

Bu nedenle Microsoft, "Kullanıcı Hesabı Denetimini" (UAC) sunmuştur. Kullanıcı Hesabı Denetimi şu işletim sistemlerinin bir parçasıdır:

- Windows Vista
- Windows 7
- Windows 8

Kullanıcı Hesabı Denetimi, yönetici olarak oturum açan kullanıcılar için daha fazla koruma sağlar. Bu nedenle, bir yönetici ilk olarak yalnızca normal kullanıcı ayrıcalıklarına sahiptir. Yönetici haklarının gerektiği eylemler, işletim sisteminde bir bilgi simgesiyle açıkça işaretlenir. Ayrıca kullanıcı, gerekli eylemi açıkça onaylamalıdır. Yalnızca bu izin alındıktan sonra işletim sistemi tarafından ayrıcalıklar artırılır ve yönetici görevi gerçekleştirilir.

Avira Professional Security ürünü, bazı eylemler için yönetici hakları gerektirir. Bu eylemler şu sembolle işaretlenir:  . Bu sembol bir düğme üzerinde de görüntülenirse, bu eylemi gerçekleştirmek için yönetici hakları gerekir. Geçerli kullanıcı hesabınız yönetici haklarına sahip değilse, Kullanıcı Hesabı Denetiminin Windows iletişim kutusu, yönetici parolasını girmenizi ister. Yönetici parolanız yoksa, bu eylemi gerçekleştiremezsiniz.

2.2.3 Diğer programlarla uyumsuzluk

Avira Professional Security

Avira Professional Security şu anda aşağıdaki ürünlerle birlikte kullanılamaz:

- PGP Desktop Home
- PGP Desktop Professional 9.0

- CyberPatrol

Yukarıda bahsedilen ürünlerdeki bir hata, Avira Professional Security ürününde Avira E-Posta Koruması (POP3 tarayıcı) ürününün çalışmamasına veya sistemin kararsız hale gelmesine neden olabilir. Avira, sorunu çözmek için PGP ve CyberPatrol ile birlikte çalışmaktadır. Bir çözüm bulununcaya kadar, Avira Professional Security ürününü kurmadan önce bahsedilen ürünleri mutlaka kaldırmanızı öneririz.

Avira Web Koruması

Avira Web Koruması, aşağıdaki ürünlerle uyumlu değildir:

- Bigfoot Networks Killer Ethernet Controller
- - Tennyson Maxwell, Inc şirketinin Teleport Pro ürünü
- - SCM Microsystems şirketinin CHIPDRIVE® Time Recording ürünü
- - Microsoft'un MSN Messenger ürünü

Bu ürünler tarafından gönderilen veya istenen veriler, Avira Web Koruması tarafından yok sayılır.

> **Not**
> Bir posta sunucusu (örn. AVM KEN, Exchange) önceden bilgisayarda kuruluysa, Avira E-posta Koruması çalışmaz.

Not
Avira Server Security ve Avira Professional Security aynı bilgisayarda aynı anda kurulu olmamalıdır.

2.3 Lisanslama ve Yükseltme

2.3.1 Lisanslama

Avira ürününüzü kullanabilmeniz için bir lisans gerekir. Böylece lisans koşullarını kabul edersiniz.

Lisans, bir *.KEY* dosyası biçiminde dijital bir lisans aracılığıyla verilir. Bu dijital lisans dosyası, kişisel lisansınızın anahtarıdır. Size hangi programın lisansının ve kadar süreyle verildiğine dair tam ayrıntıları içerir. Bu nedenle dijital lisans dosyası, birden çok ürünün lisansını içerir.

Avira ürününüzü İnternet'ten veya bir program CD/DVD'si aracılığıyla satın aldıysanız, dijital lisans dosyası size e-postayla gönderilir. Lisans anahtarını programın kurulumu esnasında yükleyebilir veya daha sonra Lisans Yöneticisi'nde kurabilirsiniz.

2.3.2 Bir lisansın süresini uzatma

Lisansınızın süresi bitmek üzereyse, Avira size lisansınızı uzatmanızı hatırlatan bir slide-up gönderir. Bunu yapmak için bir bağlantıyı tıklattığınızda Avira çevrimiçi mağazaya yönlendirilirsiniz. altındaki Lisans Yöneticisi üzerinden de uzattırabilirsiniz

Avira'nın lisanslandırma portalından kayıt yaptırdıysanız, lisansınızı ayrıca doğrudan çevrimiçi, **Lisansa Genel Bakış** üzerinden uzatabilir veya lisansınızın otomatik olarak yenilenmesini seçebilirsiniz.

> **Not**
> Avira ürününüz AMC ile yönetiliyorsa, yükseltme işlemini yöneticiniz gerçekleştirir. Verilerinizi kaydetmeniz ve bilgisayarınızı yeniden başlatmanız istenir, bunu yapmazsanız korunmazsınız.

2.3.3 Lisans yöneticisi

Avira Professional Security Lisans Yöneticisi, Avira Professional Security lisansının çok kolay bir şekilde kurulmasını sağlar.

Avira Professional Security Lisans Yöneticisi

Dosya yöneticinizde veya etkinleştirme e-postasında lisans dosyasını çift tıklatıp seçerek ve ekrandaki ilgili yönergeleri izleyerek lisansı kurabilirsiniz.

Not
Avira Professional Security Lisans Yöneticisi, karşılık gelen lisansı ilgili ürün klasörüne otomatik olarak kopyalar. Bir lisans zaten varsa, varolan lisans dosyasının değiştirileceğine ilişkin bir not görüntülenir. Bu durumda, yeni lisans dosyası, varsayılan dosyanın üzerine yazılır.

3. Kurulum ve kaldırma

Bu bölüm Avira Professional Security ürününün kurulumu ile ilgili bilgi içerir.

3.1 Kurulum için hazırlık

✓ Kurulumdan önce, bilgisayarınızın tüm minimum Sistem Gereksinmelerini karşılayıp karşılamadığını kontrol edin.
✓ Çalışan tüm uygulamaları kapatın.
✓ Başka virüs koruma çözümlerinin kurulu olmadığından emin olun. Çeşitli güvenlik çözümlerinin otomatik koruma işlevleri birbiriyle etkileşim kurabilir. (otomatik seçenekler için, bkz. Uyumsuz yazılımların kaldırılması).
✓ Gerekirse, Avira SearchFree Araç Çubuğu'nu kurmadan önce lütfen önceden kurulu olan arama araç çubuklarını kaldırın. Aksi takdirde, Avira Araç Çubuğu 'nu kuramazsınız.
✓ Bir İnternet bağlantısı kurun.

- Aşağıdaki kurulum adımlarının gerçekleştirilmesi için Internet bağlantısı gerekir:
  - Kurulum programı aracılığıyla geçerli program dosyasını, tarama motorunu ve en son virüs tanımı dosyalarını karşıdan yükleme (internet tabanlı kurulum için)
  - Programı etkinleştirme
  - Kullanıcı olarak kaydolma
  - Gerekirse, tamamlanan kurulumdan sonra güncelleme gerçekleştirin

✓ Programı etkinleştirmek istediğiniz zaman Avira Professional Security ürününüzün etkinleştirme kodunu veya lisans dosyasını elinizin altında bulundurun Bu bilgi iç kısma basılmıştır.
✓ Ürün etkinleştirmesi veya kaydedilmesi için Avira Professional Security ürününüz, Avira sunucularıyla iletişim kurmak için HTTP protokolünü, 80 numaralı bağlantı noktasını (web iletişimi), SSL şifreleme protokolü ve 443 numaralı bağlantı noktasını kullanır. Bir güvenlik duvarı kullanıyorsanız, lütfen gerekli bağlantıların ve/veya gelen ya da giden verilerin güvenlik duvarı tarafından engellenmediğinden emin olun.

3.2 Çevrimiçiyken CD'den kurulum

- Avira Professional Security CD'sini takın.

  Otomatik başlat etkinse dosyaları görmek için **Klasör Aç** seçeneğine tıklayın.
  VEYA

  CD sürücünüze gözatın, AVIRA öğesine sağ tıklatın ve dosyaları görmek için **Klasör Aç** seçeneğini seçin.

  Autorun.exe dosyasını çift tıklatın.

  CD menüsünden kurmak için çevrimiçi sürümü seçin.

  Program uyumsuz yazılımlar için sistemi tarar (daha fazla bilgi için: Uyumsuz yazılımları kaldırma).

  Welcome ekranında **İleri** düğmesini tıklatın.

  Dili seçin ve **İleri** düğmesini tıklatın. Kurulum için gerekli olan tüm dosyalar, Avira web sunucularından karşıdan yüklenir.

  Bir kurulum türünün seçilmesi ile devam edin.

3.3 Çevrimdışıyken CD'den kurulum

- Avira Professional Security CD'sini takın.

  Otomatik başlat etkinse dosyaları görmek için **Klasör Aç** seçeneğine tıklayın.
  VEYA

  CD sürücünüze gözatın, AVIRA öğesini sağ tıklatın ve dosyaları görmek için **Klasör Aç** seçeneğini seçin.

  Autorun.exe dosyasını çift tıklatın.

  CD menüsünden kurmak için çevrimdışı sürümü seçin.

  Program uyumsuz yazılımlar için sistemi tarar (daha fazla bilgi için: Uyumsuz yazılımları kaldırma).

  Kurulum dosyası ayıklanır. Kurulum yordamı başlatılır.

  Bir kurulum türünün seçilmesi ile devam edin.

3.4 Avira Mağazası'ndan karşıdan yüklenen yazılımın kurulumu

- www.avira.com/download adresine gidin.

  Ürünü seçin ve **Karşıdan Yükle**'ye tıklatın.

  Karşıdan yüklenen dosyayı sisteminize kaydedin.

  avira_professional_security_(en).exe kurulum dosyasına çift tıklatın.

  Kullanıcı Hesabı Kontrol penceresi açılırsa Evet'e tıklatın

Program uyumsuz yazılımlar için sistemi tarar (daha fazla bilgi için: Uyumsuz yazılımları kaldırma).

Kurulum dosyası ayıklanır. Kurulum yordamı başlatılır.

Bir kurulum tipinin seçilmesi ile devam edin.

3.5 Uyumsuz yazılımları kaldırma

Avira Professional Security ürünü bilgisayarınızdaki olası uyumsuz yazılımları arayacaktır. Olası uyumsuz yazılım algılanırsa, Avira Professional Security bu programların bir listesini oluşturur. Bilgisayarınızın kararlılığını tehlikeye atmamak için bu yazılım programlarını kaldırmanız önerilir.

- Bilgisayarınızdan otomatik olarak kaldırılması gereken bu programlar için listeden onay kutularını seçin ve **İleri**'yi tıklatın.

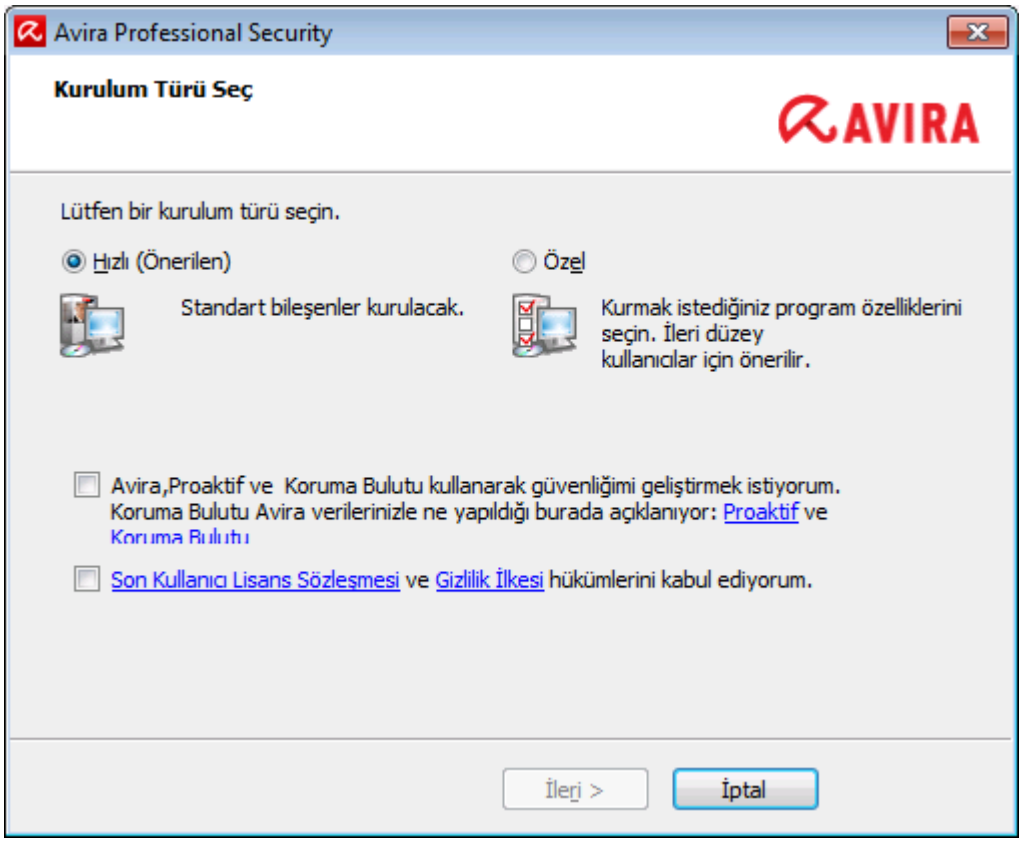
  Bazı ürünler için kaldırmanın elle onaylanması gerekir.

  Bu programları seçin ve **İleri**'yi tıklatın.

  Seçilen programlardan bir veya daha fazlasının kaldırma işlemi bilgisayarınızın yeniden başlatılmasını gerektirebilir. Sistem yeniden başlatıldıktan sonra kurulum başlar.

3.6 Bir kurulum türünün seçilmesi

Kurulum sırasında, kurulum sihirbazında bir kurulum türü seçebilirsiniz. Kurulum sihirbazı size kurulum boyunca sorunsuzca yol göstermek için tasarlanmıştır.



İlgili Konular:

- bkz. Ekspres bir Kurulum Yapma
- bkz. Özel bir Kurulum Yapma

3.6.1 Ekspres bir kurulum yapma

Ekspres kurulum önerilen kurulum yordamıdır.

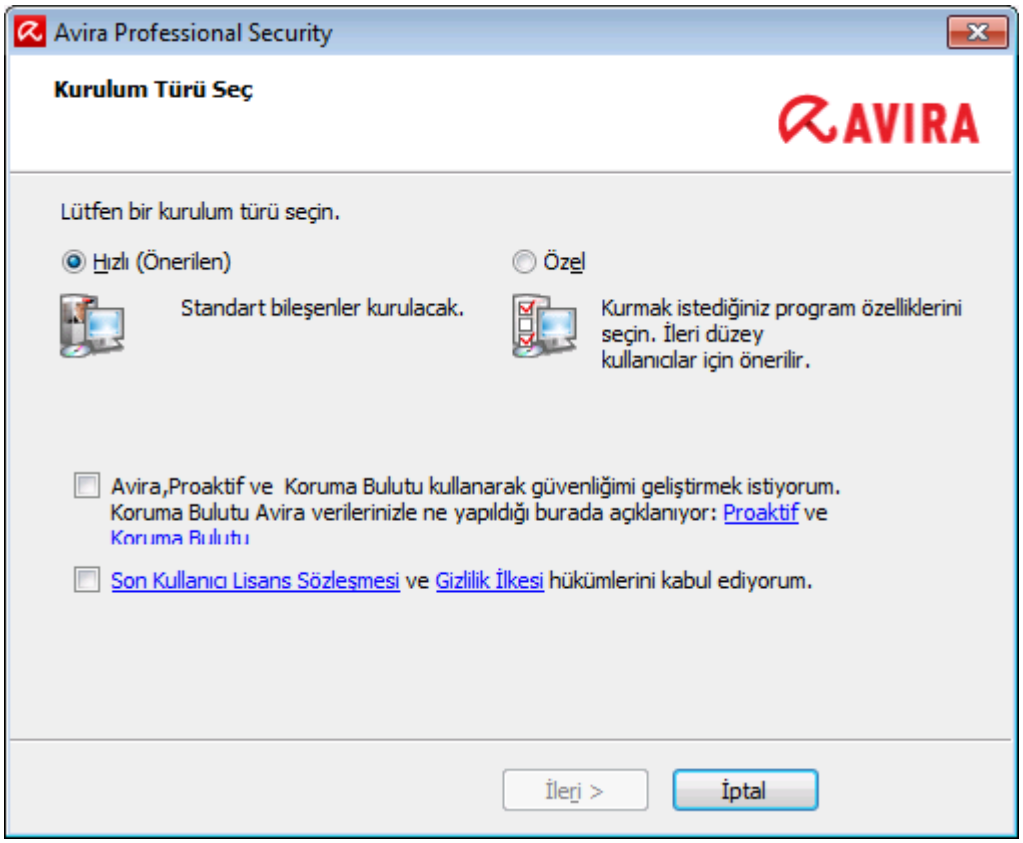
- Avira Professional Security için tüm standart bileşenleri kurar. Avira önerilen güvenlik düzeyi ayarları kullanılır.
- Varsayılan olarak aşağıdaki kurulum yollarından biri seçilir:
  - *C:\Program Files\Avira* (Windows 32bit sürümleri için) veya
  - *C:\Program Files (x86)\Avira* (Windows 64bit sürümleri için)
- Burada Avira Professional Security ile ilgili tüm dosyaları bulabilirsiniz.
- Bu kurulum tipini seçerseniz tamamlanıncaya kadar sadece **İleri** seçeneğine tıklayarak bir kurulum yapabilirsiniz.
- Bu kurulum özellikle, yazılım araçlarını yapılandırmakta kendilerini rahat hissetmeyen kullanıcılar için tasarlanmıştır.

3.6.2 Özel bir Kurulum Yapma

Özel kurulum kurulumunuzu yapılandırmanıza izin verir. Bu sadece, donanım ve yazılım konularının yanı sıra güvenlik sorunlarını da iyi bilen ileri kullanıcılar için önerilir.

- Tek tek program bileşenlerini kurmayı seçebilirsiniz.
- Kurulacak program dosyaları için bir hedef klasör seçilebilir.
- **Başlat menüsünde Masaüstü simgesi ve program grubu oluştur** seçeneğini devre dışı bırakabilirsiniz.
- Yapılandırma sihirbazını kullanarak Avira Professional Security ürününüz için özel ayarları tanımlayabilirsiniz. Kendinizi rahat hissedeceğiniz güvenlik düzeyini de seçebilirsiniz.
- Kurulumdan sonra, kurulumun ardından otomatik olarak yapılan bir kısa sistem taraması başlatabilirsiniz.

3.7 Avira Professional Security ürününün kurulması



- Avira Topluluğu'na katılmak istemiyorsanız varsayılan olarak önceden işaretlenmiş **Avira Proaktif ve Koruma Bulutu kullanarak korumamı iyileştirmek istiyorum** onay kutusunun işaretini kaldırın.

  Avira Topluluğu'na katılımınızı onaylarsanız Avira Professional Security, Avira Malware Research Center 'ne tespit edilen şüpheli programlar ile ilgili veriler

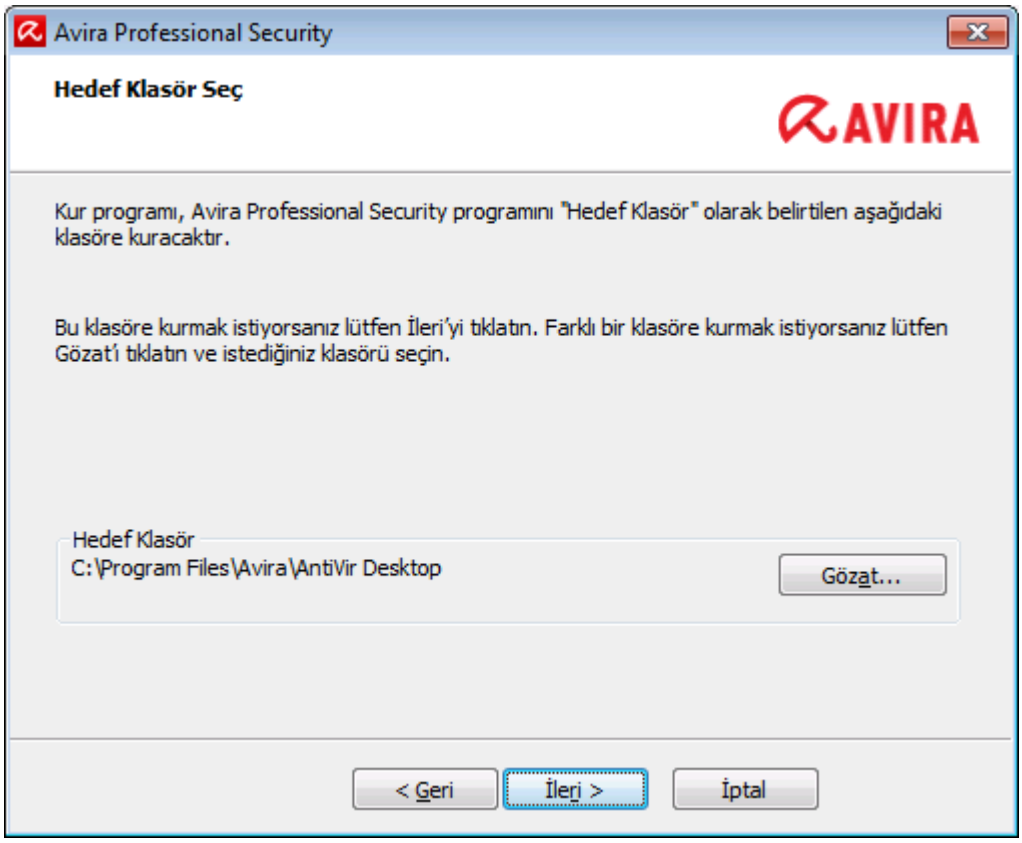
gönderir. Veriler yalnızca gelişmiş çevrimiçi tarama için ve algılama teknolojisini genişletmek ve iyileştirmek için kullanılır.

Genişletilmiş çevrimiçi ve bulut taraması hakkında daha ayrıntılı bilgi almak için **Proaktif** ve **Koruma Bulutu** bağlantılarına tıklayabilirsiniz.

Son Kullanıcı Lisans Sözleşmesi'ni kabul ettiğinizi onaylayın. **Son Kullanıcı Lisans Sözleşmesi**'nin ayrıntılı metnini okumak için EULA bağlantısını tıklatın.

3.7.1 Bir hedef klasör seçme

Özel kurulum, Avira Professional Security ürününü kurmak istediğiniz klasörü seçmenize olanak verir.



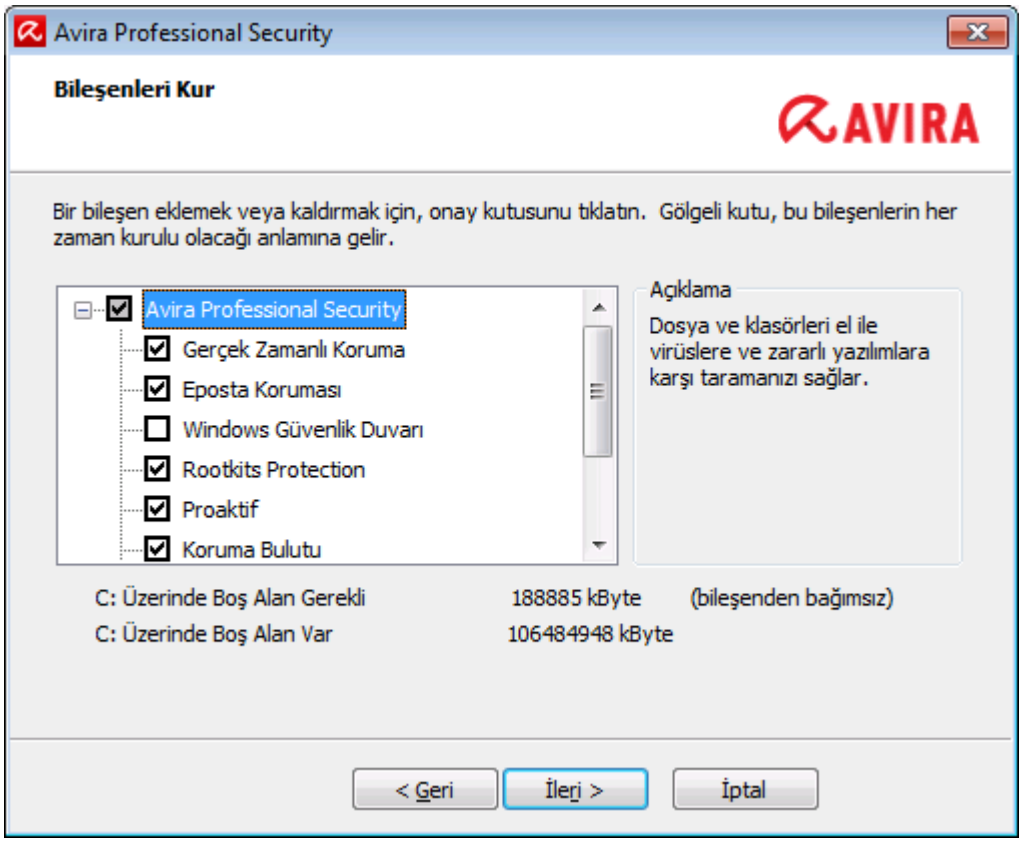
- **Gözat** düğmesine tıklatın ve Avira Professional Security ürününü kurmak istediğiniz klasörü bulun.

  Hedef Klasör Seç penceresinde Avira Professional Security ürününü kurmak istediğiniz klasörü seçin.

  İleri'yi tıklatın.

3.7.2 Kurulum bileşenlerinin seçilmesi

Kullanıcı tanımlı bir kurulumda veya bir değişiklik kurulumunda, aşağıdaki kurulum modülleri seçilebilir, eklenebilir ya da kaldırılabilir.



Bileşenleri yükle diyalogundaki listeden bileşenler seçin veya seçimlerini kaldırın.

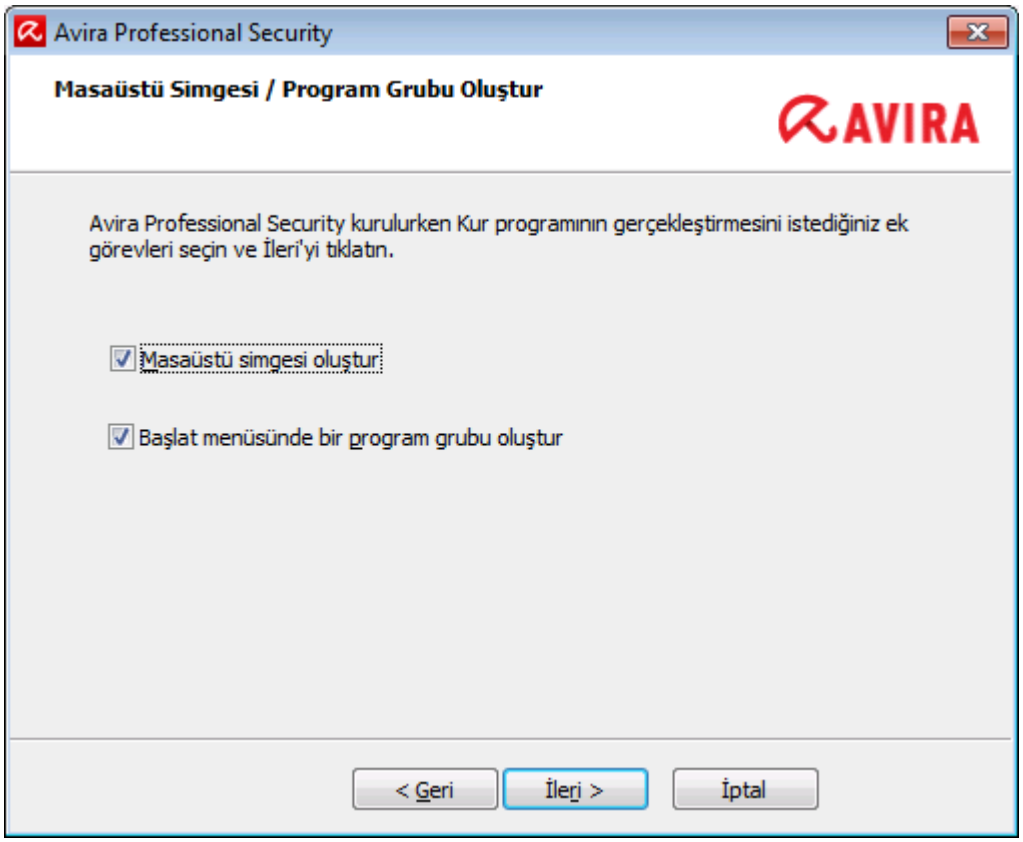
- **Avira Professional Security**
  Bu modül, Avira ürününüzün başarılı kurulumu için gerekli tüm bileşenleri içerir.
  - **Gerçek Zamanlı Koruma**
    Avira Gerçek Zamanlı Koruma arka planda çalışır. Erişim modunda açma, yazma ve kopyalama gibi işlemler sırasında mümkünse dosyaları izler ve onarır. Erişim modu, kullanıcı her dosya işlemi (örn. belge yükleme, yürütme, kopyalama) gerçekleştirdiğinde, Avira Professional Security ürününün otomatik olarak dosyayı taraması demektir. Dosya yeniden adlandırılır, ancak, Avira Gerçek Zamanlı Koruma tarafından bir tarama tetiklemez.
  - **EPosta Koruması**
    EPosta Koruması, bilgisayarınız ile e-posta programınızın (e-posta istemcisi) e-postaları karşıdan yüklediği e-posta sunucusu arasındaki arabirimdir. EPosta Koruması e-posta programı ile e-posta sunucusu arasında proxy olarak bağlanır. Tüm gelen e-postalar bu proxy üzerinden yönlendirilir, virüslere ve istenmeyen programlara karşı taranır ve e-posta programınıza iletilir. Yapılandırmaya bağlı olarak, program etkilenen e-postaları otomatik olarak işler veya sizden belirli bir eylem yapmanızı ister.
  - **Avira Güvenlik Duvarı** (Windows XP'ye kadar)
    Avira Güvenlik Duvarı, bilgisayarınıza gelen ve giden iletişimi kontrol eder. Güvenlik ilkelerinize bağlı olarak iletişimlere izin verir veya iletişimleri reddeder.
  - **Windows Güvenlik Duvarı** (Windows 7'den itibaren)
    Bu bileşen Windows Güvenlik Duvarını Avira Professional Security ürününüzden yönetir.

- **Kök kullanıcı takımı Koruma**
  Avira Kök kullanıcı takımı Koruma bilgisayar sistemine girdikten sonra geleneksel zararlı yazılım koruması yöntemleriyle algılanamayan yazılımların önceden bilgisayarınıza kurulmuş olup olmadığını kontrol eder.
- **Proaktif**
  Proaktif bileşeni, uygulama eylemlerini izler ve şüpheli uygulama davranışı konusunda kullanıcıları uyarır. Bu davranışa dayalı tanıma, bilinmeyen zararlı yazılımlara karşı kendinizi korumanıza olanak sağlar. Proaktif bileşeni Avira Gerçek Zamanlı Koruma ile entegredir.
- **Koruma Bulutu**
  Koruma Bulutu bileşeni, henüz bilinmeyen zararlı yazılımların dinamik çevrimiçi algılanması için bir modüldür. Bu, dosyaların uzak bir karşıya kaydetme konumuna yüklenmeleri ve gerçek zamanda (zamanlamasız ve gecikme olmadan) bilinen dosyaların yanı sıra yüklenen diğer dosyalarla karşılaştırılıp analiz edilmeleri demektir. Bu şekilde veri tabanı sürekli güncellenir, bu nedenle daha da yüksek bir düzeyde güvenlik sağlanabilir.
  Koruma Bulutu bileşenini kurmayı, ancak analiz için Buluta hangi dosyaların gönderileceğini el ile onaylamayı seçtiyseniz, **Avira 'ya şüpheli dosyaları gönderirken El İle Onayla** seçeneğini etkinleştirebilirsiniz.
- **Web Koruması**
  İnternette gezinirken web tarayıcınızı bir web sunucusundan veri isteğinde bulunmak için kullanırsınız. Web sunucusundan aktarılan veriler (HTML dosyaları, komut ve görüntü dosyaları, Flash dosyaları, video ve müzik akışları, vb.), web tarayıcısında görüntüleme için normal şekilde doğrudan tarayıcı önbelleğine taşınır; başka bir deyişle, Avira Gerçek Zamanlı Koruma tarafından gerçekleştirildiği gibi erişim taraması mümkün değildir. Bu, virüs ve istenmeyen programların bilgisayar sisteminize erişmesine olanak sağlayabilir. Web Koruması, veri aktarımı için kullanılan bağlantı noktalarını (80, 8080, 3128) izleyen bir HTTP proxy olarak bilinir ve aktarılan verileri virüslere ve istenmeyen programlara karşı tarar. Yapılandırmaya bağlı olarak, program etkilenen dosyaları otomatik olarak işleyebilir veya kullanıcıdan belirli bir eylem yapmasını isteyebilir.
- **Shell Extension**
  Kabuk Uzantısı, Windows Gezgini'nin bağlam menüsünde (sağ fare düğmesi) bir **Seçilen dosyaları Avira ile tara** girdisi oluşturur. Bu girdiyle, doğrudan dosyaları veya dizinleri tarayabilirsiniz.

İlgili Konular:
Bir kurulumu değiştirme

3.7.3 Avira Professional Security için kısayollar oluşturma

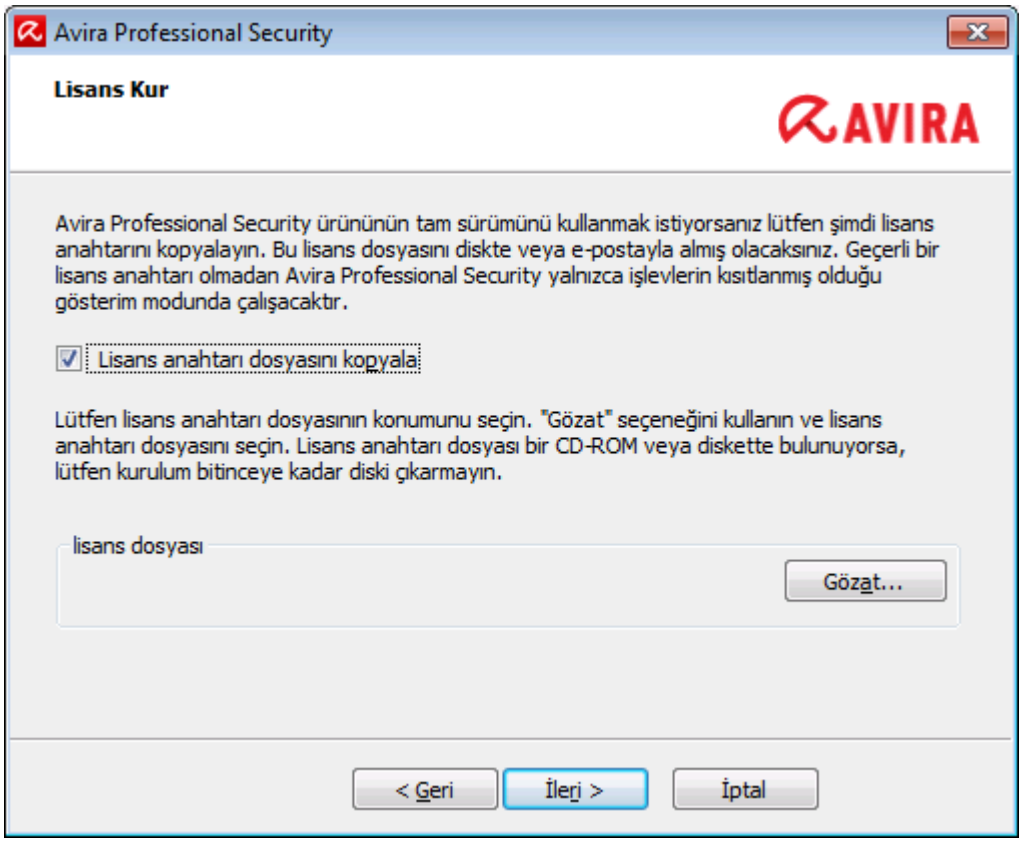
Bir masaüstü simgesi ve/veya Başlat menüsünde bir program grubu, Avira Professional Security ürününe daha hızlı ve daha kolay ulaşımınıza yardımcı olur.



- Avira Professional Security için bir masaüstü kısayolu ve/veya **Başlat menüsünde** bir program grubu oluşturmak için bu seçeneği (seçenekleri) etkinleşmiş olarak bırakın.

3.7.4 Avira Professional Security ürününü etkinleştirme

Avira Professional Security ürününüzü etkinleştirmenin birkaç yolu vardır.



- Ambalajda basılı olan etkinleştirme kodunu girin.

  Önceden almış bulunduğunuz bir etkinleştirme kodu varsa sağlanan alanlara o etkinleştirme kodunu girin.

- Bir etkinleştirme kodu almanız gerekiyorsa bağlantıya tıklatarak bir etkinleştirme kodu satın alın.

  Bir etkinleştirme kodu alabileceğiniz Avira web sitesine yönlendirilirsiniz.

- Ürünü sadece test etmek istiyorsanız **Ürünü sına** seçeneğini işaretleyin ve gerekli kayıt alanlarına bilgilerinizi girin.

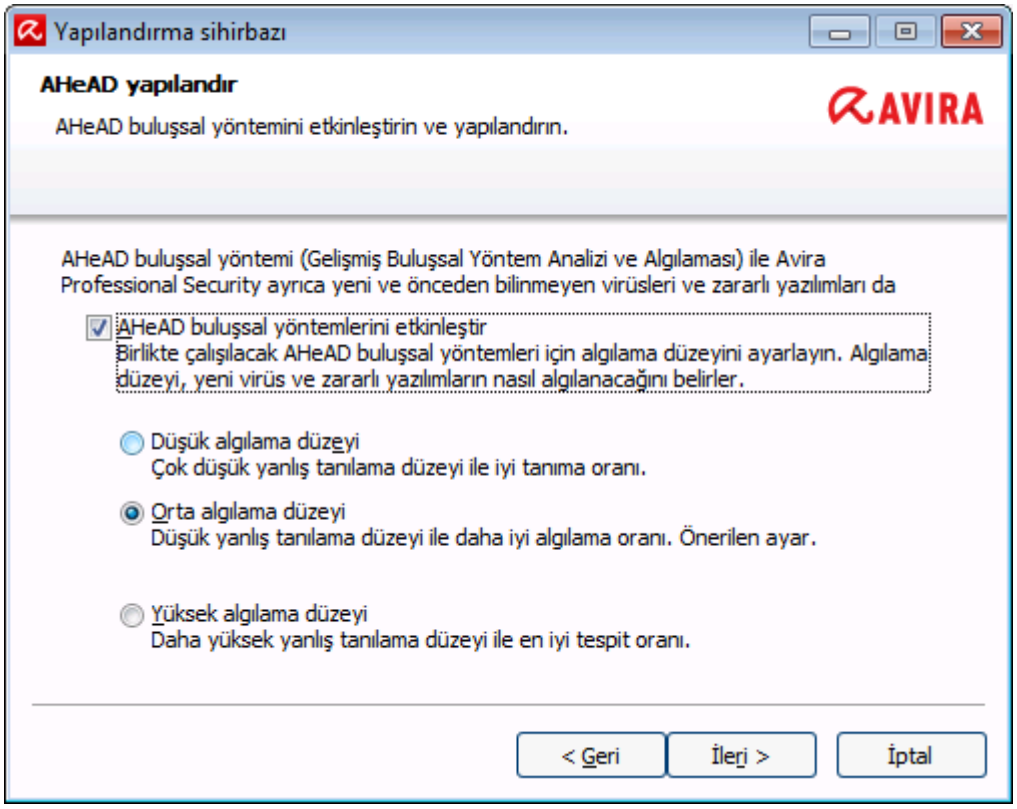
  Değerlendirme lisansınız 31 gün boyunca geçerlidir.

- Daha önce etkinleştirmiş olduğunuz bir ürün var ve Avira ürününüzü yeniden kurmak istiyorsanız **Geçerli bir lisans dosyam var** seçeneğini işaretleyin.

  Bir tarayıcı penceresi açılır ve sisteminizdeki *hbedv.key* dosyasına gözatabilirsiniz.

3.7.5 Buluşsal algılama düzeyini yapılandırma (AHeAD)

Avira Professional Security, Avira AHeAD (*Gelişmiş Buluşsal Analiz ve Algılama*) teknolojisi biçiminde çok güçlü bir araç içerir. Bu teknoloji desen analizi tekniklerini kullanır, böylece önceden analiz edilmiş başka zararlı yazılımlardan bilinmeyen (yeni) zararlı yazılımlarını saptayabilir.

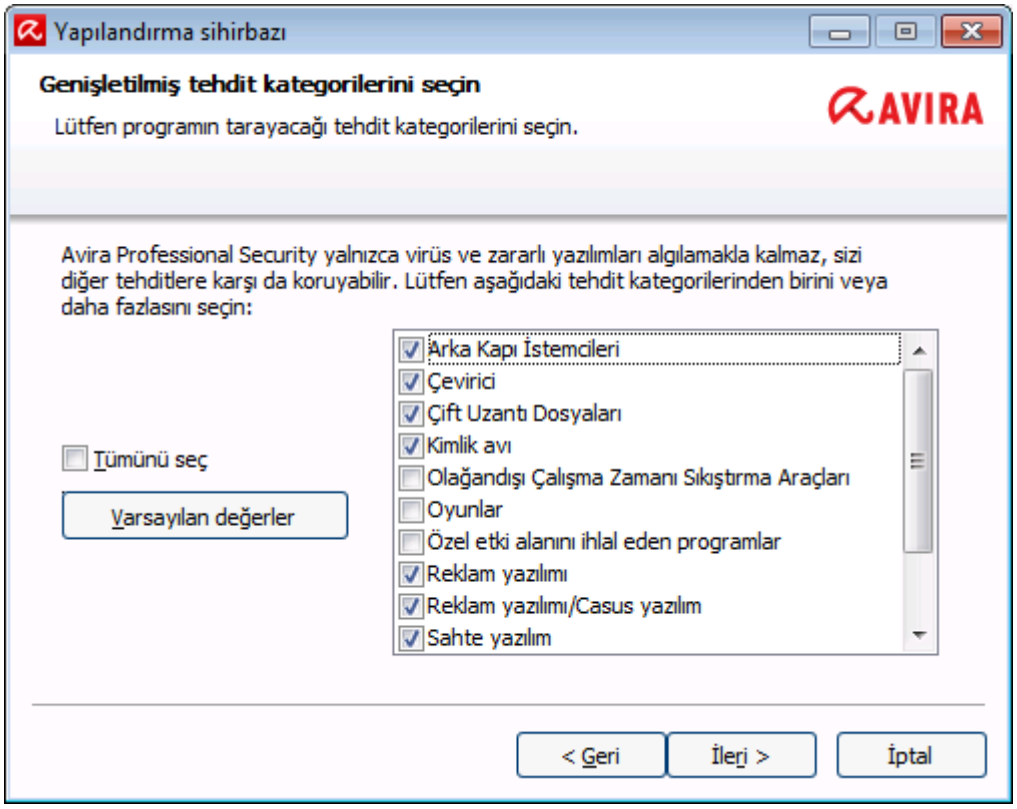


- **AHeAD yapılandır** diyalog kutusunda bir algılama düzeyi seçin ve **İleri**. seçeneğine tıklayın.

  Seçilen algılama düzeyi, Sistem Tarayıcı (istek üzerine tarama) ve Gerçek Zamanlı Koruma (Erişim taraması) AHeAD teknolojisi ayarları için kullanılır.

3.7.6 Genişletilmiş tehdit kategorilerini seçme

Bilgisayar sisteminiz için tehlike oluşturanlar sadece virüsler ve zararlı yazılımlar değildir. Sizin için tam bir liste tanımladık ve bunları genişletilmiş tehdit kategorilerinde sıraladık.



- Tehdit kategorilerinden birçoğu varsayılan olarak önceden seçilmişlerdir.

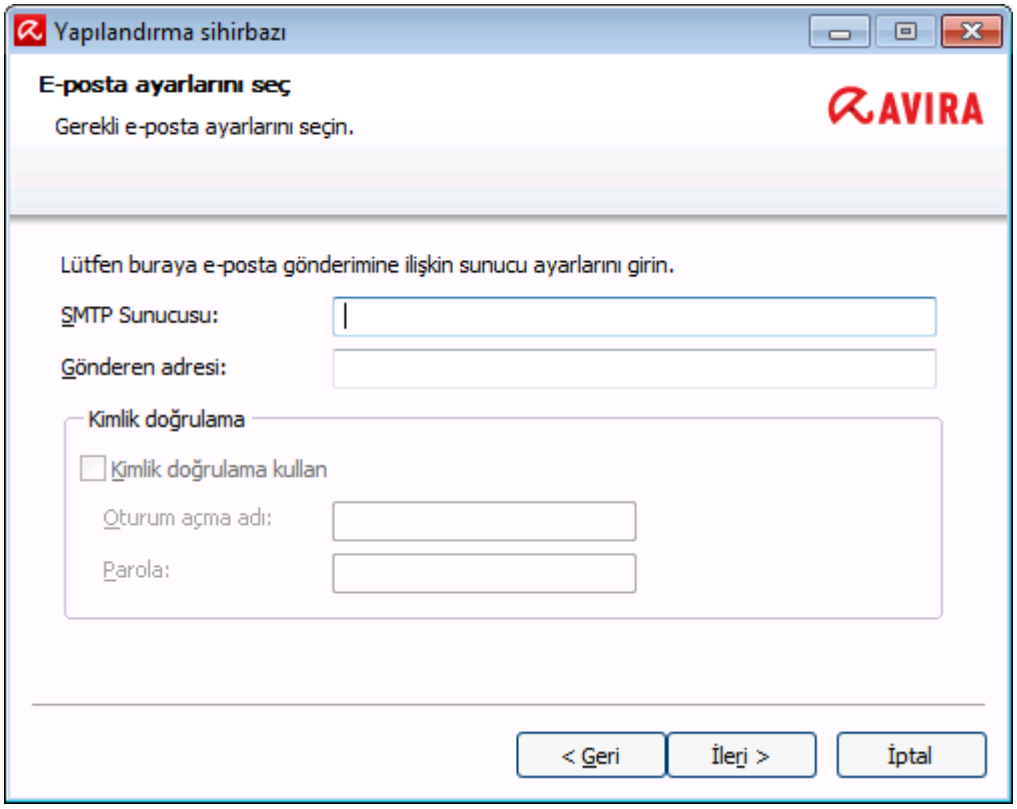
  Gerekli durumlarda, **Genişletilmiş tehdit kategorilerini seçin** iletişim kutusunda başka tehdit kategorilerini etkinleştirin.

  Fikrinizi değiştirirseniz **Varsayılan değerler** düğmesine tıklayarak önerilen değerlere dönebilirsiniz.

  Kuruluma devam etmek için **İleri** seçeneğine tıklatın.

3.7.7 E-posta ayarlarını seçme

Avira Professional Security ürününüz, e-posta göndermek, şüpheli nesneleri Karantina'dan Avira Malware Research Center'ne iletmek ve e-posta uyarıları göndermek için SMTP kullanır.



- Bu otomatik e-postaları SMTP yoluyla gönderebilmek istiyorsanız **E-posta ayarlarını seç** iletişim kutusunda e-posta gönderimi için sunucu ayarlarını tanımlayın.

SMTP Sunucusu

Kullanmak istediğiniz SMTP sunucusunun bilgisayar adını veya IP adresini girin.

Örnekler:

Adres: smtp.company.com

Adres: 192.168.1.100

Gönderen adresi

Gönderenin e-posta adresini girin.

Kimlik doğrulama

Bazı posta sunucuları, bir e-posta gönderilmeden önce programın sunucuya kendini doğrulatmasını (oturum açmasını) bekler. E-posta aracılığıyla bir SMTP sunucusuna kimlik doğrulaması ile uyarılar iletilebilir.

Kimlik doğrulama kullan

Bu seçenek etkinleştirilirse, oturum açma (kimlik doğrulama) için ilgili kutulara bir kullanıcı adı ve parola girilebilir.

Oturum açma adı:

Buraya kullanıcı adınızı girin.

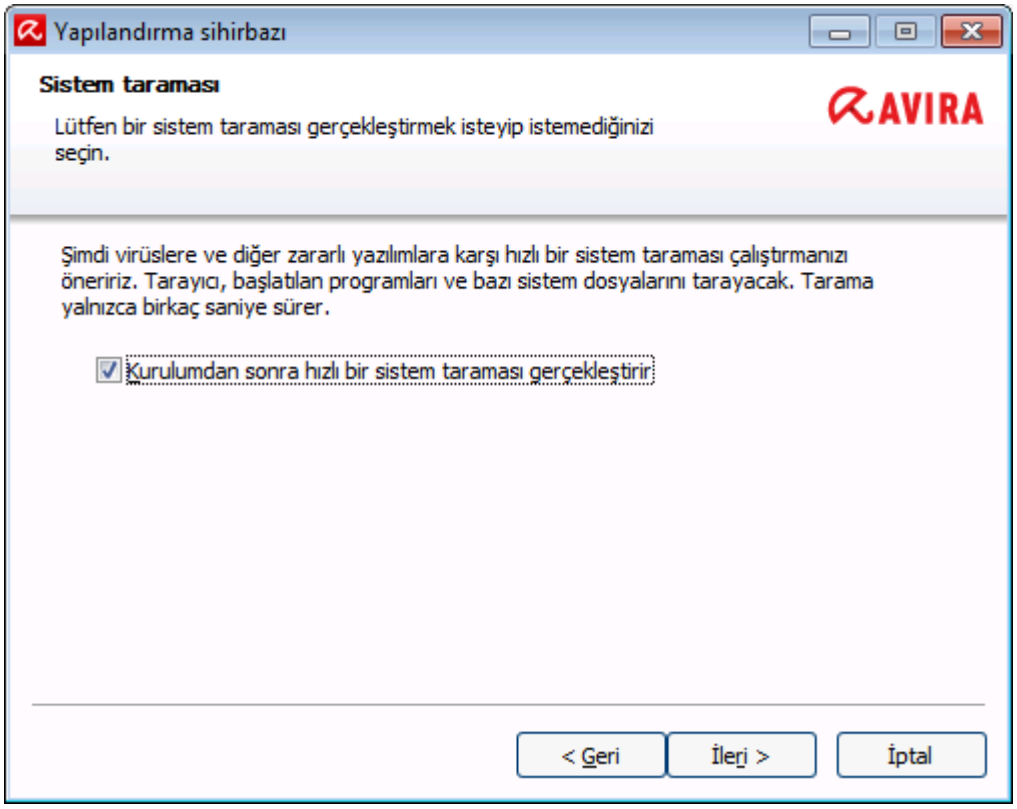
Parola:

İlgili parolayı buraya girin. Parola, şifrelenmiş şekilde kaydedilir. Güvenlik nedenleriyle, bu alana yazdığınız gerçek karakterlerin yerini yıldız işaretleri (*) alır.

İleri'yi tıklatın.

3.7.8 Kurulumdan sonra bir tarama başlatma

Bilgisayarın mevcut güvenlik durumunu kontrol etmek için, yapılandırma tamamlandıktan sonra ve bilgisayar yeniden başlatılmadan önce bir hızlı sistem taraması yapılabilir. Sistem Tarayıcı çalışan programları ve en önemli sistem dosyalarını virüsler ve zararlı yazılımlar için tarar.



- Bir hızlı sistem taraması yapmak isterseniz **Hızlı Sistem Taraması** seçeneğini etkinleştirilmiş olarak bırakın.

  İleri düğmesine tıklayın.

  Son düğmesine tıklayarak yapılandırmayı tamamlayın.

  Hızlı Sistem Taraması seçeneğinin etkinliğini kaldırırsanız *Luke Filewalker* açılır.

  Sistem Tarayıcı bir hızlı sistem taraması gerçekleştirir.

3.7.9 Ağ üzerinde kurulum ve kaldırma

Sistem yöneticisi için Avira ürünlerini birden çok istemci bilgisayarları ağında kurulumunu kolaylaştırmak üzere Avira ürününüz başlangıç kurulumu ve değişiklik kurulumu için özel bir yordama sahiptir.

Otomatik kurulum için, kurulum programı *setup.inf* kontrol dosyasıyla birlikte çalışır. Kurulum programı (*presetup.exe*), programın kurulum paketinde bulunur. Kurulum bir komut dosyası veya toplu iş dosyasıyla başlatılır ve tüm gerekli bilgiler kontrol dosyasından alınır. Bu nedenle komut dosyası komutları, kurulum sırasında normal el ile girişlerin yerini alır.

Not
Lütfen lisans dosyasının ağ üzerinde başlangıç kurulumu için zorunlu olduğunu unutmayın.

Not
Lütfen ağ aracılığıyla kurulum için Avira ürününüz yönelik bir kurulum paketinin gerekli olduğunu unutmayın. Internet tabanlı kurulum için bir kurulum dosyası kullanılamaz.

Avira ürünleri, ağda bir sunucu oturum açma komut dosyası ile veya SMS aracılığıyla kolayca paylaşılabilir.

Ağ üzerinde kurulum ve kaldırma işlemiyle ilgili bilgi için:

- bkz. Bölüm: Kurulum programı için komut satırı parametreleri
- bkz. Bölüm: *setup.inf* dosyasının parametresi
- bkz. Bölüm: Ağ üzerinde kurulum
- bkz. Bölüm: Ağ üzerinde kaldırma

Not
Avira Yönetim Konsolu, ağ üzerinde Avira ürünlerinin kurulumu ve kaldırılması için başka bir kolay seçenek sağlar. Avira Güvenlik Konsolu, ağ üzerinde Avira ürünlerinin uzaktan kurulumunu ve bakımını etkinleştirir. Daha fazla bilgi için lütfen web sitemize bakın.
http://www.avira.com/tr

Ağ üzerinde kurulum

Kurulum, toplu iş modunda komut dosyası denetimli olabilir.

Kurulum programı, aşağıdaki kurulumlar için uygundur:

- Ağ aracılığıyla başlangıç kurulumu (katılımsız kurulum)
- Tek kullanıcılı bilgisayarlarda kurulum
  - Değişiklik kurulumu ve güncelleme

> **Not**
> Ağ üzerinde kurulum yordamını uygulamadan önce otomatik kurulumu sınamanızı öneririz.

> Not
> Bir sunucu işletim sistemine kurulum yaparken, Gerçek Zamanlı Koruma ve dosya koruması kullanılamaz.

Ağ üzerinde Avira ürününü otomatik olarak kurmak için:

✓ Yönetici haklarına sahip olmanız gerekir (toplu iş modunda da gerekir)

- *setup.inf* dosyasının parametresini yapılandırın ve dosyayı kaydedin.
- /inf parametresiyle kuruluma başlayın veya parametreyi sunucunun oturum açma komut dosyasıyla tümleştirin.

  Örnek: `presetup.exe /inf="c:\temp\setup.inf"`

  ↪ Kurulum işlemi otomatik olarak başlar.

Kurulum programı için komut satırı parametreleri

> **Not**
> Yol ve dosya adları içeren parametreler tırnak içerisinde belirtilmelidir (Örneğin: `InstallPath="%PROGRAMFILES%\Avira\AntiVir Server\"`).

Aşağıdaki parametre, kurulum için mümkündür:

- `/inf`

  Kurulum programı, sözü edilen komut dosyasıyla başlar ve gerekli tüm parametreleri alır.
  Örnek: `presetup.exe /inf="c:\temp\setup.inf"`

Aşağıdaki parametreler, kaldırma için mümkündür:

- `/remove`

  Kurulum programı, Avira ürününü kaldırır.
  Örnek: `presetup.exe /remove`

- `/remsilent`

Kurulum programı, iletişim kutularını görüntülemeden Avira ürününü kaldırır. Kaldırma işleminden sonra bilgisayar yeniden başlatılır.
Örnek: `presetup.exe /remsilent`

- `/remsilentaskreboot`

  Kurulum programı, iletişim kutularını görüntülemeden Avira ürününü kaldırır ve kaldırma işleminden sonra bilgisayarın yeniden başlatılmasını ister.
  Örnek: `presetup.exe /remsilentaskreboot`

Aşağıdaki parametre, kaldırma günlüğü için bir seçenek olarak kullanılabilir:

- `/unsetuplog`

  Kaldırma işlemi sırasında tüm eylemler günlüğe kaydedilir.
  Örnek: `presetup.exe /remsilent /unsetuplog="c:\logfiles\unsetup.log"`

setup.inf dosyasının parametreleri

setup.inf kontrol dosyasında, Avira ürününün otomatik kurulumu için [VERİ] alanındaki şu parametreleri ayarlayabilirsiniz. Parametrelerin sırası önemli değildir. Bir parametre ayarı eksik veya yanlışsa, kurulum yordamı iptal edilir ve bir hata iletisi görüntülenir.

> **Not**
> Yol ve dosya adları içeren parametreler tırnak içerisinde belirtilmelidir (Örneğin: `InstallPath="%PROGRAMFILES%\Avira\AntiVir Server\"`).

- `DestinationPath`

  Programın kurulduğu hedef yolu. Komut dosyasına dahil edilmesi gerekir. Lütfen kurulumun şirket adını ve ürün adını otomatik olarak içerdiğini unutmayın. Ortam değişkenleri kullanılabilir.
  Örnek: `DestinationPath=%PROGRAMFILES%`, `C:\Program Files\Avira\AntiVir Desktop` kurulum yolunu oluşturur

- `ProgramGroup`

  Windows'un Başlat menüsünde bilgisayarın tüm kullanıcıları için bir program grubu oluşturur.
  `1`: Program grubu oluştur
  `0`: Program grubu oluşturma
  Örnek: `ProgramGroup=1`

- `DesktopIcon`

  Masaüstünde bilgisayarın tüm kullanıcıları için bir masaüstü kısayol simgesi oluşturur.
  `1`: Masaüstü simgesi oluştur
  `0`: Masaüstü simgesi oluşturma
  Örnek: `DesktopIcon=1`

- `ShellExtension`

Kabuk uzantısını kayıt defterine kaydeder. Kabuk uzantısı ile dosyalar veya dizinler, sağ fare düğmesinin bağlam menüsü aracılığıyla virüslere ve zararlı yazılımlara karşı taranabilir.
`1`: Kabuk uzantısı kaydet
`0`: Kabuk uzantısı kaydetme
Örnek: `ShellExtension=1`

- `Koruma`

  Avira Gerçek Zamanlı Koruma'yı kurar (erişim Tarayıcısı).
  `1`: Avira Gerçek Zamanlı Koruma'yı kur
  `0`: Avira Gerçek Zamanlı Koruma'yı kurma
  Örnek: `Koruma=1`

- `EPostaTarayıcı`

  Avira EPosta Koruması'nı kurar.
  `1`: Avira EPosta Koruması'nı kur
  `0`: Avira EPosta Koruması'n kurma
  Örnek: `EPostaTarayıcı=1`

- `KeyFile`

  Kurulum sırasında kopyalanan lisans dosyasının yolunu belirtir. Başlangıç kurulumu için: zorunlu. Dosya adı tamamen belirtilmelidir (tam nitelendirilmiş). (Değişiklik kurulumu için: isteğe bağlı.)
  Örnek: `KeyFile=D:\inst\license\hbedv.key`

- `ShowReadMe`

  Kurulumdan sonra *readme.txt* dosyasını görüntüler.
  `1`: Dosyayı görüntüle
  `0`: Dosyayı görüntüleme
  Örnek: `ShowReadMe=1`

- `RestartWindows`

  Kurulumdan sonra bilgisayarı yeniden başlatır. Bu girdi, `ShowRestartMessage`'dan daha yüksek önceliğe sahiptir.
  `1`: Bilgisayarı yeniden başlat
  `0`: Bilgisayarı yeniden başlatma
  Örnek: `RestartWindows=1`

- `ShowRestartMessage`

  Otomatik bir yeniden başlatma gerçekleştirilmeden önce kurulum sırasında bilgileri görüntüler.
  `0`: Bilgileri görüntüleme
  `1`: Bilgileri görüntüle
  Örnek: `ShowRestartMessage=1`

- `SetupMode`

  Başlangıç kurulumu için gerekli değildir. Kurulum programı, bir başlangıç kurulumu gerçekleştirilip gerçekleştirilmediğini bilir. Kurulum türünü belirtir. Bir kurulum kullanıma hazırsa, `SetupMode` bu kurulumun yalnızca bir güncelleme mi yoksa bir

değişiklik kurulumu (yeniden yapılandırma) veya kaldırma işlemi mi olduğu belirtmelidir.
`Güncelle`: Varolan bir kurulumu günceller. Bu durumda yapılandırma parametreleri, örneğin, Koruyucu yoksayılır.
`Değiştir`: Varolan bir kurulumu değiştirir (yeniden yapılandırır). İşlemde, hedef yoluna bir dosya kopyalanmaz.
`Kaldır`: Avira ürününüzü sistemden kaldırır.
Örnek: `SetupMode=Güncelle`

- `AVWinIni (isteğe bağlı)`

  Kurulum sırasında kopyalanabilen yapılandırma dosyası için hedef yolunu belirtir. Dosya adı tamamen belirtilmelidir (tam nitelendirilmiş).
  Örnek: `AVWinIni=d:\inst\config\avwin.ini`

- `Parola`

  Bu seçenek, (değişiklik) kurulum ve kaldırma için ayarlanmış parolayı kurulum yordamına atar. Girdi yalnızca bir parola ayarlandıysa kurulum yordamı tarafından taranır. Bir parola ayarlandıysa ve parola parametresi eksik veya yanlışsa, kurulum yordamı iptal edilir.
  Örnek: `Parola=Password123`

- `WebGuard`

  Avira Web Koruması'nı kurar.
  `1`: Avira Web Koruması'nı kur
  `0`: Avira Web Koruması'nı kurma
  Örnek: `WebGuard=1`

- `KökKullanıcıTakımı`

  Avira Kök Kullanıcı Takımı Koruma modülünü kurar. Avira Kök Kullanıcı Takımı Koruma olmadan, Sistem Tarayıcı, sistemdeki kök takımlara karşı tarama yapamaz!
  `1`: Avira Kök Kullanıcı Takımı Koruma'yı kur
  `0`: Avira Kök Kullanıcı Takımı Koruma'yı kurma
  Örnek: `RootKit=1`

- `Proaktif`

  Avira Proaktif bileşenini kurar. Avira Proaktif, henüz bilinmeyen zararlı yazılımın algılanmasını sağlayan desene dayalı bir algılama teknolojisidir.
  `1`: Proaktif'i kur
  `0`: Proaktif'i kurma
  Örnek: `ProActiv=1`

- `Güvenlik Duvarı`

  Avira Güvenlik Duvarı bileşenini kurar (Windows 7'ye kadar). Avira Güvenlik Duvarı, bilgisayar sisteminizdeki gelen ve giden veri trafiğini izleyip denetler ve bilgisayarlarınızı Internet'ten veya diğer ağ ortamlarından gelebilecek tehditlere karşı korur.
  `1`: Güvenlik Duvarı kur
  `0`: Güvenlik Duvarı kurma
  Örnek: `FireWall=1`

- `MgtFirewall`

  Windows Güvenlik Duvarı yönetim bileşenini kurar. Windows 8'den başlayarak, Avira Professional Security Avira Güvenlik Duvarı içermemektedir. Windows Güvenlik Duvarı artık Avira ürünü üzerinden yönetilmektedir.
  `1`: Windows Güvenlik Duvarı yönetim bileşenini kurun
  `0`: Windows Güvenlik Duvarı yönetim bileşenini kurmayın
  Örnek: `MgtFirewall=1`

3.8 Kurulumu değiştirme

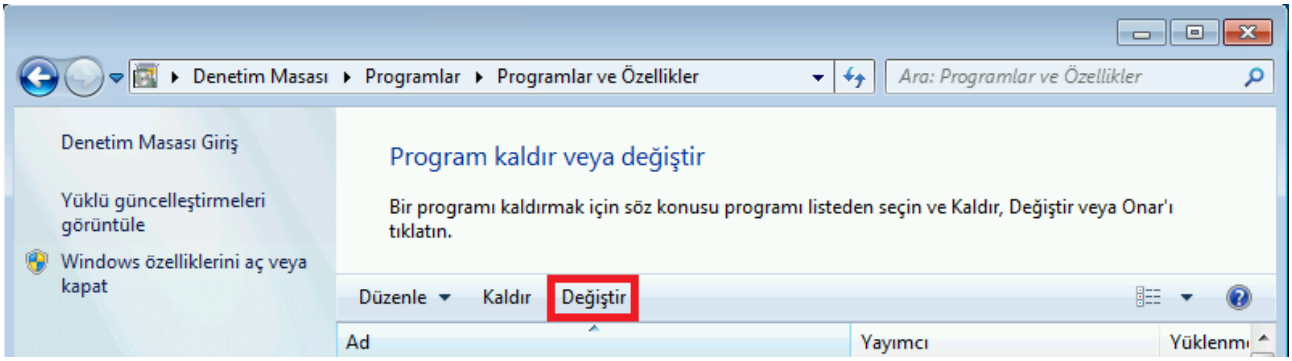
3.8.1 Kurulumu değiştirme

Geçerli kurulumun modüllerini eklemek veya kaldırmak isterseniz bunu, Avira Professional Security ürününü kaldırmadan yapabilirsiniz. Şu şekilde:

- Windows 8'de bir kurulumu değiştirme
- Windows 7'de bir kurulumu değiştirme
- Windows XP'de bir kurulumu değiştirme

3.8.2 Windows 8'de bir kurulumu değiştirme

Avira Professional Security ürünü kurulumunun program bileşenlerini ayrı ayrı ekleme veya kaldırma seçeneğiniz vardır (bkz. Kurulum bileşenlerini seçme).



Geçerli kurulumun modüllerini eklemek veya kaldırmak isterseniz programları **Değiştirmek/Kaldırmak** için **Windows denetim masasında Programları Kaldır** seçeneğini kullanabilirsiniz.

- Ekrana sağ tıklayın.

  Tüm uygulamalar sembolü görüntülenir.

  Bu sembole tıklatın ve *Uygulamalar - Windows Sistemi* kısmında **Denetim Masası**na bakın.

  Denetim Masası sembolüne çift tıklatın.

Programlar - Program kaldır öğesine tıklatın.

Programlar ve Özellikler - Program kaldır öğesine tıklatın.

Avira Professional Security öğesini seçin ve **Değiştir**'e tıklatın.

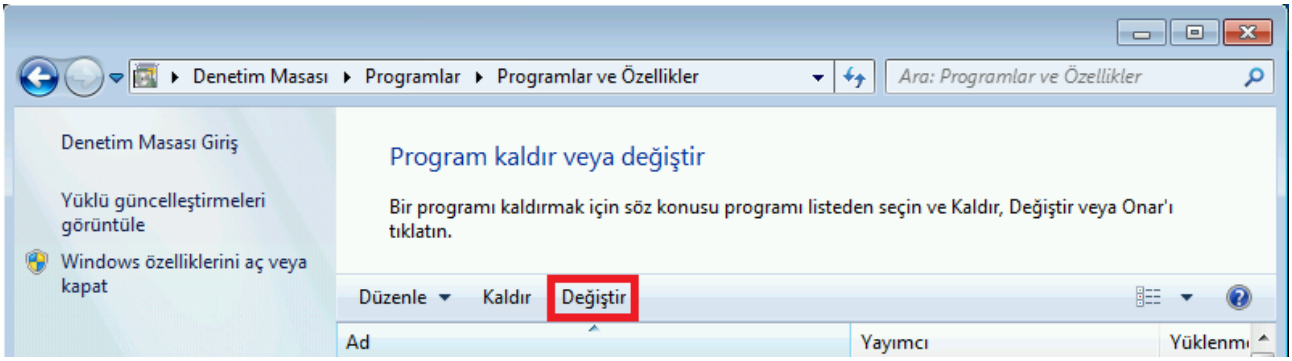
Programın **Hoş Geldiniz** iletişim kutusunda **Değiştir** seçeneğini seçin. Kurulum değişiklikleri boyunca size yol gösterilecektir.

Not
Avira SearchFree Araç Çubuğu ürününü kaldırıyorsanız Web Koruması de kaldırılır.

İlgili Konular:
Kurulum bileşenlerinin seçilmesi

3.8.3 Windows 7'de bir kurulumu değiştirme

Avira Professional Security ürünü kurulumunun program bileşenlerini ayrı ayrı ekleme veya kaldırma seçeneğiniz vardır (bkz. Kurulum bileşenlerini seçme).



Geçerli kurulumun modüllerini eklemek veya kaldırmak istiyorsanız, programları **Değiştirmek/Kaldırmak** için **Windows denetim masasında Program Ekle veya Kaldır** seçeneğini kullanabilirsiniz.

- Windows'un **Başlat** menüsünden **Denetim Masası**'nı açın.

  Programlar ve Özellikler öğesine çift tıklatın.

  Avira Professional Security öğesini seçin ve **Değiştir**'e tıklatın.

  Programın **Hoş Geldiniz** iletişim kutusunda **Değiştir** seçeneğini seçin. Kurulum değişiklikleri boyunca size yol gösterilecektir.

İlgili Konular:
Kurulum bileşenlerinin seçilmesi

3.8.4 Windows XP'de bir kurulumu değiştirme

Avira Professional Security ürünü kurulumunun program bileşenlerini ayrı ayrı ekleme veya kaldırma seçeneğiniz vardır (bkz. Kurulum modüllerini seçme).

Geçerli kurulumun modüllerini eklemek veya kaldırmak istiyorsanız, programları **Değiştirmek/Kaldırmak** için **Windows denetim masasında Program Ekle veya Kaldır** seçeneğini kullanabilirsiniz.

- Windows'un **Başlat > Ayarlar** menüsünden **Denetim Masası**'nı açın.

  Program Ekle veya Kaldır öğesine çift tıklatın.

  Avira Professional Security öğesini seçin ve **Değiştir**'e tıklatın.

  Programın **Hoş Geldiniz** iletişim kutusunda **Değiştir** seçeneğini seçin. Kurulum değişiklikleri boyunca size yol gösterilecektir.

> **Not**
> Avira SearchFree Araç Çubuğu ürününü kaldırıyorsanız Web Koruması de kaldırılır.

İlgili Konular:
Kurulum bileşenlerinin seçilmesi

3.9 Avira Professional Security ürününü kaldırma

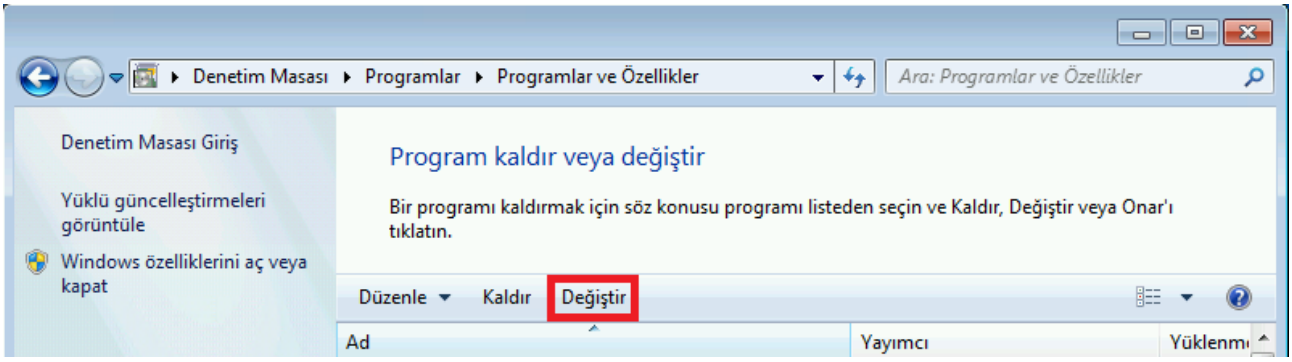
3.9.1 Avira Professional Security ürününü kaldırma

Herhangi bir zamanda Avira Professional Security ürününü kaldırma ihtiyacı duyarsanız şöyle yapmalısınız:

- Windows 8'de Avira Professional Security ürününü kaldırma
- Windows 7'de Avira Professional Security ürününü kaldırma
- Windows XP'de Avira Professional Security ürününü kaldırma

3.9.2 Windows 7' de Avira Professional Security ürününü kaldırma

Avira Professional Security ürününü bilgisayarınızdan kaldırmak için, Windows Denetim Masasındaki **Programlar ve Özellikler** seçeneğini kullanın.



- Windows'un **Başlat** menüsünden **Denetim Masası**'nı açın.

  Programlar ve Özellikler seçeneğini tıklatın.

  Listeden Avira Professional Security öğesini seçin ve **Kaldır** seçeneğini tıklatın.

  Uygulamayı ve tüm bileşenlerini kaldırmayı gerçekten isteyip istemediğiniz sorulunca, **Evet**'i tıklatıp onaylayın.

  Windows Güvenlik Duvarını etkinleştirmek isteyip istemediğiniz sorulunca (Avira Güvenlik Duvarı kaldırılır), sisteminizde bir miktar koruma kalması için **Evet**'i tıklatın.

  Tüm program bileşenleri kaldırılacaktır.

  Kurulumu tamamlamak için **Son**'u tıklatın.

  Bilgisayarınızın yeniden başlatılmasını öneren bir iletişim kutusu görüntülenirse **Evet**'i tıklatıp onaylayın.

  Bilgisayarınız yeniden başlatıldığında Avira Professional Security ürününüz kaldırılmış ve programın tüm dizinleri, dosyaları ve kayıt defteri girdileri silinmiştir.

Not
Avira SearchFree Araç Çubuğu kaldırma programına dahil edilmemiş olup yukarıda ayrıntıları verilen adımlar izlenerek ayrı ayrı kaldırılmalıdır.

Not
Avira SearchFree Araç Çubuğu ürününü kaldırıyorsanız Web Koruması de kaldırılır.

3.9.3 Windows XP'de Avira Professional Security ürününü kaldırma

Avira Professional Security ürününü bilgisayarınızdan kaldırmak için, Windows Denetim Masasındaki **Program Ekle veya Kaldır** seçeneğini kullanın.

- Windows'un **Başlat > Ayarlar** menüsünden **Denetim Masası**'nı açın.

  Program Ekle veya Kaldır öğesini çift tıklatın.

  Listeden Avira Professional Security öğesini seçin ve **Kaldır** seçeneğini tıklatın.

Uygulamayı ve tüm bileşenlerini kaldırmayı gerçekten isteyip istemediğiniz sorulunca, **Evet**'i tıklatıp onaylayın.

Tüm program bileşenleri kaldırılacaktır.

Kurulumu tamamlamak için **Son**'u tıklatın.

Bilgisayarınızın yeniden başlatılmasını öneren bir iletişim kutusu görüntülenirse **Evet**'i tıklatıp onaylayın.

Bilgisayarınız yeniden başlatıldığında Avira Professional Security ürününüz kaldırılmış ve programın tüm dizinleri, dosyaları ve kayıt defteri girdileri silinmiştir.

Not
Avira SearchFree Araç Çubuğu kaldırma programına dahil edilmemiş olup yukarıda ayrıntıları verilen adımlar izlenerek ayrı ayrı kaldırılmalıdır.

Not
Avira SearchFree Araç Çubuğu ürününü kaldırıyorsanız Web Koruması de kaldırılır.

3.9.4 Ağ üzerinde kaldırma

Ağ üzerinde Avira ürünlerini otomatik olarak kaldırmak için:

✓ Yönetici haklarına sahip olmanız gerekir (toplu iş modunda da gerekir)

- `/remsilent` veya `/remsilentaskreboot` parametresiyle kaldırma işlemini başlatın veya parametreyi sunucunun oturum açma komut dosyasıyla tümleştirin.

  Ayrıca kaldırma günlüğü için de parametre belirtebilirsiniz.

  Örnek: `presetup.exe /remsilent /unsetuplog="c:\logfiles\unsetup.log"`

  ↳ Kaldırma işlemi otomatik olarak başlar.

Not
Kaldırma kurulum programı, Avira ürününün kaldırılacağı kişisel bilgisayarda başlatılmalıdır; kurulum programını bir ağ sürücüsünden başlatmayın.

3.9.5 Avira SearchFree Toolbar'nu kaldırma

Windows XP' de Avira SearchFree Araç Çubuğu 'nu kaldırma

Avira SearchFree Araç Çubuğu'nu kaldırmak için:

- Web tarayıcınızı kapatın.

Windows'un **Başlat > Ayarlar** menüsünden **Denetim Masası**'nı açın.

Program Ekle veya Kaldır öğesini çift tıklatın.

Listeden Avira SearchFree Araç Çubuğu 'nu ve Web Koruması 'nı seçin ve **Kaldır**'a tıklatın.

Gerçekten bu ürünü kaldırmak isteyip istemediğiniz sorulacaktır.

Onaylamak için **Evet**'i tıklatın.

Bilgisayarınız yeniden başlatıldığında Avira SearchFree Araç Çubuğu ve Web Koruması kaldırılır ve Avira SearchFree Araç Çubuğu ve Web Koruması 'na ait tüm dizinler, dosyalar ve kayıt defteri girdileri silinir.

4. Avira Professional Security ürününe genel bakış

Bu bölümde, Avira ürününüzün işlevselliğine ve çalışmasına genel bakış yer alır.

- bkz. Kullanıcı arabirimi ve çalışma Bölümü
- bkz. Nasıl yapılır? Bölümü

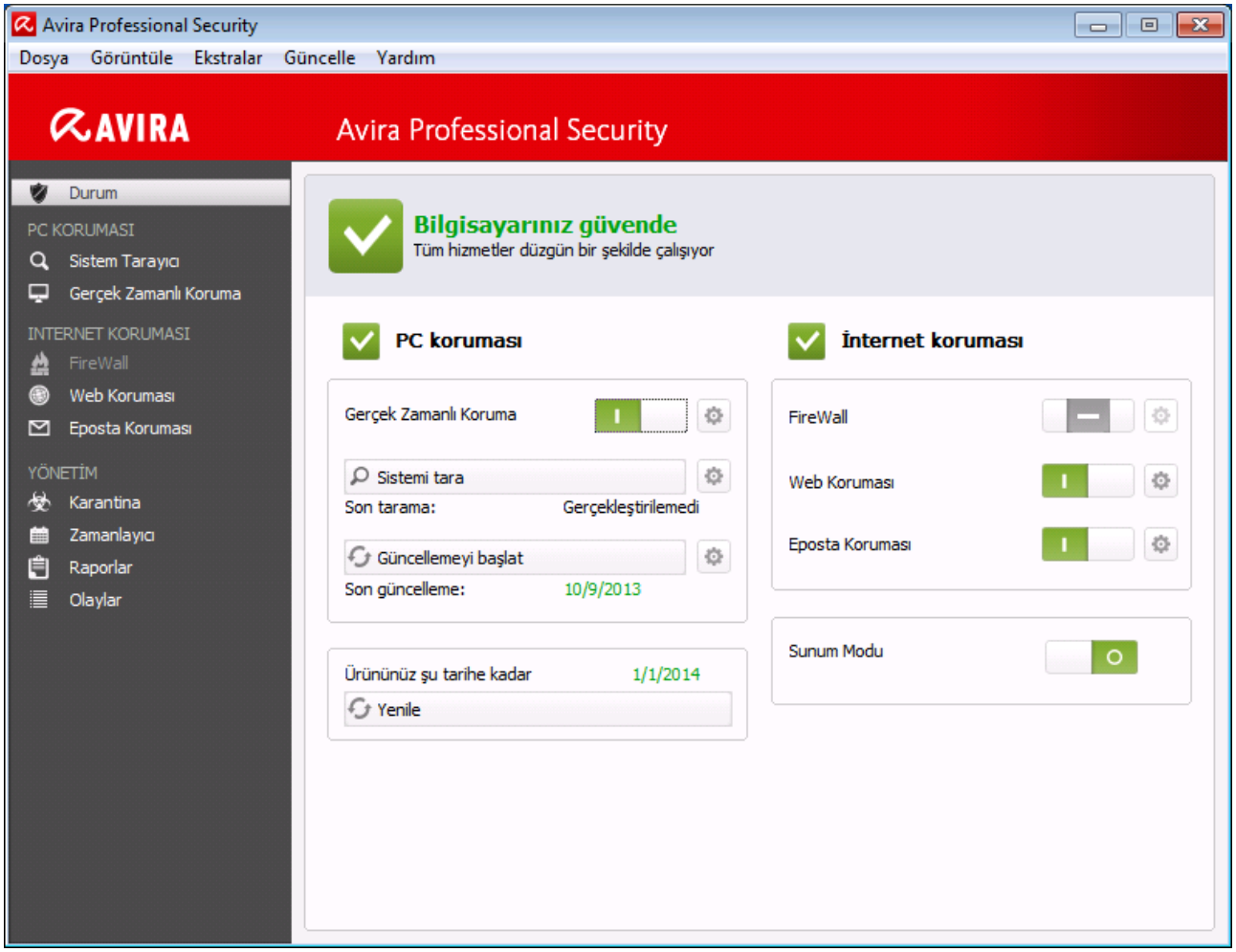
4.1 Kullanıcı arabirimi ve çalışma

Avira ürününüzü üç program arabirimi öğesi aracılığıyla çalıştırırsınız:

- Kontrol Merkezi: Avira ürününün izlenmesi ve denetlenmesi
- Yapılandırma: Avira ürününü yapılandırma
- Tepsi Simgesi, görev çubuğunun sistem tepsisinde: Kontrol Merkezi'ni ve diğer işlevleri açma

4.1.1 Kontrol Merkezi

Kontrol Merkezi, bilgisayar sistemlerinizin koruma durumunu izlemek ve Avira ürününüzün koruma bileşenlerini ve işlevlerini denetlemek ve çalıştırmak için tasarlanmıştır.



Kontrol Merkezi penceresi üç alana ayrılmıştır: **Menü çubuğu**, **Gezinti alanı** ve **Durum** ayrıntı penceresi:

- **Menü çubuğu:** Kontrol Merkezi menü çubuğunda, genel program işlevlerine ve programla ilgili bilgilere erişebilirsiniz.
- **Gezinti alanı:** Gezinti alanında, Kontrol Merkezi'nin tek tek bölümleri arasında kolayca geçiş yapabilirsiniz. Tek tek bölümler, program bileşenlerinin bilgi ve işlevlerini içerir ve gezinti çubuğunda etkinliğe göre düzenlenir. Örnek: Eylem *PC KORUMA* - Bölüm **Gerçek Zamanlı Koruma**.
- **Durum:** Kontrol Merkezi, bir bakışta bilgisayarınızın güvenli olup olmadığını görebileceğiniz ve aktif modüller, son yedeklemenin tarihi ve son sistem taramasının tarihine dair bir genel bakışın sunulduğu **Durum** görünümü ile açılır. **Durum** görünümü bunun yanı sıra **Gerçek Zamanlı Koruma**'ı başlatmak veya durdurmak gibi özellikleri ya da eylemleri başlatmak için düğmeler içerir.

Kontrol Merkezi'nin başlatılması ve kapatılması

Kontrol Merkezi'ni başlatmak için, aşağıdaki seçenekler kullanılabilir:

- Masaüstünüzdeki program simgesini çift tıklatın
- **Başlat > Programlar** menüsündeki program girdisi aracılığıyla.

- Avira ürününüzün Tepsi Simgesi aracılığıyla.

Dosya menüsündeki **Kapat** menü komutu aracılığıyla veya Kontrol Merkezi'ndeki kapat sekmesini tıklatarak Kontrol Merkezi'ni kapatın.

Kontrol Merkezi'ni çalıştırma

Kontrol Merkezi'nde gezinmek için

- Gezinti çubuğunda bir etkinlik seçin.
  - ↪ Etkinlik açılır ve diğer bölümler görüntülenir. Görünümde etkinliğin birinci bölümü seçilir ve görüntülenir.
- Gerekirse, ayrıntı penceresinde bunu görüntülemek için başka bir bölümü tıklatın.

> **Not**
> [**Alt**] tuşunun yardımıyla menü çubuğunda klavye gezintisini etkinleştirebilirsiniz. Gezinti etkinleştirilirse, **ok** tuşlarıyla menü içinde hareket edebilirsiniz. **Geri dön** tuşu ile etkin menü öğesini etkinleştirirsiniz.
> Kontrol Merkezi'nde menüleri açmak veya kapatmak ya da menüler içinde gezinmek için, şu tuş birleşimlerini de kullanabilirsiniz: [**Alt**] + menüde veya menü komutunda altı çizili harf. Bir menüye, menü komutuna veya alt menüye erişmek istiyorsanız, [**Alt**] tuşunu basılı tutun.

Ayrıntı penceresinde görüntülenen verileri veya nesneleri işlemek için:

- Düzenlemek istediğiniz veriyi veya nesneyi vurgulayın.

  Birden çok öğeyi (sütunlardaki öğeleri) vurgulamak için, **kontrol** tuşunu veya **shift** tuşunu basılı tutarken öğeleri seçin.
- Nesneyi düzenlemek için ayrıntı penceresinin üst çubuğundaki uygun düğmeyi tıklatın.

Kontrol Merkezi'ne genel bakış

- **Durum**: **Durum** çubuğunu tıklatarak ürünün işlev ve performansına genel bakışa ulaşabilirsiniz (bkz. Durum).
  - **Durum** bölümü, hangi modüllerin etkin olduğunu bir bakışta görmenize olanak verir ve gerçekleştirilen son güncellemeyle ilgili bilgi sağlar.
- *PC KORUMA*: Bu bölümde bilgisayar sisteminizdeki dosyaları virüs ve zararlı yazılımlara karşı denetlemeye yönelik bileşenler bulursunuz.
  - Sistem Tarayıcı bölümü, kolayca bir istek üzerine taramayı yapılandırmanıza ve başlatmanıza olanak sağlar. Önceden tanımlı profiller, önceden uyarlanmış varsayılan seçeneklerle bir taramayı etkinleştirir. Aynı şekilde, el ile seçim yardımıyla (kaydedilecektir) veya kullanıcı tanımlı profiller oluşturularak virüs ve istenmeyen programlara karşı taramayı kişisel gereksinimlerinize uyarlamanız mümkündür.

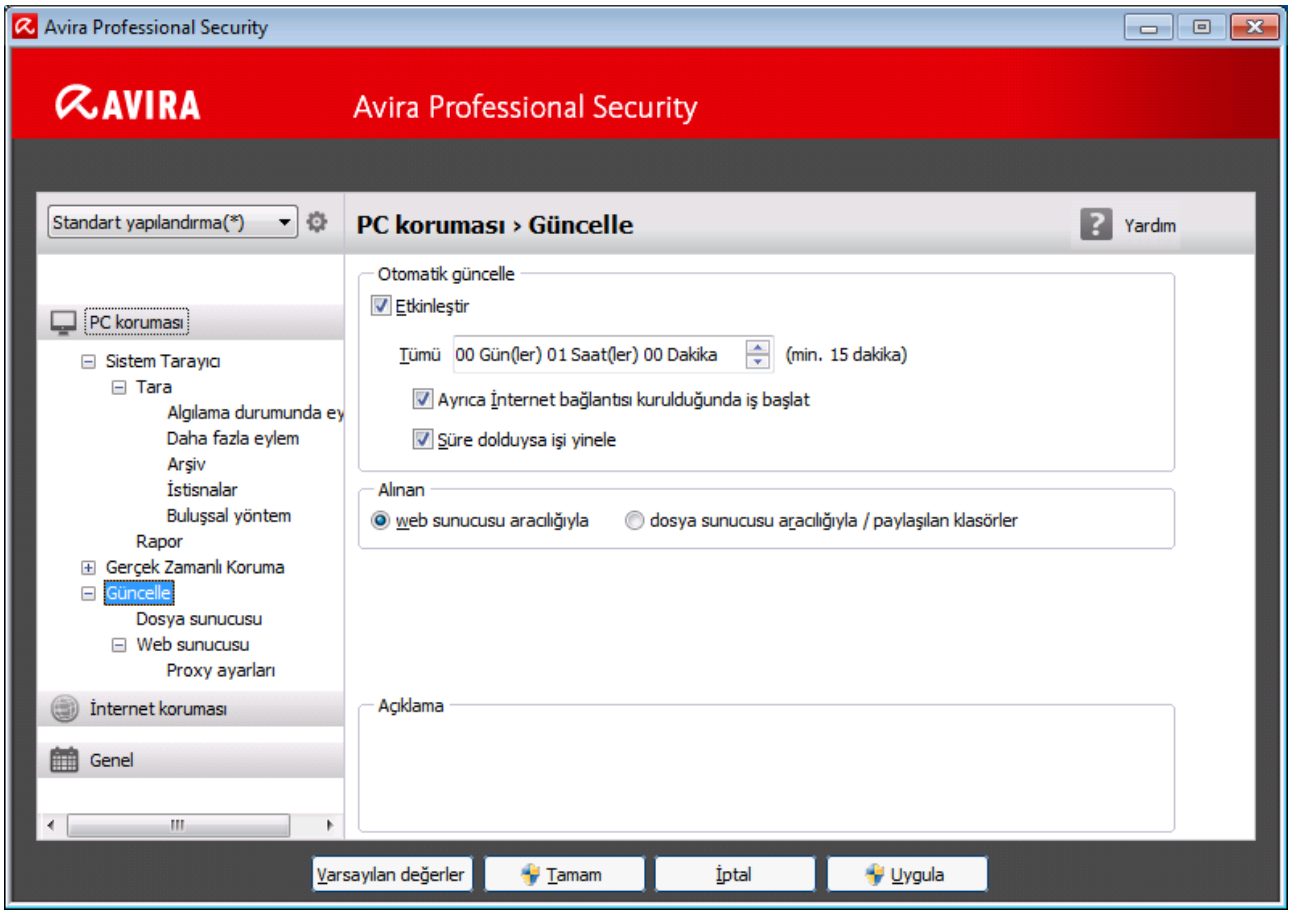
- Gerçek Zamanlı Koruma bölümünde, taranmış dosyalarla ilgili bilgiler ve diğer istatistiksel veriler görüntülenir ve bu istendiği zaman sıfırlanabilir ve rapor dosyasına erişilmesini sağlar. Algılanan son virüs veya istenmeyen programla ilgili daha ayrıntılı bilgi "bir düğme basışıyla" pratik olarak edinilebilir.

- *İNTERNET KORUMASI*: Bu bölümde bilgisayar sisteminizi Internet'ten gelen virüs ve zararlı yazılımlara karşı ve yetkisiz ağ erişimine karşı korumaya yönelik bileşenler bulursunuz.
  - Güvenlik Duvarı bölümü Güvenlik Duvarı için temel ayarları yapılandırmanıza olanak sağlar. Ayrıca, geçerli veri aktarım hızı ve ağ bağlantısı kullanan tüm etkin uygulamalar da görüntülenir.
  - Web Koruması bölümünde, taranan URL'ler ve algılanan virüslerle ilgili bilgilerin yanı sıra diğer istatistiksel veriler görüntülenir ve bu istendiği zaman sıfırlanabilir ve rapor dosyasına erişilmesini sağlar. Algılanan son virüs veya istenmeyen programla ilgili daha ayrıntılı bilgi "bir düğme basışıyla" pratik olarak edinilebilir.
  - EPosta Koruması bölümünde, EPosta Koruması tarafından taranan tüm e-postalar, bunların özellikleri ve diğer istatistiksel veriler gösterilir.

- *YÖNETİM*: Bu bölümde şüpheli veya etkilenmiş dosyaları yalıtıp yönetmeye ve yinelenen görevleri planlamaya yönelik araçlar bulursunuz.
  - Karantina bölümünde, karantina yöneticisi yer alır. Bu, önceden karantinaya yerleştirilmiş dosyalar veya karantinaya yerleştirmek istediğiniz şüpheli dosyalar için merkezi noktadır. Seçilen bir dosyayı e-posta yoluyla Avira Zararlı Yazılım Araştırma Merkezi'ne de gönderebilirsiniz.
  - Zamanlayıcı bölümü, zamanlanan tarama ve güncelleme işleri, yedekleme işleri yapılandırmanıza ve varolan işleri uyarlamanıza veya silmenize olanak sağlar.
  - Raporlar bölümü, gerçekleştirilen eylemlerin sonuçlarını görüntülemenize olanak sağlar.
  - Olaylar bölümü, belirli program modülleri tarafından oluşturulan olayları görüntülemenize olanak sağlar.

4.1.2 Yapılandırma

Yapılandırma'da Avira ürününüz için ayarları tanımlayabilirsiniz. Kurulumdan sonra, Avira ürününüz standart ayarlarla yapılandırılarak bilgisayar sisteminiz için en iyi koruma sağlanır. Ancak bilgisayar sisteminiz veya Avira ürününüze ilişkin belirli gereksinimler, programın koruyucu bileşenlerini uyarlamanız gerektiği anlamına gelebilir.



Yapılandırma bir iletişim kutusu açar: **Tamam** veya **Uygula** düğmeleriyle yapılandırma ayarlarınızı kaydedebilir, İptal düğmesini tıklatarak ayarlarınızı silebilir veya **Varsayılan değerler** düğmesini kullanarak varsayılan yapılandırma ayarlarınızı geri yükleyebilirsiniz. Soldaki gezinti çubuğunda tek tek yapılandırma bölümlerini seçebilirsiniz.

Yapılandırmaya Erişme

Yapılandırmaya erişmeye ilişkin birçok seçeneğiniz vardır:

- Windows denetim masası aracılığıyla.
- Windows Güvenlik Merkezi aracılığıyla - Windows XP Service Pack 2'den.
- Avira ürününüzün Tepsi Simgesi aracılığıyla.
- Kontrol Merkezi'nde Ekstralar > Yapılandırma menü öğesi aracılığıyla.
- Kontrol Merkezi'nde Yapılandırma düğmesi aracılığıyla.

> **Not**
> Kontrol Merkezi'ndeki **Yapılandırma** düğmesi aracılığıyla yapılandırmaya erişiyorsanız, Kontrol Merkezi'nde etkin olan bölümün Yapılandırma kaydına gidin. Tek tek yapılandırma kayıtları seçmek için

Yapılandırma işlemi

Yapılandırma penceresinde, Windows Gezgini'nde olduğu gibi gezinin:

- Ayrıntı penceresinde bu yapılandırma bölümünü görüntülemek için ağaç yapısında bir girdiyi tıklatın.
- Yapılandırma bölümünü genişletmek ve ağaç yapısında yapılandırma alt bölümlerini görüntülemek için bir girdinin önündeki artı sembolünü tıklatın.
- Yapılandırma alt bölümlerini gizlemek için, genişletilmiş yapılandırma bölümünün önündeki eksi sembolünü tıklatın.

> **Not**
> Yapılandırma seçeneklerini etkinleştirmek veya devre dışı bırakmak ve düğmeleri kullanmak için, şu tuş birleşimlerini de kullanabilirsiniz: [**Alt**] + seçenek adında veya düğme açıklamasında altı çizili harf.

Yapılandırma ayarlarınızı onaylamak istiyorsanız:

- **Tamam**'ı tıklatın.
  - ↪ Yapılandırma penceresi kapatılır ve ayarlar kabul edilir.

  - VEYA -
- **Uygula** düğmesine tıkla.
  - ↪ Ayarlar uygulanır. Yapılandırma penceresi açık kalır.

Ayarlarınızı onaylamadan yapılandırmayı bitirmek istiyorsanız:

- **İptal**'i tıklatın.
  - ↪ Yapılandırma penceresi kapatılır ve ayarlar atılır.

Tüm yapılandırma ayarlarını varsayılan değerlere geri yüklemek istiyorsanız:

- **Varsayılan değerler** seçeneğine tıklayın.
  - ↪ Yapılandırmanın tüm ayarları, varsayılan değerlere geri yüklenir. Varsayılan ayarlar geri yüklendiğinde tüm değişiklikler ve özel girdiler kaybedilir.

Yapılandırma profilleri

Yapılandırma ayarlarınızı yapılandırma profilleri olarak kaydetme seçeneğiniz vardır. Yapılandırma profilinde, başka bir deyişle bir yapılandırmanın tüm yapılandırma seçenekleri bir gruba kaydedilir. Yapılandırma, gezinti çubuğunda bir düğüm olarak görüntülenir. Varsayılan yapılandırmaya başka yapılandırmalar ekleyebilirsiniz. Belirli bir yapılandırmaya geçiş yapmak için aynı zamanda kurallar tanımlayabilirsiniz:
Kurala dayalı bir yordam kullanarak yapılandırma değiştirilirken, yapılandırma bir LAN veya Internet bağlantısı kullanımına bağlantılandırılabilir (varsayılan ağ geçidi yoluyla

tanımlama). Böylece, farklı dizüstü bilgisayar kullanım senaryoları için yapılandırma profilleri oluşturulabilir:

- Şirket ağlarında kullanım: İntranet sunucusu aracılığıyla güncelleme, Web Koruması devre dışı
- Evde kullanım: Varsayılan Avira web sunucusu aracılığıyla güncelleme, Web Koruması etkin

Bir geçiş yapma kuralı tanımlanmadıysa, tepsi simgesinin bağlam menüsünde el ile bir yapılandırmaya geçiş yapabilirsiniz. Gezinti çubuğundaki düğmeleri kullanarak veya yapılandırma menüsündeki bağlam menüsünde yer alan komutları kullanarak yapılandırmalar ekleyebilir, yeniden adlandırabilir, silebilir, kopyalayabilir ya da geri yükleyebilir ve yapılandırmaları değiştirme kuralları tanımlayabilirsiniz.

> **Not**
> Kullanıcı Hesabı Kontrolü (UAC), Windows Vista gibi işletim sistemlerinde Gerçek Zamanlı Koruma, Güvenlik Duvarı Web Koruması ve EPosta Koruması gibi hizmetleri etkinleştirmek veya devre dışı bırakmak için izninizi isteyecektir.

Yapılandırma seçeneklerine genel bakış

Aşağıdaki yapılandırma seçenekleri kullanılabilir:

- **Sistem Tarayıcı**: İstek üzerine taramanın yapılandırması
  - Tarama seçenekleri
  - Algılama durumunda eylem
  - Daha fazla eylem
  - Tarama seçeneklerini arşivle
  - Sistem taraması istisnaları
  - Sistem taraması buluşsal yöntemleri
  - Rapor işlevi ayarı
- **Gerçek Zamanlı Koruma**: Erişim taraması yapılandırması
  - Tarama seçenekleri
  - Algılama durumunda eylem
  - Daha fazla eylem
  - Erişim taraması istisnaları
  - Erişim taraması buluşsal yöntemi
  - Rapor işlevi ayarı
- **Güncelleme**: Güncelleme ayarlarının yapılandırması, Web sunucusu veya dosya sunucusu aracılığıyla karşıdan yükleme
  - Dosya sunucusu aracılığıyla karşıdan yükleme
  - Web sunucusu aracılığıyla karşıdan yükleme

- Proxy ayarları

- **Güvenlik Duvarı**: Güvenlik Duvarı yapılandırması
  - Bağdaştırıcı kuralı ayarı
  - Kullanıcı tanımlı uygulama kuralı ayarları
  - Güvenilen üreticiler listesi (uygulamalar tarafından ağ erişimine ilişkin istisnalar)
  - Genişletilmiş ayarlar: Otomatik kural zaman aşımı, Windows Güvenlik Duvarı'nı durdurma, bildirimler
  - Açılır pencere ayarları (uygulamalar tarafından ağ erişimine ilişkin uyarılar)
- **Web Koruması**: Web Koruması yapılandırması
  - Tarama seçenekleri, Web Koruması etkinleştirme ve devre dışı bırakma
  - Algılama durumunda eylem
  - Engellenen erişim: İstenmeyen dosya türleri ve MIME türleri, bilinen istenmeyen URL'ler için web filtresi (zararlı yazılım, kimlik avı, vb.)
  - Web Koruması tarama istisnaları: URL'ler, dosya türleri, MIME türleri
  - Web Koruması buluşsal yöntemi
  - Rapor işlevi ayarı
- **EPosta Koruması**: EPosta Koruması yapılandırması
  - Tarama seçenekleri: POP3 hesaplarının, IMAP hesaplarının, giden e-postaların (SMTP) izlenmesini etkinleştir
  - Algılama durumunda eylemler
  - Daha fazla eylem
  - EPosta Koruması taraması buluşsal yöntemi
  - İstenmeyen Posta Gönderimi Engelleme işlevi: İzin verilen SMTP sunucuları, izin verilen e-posta gönderenler
  - EPosta Koruması taraması istisnaları
  - Önbellek yapılandırması, boş önbellek
  - Gönderilen e-postalarda altbilgi yapılandırması
  - Rapor işlevi ayarı
- **Genel**:
  - SMTP kullanılarak e-posta yapılandırması
  - Sistem Tarayıcı ve Gerçek Zamanlı Koruma tehdit kategorileri
  - Gelişmiş koruma: Proaktif ve Koruma Bulutu özelliklerini etkinleştirme seçenekleri.
  - Uygulama filtresi: Engellenen veya izin verilen uygulamalar
  - Kontrol Merkezi ve Yapılandırma erişimi için parola koruması
  - Güvenlik: otomatik başlama işlevini engelle, ürün koruma, Windows ana bilgisayar dosyalarını koru
  - WMI: WMI desteğini etkinleştir
  - Olay günlüğü yapılandırması
  - Rapor işlevlerinin yapılandırması
  - Kullanılan dizinlerin ayarı

- Uyarılar:

  Bileşen(ler) için ağ uyarılarının yapılandırılması:

  - Sistem Tarayıcı
  - Gerçek Zamanlı Koruma

  Bileşen(ler) için e-posta uyarılarının yapılandırması:

  - Sistem Tarayıcı
  - Gerçek Zamanlı Koruma
  - Güncelleyici
- Zararlı yazılım algılanması durumunda verilen sesli uyarıların yapılandırması

4.1.3 Tepsi simgesi

Kurulumdan sonra, Avira ürününüzün tepsi simgesini, görev çubuğunun sistem tepsisinde görürsünüz:

Simge	Açıklama
	Avira Gerçek Zamanlı Koruma etkin ve Güvenlik Duvarı etkin
	Avira Gerçek Zamanlı Koruma devre dışı veya Güvenlik Duvarı devre dışı

Tepsi simgesi, Gerçek Zamanlı Koruma ve Güvenlik Duvarı hizmetinin durumunu görüntüler.

Avira ürününüzün merkezi işlevlerine, **tepsi simgesinin** bağlam menüsü aracılığıyla hızlı şekilde erişilebilir. Bağlam menüsünü açmak için, sağ fare düğmesiyle **tepsi simgesini** tıklatın.

Bağlam menüsündeki girdiler

- **Gerçek Zamanlı Koruma'yı etkinleştir**: Avira Gerçek Zamanlı Koruma'yı etkinleştirir veya devre dışı bırakır.
- **EPosta Koruması'nı etkinleştir**: Avira EPosta Koruması'nı etkinleştirir veya devre dışı bırakır.
- **Web Koruması'nı etkinleştir**: Avira Web Koruması'nı etkinleştirir veya devre dışı bırakır.
- **Güvenlik Duvarı**:

  - **Güvenlik Duvarı'nı etkinleştir**: Avira Güvenlik Duvarı'nı etkinleştirir veya devre dışı bırakır
  - **Güvenlik Duvarı'nı etkinleştir**: Windows Güvenlik Duvarı'nı etkinleştirir veya devre dışı bırakır (bu özellik Windows 8'den itibaren sunulmaktadır).
  - **Tüm trafiği engelle**: Etkin. Ana bilgisayar sistemine yapılan aktarımlar dışında tüm veri aktarımlarını engeller (Yerel Ana Bilgisayar/IP 127.0.0.1).
- **Avira Professional Security'i başlat**: Kontrol Merkezi'ni açar.
- **Avira Professional Security'i yapılandır**: Yapılandırma'yı açar.
- **Güncellemeyi başlat** Bir güncelleme başlatır.
- **Yapılandırmayı seç**:Kullanılabilir yapılandırma profillerini içeren bir alt menü açar. Bu yapılandırmayı etkinleştirmek için bir yapılandırmayı tıklatın. Önceden bir yapılandırmaya otomatik geçiş yapma kuralı tanımladıysanız, menü komutu devre dışı bırakılır.
- **Yardım**: Online Yardım'ı açar.
- **Avira Professional Security hakkında:** Avira ürününüz hakkında bilgiler içeren bir iletişim kutusu açar: Ürün bilgileri, Sürüm bilgileri, Lisans bilgileri.
- **Internet'te Avira**: Internet'te Avira web portalını açar. Bunun koşulu, etkin bir Internet bağlantısının olmasıdır.

4.2 Nasıl yapılır...?

"Nasıl yapılır...?" bölümleri lisans ve ürün etkinleştirmesi hakkında kısa talimatlar ve Avira ürününüzün en önemli işlevleri hakkında bilgiler sağlar. Seçilen kısa makaleler Avira ürününüzün işlevselliği ile ilgili genel bir bakış görevi görür. Bu makaleler, bu yardım merkezinin her bir bölümünde yer alan ayrıntılı bilginin yerine geçmez.

4.2.1 Lisans etkinleştirme

Avira ürününüzün lisansını etkinleştirmek için:

.KEY lisans dosyası ile Avira ürününüzün lisansını etkinleştirin. Lisans dosyasını e-posta yoluyla Avira tarafından edinebilirsiniz. Lisans dosyası, tek bir sipariş işleminde sipariş ettiğiniz tüm ürünlerin lisansını içerir.

Avira ürününüzü henüz kurmadıysanız:

- Lisans dosyasını bilgisayarınızdaki yerel bir dizine kaydedin.
- Avira ürününüzü kurun.
- Kurulum sırasında, lisans dosyasının kaydetme konumuna girin.

Avira ürününüzü zaten kurduysanız:

- Dosya Yöneticisi'nde veya etkinleştirme e-postasında lisans dosyasını çift tıklatın ve Lisans Yöneticisi açıldığında ekrandaki yönergeleri izleyin.

- VEYA -

Avira ürününüzün Kontrol Merkezi'nde, **Yardım > Lisans dosyasını yükle…** menü öğesini seçin

Not
Windows Vista'dan itibaren Kullanıcı Hesabı Denetimi iletişim kutusu görüntülenir. Gerekirse, yönetici olarak oturum açın. **Devam**'ı tıklatın.

- Lisans dosyasını vurgulayın ve **Aç**'ı tıklatın.
  - ↪ Bir ileti görüntülenir.
- Onaylamak için **Tamam**'ı tıklatın.
  - ↪ Lisans etkinleştirilir.
- Gerekirse, sisteminizi yeniden başlatın.

4.2.2 Otomatik güncelleme gerçekleştir

Avira ürününüzü otomatik olarak güncellemek üzere Avira Zamanlayıcı ile bir iş oluşturmak için:

- Kontrol Merkezi'nde, *YÖNETİM* **> Zamanlayıcı** bölümünü seçin.
-  **Yeni iş ekle** simgesini tıklatın.
  - ↪ **İşin adı ve açıklaması** iletişim kutusu görüntülenir.
- İşe bir ad verin ve gerekirse bir açıklama girin.
- **İleri**'yi tıklatın.
  - ↪ **İş türü** iletişim kutusu görüntülenir.
- Listeden **İşi güncelle** seçeneğini belirleyin.
- **İleri**'yi tıklatın.
  - ↪ **İş zamanı** iletişim kutusu görüntülenir.
- Güncelleme için bir zaman seçin:

- **Hemen**
- **Günlük**
- **Haftalık**
- **Aralık**
- **Tek**
- **Oturum aç**

Not
Düzenli otomatik güncellemeler öneririz. Önerilen güncelleme aralığı: 60 dakika.

- Gerekirse, seçime göre bir tarih belirtin.
- Gerekirse, ek seçenekleri belirleyin (kullanılabilirlik durumu, iş türüne bağlıdır):

- **Süre dolduysa işi yinele**
  Örneğin, bilgisayar kapatıldığı için gerekli zamanda gerçekleştirilemeyen geçmiş işler gerçekleştirilir.
- **İnternet'e bağlanırken (çevirmeli) iş başlat**
  Tanımlanmış sıklığa ek olarak, bir İnternet bağlantısı kurulduğunda iş gerçekleştirilir.

- **İleri**'yi tıklatın.
  ↪ **Görüntü modu seç** iletişim kutusu görüntülenir.
- İş penceresinin görüntü modunu seçin:

- **Görünmez**: İş penceresi yok
- **Simge durumuna küçült**: yalnızca ilerleme çubuğu
- **Ekranı kapla**: Tüm iş penceresi

- **Son**'u tıklatın.
  ↪ Yeni oluşturduğunuz iş *YÖNETİM* **> Zamanlayıcı** bölümünün başlangıç sayfasında etkinleştirilen durum (onay işareti) ile görüntülenir.
- Gerekirse, gerçekleştirilmeyecek işleri devre dışı bırakın.

İşlerinizi daha fazla tanımlamak için aşağıdaki simgeleri kullanın:

 Bir işin özelliklerini görüntüle

 İşi düzenle

 İşi sil

 İş başlat

 İşi durdur

4.2.3 El ile güncelleme başlat

Bir güncellemeyi el ile başlatmak için birkaç seçeneğiniz vardır: Bir güncelleme otomatik olarak başlatıldığında, virüs tanımı dosyası ve tarama motoru otomatik olarak güncellenir.

Avira ürününüzün güncellemesini otomatik olarak başlatmak için:

- Sağ fare düğmesiyle görev çubuğundaki Avira tepsi simgesini tıklatın.
  ↪ Bir bağlam menüsü görüntülenir.
- **Güncellemeyi başlat** seçeneğini belirleyin.
  ↪ **Güncelleyici** iletişim kutusu görüntülenir.

- VEYA -

- Kontrol Merkezi'nde **Durum**'u seçin.
- **Son güncelleme** alanında **Güncellemeyi başlat** bağlantısını tıklatın.
  ↪ Güncelleyici iletişim kutusu görüntülenir.

- VEYA -

- Kontrol Merkezi'nde **Güncelle** menüsünde **Güncellemeyi başlat** menü komutunu seçin.
  ↪ Güncelleyici iletişim kutusu görüntülenir.

Not
Düzenli otomatik güncellemeler öneririz. Önerilen güncelleme aralığı: 60 dakika.

Not
Ayrıca Windows güvenlik merkezi aracılığıyla doğrudan el ile güncelleme yürütebilirsiniz.

4.2.4 Virüslere ve zararlı yazılımlara karşı tarama yapmak için bir tarama profili kullanma

Tarama profili, taranacak sürücü ve dizin kümesidir.

Aşağıdaki seçenekler, bir tarama profili aracılığıyla tarama için kullanılabilir:

Önceden tanımlı tarama profilini kullan

Önceden tanımlı tarama profili, gereksinimlerinize karşılık veriyorsa.

Tarama profilini özelleştir ve uygula (el ile seçim)

Özelleştirilmiş bir tarama profiliyle tarama yapmak istiyorsanız.

Yeni tarama profili oluştur ve uygula

Kendi tarama profilinizi oluşturmak istiyorsanız.

İşletim sistemine bağlı olarak, bir tarama profili başlatılmasına yönelik çeşitli simgeler kullanılabilir:

- Windows XP'de:

   Bu simge bir tarama profili aracılığıyla taramayı başlatır.

- Windows Vista'dan itibaren:

  Microsoft Windows Vista'dan itibaren, Kontrol Merkezi şu anda yalnızca sınırlı haklara; örneğin, dizinlere ve dosyalara erişim haklarına sahiptir. Belirli eylemler ve dosya erişimleri yalnızca genişletilmiş yönetici hakları ile Kontrol Merkezi'nde gerçekleştirilebilir. Bu genişletilmiş yönetici hakları bir tarama profili aracılığıyla her bir tarama başlangıcında verilebilir.

  -  Bu simge bir tarama profili aracılığıyla sınırlı bir taramayı başlatır. Yalnızca işletim sisteminin erişim hakkı verdiği dizinler ve dosyalar taranır.
  -  Bu simge, genişletilmiş yönetici hakları ile taramayı başlatır. Onaylamadan sonra, seçilen profildeki tüm dizinler ve dosyalar taranır.

Bir tarama profili ile virüslere ve zararlı yazılımlara karşı tarama yapmak için:

1. Kontrol Merkezi'ne gidin ve *PC KORUMASI* **> Sistem Tarayıcı** bölümünü seçin.
   ↪ Önceden tanımlı tarama profilleri görüntülenir.
2. Önceden tanımlı tarama profillerinden birini seçin.

   -VEYA-

   El ile seçim tarama profilini uyarlayın.

   -VEYA-

   Yeni bir tarama profili oluştur
3. Simgeyi tıklatın (Windows XP:  veya Windows Vista'dan itibaren: ).
4. **Luke Filewalker** penceresi görüntülenir ve sistem taraması başlatılır.
   ↪ Tarama tamamlandığında, sonuçlar görüntülenir.

Bir tarama profilini uyarlamak istiyorsanız:

1. Tarama profilinde **El İle Seçim** dosya ağacını genişletin, böylece taramak istediğiniz tüm sürücüler ve dizinler açılır.
   - **+** simgesini tıklatın: Sonraki dizin düzeyi görüntülenir.
   - **-** simgesini tıklatın: Sonraki dizin düzeyi gizlenir.
2. İlgili dizin düzeyinin ilgili kutusunu tıklatarak, taramak istediğiniz düğümleri ve dizinleri vurgulayın:

   Aşağıdaki seçenekler, dizinleri seçme için kullanılabilir:
   - Alt dizinleri de içeren dizin (siyah onay işareti)

- Yalnızca tek bir dizinin alt dizinleri (gri onay işareti, alt dizinlerin siyah onay işaretleri vardır)
- Dizin yok (onay işareti yoktur)

Yeni bir tarama profili oluşturmak istiyorsanız:

-  **Yeni profil oluştur** simgesini tıklatın.
  - ↪ **Yeni profil** profili, önceden oluşturulan profillerin aşağısında görüntülenir.
- Gerekirse,  simgesini tıklatarak tarama profilini yeniden adlandırın.
- İlgili dizin düzeyinin onay kutusunu tıklatarak, kaydedilecek düğümleri ve dizinleri vurgulayın.

  Aşağıdaki seçenekler, dizinleri seçme için kullanılabilir:

- Alt dizinleri de içeren dizin (siyah onay işareti)
- Yalnızca tek bir dizinin alt dizinleri (gri onay işareti, alt dizinlerin siyah onay işaretleri vardır)
- Dizin yok (onay işareti yoktur)

4.2.5 Sürükleyip Bırak yöntemini kullanarak virüslere ve zararlı yazılımlara karşı tarama yapma

Sürükleyip bırak yöntemini kullanarak virüslere ve zararlı yazılımlara karşı tarama yapmak için:

- ✓ Avira ürününüzün Kontrol Merkezi açıldı.
- Taramak istediğiniz dosyayı veya dizini vurgulayın.
- Vurgulanan dosyayı veya dizini **Kontrol Merkezi'ne** sürüklemek için sol fare düğmesini kullanın.
  - ↪ **Luke Filewalker** penceresi görüntülenir ve sistem taraması başlatılır.
  - ↪ Tarama tamamlandığında, sonuçlar görüntülenir.

4.2.6 Bağlam menüsü aracılığıyla virüslere ve zararlı yazılımlara karşı tarama yapma

Bağlam menüsü aracılığıyla virüslere ve zararlı yazılımlara karşı sistematik şekilde tarama yapmak için:

- Taramak istediğiniz dosyayı veya dizini sağ fare düğmesiyle tıklatın (örn. Windows Gezgini'nde, masaüstünde veya açık bir Windows dizininde).
  - ↪ Windows Gezgini bağlam menüsü görüntülenir.
- Bağlam menüsünde **Seçilen dosyaları Avira ile tara** seçeneğini belirleyin.
  - ↪ **Luke Filewalker** penceresi görüntülenir ve sistem taraması başlatılır.

↳ Tarama tamamlandığında, sonuçlar görüntülenir.

4.2.7 Virüslere ve zararlı yazılımlara karşı otomatik olarak tarama yapma

Not
Kurulumdan sonra **Tam sistem taraması** tarama işi Zamanlayıcı'da oluşturulur: Önerilen aralıkta bir tam sistem taraması otomatik olarak gerçekleştirilir.

Virüslere ve zararlı yazılımlara karşı otomatik olarak tarama yapmak üzere bir iş oluşturmak için:

- Kontrol Merkezi'nde, *YÖNETİM* **> Zamanlayıcı** bölümünü seçin.
-  simgesini tıklatın.
  ↳ **İşin adı ve açıklaması** iletişim kutusu görüntülenir.
- İşe bir ad verin ve gerekirse bir açıklama girin.
- **İleri**'yi tıklatın.
  ↳ **İş türü** iletişim kutusu görüntülenir.
- **Tarama işi** seçeneğini belirleyin.
- **İleri**'yi tıklatın.
  ↳ **Profil seçimi** iletişim kutusu görüntülenir.
- Taranacak profili seçin.
- **İleri**'yi tıklatın.
  ↳ **İşin zamanı** iletişim kutusu görüntülenir.
- Tarama için bir zaman seçin:

- **Hemen**
- **Günlük**
- **Haftalık**
- **Aralık**
- **Tek**
- **Oturum aç**

- Gerekirse, seçime göre bir tarih belirtin.
- Gerekirse, aşağıdaki ek seçenekleri belirleyin (kullanılabilirlik durumu, iş türüne bağlıdır):

  Süre önceden dolduysa işi yinele

  Örneğin, bilgisayar kapatıldığı için gerekli zamanda gerçekleştirilemeyen geçmiş işler gerçekleştirilir.
- **İleri**'yi tıklatın.

↳ **Görüntü modu seçimi** iletişim kutusu görüntülenir.

- İş penceresinin görüntü modunu seçin:

- **Görünmez**: İş penceresi yok
- **Simge durumuna küçült**: yalnızca ilerleme çubuğu
- **Ekranı kapla**: Tüm iş penceresi

- Tarama bittiğinde bilgisayarın otomatik olarak kapatılmasını istiyorsanız, **İş bittiğinde bilgisayarı kapat** seçeneğini belirleyin. Bu seçenek yalnızca görüntü modu simge durumuna küçültülmüşse veya ekranı kaplamışsa kullanılabilir.
- **Son**'u tıklatın.

  ↳ Yeni oluşturduğunuz iş *YÖNETİM* **> Zamanlayıcı** bölümünün başlangıç sayfasında etkinleştirilen durum (onay işareti) ile görüntülenir.
- Gerekirse, gerçekleştirilmeyecek işleri devre dışı bırakın.

İşlerinizi daha fazla tanımlamak için aşağıdaki simgeleri kullanın:

 Bir işin özelliklerini görüntüle

 İşi düzenle

 İşi sil

 İş başlat

İşi durdur

4.2.8 Kök kullanıcı takımına ve etkin zararlı yazılımlara karşı hedeflenmiş tarama

Etkin kök kullanıcı takımına karşı tarama yapmak için, **Kök kullanıcı takımı ve etkin zararlı yazılımlara karşı tara** önceden tanımlı tarama profilini kullanın.

Etkin kök kullanıcı takımına karşı sistematik olarak tarama yapmak için:

- Kontrol Merkezi'ne gidin ve *PC KORUMASI* **> Sistem Tarayıcı** bölümünü seçin.

  ↳ Önceden tanımlı tarama profilleri görüntülenir.
- **Kök kullanıcı takımı ve etkin zararlı yazılımlara karşı tara** önceden tanımlı tarama profilini seçin.
- Gerekirse, dizin düzeyinin onay kutusunu tıklatarak, taranacak diğer düğümleri ve dizinleri vurgulayın.
- Simgeyi tıklatın (Windows XP:  veya Windows Vista'dan itibaren: ).

- **Luke Filewalker** penceresi görüntülenir ve sistem taraması başlatılır.
- Tarama tamamlandığında, sonuçlar görüntülenir.

4.2.9 Algilanan virüslere ve zararli yazilimlara yanit verme

Algilama durumunda eylem bölümündeki **Yapilandirma'da** Avira ürününüzün tek tek koruma bilesenleri için Avira ürününüzün algilanan bir virüse veya istenmeyen programa nasil yanit verecegini tanimlayabilirsiniz.

Gerçek Zamanli Koruma'nin Proaktif bileseni için kullanilabilir durumda bir yapilandirilabilir eylem seçenegi yoktur: Bir algilama olduguna dair bildirim her zaman **Gerçek Zamanli Koruma: Süpheli uygulama davranisi** penceresinde gösterilir.

Sistem Tarayici için eylem seçenekleri:

Etkilesimli

Etkilesimli eylem modunda, Sistem Tarayici taramasinin sonuçlari bir iletisim kutusunda görüntülenir. Bu seçenek, varsayilan ayar olarak etkinlestirilir.

Sistem Tarayici taramasi olmasi durumunda, tarama tamamlandiginda etkilenen dosyalarin listesi ile birlikte bir uyari alirsiniz. Çesitli etkilenen dosyalar için yürütülecek bir eylem seçmek için baglama duyarli menüyü kullanabilirsiniz. Tüm etkilenen dosyalar için standart eylemleri yürütebilir veya Sistem Tarayici'yi iptal edebilirsiniz.

Otomatik

Otomatik eylem modunda bir virüs veya istenmeyen bir program algilandiginda, bu alanda seçtiginiz eylem otomatik olarak uygulanir. **Algilama uyarilarini görüntüle** seçenegini etkinlestirdiginizde, bir virüs algilandiginda eylemin uygulandigini gösteren bir uyari alirsiniz.

Gerçek Zamanli Koruma için eylem seçenekleri:

Etkilesimli

Etkilesimli eylem modunda, veri erisimi reddedilir ve bir masaüstü bildirimi görüntülenir. Masaüstü bildiriminde, algilanan zararli yazilimi kaldirabilir veya **Ayrintilar** dügmesini kullanarak zararli yazilimi daha fazla virüs yönetimi için Sistem Tarayici bilesenine aktarabilirsiniz. Sistem Tarayici, algilama bildirimini içeren ve etkilenen dosyanin bir baglam menüsü araciligiyla yönetilmesine iliskin çesitli seçenekleri size sunan bir pencereyi açar (bkz.Algilama > Sistem Tarayici):

Otomatik

Otomatik eylem modunda bir virüs veya istenmeyen bir program algilandiginda, bu alanda seçtiginiz eylem otomatik olarak uygulanir. **Algilama uyarilarini görüntüle** seçenegini etkinlestirdiginizde, bir virüs algilandiginda bir masaüstü bildirimi alirsiniz.

EPosta Korumasi,Web Korumasi algilamalari için eylem seçenekleri:

Etkilesimli

Etkilesimli eylem modunda, bir virüs veya istenmeyen program algilanmasi durumunda, etkilenen nesnenin ne yapilacagini seçebileceginiz bir iletisim kutusu görüntülenir. Bu seçenek, varsayilan ayar olarak etkinlestirilir.

Otomatik

Otomatik eylem modunda bir virüs veya istenmeyen bir program algilandiginda, bu alanda seçtiginiz eylem otomatik olarak uygulanir. **Ilerleme çubugunu göster** seçenegini etkinlestirdiginizde, bir virüs algilandiginda bir uyari alirsiniz. Uyari, gerçeklestirilecek eylemi onaylamaniza olanak saglar.

Etkilesimli eylem modunda, uyaridaki etkilenen nesne için bir eylem seçerek ve **Onayla**'yi tiklatip seçilen eylemi yürüterek, algilanan virüslere ve istenmeyen programlara yanit verebilirsiniz.

Etkilenen nesneleri ele almaya yönelik asagidaki eylemler seçilebilir:

Not
Hangi eylemlerin seçilebilir durumda oldugu, isletim sistemine, koruma bilesenlerine (Avira Gerçek Zamanli Koruma, Avira Sistem Tarayici, Avira EPosta Korumasi, Avira Web Korumasi) algilamanin raporlanmasina ve algilanan zararli yazilimin türüne baglidir.

Sistem Tarayici ve Gerçek Zamanli Koruma (Proaktif algilamalari degil) eylemleri:

Onar

Dosya onarilir.

Bu seçenek yalnizca etkilenen dosya onarilabiliyorsa kullanilabilir.

Yeniden Adlandir

Dosya, **.vir* uzantisiyla yeniden adlandirilir. Bu nedenle, bu dosyalara dogrudan (örnegin çift tiklatmayla) erisim artik mümkün degildir. Dosyalar daha sonra onarilabilir ve özgün adlariyla adlandirilabilir.

Karantina

Dosya özel bir biçimde (**.qua*) paketlenir ve sabit diskinizdeki *ETKILENEN* Karantina dizinine tasinir, böylece dogrudan erisim artik mümkün degildir. Bu dizindeki dosyalar daha ileri bir tarihte Karantina'da onarilabilir veya gerekirse Avira sirketine gönderilebilir.

Sil

Dosya silinecektir. Bu islem, **Üzerine yaz ve sil** isleminden daha hizlidir. Bir önyükleme sektörü virüsü algilandiginda bu virüs, önyükleme sektörünü silerek silinebilir. Yeni bir önyükleme sektörü yazilir.

Yoksay

Baska bir eylem gerçeklestirilmez. Etkilenen dosya, bilgisayarinizda etkin kalir.

Üzerine yaz ve sil

Varsayilan bir sablonla dosyanin üzerine yazilir ve sonra dosya silinir. Geri yüklenemez.

> **Uyari**
> Bu, veri kaybi ve isletim sistemi hasariyla sonuçlanabilir! Yalnizca özel durumlarda **Yoksay** seçenegini belirleyin.

Her zaman yoksay

Gerçek Zamanli Koruma algilamalari için eyleme seçenegi: Gerçek Zamanli Koruma baska bir eylem gerçeklestirmez. Dosyaya erisime izin verilir. Bu dosyaya diger tüm erisimlere izin verilir ve bilgisayar yeniden baslatilincaya veya virüs tanimi dosyasi güncellenince kadar baska bir bildirim saglanmaz.

Karantinaya kopyala

Kök kullanici takimlarinin algilamasi için eylem seçenegi: Algilama, karantinaya kopyalanir.

Önyükleme sektörünü onar | Onarim aracini karsidan yükleyin

Etkilenen önyükleme sektörleri algilandiginda eylem seçenekleri: Etkilenen disket sürücülerini onarmak için birkaç seçenek mevcuttur. Avira ürününüz onarim gerçeklestiremiyorsa, önyükleme sektörü virüslerinin algilanmasi ve kaldirilmasi için özel bir araç karsidan yükleyebilirsiniz.

> **Not**
> Çalismakta olan islemlerle ilgili eylemler yürütürseniz, eylemler gerçeklestirilmeden önce söz konusu islemler sonlandirilir.

Proaktif bileseni tarafindan yapilan algilamalar için Gerçek Zamanli Koruma eylemleri (bir uygulamanin süpheli eylemlerine iliskin bildirim):

Güvenilen program

Uygulama çalismaya devam eder. Program, izin verilen uygulamalar listesine eklenir ve Proaktif bileseninin izlemesi disinda birakilir. Izin verilen uygulamalar listesine

ekleme yapilirken, izleme türü *Içerik* olarak ayarlanir. Baska bir deyisle, uygulama, yalnizca içerik degistirilmeden kalirsa Proaktif bileseni izlemesi disinda birakilir (bkz. Uygulama filtresi: Izin verilen uygulamalar).

Programi bir defa engelle

Uygulama engellenir; baska bir deyisle, uygulama sonlandirilir. Uygulama eylemleri, Proaktif bileseni tarafindan izlenmeye devam eder.

Bu programi her zaman engelle

Uygulama engellenir; baska bir deyisle, uygulama sonlandirilir. Program, engellenen uygulamalar listesine eklenir ve artik çalistirilamaz (bkz. Uygulama filtresi: Engellecek uygulamalar).

Yoksay

Uygulama çalismaya devam eder. Uygulama eylemleri, Proaktif bileseni tarafindan izlenmeye devam eder.

EPosta Korumasi eylemleri: Gelen e-postalar

Karantinaya tasi

Tüm ekleri içeren e-posta, karantinaya tasinir. Etkilenen e-posta silinir. E-posta metninin gövdesi ve ekler, bir varsayilan metin ile degistirilir.

Postayi sil

Etkilenen e-posta silinir. E-posta metninin gövdesi ve ekler, bir varsayilan metin ile degistirilir.

Eki sil

Etkilenen ek, varsayilan bir metin ile degistirilir. E-posta gövdesi etkilendiyse, silinir ve yerine varsayilan bir metin gelir. E-posta teslim edilir.

Eki karantinaya tasi

Etkilenen ek, karantinaya yerlestirilir ve sonra silinir (varsayilan metin ile degistirilir). E-posta gövdesi teslim edilir. Etkilenen ek daha sonra karantina yöneticisi araciligiyla gönderilebilir.

Yoksay

Etkilenen e-posta teslim edilir.

Uyari
Bu, virüs ve istenmeyen programlarin bilgisayar sisteminize erismesine olanak saglar. Yalnizca özel durumlarda **Yoksay** seçenegini belirleyin. Posta istemcinizde önizlemeyi devre disi birakin, asla ekleri çift tiklatarak açmayin!

EPosta Korumasi eylemleri: Giden e-postalar

Postayi karantinaya tasi (gönderme)

Tüm eklerle birlikte e-posta Karantinaya tasinir ve gönderilmez. E-posta, e-posta istemcinizin giden kutusunda kalir. E-posta programinizda bir hata iletisi alirsiniz. E-posta hesabinizdan gönderilen diger tüm e-postalar, zararli yazilima karsi taranir.

Postalarin gönderimini engelle (gönderme)

E-posta gönderilmez ve e-posta istemcinizin giden kutusunda kalir. E-posta programinizda bir hata iletisi alirsiniz. E-posta hesabinizdan gönderilen diger tüm e-postalar, zararli yazilima karsi taranir.

Yoksay

Etkilenen e-posta gönderilir.

Uyari
Virüsler ve istenmeyen programlar, bu sekilde e-posta alicisinin bilgisayar sistemine girebilir.

Web Korumasi eylemleri:

Erisimi reddet

Web sunucusundan istenen web sitesi ve/veya aktarilan veri ya da dosyalar, web tarayiciniza gönderilmez. Web tarayicisinda, erisimin reddedildigini bildiren bir hata iletisi görüntülenir.

Karantinaya tasi

Web sunucusundan istenen web sitesi ve/veya aktarilan veri ya da dosyalar karantinaya tasinir. Etkilenen dosya, bilgilendirici bir degere sahipse karantina yöneticisinden kurtarilabilir veya gerekirse, Avira Zararli Yazilim Arastirma Merkezi'ne gönderilir.

Yoksay

Web sunucusundan istenen web sitesi ve/veya aktarilan veri ve dosyalar, Web Korumasi tarafindan web tarayiciniza iletilir.

Uyari
Bu, virüs ve istenmeyen programlarin bilgisayar sisteminize erismesine olanak saglar. Yalnizca özel durumlarda **Yoksay** seçenegini belirleyin.

Not
Onarilamayan süpheli dosyalari karantinaya tasimanizi öneririz.

Not
Ayrica bulussal yöntemin bildirdigi dosyalari analiz için bize de gönderebilirsiniz. Örnegin bu dosyalari web sitemize yükleyebilirsiniz:
http://www.avira.com/tr/sample-upload
HEUR/ veya *HEURISTIC/* göstergesinden örnegin *HEUR/testfile.** dosya adina ön ek olarak getirilen bulussal yöntemin bildirdigi dosyalari tanimlayabilirsiniz.

4.2.10 Karantinaya alınan dosyaları (*.qua) işleme

Karantinaya alınan dosyaları işlemek için:

- Kontrol Merkezi'nde, *YÖNETİM* **> Karantina** bölümünü seçin.
- Hangi dosyaların dahil edildiğini kontrol edin, böylece gerekirse, başka bir konumdan bilgisayarınıza özgün olanı yeniden yükleyebilirsiniz.

Bir dosyayla ilgili daha fazla bilgi görüntülemek isterseniz:

- Dosyayı vurgulayın ve  öğesini tıklatın.
  - ↪ Dosyayla ilgili daha fazla bilgi içeren **Özellikler** iletişim kutusu açılır.

Bir dosyayı yeniden taramak istiyorsanız:

Avira ürününüzün virüs tanımı dosyası güncellendiyse ve yanlış pozitif rapor olmasından şüpheleniliyorsa, dosyanın taranması önerilir. Bu, bir yanlış pozitifi yeniden tarama ile onaylamanıza ve dosyayı geri yüklemenize olanak sağlar.

- Dosyayı vurgulayın ve  öğesini tıklatın.
  - ↪ Sistem tarama ayarları kullanılarak dosya virüslere ve zararlı yazılımlara karşı taranır.
  - ↪ Taramadan sonra, yeniden tarama öncesinde ve sonrasında dosyanın durumuyla ilgili istatistikleri görüntüleyen **Yeniden tarama istatistikleri** iletişim kutusu görüntülenir.

Bir dosyayı silmek için:

- Dosyayı vurgulayın ve  öğesini tıklatın.
- Seçiminizi **Evet** ile onaylamanız gerekir.

Dosyayı, analiz için Avira Zararlı Yazılım Araştırma Merkezi web sunucusuna karşıya yüklemek istiyorsanız:

- Karşıya yüklemek istediğiniz dosyayı vurgulayın.
-  öğesini tıklatın.
  - ↳ İlgili kişi verilerinizi girmeniz için bir form bulunan iletişim kutusu açılır.
- Tüm gerekli verileri girin.
- Bir tür seçin: **Şüpheli dosya** veya **Şüpheli yanlış tespit**.
- Bir yanıt biçimi seçin: **HTML**, **Metin**, **HTML ve Metin**.
- **Tamam**'ı tıklatın.
  - ↳ Dosya, sıkıştırılmış şekilde Avira Zararlı Yazılım Araştırma Merkezi web sunucusuna karşıya yüklenir.

Not
Aşağıdaki durumlarda Avira Zararlı Yazılım Araştırma Merkezi tarafından bir analiz yapılması önerilir:
Buluşsal yöntem isabetleri (Şüpheli dosya): Bir tarama esnasında bir dosya Avira ürününüz tarafından şüpheli olarak sıfırlandırıldı ve karantinaya alındı: Virüs algılama iletişim ktuusunda veya tarama tarafından oluşturulan rapor dosyasında dosyanın Avira Zararlı Yazılım Araştırma Merkezi tarafından analiz edilmesi önerildi.
Şüpheli dosya: Bir dosyanın şüpheli olduğunu düşündüğünüzden, bu dosyayı karantinaya taşıdınız, ancak dosyanın virüslere ve zararlı yazılıma karşı taraması negatiftir.
Şüpheli yanlış tespit: Bir virüs tespitinin bir yanlış pozitif olduğunu düşünüyorsunuz: Avira ürününüz zararlı yazılım tarafından etkilenmiş olma ihtimali çok düşük olan bir dosyada bir algılama bildiriyor.

Not
Karşıya yüklediğiniz dosyaların boyutu, 20 MB sıkıştırılmamış veya 8 MB sıkıştırılmış olarak sınırlandırılmıştır.

Karantinaya alınmış bir nesneyi, karantinadan başka bir dizine kopyalamak istiyorsanız:

- Karantinaya alınmış nesneyi vurgulayın ve  öğesini tıklatın.
  - ↳ Bir dizin seçebileceğiniz *Klasöre Gözat* iletişim kutusu açılır.
- Karantinaya alınmış nesnenin bir kopyasını kaydetmek istediğiniz bir dizini seçin ve seçiminizi onaylayın.
  - ↳ Seçilen karantinaya alınmış nesne, seçilen dizine kaydedilir.

Not
Karantinaya alınmış nesne, geri yüklenen dosya ile aynı değildir. Karantinaya alınmış nesne şifrelenir ve özgün biçiminde yürütülemez veya okunamaz.

Karantinaya alınmış nesnenin özelliklerini bir metin dosyasına dışa aktarmak istiyorsanız:

- Karantinaya alınmış nesneyi vurgulayın ve  öğesini tıklatın.
  - ↪ Seçilen karantinaya alınmış nesneden verileri içeren *karantina - Not defteri* metin dosyası açılır.
- Metin dosyasını kaydedin.

Karantinadaki dosyaları da geri yükleyebilirsiniz (bkz. Bölüm: Karantina: Karantinaya alınan dosyaları geri yükleme).

4.2.11 Karantinadaki dosyaları geri yükleme

İşletim sistemine bağlı olarak, geri yükleme yordamını farklı simgeler denetler:

- Windows XP'de:
  -  Bu simge, dosyaları özgün dizinine geri yükler.
  -  Bu simge, dosyaları istediğiniz bir dizine geri yükler.
- Windows Vista'dan itibaren:

  Microsoft Windows Vista'dan itibaren, Kontrol Merkezi şu anda yalnızca sınırlı haklara; örneğin, dizinlere ve dosyalara erişim haklarına sahiptir. Belirli eylemler ve dosya erişimleri yalnızca genişletilmiş yönetici hakları ile Kontrol Merkezi'nde gerçekleştirilebilir. Bu genişletilmiş yönetici hakları bir tarama profili aracılığıyla her bir tarama başlangıcında verilebilir.
  -  Bu simge, dosyaları istediğiniz bir dizine geri yükler.
  -  Bu simge, dosyaları özgün dizinine geri yükler. Bu dizine erişmek için genişletilmiş yönetici hakları gerekliyse, karşılık gelen bir istek görüntülenir.

Karantinadaki dosyaları geri yüklemek için:

Uyarı
Bu, veri kaybı ve bilgisayar işletim sistemi hasarıyla sonuçlanabilir! Yalnızca özel durumlarda **Seçilen nesneleri geri yükle** işlevini kullanın. Yalnızca yeni bir tarama tarafından onarılabilen dosyaları geri yükleyin.

✓ Dosya yeniden tarandı ve onarıldı.

- Kontrol Merkezi'nde, *YÖNETİM* **> Karantina** bölümünü seçin.

Not

Dosya uzantısı **.eml* olduğunda, e-postalar ve e-posta ekleri yalnızca seçeneğini kullanarak geri yüklenebilir.

Bir dosyayı özgün konumuna geri yüklemek için:

- Dosyayı vurgulayın ve simgeyi tıklatın (Windows XP: , Windows Vista'dan itibaren).

E-postalar için bu seçenek kullanılamaz.

Not

Dosya uzantısı **.eml* olduğunda, e-postalar ve e-posta ekleri yalnızca seçeneğini kullanarak geri yüklenebilir.

  - ↳ Dosyayı geri yüklemek isteyip istemediğinizi soran bir ileti görüntülenir.
- **Evet**'i tıklatın.
  - ↳ Dosya, karantinaya taşınmadan önceki dizine geri yüklenir.

Bir dosyayı belirtilen bir dizine geri yüklemek için:

- Dosyayı vurgulayın ve öğesini tıklatın.
  - ↳ Dosyayı geri yüklemek isteyip istemediğinizi soran bir ileti görüntülenir.
- **Evet**'i tıklatın.
  - ↳ Dizin seçmeye yönelik *Farklı Kaydet* Windows varsayılan penceresi görüntülenir.
- Dosyanın geri yükleneceği dizini seçin ve onaylayın.
  - ↳ Dosya, seçilen dizine geri yüklenir.

4.2.12 Şüpheli dosyaları karantinaya taşıma

Şüpheli dosyayı el ile karantinaya taşımak için:

- Kontrol Merkezi'nde, *YÖNETİM* **> Karantina** bölümünü seçin.
- öğesini tıklatın.
  - ↳ Dosya seçmeye yönelik Windows varsayılan penceresi görüntülenir.
- Dosyayı seçin ve **Aç** ile onaylayın.
  - ↳ Dosya karantinaya taşınır.

Karantinadaki dosyaları, Avira Sistem Tarayıcı ile tarayabilirsiniz (bkz. Bölüm: Karantina: Karantinaya alınan dosyaları (*.qua) işleme).

4.2.13 Bir tarama profilinde dosya türünü değiştirme veya silme

Bir tarama profilinde, taranacak ek dosya türlerini şart koşmak veya belirli dosya türlerini tarama dışında bırakmak için (yalnızca el ile seçim ve özelleştirilmiş tarama profilleri için mümkündür):

✓ Kontrol Merkezi'nde *PC KORUMA* **> Sistem Tarayıcı** bölümüne gidin.

- Sağ fare düğmesiyle, düzenlemek istediğiniz tarama profilini tıklatın.
  - ↳ Bir bağlam menüsü görüntülenir.
- **Dosya filtresi**'ni seçin.
- Bağlam menüsünün sağındaki küçük üçgeni tıklatarak bağlam menüsünü daha fazla genişletin.
  - ↳ **Varsayılan**, **Tüm dosyaları tara** ve **Kullanıcı tanımlı** girdileri görüntülenir.
- **Kullanıcı tanımlı** seçeneğini belirleyin.
  - ↳ Tarama profili ile taranacak tüm dosya türlerinin listelerini içeren **Dosya uzantıları** iletişim kutusu görüntülenir.

Bir dosya türünü tarama dışında bırakmak istiyorsanız:

- Dosya türünü vurgulayın ve **Sil**'i tıklatın.

Taramaya bir dosya türünü eklemek istiyorsanız:

- Bir dosya türü vurgulayın.
- **Ekle**'yi tıklatın ve giriş kutusuna dosya türünün dosya uzantısını girin.

Maksimum 10 karakter kullanın ve en başa nokta koymayın. Joker karakterlere (* ve ?) izin verilir.

4.2.14 Tarama profili için masaüstü kısayolu oluşturma

Avira ürününüzün Kontrol Merkezi'ne erişmeden bir tarama profiline yönelik masaüstü kısayolu aracılığıyla doğrudan masaüstünüzden sistem taraması başlatabilirsiniz.

Tarama profiline yönelik bir masaüstü kısayolu oluşturmak için:

✓ Kontrol Merkezi'nde *PC KORUMA* **> Sistem Tarayıcı** bölümüne gidin.

- Kısayolunu oluşturmak istediğiniz tarama profilini seçin.
-  simgesini tıklatın.
  - ↳ Masaüstü kısayolu oluşturulur.

4.2.15 Olayları filtreleme

Avira ürününüzün program bileşenleri tarafından oluşturulan olaylar, Kontrol Merkezi'nde *YÖNETİM* **> Olaylar** konumunda görüntülenir (Windows işletim sisteminin olay görüntüsüne benzer). Program bileşenleri alfabetik sırayla aşağıdaki gibidir:

- Güvenlik Duvarı
- Yardımcı Hizmeti
- EPosta Koruması
- Gerçek Zamanlı Koruma
- Zamanlayıcı
- Sistem Tarayıcı
- Güncelleyici
- Web Koruması
- Proaktif

Aşağıdaki olay türleri görüntülenir:

- *Bilgi*
- *Uyarı*
- *Hata*
- *Algılama*

Görüntülenen olayları filtrelemek için:

- Kontrol Merkezi'nde, *YÖNETİM* **> Olaylar** bölümünü seçin.
- Etkinleştirilen bileşenlerin olaylarını görüntülemek için, program bileşenlerinin kutusunu işaretleyin.

  - VEYA -

  Devre dışı bırakılan bileşenlerin olaylarını gizlemek için, program bileşenlerinin kutusunun işaretini kaldırın.
- Bu olayları görüntülemek için olay türü kutusunu işaretleyin.

  - VEYA -

  Bu olayları gizlemek için olay türü kutusunun işaretini kaldırın.

4.2.16 E-posta adreslerini tarama dışında bırakma

Hangi e-posta adreslerinin (gönderenler) EPosta Koruması taraması dışında bırakılacağını tanımlamak için (beyaz liste):

- Kontrol Merkezi'ne gidin ve *İNTERNET KORUMASI* **> EPosta Koruması** bölümünü seçin.

↳ Listede, gelen e-postalar gösterilir.

- EPosta Koruması taraması dışında bırakmak istediğiniz e-postayı vurgulayın.
- E-postayı EPosta Koruması taraması dışında bırakmak için simgeyi tıklatın:

▪  Seçilen e-posta adresi artık virüslere ve istenmeyen programlara karşı taranmaz.

↳ E-posta gönderen adresi, dışlama listesine dahil edilir ve artık virüslere, zararlı yazılımlara karşı taranmaz.

Uyarı
Yalnızca gönderenler tamamen güvenilirse, e-posta adreslerini EPosta Koruması taraması dışında bırakın.

Not
Yapılandırma'da, EPosta Koruması > Genel > İstisnalar konumunda, dışlama listesine başka e-posta adresleri ekleyebilir veya e-posta adreslerini dışlama listesinden kaldırabilirsiniz.

4.2.17 Güvenlik Duvarı için güvenlik düzeyini seçme

Arasından seçim yapılacak çeşitli güvenlik düzeyleri vardır. Hangisini seçtiğinize bağlı olarak, farklı bağdaştırıcı kuralı yapılandırma seçenekleriniz vardır.

Düşük

Baskın ve bağlantı noktası taraması algılanır.

Orta

Şüpheli TCP ve UDP paketleri atılır.

Baskın ve bağlantı noktası taraması önlenir.

(Varsayılan düzeye ayarla.)

Yüksek

Bilgisayar ağda görünmez.

Dışarıdan gelen yeni bağlantılara izin verilmez.

Baskın ve bağlantı noktası taraması önlenir.

Özel

Kullanıcı tanımlı kurallar: Bu güvenlik düzeyi seçilirse, program, bağdaştırıcı kurallarının değiştirildiğini otomatik olarak tanır.

Tümünü engelle

Tüm mevcut ağ bağlantıları kapanacak.

> **Not**
> Avira Güvenlik Duvarı'nın tüm önceden tanımlı kuralları için varsayılan Güvenlik düzeyi ayarı, **Orta**'dır.

Güvenlik Duvarı'na yönelik güvenlik düzeyini tanımlamak için:

- Kontrol Merkezi'ne gidin ve *İNTERNET KORUMASI* **> Güvenlik Duvarı** bölümünü seçin.
- Kaydırıcıyı gerekli güvenlik düzeyine getirin.
  - ↪ Seçilen güvenlik düzeyi, hemen uygulanır.

5. Algılama

5.1 Genel bakış

Bir virüs algılandığında, Avira programınız otomatik olarak belirli eylemleri yürütebilir veya etkileşimli şekilde yanıt verebilir. Etkileşimli eylem modunda, bir virüs algılandığında, virüsün daha sonra nasıl ele alınacağını (sil, yoksay, vb.) denetleyebileceğiniz veya başlatabileceğiniz bir iletişim kutusu açılır. Otomatik modda, bir virüs algılandığında uyarı görüntüleme seçeneği vardır. Otomatik olarak yürütülen eylem, iletide görüntülenir.

Bu bölümde, modüle göre düzenlenmiş, algılama iletileriyle ilgili kapsamlı bilgiler yer alır.

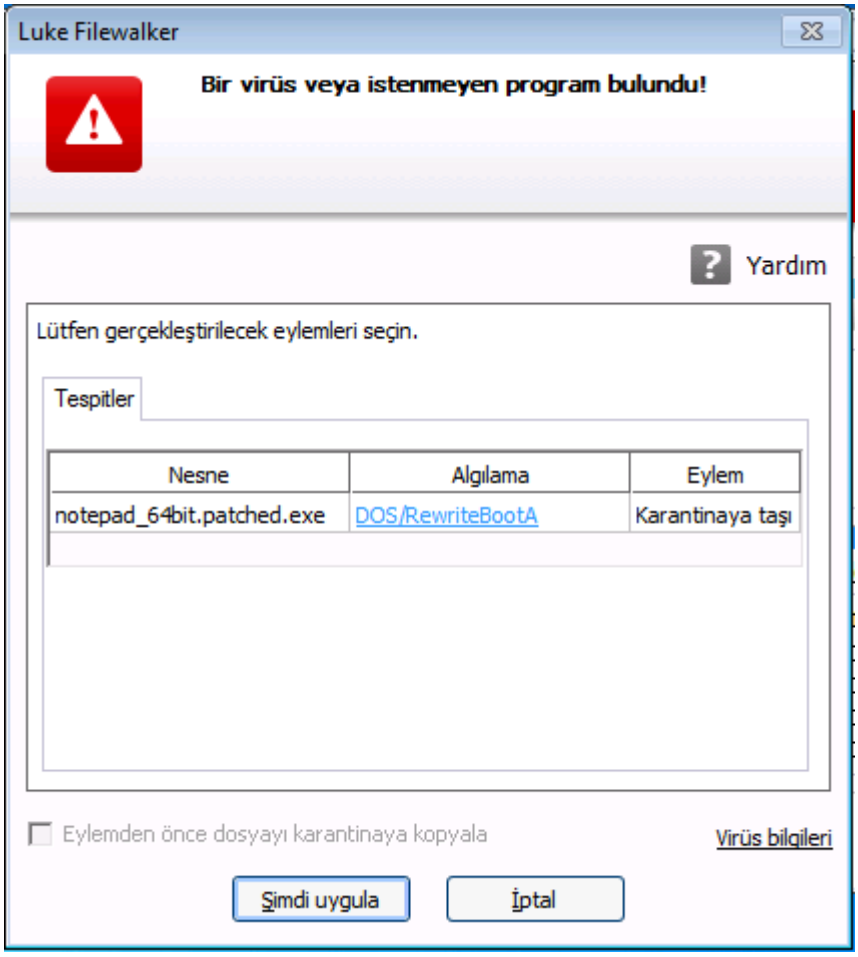
- bkz. Bölüm Sistem Tarayıcı: Etkileşimli eylem modu
- bkz. Bölüm Sistem Tarayıcı: Otomatik eylem modu
- bkz. Bölüm Sistem Tarayıcı: Koruma Bulutuna dosya gönderme
- bkz. Bölüm Gerçek Zamanlı Koruma
- bkz. Bölüm Gerçek Zamanlı Koruma: Şüpheli davranış
- bkz. Bölüm EPosta Koruması: Gelen e-postalar
- bkz. Bölüm EPosta Koruması: Giden e-postalar
- bkz. Bölüm E-posta gönderme: Gönderen
- bkz. Bölüm E-posta gönderme: Sunucu
- bkz. Bölüm Web Koruması

5.2 Etkileşimli eylem modu

Bir virüs algılandığında eylem modu olarak *Etkileşimli* modunu seçmeniz durumunda, tarama tamamlandığında etkilenen dosyaların listesini içeren bir uyarı alırsınız (Sistem Tarayıcı > Tara > Algılama durumunda eylem yapılandırma bölümüne bakın).
Çeşitli etkilenen dosyalar için yürütülecek bir eylem seçmek için bağlama duyarlı menüyü kullanabilirsiniz. Tüm etkilenen dosyalar için standart eylemleri yürütebilir veya Sistem Tarayıcı'yı iptal edebilirsiniz.

Not
Eğerraporlama etkinleştirilirse, Sistem Tarayıcı her algılamayı Rapor dosyasına girer.

5.2.1 Uyarı



5.2.2 Algılama, Hatalar, Uyarılar

Algılama, **Hatalar** ve **Uyarılar** sekmelerinde, algılanan virüsler ve iletiler için ayrıntılı bilgi ve eylem seçenekleri görüntülenir:

- **Algılama:**
  - *Nesne:* Etkilenen dosyanın dosya adı
  - *Algılama:* Virüsün veya istenmeyen programın adı
  - *Eylem:* Etkilenen dosyaya uygulanacak seçilen eylem
    Görüntülenen eylemle ilişkili bağlam menüsünden zararlı yazılımlara uygulanacak diğer eylemleri seçebilirsiniz.
- **Hata:** Tarama sırasında oluşan hatalarla ilgili iletiler
- **Uyarılar:** Algılanan virüslerle ilgili uyarılar

> **Not**
> Nesneye ait araç ipucunda aşağıdaki bilgiler gösterilir: Etkilenen dosyanın adı ve tam yolu, virüsün adı ve **Şimdi Uygula** düğmesiyle gerçekleştirilecek eylem.

Not
Varsayılan Sistem Tarayıcı eylemi, yürütülecek eylem olarak görüntülenir. Etkilenen dosyalara uygulanacak varsayılan Sistem Tarayıcı eylemi, *İzin Verilen Eylemler* alanında Sistem Tarayıcı > Tara > Algılama durumunda eylem yapılandırma bölümünde ayarlanabilir.

5.2.3 Bağlam menüsü eylemleri

Not
Algılama bir buluşsal yöntem isabetiyse (HEUR/), olağandışı çalışma zamanı paketleyicisiyse (PCK/) veya gizli dosya uzantısı içeren bir dosyaysa (HEUR-DBLEXT/), etkileşimli modda yalnızca Karantinaya taşı ve Yoksay seçenekleri kullanılabilir. Otomatik modda algılama otomatik olarak Karantina
'ya taşınır. Bu kısıtlama, yanlış alarm olabilecek algılanmış dosyaların doğrudan bilgisayarınızdan kaldırılmasını (silinmesini) önler. Bu dosya, istendiği zaman Karantina Yöneticisiyardımıyla kurtarılabilir.
Yapılandırmaya bağlı olarak, çeşitli seçenekler kullanılabilir olmayabilir.

Onar

Bu seçenek etkinleştirilirse, Scanner, etkilenen dosyayı onarır.

Not
Onar seçeneği yalnızca algılanan dosyanın onarımı mümkünse etkinleştirilebilir.

Karantina

Bu seçenek etkinleştirilirse, Scanner, dosyayı karantinaya taşır. Dosya, bilgilendirici bir değere sahipse karantina yöneticisinden kurtarılabilir veya gerekirse, Avira Zararlı Yazılım Araştırma Merkezi'ne gönderilir. Dosyaya bağlı olarak, karantina yöneticisinde daha fazla seçenek kullanılabilir.

Sil

Bu seçenek etkinleştirilirse, dosya silinir. Bu işlem, "üzerine yaz ve sil" işleminden daha hızlıdır.

Üzerine yaz ve sil

Bu seçenek etkinleştirilirse, Scanner varsayılan bir desenle dosyanın üzerine yazar ve sonra dosyayı siler. Geri yüklenemez.

Yeniden Adlandır

Bu seçenek etkinleştirilirse, Scanner, dosyayı yeniden adlandırır. Bu nedenle, bu dosyalara doğrudan (örneğin çift tıklatmayla) erişim artık mümkün değildir. Dosyalar daha sonra tekrar onarılabilir ve özgün adlarıyla adlandırılabilir.

Yoksay

Bu seçenek etkinleştirilirse, dosyaya erişime izin verilir ve dosya olduğu gibi bırakılır.

Her zaman yoksay

Gerçek Zamanlı Koruma algılamaları için eyleme seçeneği: Gerçek Zamanlı Koruma başka bir eylem gerçekleştirmez. Dosyaya erişime izin verilir. Bu dosyaya diğer tüm erişimlere izin verilir ve bilgisayar yeniden başlatılıncaya veya virüs tanımı dosyası güncelleninceye kadar başka bir bildirim sağlanmaz.

Uyarı
Seçenekleri yoksayarsanız veya **Her zaman yoksay** seçeneğini belirlerseniz, etkilenen dosyalar bilgisayarınızda etkin kalır! Bu, iş istasyonunuzda ciddi hasara neden olabilir!

5.2.4 Etkilenen önyükleme sektörleri, kök kullanıcı takımları ve etkin zararlı yazılım algılandığında özel işlevler

Etkilenen önyükleme sektörleri algılandığında, bunların onarılması için eylem seçenekleri kullanılabilir:

722 KB | 1,44 MB | 2,88 MB | 360 KB | 1,2 MB önyükleme sektörünü onar

Disket sürücüleri için bu seçenekler kullanılabilir.

Kurtarma CD'sini karşıdan yükleyin

Bu seçenek sizi önyükleme sektörü virüslerinin algılanması ve kaldırılması için özel bir araç karşıdan yükleyebileceğiniz Avira web sitesine götürür.

Çalışmakta olan işlemlerle ilgili eylemler yürütürseniz, eylemler gerçekleştirilmeden önce söz konusu işlemler sonlandırılır.

5.2.5 Düğmeler ve bağlantılar

Düğme / bağlantı	Beschreibung
Şimdi uygula	Seçilen eylemler, tüm etkilenen dosyaları işlemek için yürütülür.
İptal	Scanner daha fazla eylem olmadan kapatılır. Etkilenen dosyalar, bilgisayar sisteminizde değişmeden kalır.
Yardım	Online yardımın bu sayfası, bu düğme veya bağlantı aracılığıyla açılır.

Uyarı
Yalnızca özel durumlarda *İptal* eylemini yürütün. İptal işleminden sonra, etkilenen dosyalar iş istasyonunuzda etkin kalır! Bu, iş istasyonunuzda ciddi hasara neden olabilir!

5.2.6 Web Koruması devre dışıyken zararlı yazılım algılandığında özel işlevler

Web Koruması'nı devre dışı bıraktıysanız, Sistem Tarayıcı algıladığı aktif zararlı yazılımı sistemi tararken bir slide-up aracılığıyla bildirir. Sisteminizi onarmadan önce, bir geri yükleme noktası oluşturabilirsiniz.

✓ Öncelikle Windows sisteminizde Sistem Geri Yükleme özelliğini etkinleştirmeniz gerekir.

- Slide-up'ta **Ayrıntılara** seçeneğine tıklayın.
  - ↳ *Sistem taranıyor* penceresi görüntülenir.
- **Onarımdan önce sistem geri yükleme noktası oluştur** seçeneğini etkinleştir.
- **Uygula** düğmesine tıkla.
  - ↳ Sistem geri yükleme noktası oluşturuldu. Şimdi gerekiyorsa Windows Denetim Masası'nı kullanarak sistem geri yüklemesi yapabilirsiniz.

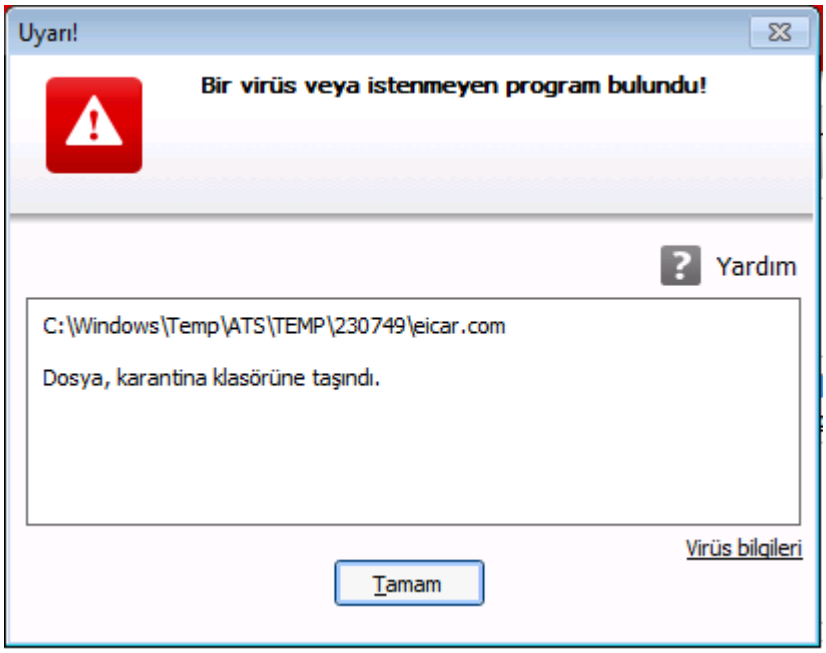
5.3 Otomatik eylem modu

Bir virüs algılandığında eylem modu olarak *Otomatik* modunu ve *Uyarı görüntüle* seçeneğini belirlediyseniz, Sistem Tarayıcı dosyada her virüs algıladığında bir uyarı alırsınız (Sistem Tarayıcı > Tara > Algılama durumunda eylem yapılandırma bölümüne bakın). Uyarı ile otomatik modda algılanan virüsü işleme seçeneği yoktur. Virüsle

ilgilenmek için yapılandırmada seçilen eylem gerçekleştirilir. Otomatik olarak yürütülen eylem, iletide görüntülenir.

> **Not**
> Eğerraporlama etkinleştirilirse, Sistem Tarayıcı her algılamayı Rapor dosyasına girer.

5.3.1 Uyarı



5.3.2 Düğmeler ve bağlantılar

Düğme / bağlantı	Açıklama
Yardım	Online yardımın bu sayfası, bu düğme veya bağlantı aracılığıyla açılır.

5.4 Koruma Bulutuna dosya gönderme

Hızlı sistem tarama görevi yürütüldüğünde zararlı yazılımlar tarafından sık olarak hedeflenen dosya konumlarının listesi oluşturulur. Bu liste yürütülen işlemleri, başlangıçta çalışan programları ve hizmetleri içerir. Bilinmeyen program dosyaları analiz için Avira Koruma Bulutu'na yüklenir.

Özel kurulum sırasında veya daha sonra **Gelişmiş Koruma** yapılandırması altında **Şüpheli dosyaları Avira'ya gönderirken manüel olarak onayla** seçeneğini etkinleştirdiyseniz, Koruma Bulutu'na gönderilmesi gereken şüpheli dosyaların bir listesini

görürsünüz ve göndermek istediğiniz dosyaları seçebilirsiniz. Varsayılan olarak, tüm şüpheli dosyalar daha detaylı analiz için Avira Koruma Bulutu'na gönderilmek üzere işaretlenir.

> **Not**
> **Genişletilmiş** raporlama modunu etkinleştirdiyseniz, Sistem Tarayıcı her algılamayı Rapor dosyasına kaydeder ve Koruma Bulutu tarafından gerçekleştirile algılamalara *(Bulut)* sonekini ekler.

5.4.1 Görüntülenen bilgi

Avira Koruma Bulutu'na gönderilecek şüpheli dosyaların listesi.

- *Gönder:* Avira Koruma Bulutu'na gönderilecek dosyaları seçebilirsiniz.
- *Dosya:* Şüpheli dosyanın adı.
- *Yol:* Şüpheli dosyanın yolu.

Dosyaları daima otomatik olarak gönder

Bu seçenek etkinleştirilirse, şüpheli dosyalar, her **Hızlı sistem tarama** görevi sonrasında, manüel onay istenmeden analiz için doğrudan Koruma Bulutu'na gönderilir.

5.4.2 Düğmeler ve bağlantılar

Düğme / bağlantı	Açıklama
Gönder	Seçili dosyalar Avira Koruma Bulutu'na gönderilecek.
İptal	Sistem Tarayıcı daha fazla eylem olmadan kapatılır. Şüpheli dosyalar, bilgisayar sisteminizde değişmeden kalır.
Yardım	Bu çevrimiçi yardım sayfası açılır.
Koruma Bulutu Hakkında	Avira Koruma Bulutu web sayfası açılır.

İlgili konular:

- Gelişmiş Koruma yapılandırması
- Özel kurulum
- Rapor yapılandırma

- Raporların görünümü

5.5 Gerçek Zamanlı Koruma

Gerçek Zamanlı Koruma tarafından virüs algılanırsa, dosya erişimi reddedilir ve bir masaüstü bildirimi görüntülenir, virüs algılamaları için eylem modu olarak *etkileşimli* modunu seçtiyseniz veya **Uyarı görüntüle** seçeneğiyle birlikte *otomatik* modunu seçtiyseniz (Gerçek Zamanlı Koruma > Tara > Algılama durumunda eylem Yapılandırma bölümüne bakın).

Bildirim

Bildirimde aşağıdaki bilgiler görüntülenir:

- Algılamanın tarihi ve saati
- Etkilenen dosyanın yolu ve adı
- Zararlı yazılımın adı

> **Not**
> Varsayılan Gerçek Zamanlı Koruma başlangıç modu (Normal başlangıç) seçildiğinde ve başlangıç oturum açma işlemi hızlı gerçekleştirildiğinde, başlangıçta otomatik olarak başlamak üzere yapılandırılmış programlar taranamayabilir, çünkü bu programlar Gerçek Zamanlı Koruma tamamen başlatılmadan önce çalışıyor durumda olabilirler.

Etkileşimli modda aşağıdaki seçeneklere sahip olursunuz:

Kaldır

Etkilenen dosya, Sistem Tarayıcı bileşenine aktarılır ve Sistem Tarayıcı tarafından silinir. Başka bir ileti görüntülenmez.

Ayrıntılar

Etkilenen dosya, Sistem Tarayıcı bileşenine aktarılır. Sistem Tarayıcı, algılama bildirimini ve etkilenen dosyanın yönetilmesine ilişkin çeşitli seçenekleri içeren bir pencereyi açar.

> **Not**
> Lütfen Algılama > Sistem Tarayıcı konumundaki virüs yönetimiyle ilgili bilgileri dikkate alın.

Not
Virüs yönetimi için, Gerçek Zamanlı Koruma > Tara > Algılama durumunda eylem konumundaki Yapılandırma'da varsayılan eylem olarak seçtiğiniz eylem görüntülenir. Bağlam menüsü aracılığıyla daha fazla eylem seçilebilir.

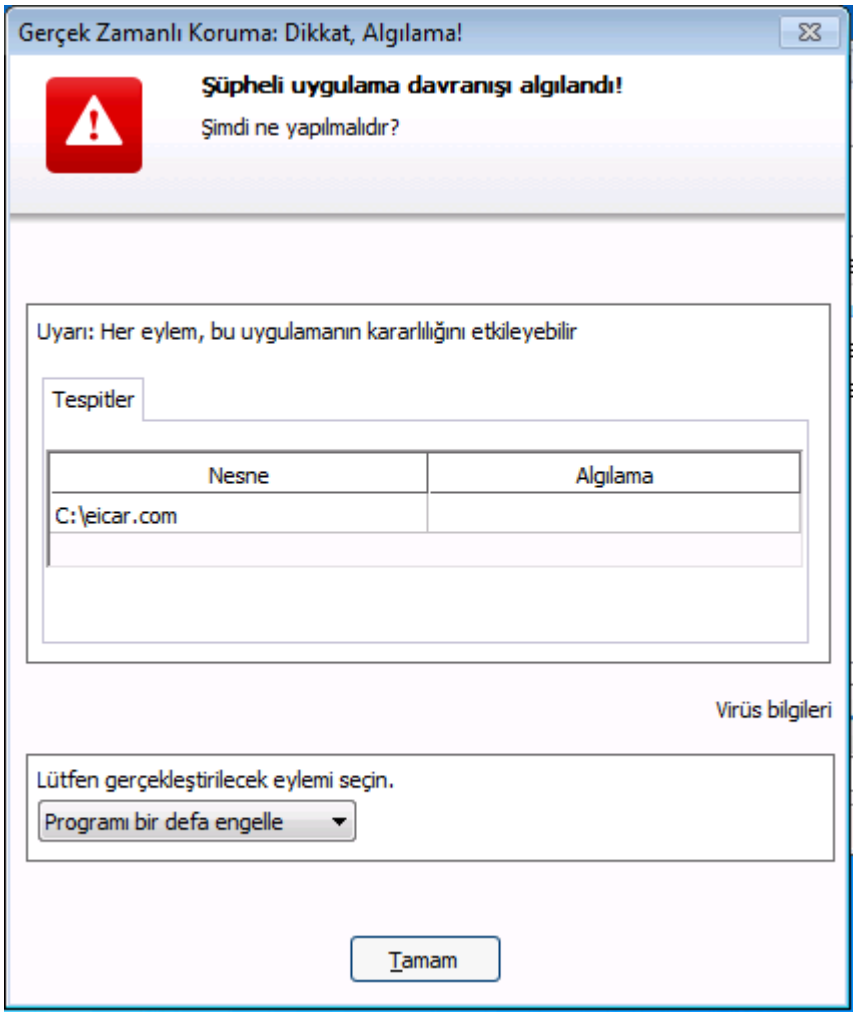
Kapat

İleti kapatılır. Virüs yönetimi sonlandırılır.

5.6 Şüpheli davranış

Gerçek Zamanlı Koruma'nın Proaktif bileşenini etkinleştirirseniz, uygulama eylemleri izlenir ve zararlı yazılımlar için tipik olan şüpheli davranışa karşı taranır. Bir uygulamada şüpheli davranış algılanırsa, bir uyarı alırsınız. Algılamanın nasıl işleneceğine yönelik çeşitli seçenekleriniz vardır.

5.6.1 Gerçek Zamanlı Koruma Uyarısı: Şüpheli uygulama davranışı algılandı



5.6.2 Şu anda algılanan şüpheli programın adı ve yolu

Ortadaki ileti penceresinde, şüpheli eylemler yürüten uygulamanın adı ve yolu görüntülenir.

5.6.3 Seçenekler

Güvenilen program

Bu seçenek etkinleştirilirse, uygulama çalışmaya devam eder. Program, izin verilen uygulamalar listesine eklenir ve Proaktif bileşeninin izlemesi dışında bırakılır. İzin verilen uygulamalar listesine ekleme yapılırken, izleme türü *İçerik* olarak ayarlanır. Başka bir deyişle, uygulama, yalnızca içerik değiştirilmeden kalırsa Proaktif bileşeni izlemesi dışında bırakılır (bkz. Yapılandırma > Genel > Gelişmiş koruma > Uygulama filtresi: İzin verilen uygulamalar).

Programı bir defa engelle

Bu seçenek etkinleştirilirse, uygulama engellenir; başka bir deyişle, uygulama sonlandırılır. Uygulama eylemleri, Proaktif bileşeni tarafından izlenmeye devam eder.

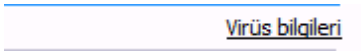
Bu programı her zaman engelle

Bu seçenek etkinleştirilirse, uygulama engellenir; başka bir deyişle, uygulama sonlandırılır. Program, engellenen uygulamalar listesine eklenir ve artık çalıştırılamaz (bkz. Yapılandırma > Genel > Gelişmiş koruma > Uygulama filtresi: Engellecek uygulamalar).

Yoksay

Bu seçenek etkinleştirilirse, uygulama çalışmaya devam eder. Uygulama eylemleri, Proaktif bileşeni tarafından izlenmeye devam eder.

5.6.4 Düğmeler ve bağlantılar

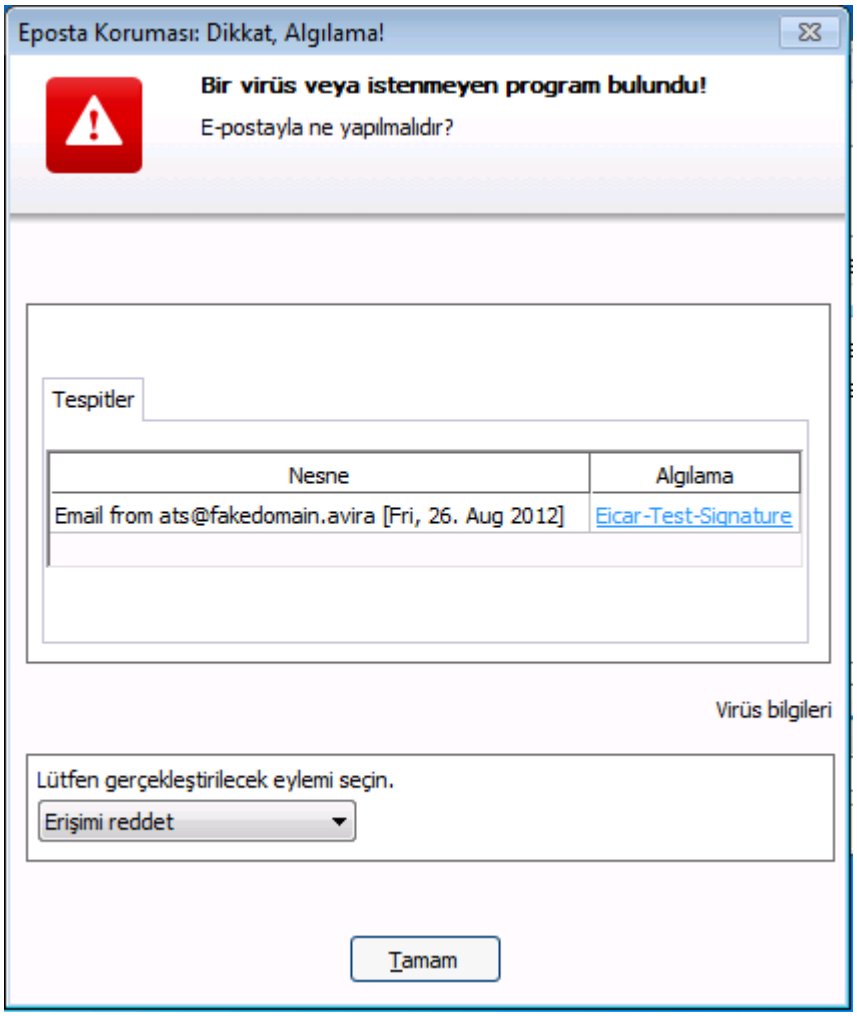
Düğme / bağlantı	Açıklama
	Bu bağlantı ve etkin bir İnternet bağlantısı yardımıyla, bu virüs veya istenmeyen programla ilgili daha fazla bilgi içeren bir İnternet sayfasına erişebilirsiniz.
	Online yardımın bu sayfası, bu düğme veya bağlantı aracılığıyla açılır.

5.7 Gelen e-postalar

EPosta Koruması bir virüs algılarsa, bir virüs algılandığında eylem modu olarak *etkileşimli* modunu seçmeniz durumunda bir uyarı alırsınız (EPosta Koruması > Tara > Algılama durumunda eylem Yapılandırma bölümüne bakın). Etkileşimli moddayken, iletişim kutusunda e-posta veya ek ile ne yapılacağını seçebilirsiniz.

Gelen e-postada bir virüs algılanırsa, aşağıda gösterilen uyarıyı alırsınız.

5.7.1 Uyarı



5.7.2 Algılamalar, Hatalar, Uyarılar

Algılamalar, **Hatalar** ve **Uyarılar** sekmelerinde, iletiler ve söz konusu e-postalarla ilgili daha ayrıntılı bilgiler görüntülenir:

- **Algılamalar:** Nesne: Gönderenin adını ve e-postanın gönderildiği zamanı gösteren söz konusu e-posta

  Algılama: Algılanan virüsün veya istenmeyen programın adı

- **Hata:** EPosta Koruması taraması sırasında oluşan hatalarla ilgili iletiler
- **Uyarılar:** Etkilenen nesnelerle ilgili uyarılar

5.7.3 Seçenekler

Not
Algılama bir buluşsal yöntem isabetiyse (HEUR/), olağandışı çalışma zamanı paketleyicisiyse (PCK/) veya gizli dosya uzantısı içeren bir dosyaysa (HEUR-DBLEXT/), etkileşimli modda yalnızca Karantinaya taşı ve Yoksay seçenekleri kullanılabilir. Otomatik modda algılama otomatik olarak Karantina'ya taşınır. Bu kısıtlama, yanlış alarm olabilecek algılanmış dosyaların doğrudan bilgisayarınızdan kaldırılmasını (silinmesini) önler. Bu dosya, istendiği zaman karantina yöneticisi yardımıyla kurtarılabilir.

Karantinaya taşı

Bu seçenek etkinleştirilirse, tüm ekleri içeren e-posta, karantinaya taşınır. Daha sonra karantina yöneticisi aracılığıyla gönderilebilir. Etkilenen e-posta silinir. E-posta metninin gövdesi ve ekler, bir varsayılan metin ile değiştirilir.

E-postayı sil

Bu seçenek etkinleştirilirse, bir virüs veya istenmeyen program algılandığında etkilenen e-posta silinir. E-posta metninin gövdesi ve ekler, bir varsayılan metin ile değiştirilir.

Eki sil

Bu seçenek etkinleştirilirse, etkilenen ek, bir varsayılan metin ile değiştirilir. E-posta gövdesi etkilendiyse, silinir ve yerine varsayılan bir metin gelir. E-posta teslim edilir.

Eki karantinaya taşı

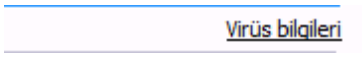
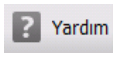
Bu seçenek etkinleştirilirse, etkilenen ek, karantinaya taşınır ve sonra silinir (bir varsayılan metin ile değiştirilir). E-posta gövdesi teslim edilir. Etkilenen ek daha sonra karantina yöneticisi aracılığıyla gönderilebilir.

Yoksay

Bu seçenek etkinleştirilirse, bir virüs veya istenmeyen program algılanmasına rağmen etkilenen e-posta teslim edilir.

Uyarı
Bu, virüs ve istenmeyen programların bilgisayar sisteminize erişmesini mümkün kılabilir. Yalnızca özel durumlarda **Yoksay** seçeneğini belirleyin. Posta istemcinizde önizlemeyi devre dışı bırakın, asla ekleri çift tıklatarak açmayın!

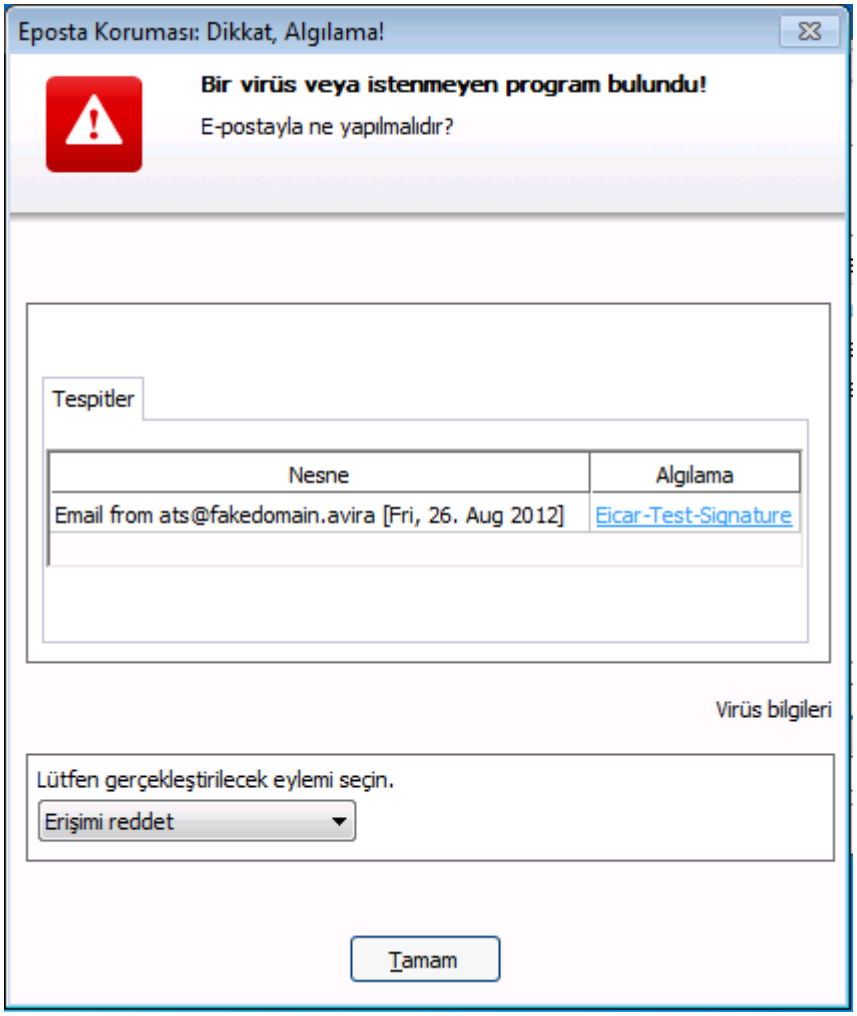
5.7.4 Düğmeler ve bağlantılar

Düğme / bağlantı	Açıklama
	Bu bağlantı ve etkin bir İnternet bağlantısı yardımıyla, bu virüs veya istenmeyen programla ilgili daha fazla bilgi içeren bir İnternet sayfasına erişebilirsiniz.
	Online yardımın bu sayfası, bu düğme veya bağlantı aracılığıyla açılır.

5.8 Giden e-postalar

EPosta Koruması bir virüs algılarsa, bir virüs algılandığında eylem modu olarak *etkileşimli* modunu seçmeniz durumunda bir uyarı alırsınız (EPosta Koruması > Tara > Algılama durumunda eylem Yapılandırma bölümüne bakın). Etkileşimli moddayken, iletişim kutusunda e-posta veya ek ile ne yapılacağını seçebilirsiniz.

5.8.1 Uyarı



5.8.2 Algılamalar, Hatalar, Uyarılar

Algılamalar, **Hatalar** ve **Uyarılar** sekmelerinde, iletiler ve söz konusu e-postalarla ilgili daha ayrıntılı bilgiler görüntülenir:

- **Algılamalar:** Nesne: Gönderenin adını ve e-postanın gönderildiği zamanı gösteren söz konusu e-posta

  Algılama: Algılanan virüsün veya istenmeyen programın adı
- **Hata:** EPosta Koruması taraması sırasında oluşan hatalarla ilgili iletiler
- **Uyarılar:** Etkilenen nesnelerle ilgili uyarılar

5.8.3 Seçenekler

Postayı karantinaya taşı (gönderme)

Bu seçenek etkinleştirilirse, tüm eklerle birlikte e-posta Karantinaya taşınır ve gönderilmez. E-posta, e-posta istemcinizin giden kutusunda kalır. E-posta

programınızda bir hata iletisi alırsınız. E-posta hesabınızdan gönderilen diğer tüm e-postalar, zararlı yazılıma karşı taranır.

Postaların gönderimini engelle (gönderme)

E-posta gönderilmez ve e-posta istemcinizin giden kutusunda kalır. E-posta programınızda bir hata iletisi alırsınız. E-posta hesabınızdan gönderilen diğer tüm e-postalar, zararlı yazılıma karşı taranır.

Yoksay

Bu seçenek etkinleştirilirse, bir virüs veya istenmeyen program algılanmasına rağmen etkilenen e-posta gönderilir.

Uyarı
Virüsler ve istenmeyen programlar, bu şekilde e-posta alıcısının bilgisayar sistemine girebilir.

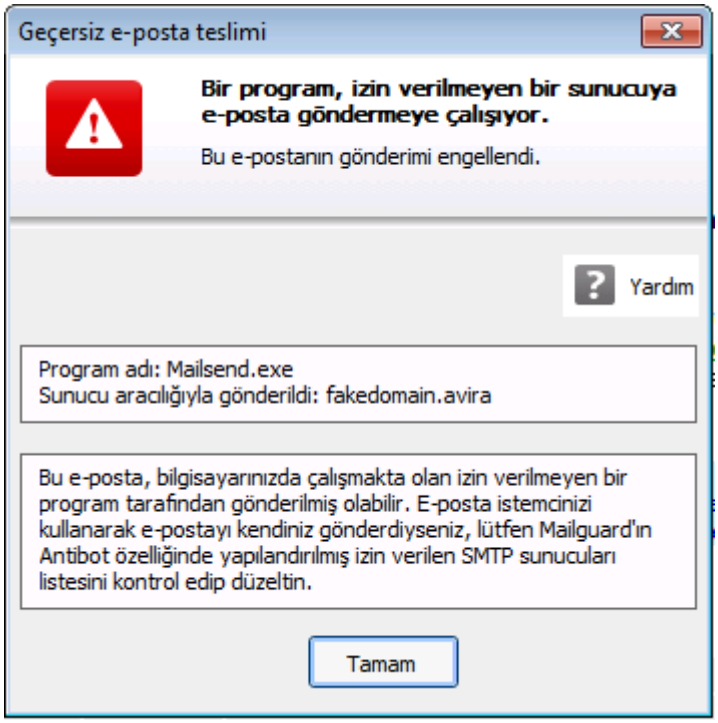
5.8.4 Düğmeler ve bağlantılar

Düğme / bağlantı	Açıklama
Virüs bilgileri	Bu bağlantı ve etkin bir İnternet bağlantısı yardımıyla, bu virüs veya istenmeyen programla ilgili daha fazla bilgi içeren bir İnternet sayfasına erişebilirsiniz.
Yardım	Online yardımın bu sayfası, bu düğme veya bağlantı aracılığıyla açılır.

5.9 Gönderen

EPosta Koruması'nın İstenmeyen Posta Gönderimi Engelleme işlevini kullanıyorsanız, yetkisiz gönderenlerden gelen e-postalar, EPosta Koruması tarafından engellenir. EPosta Koruması > Tara > İstenmeyen Posta Gönderimi Engelleme konumundaki yapılandırmada oluşturduğunuz izin verilen gönderenler listesi kullanılarak gönderen denetlenir. Engellenen e-posta bir iletişim kutusunda görüntülenir.

5.9.1 Uyarı



5.9.2 Kullanılan program, kullanılan SMTP sunucusu ve e-posta gönderenin adresi

Aşağıdaki bilgiler, ortadaki ileti penceresinde görüntülenir:

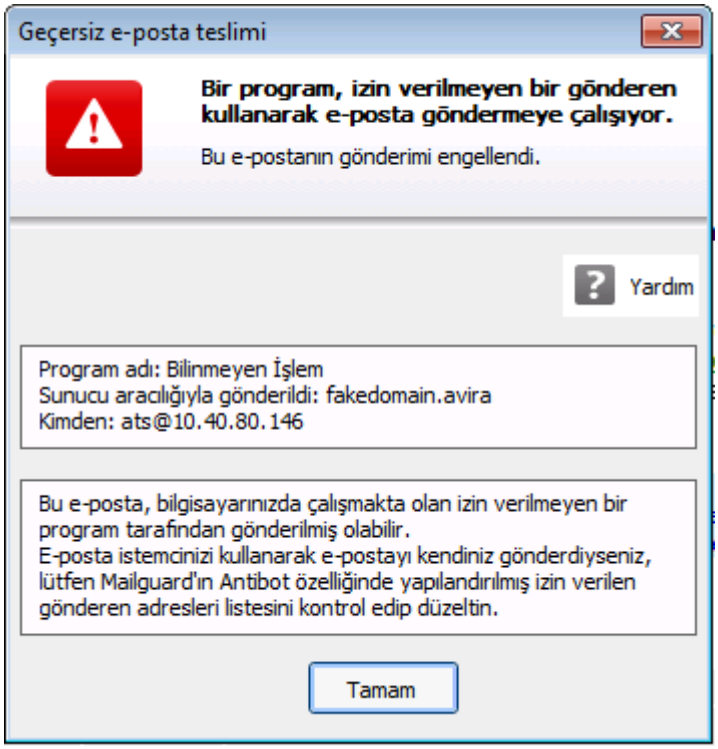
- E-posta göndermek için kullanılan programın adı
- E-posta göndermek için kullanılan SMTP sunucusunun adı
- E-posta gönderenin adresi

Söz konusu e-postayı, e-posta programınızı kullanarak gönderdiyseniz, EPosta Koruması > Tara > İstenmeyen Posta Gönderimi Engelleme konumundaki yapılandırmada izin verilen gönderenler listesini, e-posta istemcisi programınızdaki e-posta hesaplarında kullandığınız gönderen adresleriyle karşılaştırın. Yapılandırmadaki yetkili gönderenler listesi eksikse, kullandığınız diğer gönderen adreslerini bu listeye ekleyin. Engellenmiş e-postayı, e-posta istemci programınızın giden kutusunda bulabilirsiniz. Engellenmiş e-postayı göndermek için, yapılandırmayı tamamlayın ve sonra e-postayı yeniden gönderin.

5.10 Sunucu

EPosta Koruması'nın İstenmeyen Posta Gönderimi Engelleme işlevini kullanıyorsanız, yetkisiz SMTP sunucularının gönderdiği e-postalar, EPosta Koruması tarafından engellenir. EPosta Koruması > Tara > İstenmeyen Posta Gönderimi Engelleme konumundaki yapılandırmaya eklediğiniz izin verilen sunucular listesi kullanılarak, hangi SMTP sunucusunun kullanıldığı denetlenir. Engellenen e-posta bir iletişim kutusunda görüntülenir.

5.10.1 Uyarı



5.10.2 Kullanılan program, kullanılan SMTP sunucusu

Aşağıdaki bilgiler, ortadaki ileti penceresinde görüntülenir:

- E-posta göndermek için kullanılan programın adı
- E-posta göndermek için kullanılan SMTP sunucusunun adı

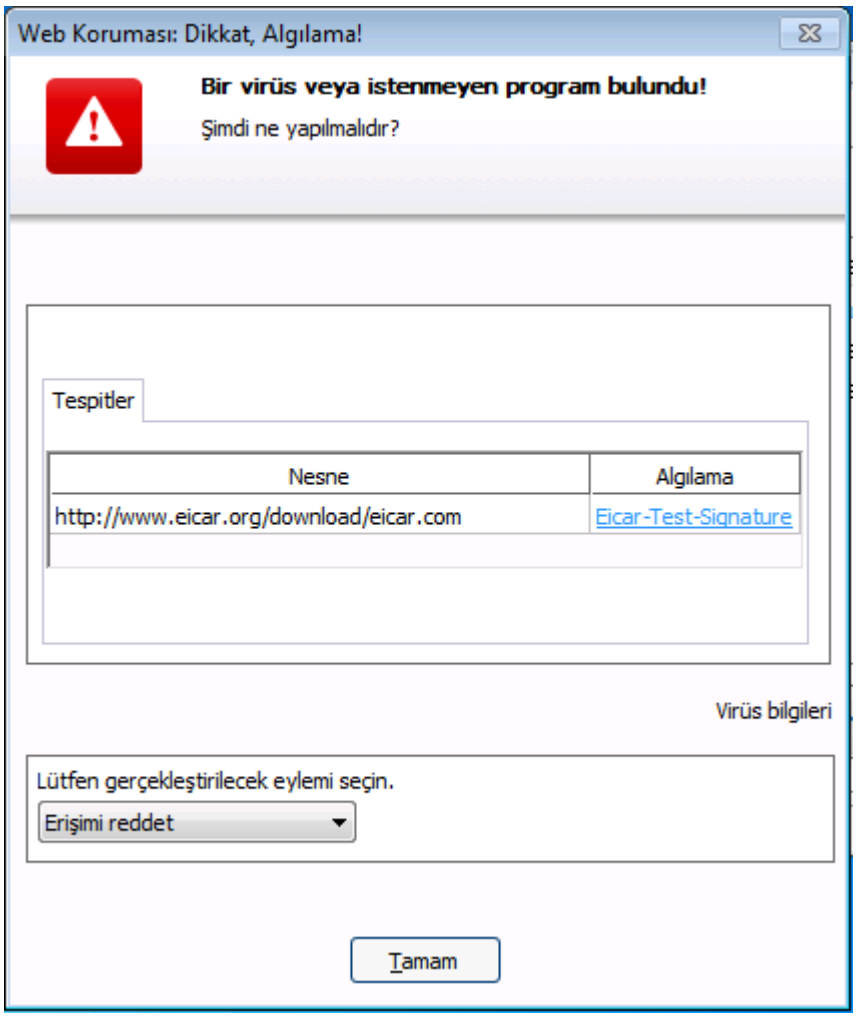
Söz konusu e-postayı, e-posta programınızı kullanarak gönderdiyseniz, EPosta Koruması > Tara > İstenmeyen Posta Gönderimi Engelleme konumundaki yapılandırmada izin verilen sunucular listesini, e-postaları göndermek için kullandığınız SMTP sunucularıyla karşılaştırın. E-posta istemci programınızda kullanılan SMTP sunucularını, kullanılan e-posta hesapları altında bulabilirsiniz. Yapılandırmadaki yetkili sunucular listesi eksikse, kullandığınız diğer SMTP sunucularını bu listeye ekleyin. Engellenmiş e-postayı, e-posta istemci programınızın giden kutusunda bulabilirsiniz. Engellenmiş e-postayı göndermek için, yapılandırmayı tamamlayın ve sonra e-postayı yeniden gönderin.

5.11 Web Koruması

Web Koruması tarafından virüsler algılanırsa, *etkileşimli* modu veya *otomatik* modu, virüs algılaması için eylem modu olarak, *Algılama Uyarılarını Görüntüle* ile birlikte seçeneğini belirlediyseniz, bir uyarı alırsınız (Web Koruması > Tara > Algılama durumunda eylem yapılandırma bölümüne bakın). Etkileşimli moddayken, iletişim kutusunda web sunucusu tarafından gönderilen veriler ile ne yapılacağını seçebilirsiniz. Uyarı ile otomatik modda algılanan virüsü işleme seçeneği yoktur. Uyarıda, otomatik olarak gerçekleştirilecek eylemi onaylayabilir veya Web Koruması'nı iptal edebilirsiniz.

Not
Aşağıda gösterilen iletişim kutusu, etkileşimli modda bir virüs algılamasına yönelik iletidir.

Uyarı



Algılama, Hatalar, Uyarılar

Algılama, **Hatalar** ve **Uyarılar** sekmelerinde, algılanan virüslerle ilgili ayrıntılı bilgi ve iletiler görüntülenir:

- **Algılama:** Algılanan virüsün veya istenmeyen programın URL'si ve adı
- **Hata:** Web Koruması taraması sırasında oluşan hatalarla ilgili iletiler
- **Uyarılar:** Algılanan virüslerle ilgili uyarılar

Olası eylemler

Not
Algılama bir buluşsal yöntem isabetiyse (HEUR/), olağandışı çalışma zamanı paketleyicisiyse (PCK/) veya gizli dosya uzantısı içeren bir dosyaysa (HEUR-DBLEXT/), etkileşimli modda yalnızca Karantinaya taşı ve Yoksay seçenekleri kullanılabilir. Otomatik modda algılama otomatik olarak Karantina'ya taşınır. Bu kısıtlama, yanlış alarm olabilecek algılanmış dosyaların doğrudan bilgisayarınızdan kaldırılmasını (silinmesini) önler. Bu dosya, istendiği zaman Karantina Yöneticisiyardımıyla kurtarılabilir.
Yapılandırmaya bağlı olarak, çeşitli seçenekler kullanılabilir olmayabilir.

Erişimi reddet

Web sunucusundan istenen web sitesi ve/veya aktarılan veri ya da dosyalar, web tarayıcınıza gönderilmez. Web tarayıcısında, erişimin reddedildiğini bildiren bir hata iletisi görüntülenir. Rapor işlevi etkinleştirilirse, Web Koruması, algılamayı rapor dosyasına kaydeder.

Karantinaya taşı

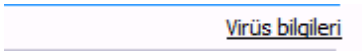
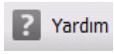
Bir virüs veya zararlı yazılım algılanması durumunda, web sunucusundan istenen web sitesi ve/veya aktarılan veri ve dosyalar, karantinaya taşınır. Etkilenen dosya, bilgilendirici bir değere sahipse karantina yöneticisinden kurtarılabilir veya gerekirse, Avira Zararlı Yazılım Araştırma Merkezi'ne gönderilir.

Yoksay

Web sunucusundan istenen web sitesi ve/veya aktarılan veri ve dosyalar, Web Koruması tarafından web tarayıcınıza iletilir.

Uyarı
Bu, virüs ve istenmeyen programların bilgisayar sisteminize erişmesini mümkün kılabilir. Yalnızca özel durumlarda **Yoksay** seçeneğini belirleyin.

Düğmeler ve bağlantılar

Düğme / bağlantı	Açıklama
	Bu bağlantı ve etkin bir İnternet bağlantısı yardımıyla, bu virüs veya istenmeyen programla ilgili daha fazla bilgi içeren bir İnternet sayfasına erişebilirsiniz.
	Online yardımın bu sayfası, bu düğme veya bağlantı aracılığıyla açılır.

6. Sistem Tarayıcı

6.1 Sistem Tarayıcı

Sistem Tarayıcı bileşeni ile, virüslere ve istenmeyen programlara karşı hedeflenmiş taramalar (istek üzerine taramalar) yürütebilirsiniz. Aşağıdaki seçenekler, etkilenen dosyalara karşı tarama için kullanılabilir:

- **Bağlam menüsü aracılığıyla sistem taraması**
  Örneğin, tek tek dosyaları ve dizinleri taramak istiyorsanız, bağlam menüsü aracılığıyla sistem taraması yapılması (sağ fare düğmesi - **Seçilen dosyaları Avira ile tara** girdisi) önerilir. Diğer bir avantaj da, bağlam menüsü aracılığıyla sistem taraması için önce Kontrol Merkezi'ni başlatmanın gerekmemesidir.
- **Sürükle ve bırak aracılığıyla sistem taraması**
  Kontrol Merkezi'nin program penceresine bir dosya veya dizin sürüklendiğinde, Sistem Tarayıcı dosyayı veya dizini ve içerdiği tüm alt dizinleri tarar. Örneğin, masaüstünüze kaydettiğiniz tek tek dosyaları ve dizinleri taramak istiyorsanız, bu yordam önerilir.
- **Profiller aracılığıyla sistem taraması**
  Belirli dizinleri ve sürücüleri (örn. yeni dosyaları düzenli olarak depoladığınız çalışma dizininiz veya sürücüler) düzenli olarak taramak istiyorsanız bu yordam önerilir. Her yeni tarama için bu dizinleri ve sürücüleri seçmeniz gerekmez, yalnızca ilgili profili kullanarak seçim yaparsınız.
- **Zamanlayıcı aracılığıyla sistem taraması**
  Zamanlayıcı, zaman denetimli taramalar gerçekleştirmenize olanak sağlar. Bkz. Zamanlayıcı aracılığıyla sistem taraması.

Kök kullanıcı takımına, önyükleme sektörü virüslerine karşı tarama yapılırken ve etkin işlemler taranırken özel işlemler gerekir. Aşağıdaki seçenekler kullanılabilir:

- **Kök kullanıcı takımına ve etkin zararlı yazılımlara karşı tara** tarama profiliyle Kök kullanıcı takımlarına karşı tara
- **Etkin işlemler** tarama profili aracılığıyla etkin işlemleri tara
- **Ekstralar** menüsünde **Önyükleme kayıtları taraması...** menü komutu aracılığıyla önyükleme sektörü virüslerini tara

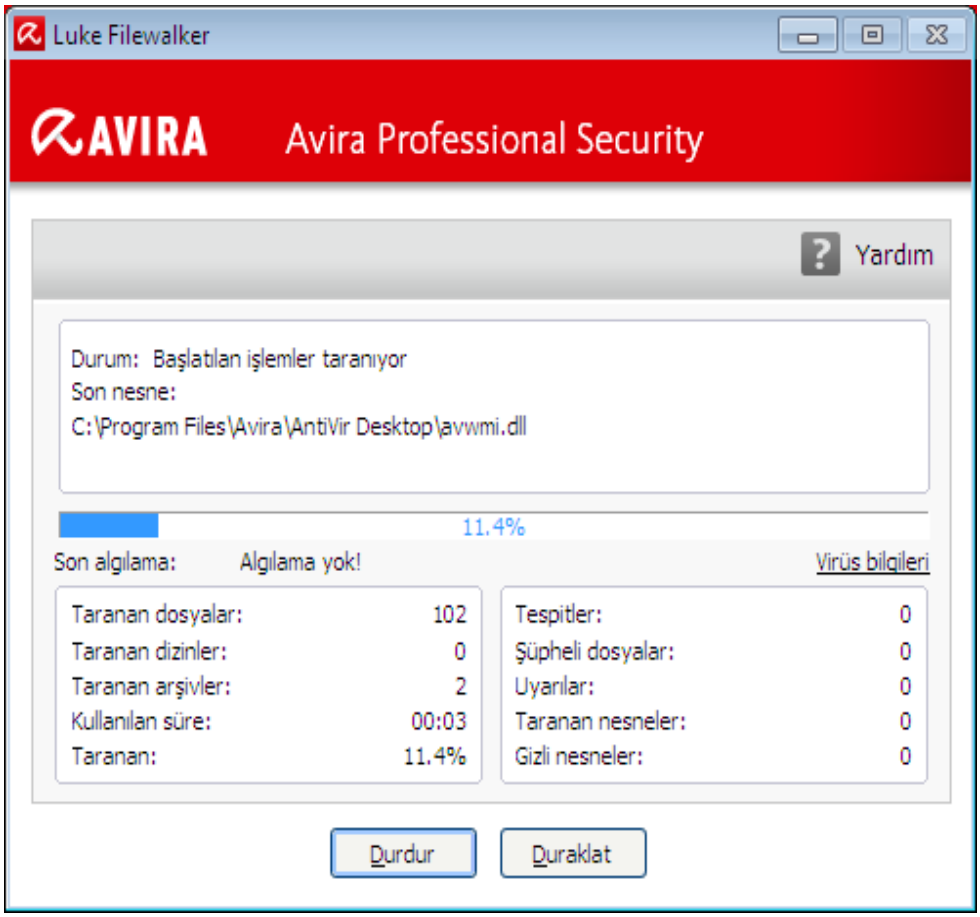
6.2 Luke Filewalker

Sistem taraması sırasında, tarama durumuyla ilgili tam bilgileri size sağlayan **Luke Filewalker** durum penceresi görüntülenir.

Algılama durumunda eylem grubundaki Sistem Tarayıcı yapılandırmasında **etkileşimli** seçeneği belirlenirse, algılanan virüs veya istenmeyen programla ne yapılacağı size sorulur. **Otomatik** seçeneği belirlenirse, tüm algılamalar Tarayıcı raporunda gösterilir.

Tarama tamamlandığında, sonuçları (istatistikler), uyarılar ve hata iletileri yeni bir iletişim kutusunda görüntülenir.

6.2.1 Luke Filewalker: Tarama durumu penceresi



Görüntülenen bilgi

Durum: Farklı durum iletileri vardır:

- *Program başlatılacak*
- *Gizli nesne araması çalışıyor!*
- *Başlatılan işlemler taranıyor*
- *Dosya taranıyor*
- *Arşivi başlat*
- *Boş bellek*
- *Dosya paketten çıkarılıyor*
- *Önyükleme sektörleri taranıyor*
- *Ana önyükleme sektörleri taranıyor*
- *Kayıt defteri taranıyor*

- *Program sonlandırılacak!*
- *Tarama bitti*

Son nesne: Şu anda taranmakta olan veya en son taranan dosyanın adı ve yolu

Son algılama: Son algılama için çeşitli iletiler vardır:

- *Algılama yok!*
- En son algılanan virüsün veya istenmeyen programın adı

Taranan dosyalar: Taranan dosyaların sayısı

Taranan dizinler: Taranan dizinlerin sayısı

Taranan arşivler: Taranan arşivlerin sayısı

Kullanılan süre: Sistem taraması süresi

Tarandı: Tamamlanan taramanın yüzdesi

Algılamalar: Algılanan virüslerin ve istenmeyen programların sayısı

Şüpheli dosyalar: Buluşsal yöntem tarafından bildirilen dosyaların sayısı

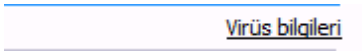
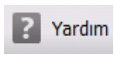
Uyarılar: Algılanan virüslerle ilgili uyarı sayısı

Taranan nesneler: Kök kullanıcı takımının taraması sırasında taranan nesnelerin sayısı

Gizli nesneler: Algılanan gizli nesnelerin toplam sayısı

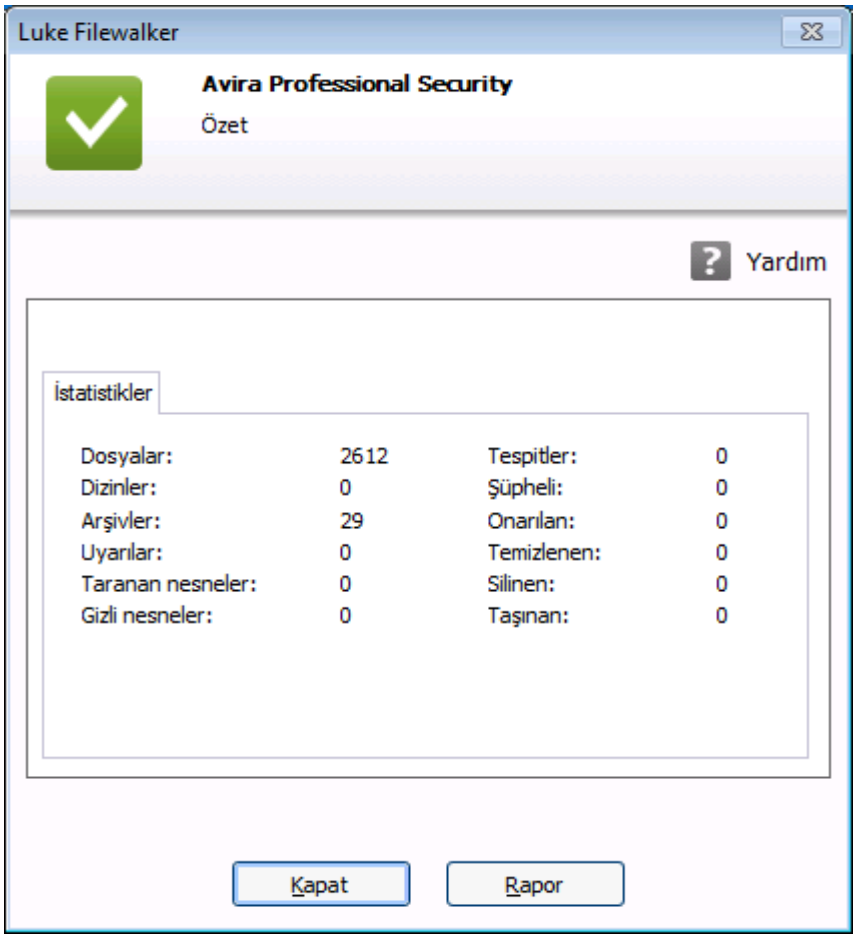
Not
Kök kullanıcı takımı, kayıt defteri girdileri veya dosyalar gibi nesneleri ve işlemleri gizleme yeteneğine sahiptir. Ancak her gizli nesne mutlaka bir kök kullanıcı takımının varlığını göstermek zorunda değildir. Gizli nesneler zararsız nesneler de olabilir. Bir taramada gizli nesneler algılanır ancak virüs tanımlama uyarısı verilmezse, hangi nesneye başvurulduğunu belirlemek ve algılanan nesneyle ilgili daha fazla bilgi edinmek için raporu kullanmanız gerekir.

Düğmeler ve bağlantılar

Düğme / Bağlantı	Açıklama
	Bu bağlantı ve etkin bir İnternet bağlantısı yardımıyla, bu virüs veya istenmeyen programla ilgili daha fazla bilgi içeren bir İnternet sayfasına erişebilirsiniz.
	Online yardımın bu sayfası, bu düğme veya bağlantı aracılığıyla açılır.
Durdur	Tarama işlemi durdurulur.
Duraklat	Tarama kesintiye uğrar ve **Sürdür** düğmesi tıklatılarak devam edebilir.
Sürdür	Kesintiye uğrayan taramaya devam edilir.
Son	Sistem Tarayıcı kapatılır.

Rapor	Taramanın rapor dosyası gösterilir.

6.2.2 Luke Filewalker: Tarama İstatistikleri



Görüntülenen bilgi: İstatistikler

Dosyalar: Taranan dosyaların sayısı

Dizinler: Taranan dizinlerin sayısı

Arşivler: Taranan arşivlerin sayısı

Uyarılar: Algılanan virüslerle ilgili uyarı sayısı

Aranan nesneler: Kök kullanıcı takımının taraması sırasında taranan nesnelerin sayısı

Gizli nesneler: Algılanan gizli nesnelerin (kök kullanıcı takımının) sayısı

Algılamalar: Algılanan virüslerin ve istenmeyen programların sayısı

Şüpheli: Buluşsal yöntem tarafından bildirilen dosyaların sayısı

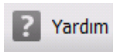
Onarılan: Onarılan dosya sayısı

Temizlenen: Üzerine yazılan dosyaların sayısı

Silinen: Silinen dosya sayısı

Taşınan: Karantinaya taşınan dosyaların sayısı

Düğmeler ve bağlantılar

Düğme / Bağlantı	Açıklama
	Online yardımın bu sayfası, bu düğme veya bağlantı aracılığıyla açılır.
Kapat	Özet penceresi kapatılır.
Rapor	Taramanın rapor dosyası gösterilir.

7. Kontrol Merkezi

7.1 Kontrol Merkezi'ne Genel Bakış

Kontrol Merkezi bir bilgi, yapılandırma ve yönetim merkezidir. Tek tek seçilebilen bölümlere ek olarak, menü çubuğundan erişilebilen çok sayıda seçenek sunar.

Menü çubuğu

Kontrol Merkezi'nin tüm işlevleri, menü çubuğunda bulunur.

Dosya

- Çıkış (Alt + F4)

Görüntüle

- Durum
- PC Koruma
  - Sistem Tarayıcı
  - Gerçek Zamanlı Koruma
- İnternet Koruması
  - Güvenlik Duvarı
  - Web Koruması
  - EPosta Koruması
- Yönetim
  - Karantina
  - Zamanlayıcı
  - Raporlar
  - Olaylar
- Yenile (F5)

Ekstralar

- Önyükleme kayıtları taraması...
- Algılama listesi...
- Kurtarma CD’sini karşıdan yükleyin
- Yapılandırma (F8)

Güncelle

- Güncellemeyi başlat...

- El ile güncelleme...

Help

- Konular
- Bana yardımcı ol
- El ile karşıdan yükle
- Lisans dosyası yükle...
- Geribildirim gönder
- Avira Professional Security hakkında

> **Not**
> [ALT] tuşunun yardımıyla menü çubuğunda klavye gezintisini etkinleştirebilirsiniz. Gezinti etkinleştirilirse, ok tuşlarıyla menü içinde hareket edebilirsiniz. Return tuşu ile etkin menü öğesini etkinleştirirsiniz.

Gezinti bölümleri

Soldaki gezinti çubuğunda aşağıdaki bölümleri bulabilirsiniz:

- **Durum**

PC KORUMA

- Sistem Tarayıcı
- Gerçek Zamanlı Koruma

İNTERNET KORUMASI

- Güvenlik Duvarı
- Web Koruması
- EPosta Koruması

YÖNETİM

- Karantina
- Zamanlayıcı
- Raporlar
- Olaylar

Gezinti açıklaması

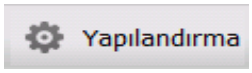
- **Durum**: **Durum** çubuğunu tıklatarak ürünün işlev ve performansına genel bakışa ulaşabilirsiniz (bkz. Durum).

- **Durum** bölümü, hangi modüllerin etkin olduğunu bir bakışta görmenize olanak verir ve gerçekleştirilen son güncellemeyle ilgili bilgi sağlar.

- *PC KORUMA*: Bu bölümde bilgisayar sisteminizdeki dosyaları virüs ve zararlı yazılımlara karşı denetlemeye yönelik bileşenler bulursunuz.
  - Sistem Tarayıcı bölümü, kolayca bir istek üzerine taramayı yapılandırmanıza ve başlatmanıza olanak sağlar. Önceden tanımlı profiller, önceden uyarlanmış varsayılan seçeneklerle bir taramayı etkinleştirir. Aynı şekilde, el ile seçim yardımıyla (kaydedilecektir) veya kullanıcı tanımlı profiller oluşturularak virüs ve istenmeyen programlara karşı taramayı kişisel gereksinimlerinize uyarlamanız mümkündür.
  - Gerçek Zamanlı Koruma bölümünde, taranmış dosyalarla ilgili bilgiler ve diğer istatistiksel veriler görüntülenir ve bu istendiği zaman sıfırlanabilir ve rapor dosyasına erişilmesini sağlar. Algılanan son virüs veya istenmeyen programla ilgili daha ayrıntılı bilgi, "bir düğme basışıyla" pratik olarak edinilebilir.
- *İNTERNET KORUMASI*: Bu bölümde bilgisayar sisteminizi Internet'ten gelen virüs ve zararlı yazılımlara karşı ve yetkisiz ağ erişimine karşı korumaya yönelik bileşenler bulursunuz.
  - Güvenlik Duvarı Güvenlik Duvaru için temel ayarları yapılandırmanıza olanak sağlar. Ayrıca, geçerli veri aktarım hızı ve ağ bağlantısı kullanan tüm etkin uygulamalar da görüntülenir.
  - Web Koruması bölümünde, taranan URL'ler ve algılanan virüslerle ilgili bilgilerin yanı sıra diğer istatistiksel veriler görüntülenir ve bu istendiği zaman sıfırlanabilir ve rapor dosyasına erişilmesini sağlar. Algılanan son virüs veya istenmeyen programla ilgili daha ayrıntılı bilgi, "bir düğme basışıyla" pratik olarak edinilebilir.
  - EPosta Koruması bölümünde, EPosta Koruması tarafından taranan tüm e-postalar, bunların özellikleri ve diğer istatistiksel veriler gösterilir. E-postalar EPosta Koruması arabelleğinden de silinebilir.
- *YÖNETİM*: Bu bölümde şüpheli veya etkilenmiş dosyaları yalıtıp yönetmeye ve yinelenen görevleri planlamaya yönelik araçlar bulursunuz.
  - Karantina bölümünde, karantina yöneticisi yer alır. Bu, önceden karantinaya yerleştirilmiş dosyalar veya karantinaya yerleştirmek istediğiniz şüpheli dosyalar için merkezi noktadır. Seçilen bir dosyayı e-posta yoluyla Avira Zararlı Yazılım Araştırma Merkezi'ne de gönderebilirsiniz.
  - Zamanlayıcı bölümü, zamanlanan tarama ve güncelleme işleri, yedekleme işleri yapılandırmanıza ve varolan işleri uyarlamanıza veya silmenize olanak sağlar.
  - Raporlar bölümü, gerçekleştirilen eylemlerin sonuçlarını görüntülemenize olanak sağlar.
  - Olaylar bölümü, belirli program modülleri tarafından oluşturulan olayları görüntülemenize olanak sağlar.

Düğmeler ve bağlantılar

Aşağıdaki düğmeler ve bağlantılar mevcut olabilir.

Düğme / bağlantı	Kısayol	Açıklama
		Bu düğme veya bağlantı, bölümün karşılık gelen yapılandırma iletişim kutusuna erişmek için kullanılır.
	F1	Bu düğme veya bağlantı, bölümün karşılık gelen online yardım konusunu açar.

7.2 Dosya

7.2.1 Çıkış

Dosya menüsündeki Çıkış menü öğesi Kontrol Merkezi'ni kapatır.

7.3 Görüntüle

7.3.1 Durum

Kontrol Merkezinin başlangıç ekranı, **Durum** bölümü, bilgisayar sisteminin korumalı olup olmadığını ve hangi Avira modüllerinin etkin olduğunu bir bakışta görmenize olanak verir. **Durum** penceresi aynı zamanda gerçekleştirilen son güncellemeyle ilgili bilgi sağlar. Lisansınızın geçerli olup olmadığını da buradan görebilirsiniz.

- PC Koruma: Gerçek Zamanlı Koruma, Son tarama, Son güncelleme, Ürününüz aktive edildi
- İnternet Koruması: Web Koruması, EPosta Koruması, Güvenlik Duvarı,, Sunum Modu,

> **Not**
> Kullanıcı Hesabı Kontrolü (UAC), Windows Vista gibi işletim sistemlerinde Gerçek Zamanlı Koruma, Güvenlik Duvarı Web Koruması ve EPosta Koruması gibi hizmetleri etkinleştirmek veya devre dışı bırakmak için izninizi isteyecektir.

PC Koruma

Bu bölümde, hizmetin geçerli durumu ve bilgisayarınızı yerel olarak virüs ve zararlı yazılımlara karşı koruyan koruyucu işlevler hakkında bilgiler görüntülenir.

Gerçek Zamanlı Koruma

Gerçek Zamanlı Koruma'nın geçerli durumuyla ilgili bilgiler bu alanda görüntülenir.

Gerçek Zamanlı Koruma'yı **AÇ/KAPAT** düğmesini tıklatarak etkinleştirebilirsiniz veya devre dışı bırakabilirsiniz. Gerçek Zamanlı Koruma için daha fazla seçeneğe, gezinti çubuğundaki **Gerçek Zamanlı Koruma** öğesine tıklayarak erişebilirsiniz. İlk olarak, bulunan son zararlı yazılım ve etkilenmiş dosyaların durumu hakkında bilgi alırsınız. **Yapılandırma** seçeneğini tıklatarak diğer ayarları belirleyebilirsiniz.

- **Yapılandırma**: Gerçek Zamanlı Koruma bileşeninin ayarlarını tanımlamak için Yapılandırma'ya gidin.

Aşağıdaki olasılıklar kullanılabilir:

Simge	Durum	Seçenek	Açıklama
	*Etkinleştirildi*	**Devre dışı bırak**	Gerçek Zamanlı Koruma hizmeti etkindir; başka bir deyişle, sisteminiz virüs ve istenmeyen programlara karşı sürekli olarak izlenir. **Not** Gerçek Zamanlı Koruma hizmetini devre dışı bırakabilirsiniz. Ancak, Gerçek Zamanlı Koruma devre dışı bırakılırsa, artık virüslere ve istenmeyen programlara karşı korunmayacağınızı unutmayın. Tüm dosyalar bildirim verilmeksizin sistemden geçebilir ve hasara neden olabilir.

	*Devre dışı bırakıldı*	**Etkinleştir**	Gerçek Zamanlı Koruma hizmeti devre dışı bırakılır; başka bir deyişle, hizmet yüklenir ancak etkin değildir. **Uyarı** Virüslere ve istenmeyen programlara karşı tarama gerçekleştirilmez. Tüm dosyalar bildirim verilmeksizin sistemden geçebilir. Virüslere ve istenmeyen programlara karşı korunmazsınız. **Not** Virüslere ve istenmeyen programlara karşı yeniden korunmak için, lütfen *PC Koruma* alanındaki **Gerçek Zamanlı Koruma** yanındaki **AÇ/KAPAT** düğmesini tıklatın.

	*Hizmet durduruldu*	**Hizmet başlat**	Gerçek Zamanlı Koruma hizmeti durdurulur. **Uyarı** Virüslere ve istenmeyen programlara karşı tarama gerçekleştirilmez. Tüm dosyalar bildirim verilmeksizin sistemden geçebilir. Virüslere ve istenmeyen programlara karşı korunmazsınız. **Not** Virüslere ve istenmeyen programlara karşı yeniden korunmak için, lütfen *PC Koruma* alanındaki **Gerçek Zamanlı Koruma** yanındaki **AÇ/KAPAT** düğmesini tıklatın. Geçerli durum yeşil renkte gösterilir, bu renk **Etkin** anlamına gelir.
	Unknown	**Help**	Bilinmeyen bir hata oluştuğunda bu durum görüntülenir. Bu durumda, lütfen Destek birimimizle iletişim kurun.

Son tarama

Gerçekleştirilen son sistem taramasıyla ilgili bilgiler bu alanda görüntülenir. Eksiksiz bir sistem denetimi gerçekleştirildiğinde, bilgisayarınızdaki tüm sabit diskler tamamen taranır. Sistem dosyalarının bütünlük kontrolü dışında tüm tarama işlemleri kullanılır: standart dosya taraması, kayıt defteri ve önyükleme sektörleri kontrolü, kök kullanıcı takımı taraması vb.

Aşağıdaki ayrıntılar görüntülenir:

- Son eksiksiz sistem taraması tarihi

Aşağıdaki olasılıklar kullanılabilir:

Sistem taraması	Seçenek	Açıklama
Gerçekleştirilemedi	**Sistemi tara**	Kurulumdan itibaren eksiksiz bir sistem denetimi yürütülmedi. **Uyarı** Sistemin durumu denetlenmedi. Bilgisayarınızda virüs veya istenmeyen programların bulunma olasılığı vardır. **Not** Bilgisayarınızı denetlemek için lütfen **Sistemi tara** bağlantısını tıklatın.
Son sistem taraması tarihi, örn. *18/09/2011*	**Sistemi tara**	Belirtilen tarihte eksiksiz bir sistem taraması gerçekleştirdiniz. **Not** Varsayılan tarama işi olan *Eksiksiz sistem taraması*'nı kullanmanızı öneririz. **Tam sistem taraması** işini etkinleştirmek için Zamanlayıcı'yı kullanın.
Unknown	**Help**	Bilinmeyen bir hata oluştuğunda bu durum görüntülenir. Bu durumda, lütfen Destek birimimizle iletişim kurun.

Son güncelleme

Gerçekleştirilen son güncellemenin geçerli durumuyla ilgili bilgiler burada görüntülenir.

Aşağıdaki ayrıntılar görüntülenir:

- Son güncelleme tarihi

  ▸ Otomatik güncellemelerde diğer ayarları belirlemek için **Yapılandırmayı Aç** düğmesini tıklatın.

Aşağıdaki olasılıklar kullanılabilir:

Simge	Durum	Seçenek	Açıklama
	*Son güncelleme tarihi, örn. 18/07/2011*	**Güncellemeyi başlat**	Program son 24 saat boyunca güncellenmiştir. **Not** **Güncellemeyi başlat** düğmesi aracılığıyla Avira ürününüzü en son sürüme güncelleyebilirsiniz.
	*Son güncelleme tarihi, örn. 18/07/2011*	**Güncellemeyi başlat**	Güncellemeden itibaren 24 saat geçmiştir ancak halen seçtiğiniz güncelleme hatırlatıcısı döngüsü içindesiniz. Bu, yapılandırmadaki ayara bağlıdır. **Not** **Güncellemeyi başlat** düğmesi aracılığıyla Avira ürününüzü en son sürüme güncelleyebilirsiniz.

	Gerçekleştirilemedi	**Güncellemeyi başlat**	Kurulumdan itibaren bir güncelleme gerçekleştirilmedi -veya- Seçtiğiniz güncelleme hatırlatıcısı döngüsü aşıldı (bkz. Yapılandırma) ve güncelleme gerçekleştirilmedi -veya- Virüs tanımı dosyası seçtiğiniz güncelleme hatırlatıcısı döngüsünden daha eski (bkz. Yapılandırma). **Not** **Güncellemeyi başlat** düğmesi aracılığıyla Avira ürününüzü en son sürüme güncelleyebilirsiniz.
		Kullanılabilir değil	Lisansın süresi dolduysa, bir güncelleme gerçekleştirilemez.

Ürününüz etkinleştirildi

Lisansınızın geçerli durumuyla ilgili bilgiler bu alanda görüntülenir.

Aşağıdaki olasılıklar kullanılabilir:

Tam sürüm

Simge	Durum	Seçenek	Anlamı
	*Tam sürüm için geçerli lisansın geçerlilik tarihi; örn. 31/10/2011*	**Yenile**	Avira ürününüz için geçerli bir lisansınız vardır. **Yenile** düğmesi aracılığıyla Avira çevrimiçi mağazasına erişebilirsiniz. Burada, geçerli lisansınızı gereksinimlerinize göre uyarlama ve Avira Premium sürümüne yükseltme olanağınız vardır.
	*Tam sürüm için geçerli lisansın geçerlilik tarihi; örn. 31/10/2011*	**Yenile**	Avira ürününüz için geçerli bir lisansınız vardır. Ancak lisans dönemi en fazla otuz gündür. Avira çevrimiçi mağazasına erişmek için **Yenile** düğmesini kullanın. Burada, geçerli lisansı uzatma seçeneğiniz vardır.
	*Lisans süresinin dolduğu tarih: örn. 31/08/2011*	**Satın al**	Avira ürününüzün lisans süresi dolmuştur. Avira çevrimiçi mağazasına erişmek için **Satın al** düğmesini kullanın. Burada, geçerli bir lisans satın alma seçeneğiniz vardır. **Uyarı** Lisansınızın süresi dolduysa, artık güncelleme mümkün olmayacak. Programın koruyucu işlevleri devre dışı bırakılır ve artık etkinleştirilemez.

Değerlendirme lisansı

Simge	Durum	Seçenek	Anlamı
	*Değerlendirme lisansının geçerlilik tarihi; örn. 31/10/2011*	**Satın al**	Belirli bir süre boyunca Avira ürününüzün tam işlev aralığını sınamanıza olanak sağlayan bir değerlendirme lisansınız vardır. Avira çevrimiçi mağazasına erişmek için **Satın al** düğmesini kullanın. Burada, geçerli bir lisans satın alma seçeneğiniz vardır.
	*Değerlendirme lisansının geçerlilik tarihi; örn. 31/10/2011*	**Yenile**	Bir değerlendirme lisansınız vardır. Ancak lisans dönemi en fazla otuz gündür. Avira çevrimiçi mağazasına erişmek için **Yenile** düğmesini kullanın. Burada, geçerli bir lisans satın alma seçeneğiniz vardır.

	*Değerlendirme lisansı süresinin dolduğu tarih: 31/10/2011*	**Satın al**	Avira ürününüzün lisans süresi dolmuştur. Avira çevrimiçi mağazasına erişmek için **Satın al** düğmesini kullanın. Burada, geçerli bir lisans satın alma seçeneğiniz vardır. **Uyarı** Lisansınızın süresi dolduysa, artık güncelleme mümkün olmayacak. Programın koruyucu işlevleri devre dışı bırakılır ve artık etkinleştirilemez.

İnternet Koruması

Bu bölümde, hizmetin koruyucu işlevler hakkında bilgiler görüntülenir.

- **Güvenlik Duvarı**: Bu hizmet, bilgisayarınıza gelen ve bilgisayarınızdan giden iletişim kanallarını izler.
- **Web Koruması**: Bu hizmet, Internet'te gezinirken web tarayıcınıza iletilen ve yüklenen verileri denetler (80, 8080, 3128 numaralı bağlantı noktalarının izlenmesi).
- **EPosta Koruması**: Bu hizmet, e-posta ve eklerde virüs ve zararlı yazılım olup olmadığını denetler.
- **Sunum Modu**: Otomatiğe ayarlıysa, tam ekranda çalışan her uygulamada Avira ürününüz otomatik olarak 'na Sunum Modu'na geçer.

Görüntülenen **AÇ/KAPAT** düğmesinin sağındaki yapılandırma simgesine tıklatılarak bu işlemlerin diğer seçeneklerine bir bağlam menüsünden erişilebilir:

- **Yapılandır**: İşlem bileşeninin ayarlarını tanımlamak için Yapılandırma'ya gidin.

Aşağıdaki olasılıklar kullanılabilir: *Hizmetler*

Simge	Durum	İşlem durumu	Seçenek	Anlamı
	*Tamam*	*Etkinleştirildi*	**Devre dışı bırak**	İnternet Koruması için tüm hizmetler etkindir. **Not** **AÇ/KAPAT** düğmesini tıklatarak bir hizmeti devre dışı bırakabilirsiniz. Ancak, bir hizmet devre dışı bırakıldıktan sonra virüslere ve zararlı yazılımlara karşı tamamen korunmayacağınızı unutmayın.
	*Kısıtlı*	*Devre dışı bırakıldı*	**Etkinleştir**	Bir hizmet devre dışı bırakılır; başka bir deyişle, hizmet başlatılmıştır ancak etkin değildir. **Uyarı** Bilgisayar sisteminiz tamamen izlenmemektedir. Virüs ve istenmeyen programların bilgisayar sisteminize erişebilme olasılığı vardır. **Not** Hizmeti etkinleştirmek için, **AÇ/KAPAT** düğmesini tıklatın.

	Uyarı	*Hizmet durduruldu*	**Hizmet başlat**	Bir hizmet durduruldu **Uyarı** Bilgisayar sisteminiz tamamen izlenmemektedir. Virüs ve istenmeyen programların bilgisayar sisteminize erişebilme olasılığı vardır. **Not** Bilgisayar sisteminizin izlenmesi için hizmeti başlatmak üzere **AÇ/KAPAT** düğmesini tıklatın. Hizmet başlatılır ve etkinleştirilir.
		Unknown	**Help**	Bilinmeyen bir hata oluştuğunda bu durum görüntülenir. Bu durumda, lütfen Destek birimimizle iletişim kurun.

7.3.2 Sunum Modu

Bilgisayar sisteminizde bir uygulama tam ekran modunda yürütüldüğünde, Sunum Modunu etkinleştirerek kendi isteğinizle masaüstü bildirimlerini açılan pencereler ve ürün mesajları olarak askıya alabilirsiniz. Avira Güvenlik Duvarı'nda yapılandırdığınız tüm tanımlı bağdaştırıcı ve uygulama kuralları geçerlidir, ancak ağ olayı bildirimi içeren bir açılır pencere görüntülenmez.

Sunum Modunu etkinleştirebilirsiniz veya **AÇ/KAPAT** düğmesini tıklatarak otomatik modda kalabilirsiniz. Sunum Modu varsayılan olarak **otomatik** olarak ayarlanmıştır ve yeşil renkte gösterilir. Varsayılan ayar bu özelliği otomatik olarak ayarlar, tam ekran modu gerektiren bir uygulama çalıştırdığınızda, Avira ürünü otomatik olarak Sunum Moduna geçer.

- Sunum Modunu etkinleştirmek için **KAPALI** düğmesinin sol yanındaki düğmeyi tıklatın.
  - ↪ Sunum Modu etkindir ve sarı renkte gösterilir.

Not
Otomatik tam ekran tanıması modu ile varsayılan ayarı geçici olarak **KAPALI**

moda değiştirmenizi öneririz, çünkü ağ olayları ve olası tehditler hakkında görünür masaüstü bildirimleri ve uyarıları almayacaksınız.

7.3.3 Sistem Tarayıcı

Sistem Tarayıcı bölümü, kolayca bir sistem taraması yapılandırmanıza ve başlatmanıza olanak sağlar. Önceden tanımlı profiller, önceden uyarlanmış varsayılan seçeneklerle bir sistem taramasını etkinleştirir. Aynı şekilde, el ile seçim yardımıyla veya kullanıcı tanımlı profiller oluşturularak virüs ve istenmeyen programlara karşı sistem taramasını kişisel gereksinimlerinize uyarlamanız mümkündür. Gerekli eylem, araç çubuğundaki simge aracılığıyla, kısayol kullanılarak veya bağlam menüsü yardımıyla seçilebilir. Seçili profille sistem taraması başlat öğesi ile bir sistem taraması başlatın.

Düzenlenebilir profillerin görüntülenmesi ve işlenmesi, Windows Gezgini'ninkilere karşılık gelir. Ana dizindeki her klasör tek bir profile karşılık gelir. Taranacak klasörler veya dosyalar taranacak klasörün ya da dosyanın önünde bir onay işareti ile seçilir veya seçilebilir.

- Dizinleri değiştirmek için, gerekli dizini çift tıklatın.
- Sürücüleri değiştirmek için, sürücünün gerekli harfini çift tıklatın.
- Klasörleri ve sürücüleri seçmek için, klasörün veya sürücü simgesinin önündeki kutuyu tıklatabilir ya da bağlam menüsü aracılığıyla seçim yapabilirsiniz.
- Kaydırma çubuğu ve kaydırma okları yardımıyla, menü yapısında gezinebilirsiniz.

Önceden tanımlı profiller

Önceden tanımlı tarama profilleri, gerekirse kullanılabilir durumdadır.

Not
Bu profiller salt okunurdur ve değiştirilemez veya silinemez. Bir profili gereksinimlerinize göre uyarlamak üzere, bir defalık tarama için El ile seçim klasörünü seçin veya Yeni profil oluştur seçeneğini belirleyerek, kaydedilebilen bir kullanıcı tanımlı profil oluşturun.

Not
Önceden tanımlı profillerin tarama seçenekleri Yapılandırma > Sistem Tarayıcı > Tara > Dosyalar altında ayarlanabilir. Bu ayarları gereksinimlerinize göre uyarlayabilirsiniz.

Yerel Sürücüler

Sisteminizdeki tüm yerel sürücüler, virüs veya istenmeyen programlara karşı taranır.

Yerel Sabit Diskler

Sisteminizdeki tüm yerel sabit diskler, virüs veya istenmeyen programlara karşı taranır.

Çıkarılabilir Sürücüler

Sisteminizin tüm kullanılabilir durumdaki çıkarılabilir sürücüleri, virüs veya istenmeyen programlara karşı taranır.

Windows Sistem Dizini

Sisteminizin Windows sistem dizini, virüs veya istenmeyen programlara karşı taranır.

Eksiksiz sistem taraması

Bilgisayarınızdaki tüm yerel sabit diskler, virüs veya istenmeyen programlara karşı taranır. Tarama esnasında sistem dosyalarının bütünlük kontrolü dışında tüm tarama işlemleri kullanılır: Standart dosya taraması, kayıt defteri ve önyükleme sektörleri taraması, kök kullanıcı takımı taraması vb. (bkz. Sistem Tarayıcı > Genel bakış). Şu konumda yer alan yapılandırmadaki tarayıcı ayarına bakılmaksızın tarama işlemleri gerçekleştirilir: Sistem Tarayıcı > Tara: Diğer ayarlar.

Hızlı sistem taraması

Sisteminizin en önemli klasörleri (*Windows*, *Programlar*, *Belgeler ve Ayarlar\Yerel Kullanıcı*, *Belgeler ve Ayarlar\Tüm Kullanıcılar* dizinleri) virüsler ve istenmeyen programlara karşı taranır.

Belgelerim

Oturum açan kullanıcının varsayılan "*Belgelerim*" konumu, virüs ve istenmeyen programlara karşı taranır.

Not
Windows'da "*Belgelerim*", kaydedilen belgeler için varsayılan konum olarak kullanılan, kullanıcı profilindeki bir dizindir. Bu dizinin varsayılan ayarı *C:\Belgeler ve Ayarlar\[kullanıcı adı]\Belgelerim* şeklindedir.

Etkin İşlemler

Tüm geçerli işlemler, virüs veya istenmeyen programlara karşı taranır.

Kök kullanıcı takımı ve etkin zararlı yazılımlara karşı tara

Bilgisayar, kök kullanıcı takımı ve etkin (çalışmakta olan) zararlı yazılım programlarına karşı taranır. Çalışmakta olan tüm işlemler denetlenir.

Not
Etkileşimli modda bir algılamaya yanıt vermenin birçok yolu vardır. Otomatik modda algılama, rapor dosyasına kaydedilir.

Not
Kök kullanıcı takımı taraması, Windows XP 64 bit için kullanılamaz!

7.3.4 El ile seçim

Taramayı bireysel gereksinimlerinize uyarlamak istiyorsanız bu klasörü seçin. Taranacak gerekli dizinleri ve dosyaları işaretleyin. Avira ürününüz Avira Yönetim Konsolu tarafından yönetiliyorsa, '?' ile ayrılmış olan birden fazla dizini taramak için **Komutlar** iletişim penceresindeki **El ile Seçim** alanını kullanabilirsiniz (örneğin: `c:\temp?d:\test`).

Not
El ile seçim profili, önce yeni bir profil oluşturmadan verileri taramak için kullanılır.

Kullanıcı tanımlı profiller

Yeni bir profil, araç çubuğu aracılığıyla, kısayol kullanılarak veya bağlam menüsü yardımıyla oluşturulabilir.

Yeni profiller, istediğiniz adla kaydedilebilir ve Zamanlayıcı yardımıyla zamanlanmış taramalar oluşturmak için el ile denetlenen taramaya ek olarak kullanışlıdır.

Araç Çubuğu ve Kısayollar

Simge	Kısayol	Açıklama
	**F3**	**Seçilen profille tarama başlat** Seçilen profil, virüslere veya istenmeyen programlara karşı taranır.
	**F6**	**Yönetici olarak seçilen simgeyle tarama başlat** Seçilen profil yönetici haklarıyla taranır
	**Ins**	**Yeni profil oluştur** Yeni bir profil oluşturulur.
	**F2**	**Seçilen profili yeniden adlandır** Seçilen profil için yeni bir ad kaydedilir.

	F4	**Seçilen profil için masaüstü bağlantısı oluştur** Masaüstünde seçilen profil için bir bağlantı oluşturulur.
	Del	**Seçilen profili sil** Seçilen profil, geri alınamaz şekilde silinir.

Bağlam menüsü

Bu bölümün bağlam menüsü, istenen profil fareyle seçilip sağ fare düğmesi basılı tutularak elde edilebilir.

Taramayı başlat

Seçilen profil, virüslere veya istenmeyen programlara karşı taranır.

Taramayı başlat (yönetici)

(Bu işlev yalnızca Windows Vista'dan itibaren kullanılabilir. Bu eylemi yürütmek için yönetici hakları gerekir.)

Seçilen profil, virüslere veya istenmeyen programlara karşı taranır.

Yeni profil oluştur

Yeni bir profil oluşturulur. Taranacak dizinleri ve dosyaları seçin.

Profili yeniden adlandır

Seçilen profile, seçtiğiniz adı verir.

> **Not**
> Bir önceden tanımlı profil seçilirse, bağlam menüsünde bu girdi seçilemez.

Profili sil

Seçilen profil, geri alınamaz şekilde silinir.

> **Not**
> Bir önceden tanımlı profil seçilirse, bağlam menüsünde bu girdi seçilemez.

Dosya filtresi

Varsayılan:

Dosyaların, Yapılandırma'nın Dosyalar grubundaki ayara göre taranacağı anlamına gelir. Bu ayarı Yapılandırma'da gereksinimlerinize göre uyarlayabilirsiniz. Yapılandırma düğmesi veya bağlantısı aracılığıyla Yapılandırma'ya erişebilirsiniz.

Tüm dosyaları tara:

Tüm dosyalar, yapılandırma içindeki ayardan bağımsız olarak taranır.

Kullanıcı tanımlı:

Taranan tüm dosya uzantılarının görüntülendiği bir iletişim kutusu açılır. Uzantılar için varsayılan girdiler tanımlanır. Ancak girdiler eklenebilir veya silinebilir.

Not
Bu girdi yalnızca fare bir onay kutusunun üzerinde olduğunda bağlam menüsünde seçilebilir.
Bu seçenek, önceden tanımlı profiller ile kullanılamaz.

Seç

Alt dizinler ile:

Seçilen düğümde (siyah onay işareti) her şey taranır.

Alt dizinler olmadan:

Yalnızca seçilen düğümdeki (yeşil onay işareti) dosyalar taranır.

Yalnızca alt dizinler:

Düğümdeki dosyalar değil, yalnızca seçilen düğümdeki alt dizinler taranır (gri onay işareti, alt dizinlerin siyah bir onay işareti vardır).

Seçim yok:

Seçim iptal edilir, şu anda seçili olan düğüm taranmaz (onay işareti yok).

Not
Bu girdi yalnızca fare bir onay kutusunun üzerinde olduğunda bağlam menüsünde seçilebilir.
Bu seçenek, önceden tanımlı profiller ile kullanılamaz.

Masaüstü bağlantısı oluştur

Masaüstünde seçilen profile bağlantı oluşturur.

Not
El ile seçim ayarları kalıcı olarak kaydedilmediğinden, El ile seçim profili seçilirse, bağlam menüsünde bu girdi seçilemez.

7.3.5 Gerçek Zamanlı Koruma

Gerçek Zamanlı Koruma bölümünde, taranmış dosyalarla ilgili bilgiler ve diğer istatistiksel veriler görüntülenir ve bu istendiği zaman sıfırlanabilir ve rapor dosyasına erişilmesini sağlar. Algılanan son virüs veya istenmeyen programla ilgili daha ayrıntılı bilgi, "bir düğme basışıyla" pratik olarak edinilebilir.

Not
Gerçek Zamanlı Koruma hizmeti başlatılmadıysa, modülün yanındaki düğme sarı renkte görüntülenir. Ancak Gerçek Zamanlı Koruma'nın rapor dosyası görüntülenebilir.

Araç çubuğu

Simge	Açıklama
	**Rapor dosyasını görüntüle** Gerçek Zamanlı Koruma'nın rapor dosyası görüntülenir.
	**İstatistik verilerini sıfırla** Bu bölümdeki istatistiksel bilgiler sıfır olarak ayarlanır.

Görüntülenen bilgi

Bulunan son dosya

Gerçek Zamanlı Koruma tarafından en son bulunan dosyanın adını ve konumunu gösterir.

Bulunan son virüs veya istenmeyen program

Bulunan son virüsün veya istenmeyen programın adını verir.

Simge/bağlantı	Açıklama
	Internet bağlantısı varsa, virüs veya istenmeyen programla ilgili ayrıntılı bilgileri görüntülemek için simgeyi veya bağlantıyı tıklatın.

Son taranan dosya

Gerçek Zamanlı Koruma tarafından en son taranan dosyanın adını ve yolunu gösterir.

İstatistikler

Dosya sayısı

Şu ana kadar taranan dosyaların sayısını gösterir.

Algılama sayısı

Şu ana kadar bulunan virüslerin ve istenmeyen programların sayısını gösterir.

Şüpheli dosya sayısı

Buluşsal yöntem tarafından bildirilen dosyaların sayısını görüntüler.

Silinen dosya sayısı

Şu ana kadar silinen dosyaların sayısını gösterir.

Onarılan dosya sayısı

Şu ana kadar onarılan dosyaların sayısını gösterir.

Taşınan dosya sayısı

Şu ana kadar taşınan dosyaların sayısını gösterir.

Yeniden adlandırılan dosya sayısı

Şu ana kadar yeniden adlandırılan dosyaların sayısını gösterir.

7.3.6 Güvenlik Duvarı

Avira Güvenlik Duvarı (Avira Professional Security)

Güvenlik Duvarı bölümünde geçerli veri aktarım hızı görüntülenir. Güvenlik Duvarı bölümü, Avira Güvenlik Duvarı için temel ayarları yapılandırmanıza olanak sağlar: Gerekli olan **Güvenlik düzeyi**'ni kaydırıcı aracılığıyla ayarlayabilirsiniz. Kullanıcı tanımlı bir güvenlik düzeyi yapılandırmak için **Yapılandırma** konumuna geçiş yapmanız gerekir.

Araç çubuğu

Simge	Açıklama
	**İstatistikleri sıfırla** Bu bölümdeki istatistiksel bilgiler sıfır olarak ayarlanır.

Güvenlik düzeyi

Aşağıdaki güvenlik düzeylerinden birini seçebilirsiniz:

> **Not**
> Güvenlik ölçeği boyunca kaydırıcıyı sürükleyerek güvenlik düzeyini değiştirebilirsiniz. Seçilen güvenlik düzeyi, seçimden hemen sonra uygulanır. Daha ayrıntılı bilgi için lütfen Güvenlik Duvarı yapılandırmasına bakın: Yapılandırma > Güvenlik Duvarı > Avira Güvenlik Duvarıu > Bağdaştırıcı kuralları.

Düşük

Baskın ve bağlantı noktası taraması algılanır.

Orta

Şüpheli TCP ve UDP paketleri atılır.

Baskın ve bağlantı noktası taraması önlenir.

(Varsayılan düzeye ayarla.)

Yüksek

Bilgisayar ağda görünmez.

Dışarıdan gelen yeni bağlantılara izin verilmez.

Baskın ve bağlantı noktası taraması önlenir.

Özel

Kullanıcı tanımlı kurallar.

Tümünü engelle

Tüm mevcut ağ bağlantıları kapanacak.

Aktar

Karşıya yüklenen (*Gönderilen*) ve karşıdan yüklenen (*Alınan*) geçerli ve toplam veri miktarıyla ilgili bilgiler bu kutuda görüntülenir. Grafiğin sol üst köşesinde maksimum değerin görüntülendiğini görebilirsiniz.

Kırmızı renk gelen paketleri, yeşil renk ise giden paketleri temsil eder. İki durumun çakıştığı alanlar gri renklidir.

Windows Güvenlik Duvarı (Windows 7 veya daha üstü)

Windows 7'den başlayarak, Avira Professional Security artık Avira Güvenlik Duvarı içermemektedir. Avira bunun yerine Kontrol ve Yapılandırma Merkezi içinden Windows Güvenlik Duvarı'nı kontrol eder.

Güvenlik Duvarı bölümü Windows Güvenlik Duvarı durumunu kontrol etmenizi ve **Sorunu onar** düğmesine tıklayarak özenerilen ayarları geri yüklemenizi sağlar.

7.3.7 Web Koruması

Web Koruması bölümünde, taranmış URL'ler ile ilgili bilgiler ve diğer istatistiksel veriler görüntülenir ve bu istendiği zaman sıfırlanabilir ve rapor dosyasına erişilmesini sağlar. Algılanan son virüs veya istenmeyen programla ilgili daha ayrıntılı bilgi, "bir düğme basışıyla" pratik olarak edinilebilir.

Araç çubuğu

Simge	Açıklama
	**Rapor dosyası göster** Web Koruması'nın rapor dosyası görüntülenir.
	**İstatistik verilerini sıfırla** Bu bölümdeki istatistiksel bilgiler sıfır olarak ayarlanır.

Görüntülenen bilgi

Son bildirilen URL

Web Koruması tarafından algılanan son URL'yi görüntüler.

Son algılanan virüs veya istenmeyen program

Bulunan son virüsün veya istenmeyen programın adını verir.

Simge/bağlantı	Açıklama
	Internet bağlantısı varsa, virüs veya istenmeyen programla ilgili ayrıntılı bilgileri görüntülemek için simgeyi veya bağlantıyı tıklatın.

Son taranan URL

Web Koruması tarafından denetlenen son URL'nin adını ve yolunu gösterir.

İstatistikler

URL sayısı

O noktaya kadar denetlenen URL'lerin sayısını gösterir.

Algılama sayısı

Şu ana kadar bulunan virüslerin ve istenmeyen programların sayısını gösterir.

Engellenen URL sayısı

Önceden engellenen URL sayısını gösterir.

Yoksayılan URL sayısı

Önceden yoksayılan URL'lerin sayısını gösterir.

7.3.8 EPosta Koruması

EPosta Koruması bölümünde, EPosta Koruması tarafından taranan tüm e-postalar, bunların özellikleri ve diğer istatistiksel veriler gösterilir.

Not
EPosta Koruması hizmeti başlatılmadıysa, modülün yanındaki düğme sarı renkte görüntülenir. Ancak EPosta Koruması'nın rapor dosyası görüntülenebilir. Avira ürününüzde modül kullanılamıyorsa, bu bölümün kutuları grileşir ve seçilemez.

Not
Yalnızca gelen e-postalarda tek tek e-posta adresleri zararlı yazılım

taramasından hariç tutulabilir. Giden e-postaların taranmasını devre dışı bırakmak için, taramayı yapılandırmada EPosta Koruması > Tara altında devre dışı bırakın.

Araç çubuğu

Simge	Açıklama
	**Rapor dosyasını görüntüle** EPosta Koruması'nın rapor dosyası görüntülenir.
	**Seçilen e-postanın özelliklerini görüntüle** Seçilen e-postayla ilgili daha fazla bilgi içeren bir iletişim kutusu açılır.
	**E-posta adresini zararlı yazılıma karşı tarama** Seçilen e-posta adresi artık gelecekte virüslere ve istenmeyen programlara karşı taranmaz. Şu konumdaki yapılandırmada bu ayarı yeniden geri alabilirsiniz: EPosta Koruması > Genel > İstisnalar.
	**Seçilen e-postaları sil** Seçilen e-posta, önbellekten silinir. Ancak e-posta, e-posta programınızda kalır.
	**İstatistik verilerini sıfırla** Bu bölümdeki istatistiksel bilgiler sıfır olarak ayarlanır.

Taranan e-postalar

Bu alanda, EPosta Koruması tarafından taranan e-postalar gösterilir.

Simge	Açıklama
	Bir virüs veya istenmeyen program bulunmadı.
	Bir virüs veya istenmeyen program bulundu.

Tür

E-postayı göndermek veya almak için kullanılan protokolü gösterir:

- POP3: POP3 aracılığıyla alınan e-posta
- IMAP: IMAP aracılığıyla alınan e-posta
- SMTP: SMTP aracılığıyla gönderilen e-posta

Kimden/Kime

E-posta gönderenin adresini gösterir.

Konu

Alınan e-postanın konusunu gösterir.

Tarih/Saat

E-postanın istenmeyen postaya karşı tarandığı zamanı gösterir.

Not
İlgili e-postayı çift tıklatarak bir e-postayla ilgili daha fazla bilgi edinebilirsiniz.

İstatistikler

E-posta eylemi

EPosta Koruması bir e-postada virüs veya istenmeyen program bulduğunda gerçekleştirilen eylemi gösterir. Etkileşimli modda burada kullanılabilir bir görüntü yoktur, algılama olayında hangi yordamın izleneceğini siz seçebilirsiniz.

Not
Bu ayarı Yapılandırma'da gereksinimlerinize göre uyarlayabilirsiniz. **Yapılandırma** düğmesi veya bağlantısı aracılığıyla Yapılandırma'ya erişebilirsiniz.

Etkilenen ekler

EPosta Koruması etkilenen bir ekte virüs veya istenmeyen program bulduğunda gerçekleştirilen eylemi gösterir. Etkileşimli modda burada kullanılabilir bir görüntü yoktur, algılama olayında hangi yordamın izleneceğini siz seçebilirsiniz.

Not
Bu ayarı Yapılandırma'da gereksinimlerinize göre uyarlayabilirsiniz. **Yapılandırma** düğmesi veya bağlantısı aracılığıyla Yapılandırma'ya erişebilirsiniz.

E-posta sayısı

EPosta Koruması tarafından taranan e-postaların sayısını gösterir.

Son algılama

Bulunan son virüsün veya istenmeyen programın adını verir.

Algılama sayısı

Önceden algılanan ve bildirilen virüslerin ve istenmeyen programların sayısını gösterir.

Şüpheli e-postalar

Buluşsal yöntem tarafından bildirilen e-postaların sayısını gösterir.

Gelen e-posta sayısı

Alınan e-postaların sayısını gösterir.

Giden e-posta sayısı

Gönderilen e-postaların sayısını gösterir.

7.3.9 Karantina

Karantina yöneticisi, etkilenen nesneleri (dosyalar ve e-postalar) yönetir. Avira ürününüz, etkilenen nesneleri özel bir biçimde karantina dizinine taşıyabilir. Bunlar yürütülemez veya açılamaz.

Not
Otomatik modda çalışıyorsanız, nesneleri Karantina yöneticisine taşımak için, **Sistem Tarayıcı** ve **Gerçek Zamanlı Koruma** ve **EPosta Koruması** - **Tara > Algılama durumunda eylem** konumundaki **Yapılandırma** içinde karantina için ilgili seçeneği belirleyin.
Alternatif olarak, **etkileşimli modda** ilgili karantina seçeneğini belirleyebilirsiniz.

Araç çubuğu, kısayollar ve bağlam menüsü

Simge	Kısayol	Açıklama
	**F2**	**Nesneleri yeniden tara** Seçilen bir nesne, virüslere ve istenmeyen programlara karşı yeniden taranır. Bunun için istek üzerine tarama ayarları kullanılır.
	**Return**	**Özellikler** Seçilen nesneyle ilgili daha ayrıntılı bilgi içeren bir iletişim kutusu açılır. **Not** Ayrıntılı bilgiler, bir nesne çift tıklatılarak da açılabilir.

  (Windows Vista)	**F3**	**Nesneleri geri yükle** Seçilen bir nesne geri yüklenir. Bu nesne daha sonra özgün konumuna gelir. **Not** Bu seçenek, e-posta türündeki nesneler için kullanılamaz. **Uyarı** Virüs ve istenmeyen programlar nedeniyle sistemde ciddi hasar oluştu! Dosyaları geri yüklerseniz: yalnızca başka bir tarama tarafından temizlenebilen dosyaların geri yüklendiğinden emin olun. **Not** Windows Vista'dan itibaren, nesneleri geri yüklemek için yönetici haklarına sahip olmanız gerekir.
	**F6**	**Nesneleri şuraya geri yükle...** Seçilen bir nesne, belirlediğiniz bir konuma geri yüklenebilir. Bu seçeneği belirlerseniz, kayıt yerini seçebileceğiniz bir "Farklı kaydet" iletişim kutusu açılır. **Uyarı** Virüs ve istenmeyen programlar nedeniyle sistemde ciddi hasar oluştu! Dosyaları geri yüklerseniz: yalnızca başka bir tarama tarafından temizlenebilen dosyaların geri yüklendiğinden emin olun.

	**Ins**	**Dosyayı karantinaya ekle** Bir dosyanın şüpheli olduğunu düşünüyorsanız, bu seçenekle onu karantina yöneticisine el ile ekleyebilirsiniz. Nesneyi gönder seçeneği ile, dosyayı incelenmesi için bir Avira Zararlı Yazılım Araştırma Merkezi web sunucusuna karşıya yükleyin.
	**F4**	**Nesneleri gönder** Nesne, Avira Zararlı Yazılım Araştırma Merkezi tarafından incelenmesi için bir Avira Zararlı Yazılım Araştırma Merkezi web sunucusuna karşıya yüklenir. **Nesneyi Gönder** düğmesini tıklattığınızda, ilgili kişi verilerinizi girebileceğiniz bir formu içeren iletişim kutusu açılır. Tüm gerekli verileri girin. Bir tür seçin: **Şüpheli dosya** veya **Şüpheli yanlış tespit**. Şüpheli dosyayı karşıya yüklemek için **Tamam**'ı tıklatın. **Not** Karşıya yüklediğiniz dosyaların boyutu, 20 MB sıkıştırılmamış veya 8 MB sıkıştırılmış olarak sınırlandırılmıştır. **Not** Karşıya yüklemek istediğiniz tüm dosyaları seçip **Nesneyi Gönder** düğmesini tıklatarak birçok dosyayı aynı anda karşıya yükleyebilirsiniz.
	**Del**	**Nesneleri sil** Seçilen bir nesne, karantina yöneticisinden silinir. Nesne geri yüklenemez.
		**Nesneleri şuraya kopyala** Vurgulanan karantinaya alınmış nesne, seçilen dizine kaydedilir. **Not** Karantinaya alınmış nesne, geri yüklenen dosya ile aynı değildir. Karantinaya alınmış nesne şifrelenir ve özgün biçiminde yürütülemez veya okunamaz.

	F7	**Tüm özellikleri dışa aktar** Vurgulanan karantinaya alınmış nesnenin özellikleri bir metin dosyasında dışa aktarılır.
	F10	**Karantina dizinini aç** ETKİLENEN dizini açar.

Not
Birden çok vurgulanmış nesnede eylemler yürütme seçeneğiniz vardır. Birden çok nesneyi (sütunlardaki nesneleri) vurgulamak için, control tuşunu veya shift tuşunu basılı tutarken karantina yöneticisindeki nesneleri seçin. Görüntülenen tüm nesneleri seçmek için **Ctrl + A** tuşlarına basın. **Özellikleri görüntüle** eylemi yürütülürken, birden fazla nesne seçilemez.

Tablo

Durum

Karantinaya yerleştirilen bir nesne farklı durumlarda olabilir:

Simge	Açıklama
	Bir virüs veya istenmeyen program bulunmadı, nesne "temiz".
	Bir virüs veya istenmeyen program bulundu.
	Şüpheli dosya, Dosya ekle seçeneğiyle karantina yöneticisine eklendiyse, bu uyarı simgesini içerir.

Tür

Gösterge	Açıklama
E-posta	Algılanan nesne bir e-postadır.
Dosya	Algılanan nesne bir dosyadır.

Algılama

Bulunan zararlı yazılımın adını gösterir.
Buluşsal yöntem bulguları HEUR/ kısaltmasıyla tanımlanır.

Kaynak

Nesnenin bulunduğu yolu gösterir.

Tarih/Saat

Algılamanın tarihini ve saatini gösterir.

Ayrıntılı bilgi

Dosya adı

Nesnenin tam yolu ve dosya adı.

Karantinaya alınmış nesne

Karantinaya alınmış nesnenin dosya adı.

Geri yüklendi

EVET/ HAYIR

EVET: Seçilen nesne geri yüklenmiştir.

HAYIR: Seçilen nesne geri yüklenmemiştir.

Avira hedefine yüklendi

EVET/ HAYIR

EVET: Nesne, Avira Zararlı Yazılım Araştırma Merkezi tarafından araştırılmak üzere önceden bir Avira Zararlı Yazılım Araştırma Merkezi

web sunucusuna yüklenmiştir.

HAYIR: Nesne, Avira Zararlı Yazılım Araştırma Merkezi tarafından araştırılmak üzere bir Avira Zararlı Yazılım Araştırma Merkezi

web sunucusuna henüz yüklenmemiştir.

İşletim sistemi

Windows XP: Bir Avira masaüstü ürünü tarafından zararlı yazılım tanımlanmıştır.

Tarama motoru

Tarama motorunun sürüm numarası

Virüs tanımı dosyası

Virüs tanımı dosyasının sürüm numarası

Algılama

Algılanan zararlı yazılımın adı.

Tarih/Saat

Algılamanın tarihi ve saati

7.3.10 Zamanlayıcı

Zamanlayıcı size zamanlanan tarama ve güncelleme işleri , oluşturma ve varolan işleri uyarlama ya da silme seçeneği sunar.

Kurulumdan sonra aşağıdaki iş varsayılan olarak oluşturulur:

- Tarama işi **Hızlı Sistem Taraması** (varsayılan olarak etkindir): Haftalık bir hızlı sistem taraması otomatik olarak gerçekleştirilir. Hızlı sistem taramasında yalnızca bilgisayarınızdaki önemli dosya ve klasörler virüs veya istenmeyen programlara karşı taranır. **Hızlı Sistem Taraması** işini değiştirebilirsiniz, ancak ihtiyaçlarınızı daha iyi yansıtan başka tarama işleri oluşturmanız önerilir.

Araç çubuğu, kısayollar ve bağlam menüsü

Simge	Kısayol	Açıklama
	**Ins**	**Yeni iş ekle** Yeni bir iş oluşturur. Bir sihirbaz, gerekli ayarlar boyunca size yol gösterir.
	**Return**	**Özellikler** Seçilen işle ilgili daha fazla bilgi içeren bir iletişim kutusu açılır.
	**F2**	**İşi düzenle** Bir iş oluşturma ve değiştirme sihirbazını açar.
	**Del**	**İşi sil** Seçilen işleri listeden siler.

		Rapor dosyasını görüntüle Zamanlayıcı'nın rapor dosyası görüntülenir.
	F3	**İş başlat** Listeden işaretlenen bir işi başlatır.
	F4	**İşi durdur** Başlatılan ve işaretlenen bir işi durdurur.

Tablo

İş türü

Simge	Açıklama
	İş bir güncelleme işidir.
	İş bir tarama işidir.

Ad

İşin adı.

Eylem

Bir işin **tarama** mı yoksa **güncelleme** mi olduğunu belirtir.

Sıklık

İşin ne sıklıkla ve ne zaman başlatıldığını belirtir.

Görüntü modu

Aşağıdaki görüntü modları kullanılabilir:

Görünmez: İş arka planda gerçekleştirilir ve görünmez. Bu, tarama işleri ve güncelleme işleri için geçerlidir.

Simge durumuna küçült: İş penceresi yalnızca bir ilerleme çubuğu görüntüler.

Ekranı kapla: İş penceresi tamamen görünür olur.

Etkin

Bu onay kutusunu etkinleştirdiğinizde, iş etkinleştirilir.

Not
İş sıklığı **Hemen** olarak ayarlandıysa, etkinleştirildiği anda iş başlatılır. Bu size gerekirse işi yeniden başlatma imkanı sunar.

Durum

İşin durumunu görüntüler:

Hazır: İş, yürütme için hazırdır.

Yürütülüyor: İş başlatılmıştır ve yürütülmektedir.

Zamanlayıcı ile işler oluştur

Planlama sihirbazı, planlama, yapılandırma ve oluşturma konusunda sizi destekler

- virüslere ve istenmeyen programlara karşı zamanlanmış tarama
- Internet veya Intranet aracılığıyla zamanlanmış güncelleme

Her iki iş türü için şunları girmeniz gerekir

- işin adı ve açıklaması
- işin ne zaman başlatılacağı
- işin ne sıklıkla gerçekleştirileceği
- işin görüntü modu

İşin sıklığı

İşin sıklığı	Açıklama
Hemen	Planlama sihirbazı tamamlandıktan hemen sonra iş başlatılır.
Günlük	İş her gün belirli bir saatte başlatılır; örn. 22:00.
Haftalık	İş her hafta belirli bir günde veya hafta içi birçok günde belirli bir saatte başlatılır; örn. Salı ve Cuma, 16:26.
Aralık	İş belirli aralıklarla gerçekleştirilir; örn. 24 saatte bir.

Tek	İş tanımlanmış bir saatte bir defa gerçekleştirilir; örn. 10.04.04 tarihinde saat 10:04'te.
Oturum aç	İş, bir Windows kullanıcısı her oturum açtığında gerçekleştirilir.

İşin başlangıç saati

İş başlangıç saati için bir hafta içi gün, tarih, saat veya aralık tanımlayabilirsiniz. Başlangıç saati olarak **Hemen** seçeneğini girdiyseniz, bu görüntülenmez.

İş türüne bağlı olarak, çeşitli ek seçenekler vardır

Ayrıca Internet'e bağlanırken de (çevirmeli) iş başlat

Tanımlanmış sıklığa ek olarak, bir İnternet bağlantısı kurulduğunda iş gerçekleştirilir. Günlük, haftalık veya başka aralıklarda gerçekleştirilecek bir güncelleme işi ile bu seçenek belirlenebilir.

Süre önceden dolduysa işi yinele

Örneğin, bilgisayar kapatıldığı için gerekli zamanda gerçekleştirilemeyen geçmiş işler gerçekleştirilir.
Günlük, haftalık, aralıklı olarak veya bir defalık gerçekleştirilecek bir güncelleme işi ve tarama işi ile bu seçenek belirlenebilir.

İş bittiğinde bilgisayarı kapat

İş bittiğinde bilgisayar kapatılır. Tarama işleri, simge durumuna küçültülmüş ve ekranı kaplayacak şekilde görüntülenebilir.

> **Not**
> Tarama işi ile hem önceden tanımlı profiller hem de kullanıcı tanımlı profiller, **Profil seçimi** iletişim kutusunda seçilebilir. El ile seçim profili her zaman geçerli seçim ile gerçekleştirilir.

7.3.11 Raporlar

Raporlar bölümü, program tarafından gerçekleştirilen eylemlerin sonuçlarına erişmenize olanak sağlar.

Araç çubuğu, kısayollar ve bağlam menüsü

Simge	Kısayol	Açıklama
	Return	**Raporu görüntüle** Seçilen eylemin sonucunun görüntülendiği bir pencereyi açar. Örneğin, bir tarama sonucu.
	F3	**Rapor dosyasını görüntüle** Seçilen raporun rapor dosyasını görüntüler.
	F4	**Rapor dosyasını yazdır** Rapor dosyasını yazdırmak için Windows'un yazdır iletişim kutusunu açar.
	Del	**Raporları sil** Seçilen raporu ve ilgili rapor dosyasını siler.

Tablo

Durum

Simge	Açıklama
	Eylem taraması: Virüs algılanmadan başarıyla bitti.
	Eylem taraması: Virüs algılandı veya başarısız şekilde bitti.
	Eylem güncellemesi: Başarıyla tamamlandı.
	Eylem güncellemesi: Başarıyla tamamlanmadı.

- **Eylem**

  Gerçekleştirilen eylemi gösterir.
- **Sonuç**

  Eylemin sonucunu gösterir.
- **Tarih/Saat**

Raporun oluşturulduğu tarihi ve saati gösterir.

7.3.12 Tarama için bir raporun içerikleri

- *Tarama tarihi:*

  Tarama tarihi.
- *Tarama başlangıç saati:*

  Tarama başlangıç saati sa:dd.
- *Gereken tarama süresi:*

  Tarama süresi dd:sn.
- *Tarama durumu:*

  Taramanın tamamlanma durumunu gösterir.
- *Son algılama:*

  Bulunan son virüsün veya istenmeyen programın adı.
- *Taranan dizinler:*

  Taranan dizinlerin toplam sayısı.
- *Taranan dosyalar:*

  Taranan dosyaların toplam sayısı.
- *Taranan arşivler:*

  Taranan arşivlerin sayısı.
- *Gizli nesneler:*

  Algılanan gizli nesnelerin toplam sayısı
- *Algılamalar:*

  Algılanan virüslerin ve istenmeyen programların toplam sayısı.
- *Şüpheli:*

  Şüpheli dosya sayısı.
- *Uyarılar:*

  Algılanan virüslerle ilgili uyarı sayısı.
- *Bilgi:*

  Yayınlanan bilgi öğeleri sayısı; örneğin, bir tarama sırasında ortaya çıkabilecek daha fazla bilgi.
- *Onarılan:*

  Onarılan dosyaların toplam sayısı
- *Karantina:*

  Karantinaya yerleştirilen dosyaların toplam sayısı.
- *Yeniden adlandırılan:*

Yeniden adlandırılan dosyaların toplam sayısı.

- *Silinen:*

  Silinen dosyaların toplam sayısı.

- *Temizlenen:*

  Üzerine yazılan dosyaların toplam sayısı.

> **Not**
> Kök kullanıcı takımı, kayıt defteri girdileri veya dosyalar gibi nesneleri ve işlemleri gizleme yeteneğine sahiptir. Ancak her gizli nesne mutlaka bir kök kullanıcı takımının varlığını göstermek zorunda değildir. Gizli nesneler zararsız nesneler de olabilir. Bir taramada gizli nesneler algılanır ancak virüs tanımlama uyarısı verilmezse, hangi nesneye başvurulduğunu belirlemek ve algılanan nesneyle ilgili daha fazla bilgi edinmek için raporu kullanmanız gerekir.

7.3.13 Olaylar

Çeşitli program bileşenleri tarafından oluşturulan olaylar, **Olaylar** konumunda görüntülenir.

Olaylar bir veritabanında depolanır. Olay veritabanının boyutunu sınırlandırabilir veya veritabanı boyutu üzerindeki kısıtlamayı devre dışı bırakabilirsiniz (bkz.). Yalnızca son 30 günün olayları varsayılan ayarda kaydedilir. **Olaylar** bölümünü seçtiğinizde, olay görüntüsü otomatik olarak güncellenir.

> **Not**
> Olay veritabanında 20.000'den fazla depolanmış olay varsa, bölüm seçildiğinde görüntü otomatik olarak güncellenmez. Bu durumda, olay görüntüleyicisini güncellemek için **F5** tuşuna basın.

Araç çubuğu, kısayollar ve bağlam menüsü

Simge	Kısayol	Açıklama
	**Return**	**Seçilen olayı göster** Seçilen eylemin sonucunun görüntülendiği bir pencereyi açar. Örneğin, bir tarama sonucu.
	**F3**	**Seçilen olay(lar)ı dışa aktar** Seçilen olayları dışa aktarır.

	**Del**	**Seçilen olay(lar)ı sil** Seçilen olayı siler.

Not
Birçok seçilen olayda eylem gerçekleştirme seçeneğiniz vardır. Çok sayıda olay seçmek için, **Ctrl tuşunu** veya **Shift tuşunu** (art arda olayları seçer) basılı tutarken istediğiniz olayları seçin. Tüm görüntülenen olayları seçmek için, **Ctrl + A** tuşlarına basın.
Seçilen olayı göster eylemi olması durumunda, birden çok nesne üzerinde eylem gerçekleştirilmesi mümkün değildir.

Modüller

Aşağıdaki modüllerin olayları (burada alfabetik sırada), olay görüntüleyicisi tarafından görüntülenebilir:

Modülün adı
Güvenlik Duvarı
Yardımcı Hizmeti
EPosta Koruması
Gerçek Zamanlı Koruma
Zamanlayıcı
Sistem Tarayıcı
Güncelleyici
Web Koruması

Tümü kutusunu işaretleyerek, tüm kullanılabilir modüllerin olaylarını görüntüleyebilirsiniz. Yalnızca belirli bir modülün olaylarını görüntülemek için lütfen gerekli modülün yanındaki kutuyu işaretleyin.

Filtre

Aşağıdaki olay sınıflandırması, olay görüntüleyicisi tarafından görüntülenebilir.

Simge	Açıklama
	Bilgi
	Uyarı
	Hata
	Algılama

Filtre kutusunu işaretleyerek, tüm kullanılabilir modüllerin olaylarını görüntüleyebilirsiniz. Yalnızca belirli olayları görüntülemek için lütfen gerekli olayın yanındaki kutuyu işaretleyin.

Tablo

Olay listesi aşağıdaki bilgileri içerir:

- **Simge**

  Olay sınıflandırmasının simgesi.
- **Tür**

  Olay önem düzeyinin sınıflandırması: *Bilgi*, *Uyarı*, *Hata*, *Algılama*.
- **Modül**

  Olayı günlüğe kaydeden modül. Örneğin, bir algılama gerçekleştiren Gerçek Zamanlı Koruma modülü.
- **Eylem**

  İlgili modülün olay açıklaması.
- **Tarih/Saat**

  Olayın oluştuğu tarih ve yerel saat.

7.3.14 Yenile

Açılan bölümün görünümünü günceller.

7.4 Ekstralar

7.4.1 Önyükleme kayıtları taraması

Sistem taraması ile iş istasyonunuzun sürücülerinin önyükleme sektörlerini de tarayabilirsiniz. Örneğin, sistem taraması bir virüs algıladığında ve önyükleme sektörlerinin etkilenmediğinden emin olmak istediğinizde bu önerilir.

Shift tuşu basılı tutulup fareyle gerekli sürücüler seçilerek birden çok önyükleme sektörü seçilebilir.

Not
Sistem taraması ile önyükleme sektörlerinin otomatik olarak taranmasını sağlayabilirsiniz (bkz. Seçili sürücülerin önyükleme sürücülerini tara).

Not
Windows Vista'dan itibaren, önyükleme sektörlerini taramak için yönetici haklarına sahip olmanız gerekir.

7.4.2 Algılama listesi

Bu işlev, Avira ürününüzün tanıdığı virüslerin ve istenmeyen programların adlarını listeler. Adlar için kullanışlı bir arama işlevi tümleşiktir.

Algılama listesini ara

Ara: kutusuna arama sözcüğü veya karakter dizisi girin.

Bir ad içindeki karakter dizisini ara

Buraya klavyeyle ardışık harf ve karakter dizisi girebilirsiniz ve işaretçi, bir adın ortasında da olsa bu diziyi içeren ad listesindeki birinci noktaya gider (örneğin: "raxa" ile "Abraxas" bulunur).

Bir adın ilk karakterinden itibaren ara

Buraya klavyeyle baş harf ve sonraki karakterleri girebilirsiniz ve işaretçi, ad listesini alfabetik olarak kaydırır (örneğin: "Ra" ile "Rabbit" bulunur).

Aranan ad veya karakter dizisi kullanılabilir durumdaysa, bulunan konum listede işaretlenir.

İleri doğru ara

Alfabetik sırayla ileri doğru aramayı başlatır.

Geriye doğru ara

Alfabetik sırayla geriye doğru aramayı başlatır.

Birinci eşleşme

Listede bulunan ilk girdiye gider.

Algılama Listesi girdileri

Bu başlık altında, tanınabilen virüslerin veya istenmeyen programların adlarının bir listesi bulunur. Bu listedeki girdilerin çoğu, Avira ürününüzle kaldırılabilir. Bunlar, alfabetik sırayla listelenir (önce özel karakterler ve sayılar, sonra harfler). Listede yukarı veya aşağı kaydırma yapmak için kaydırma çubuğunu kullanın.

7.4.3 Kurtarma CD'sini karşıdan yükleyin

Kurtarma CD'sini karşıdan yükleyin menü komutu, Avira Kurtarma CD'si paketinin karşıdan yüklemesini başlatır. Bu pakette, kişisel bilgisayarlar için önyüklenebilir bir canlı sistem ve en güncel virüs tanımı dosyası ve tarama motoru ile Avira anti-virüs Tarayıcı yer alır. Verileri kurtarmak için veya virüs ve zararlı yazılımlara karşı tarama yürütmek için, işletim sistemi hasarlıysa kişisel bilgisayarınızı CD'den veya DVD'den önyükleyip çalıştırmak üzere Avira kurtarma CD'sini kullanabilirsiniz.

Avira kurtarma CD'si paketi karşıdan yüklendikten sonra, kurtarma CD'sini yazmak için CD/DVD sürücüsü seçebileceğiniz bir iletişim kutusu görüntülenir. Ayrıca Avira kurtarma CD'si paketini kaydetme ve CD'yi daha ileri bir tarihte yazma seçeneğiniz de vardır.

Not
Avira kurtarma CD'si paketini karşıdan yüklemek için etkin bir Internet bağlantınızın olması gerekir. Kurtarma CD'sini yazmak için bir CD/DVD sürücünüzün ve yazılabilir bir CD veya DVD'nizin olması gerekir.

7.4.4 Yapılandırma

Ekstralar menüsündeki **Yapılandırma** menü öğesi, Yapılandırma'yı açar.

7.5 Güncelle

7.5.1 Güncellemeyi başlat...

Güncelle menüsündeki **Güncellemeyi başlat...** menü öğesi anında bir güncelleme başlatır. Virüs tanımı dosyası ve tarama motoru güncellenir. .

7.5.2 Elle güncelleme...

Güncelle menüsündeki **Elle güncelleme...** menü öğesi, VDF/arama motoru güncelleme paketi seçmek ve yüklemek için bir iletişim kutusu açar. Güncelleme paketi, üreticinin web sitesinden karşıdan yüklenebilir ve geçerli virüs tanımı dosyasını ve tarama motorunu içerir:
http://www.avira.com/tr

> **Not**
> Windows Vista'dan itibaren, el ile güncelleme gerçekleştirmek için yönetici haklarına sahip olmanız gerekir.

7.6 Yardım

7.6.1 İçindekiler

Yardım menüsündeki **İçindekiler** menü öğesi, online yardım içeriklerinin listesini açar.

7.6.2 Benioku

Yardım menüsündeki **Benioku** menü öğesi, *readme.txt* dosyasını açar. Bu dosya, Avira ürününüzün her yeni sürümüyle ilgili önemli bilgiler içerir. *readme.txt* dosyasını Windows Başlat menüsü aracılığıyla da açabilirsiniz: **Başlat > Tüm Programlar > Avira > Avira Desktop > Benioku dosyasını görüntüle**.

7.6.3 Bana yardımcı ol

Bir Internet bağlantısı etkin olduğunda, **Yardım** menüsündeki **Bana yardımcı ol** öğesi, Avira ürününüzün Avira web sayfasındaki ilgili Destek sayfasını açar. Burada sık sorulan soruların cevaplarını okuyabilir, bilgi bankasına başvurabilir ve Avira Desteğine ulaşabilirsiniz.

7.6.4 El ile karşıdan yükle

Bir Internet bağlantısı etkin olduğunda, **Yardım** menüsündeki **El ile Karşıdan Yükle** menü komutu, Avira ürününüzün karşıdan yükleme sayfasını açar. Buradan, Avira ürün kılavuzunuzun geçerli sürümünün karşıdan yükleme bağlantısını bulabilirsiniz.

7.6.5 Lisans dosyası yükle

Yardım menüsündeki **Lisans dosyası yükle** menü öğesi, *.KEY* adlı lisans dosyasını yüklemek için bir iletişim kutusu açar.

Not
Windows Vista'dan itibaren, lisans dosyasını yüklemek için yönetici haklarına sahip olmanız gerekir.

7.6.6 Geribildirim gönder

Bir Internet bağlantısı etkin olduğunda, **Yardım** menüsündeki **Geribildirim gönder** menü komutu, Avira ürünleri için bir geribildirim sayfası açar. Burada, ürün kalitesiyle ilgili değerlendirmelerinizin ve diğer önerilerinizin yer aldığı, Avira'ya gönderebileceğiniz bir ürün değerlendirme formunu bulabilirsiniz.

7.6.7 Avira Professional Security hakkında

- **Genel**

  Avira ürününüzle ilgili adresler ve bilgiler.
- **Sürüm bilgileri**

  Avira ürün paketindeki dosyaların sürüm bilgileri.
- **Lisans bilgileri**

  Geçerli lisansın lisans verileri ve çevrimiçi mağazaların bağlantıları (lisans satın alma veya uzatma).

Not
Lisans verilerini önbelleğe kaydedebilirsiniz. *Lisans verileri* alanını sağ tıklatın. Bir bağlam menüsü açılır. Bağlam menüsünde, **Panoya kopyala** menü komutunu tıklatın. Lisans verileriniz şimdi Windows **Ekle** komutu ile panoya kaydedilir ve e-postalara, formlara veya belgelere eklenebilir.

8. Yapılandırma

8.1 Yapılandırma

- Yapılandırma seçeneklerine genel bakış
- Yapılandırma profilleri
- Düğmeler

Yapılandırma seçeneklerine genel bakış

Aşağıdaki yapılandırma seçenekleri kullanılabilir:

- **Sistem Tarayıcı**: Sistem taraması yapılandırması (istek üzerine)
  - Tarama seçenekleri
  - Algılama durumunda eylem
  - Daha fazla eylem
  - Tarama seçeneklerini arşivle
  - Sistem taraması istisnaları
  - Sistem taraması buluşsal yöntemleri
  - Rapor işlevi ayarı
- **Gerçek Zamanlı Koruma**: Gerçek zamanlı (erişim) tarama yapılandırması
  - Tarama seçenekleri
  - Algılama durumunda eylem
  - Daha fazla eylem
  - Erişim taraması istisnaları
  - Erişim taraması buluşsal yöntemi
  - Rapor işlevi ayarı
- **Güncelleme**: Güncelleme ayarlarının yapılandırması, Web sunucusu veya dosya sunucusu aracılığıyla karşıdan yükleme, ürün güncellemelerinin kurulması
  - Dosya sunucusu aracılığıyla karşıdan yükleme
  - Web sunucusu aracılığıyla karşıdan yükleme
  - Proxy ayarları
- **Güvenlik Duvarı**: Güvenlik Duvarı yapılandırması
  - Bağdaştırıcı kuralı ayarı
  - Kullanıcı tanımlı uygulama kuralı ayarları
  - Güvenilen üreticiler listesi (uygulamalar tarafından ağ erişimine ilişkin istisnalar)
  - Genişletilmiş ayarlar: Otomatik kural zaman aşımı, Windows Güvenlik Duvarı'nı durdurma, bildirimler
  - Açılır pencere ayarları (uygulamalar tarafından ağ erişimine ilişkin uyarılar)

- **Web Koruması**: Web Koruması yapılandırması
  - Tarama seçenekleri, Web Koruması etkinleştirme ve devre dışı bırakma
  - Algılama durumunda eylem
  - Engellenen erişim: İstenmeyen dosya türleri ve MIME türleri, bilinen istenmeyen URL'ler için web filtresi (zararlı yazılım, kimlik avı, vb.)
  - Web Koruması tarama istisnaları: URL'ler, dosya türleri, MIME türleri
  - Web Koruması buluşsal yöntemi
  - Rapor işlevi ayarı
- **EPosta Koruması**: EPosta Koruması yapılandırması
  - Tarama seçenekleri: POP3 hesaplarının, IMAP hesaplarının, giden e-postaların (SMTP) izlenmesini etkinleştir
  - Algılama durumunda eylemler
  - Daha fazla eylem
  - EPosta Koruması taraması buluşsal yöntemi
  - İstenmeyen Posta Gönderimi Engelleme işlevi: İzin verilen SMTP sunucuları, izin verilen e-posta gönderenler
  - EPosta Koruması taraması istisnaları
  - Önbellek yapılandırması, boş önbellek
  - Gönderilen e-postalarda altbilgi yapılandırması
  - Rapor işlevi ayarı
- **Genel**:
  - SMTP kullanılarak e-posta yapılandırması
  - Sistem Tarayıcı ve Gerçek Zamanlı Koruma tehdit kategorileri
  - Uygulama filtresi: Engellenen veya izin verilen uygulamalar
  - Gelişmiş koruma: Proaktif ve Koruma Bulutu özelliklerini etkinleştirme seçenekleri.
  - Kontrol Merkezi ve Yapılandırma erişimi için parola koruması
  - Güvenlik: otomatik başlama işlevini engelle, tam sistem tarama durumu görüntüsü, ürün koruma, Windows ana bilgisayar dosyalarını koru
  - WMI: WMI desteğini etkinleştir
  - Olay günlüğü yapılandırması
  - Rapor işlevlerinin yapılandırması
  - Kullanılan dizinlerin ayarı
  - Uyarılar:
    Bileşen(ler) için ağ uyarılarının yapılandırması:
    Sistem Tarayıcı
    rçek Zamanlı Koruma
    Bileşen(ler) için e-posta uyarılarının yapılandırılması:
    Sistem Tarayıcı
    Gerçek Zamanlı Koruma
    Güncelleyici
  - Zararlı yazılım algılanması durumunda verilen sesli uyarıların yapılandırması

Yapılandırma profilleri

Yapılandırma profillerini yönetmek için, standart yapılandırmanın sağ tarafındaki tepsi simgesine tıklayın (bkz. Tepsi Simgesi).
Bu simgeye tıkladığınızda, birçok seçenek görüntülenecektir ve profil yapılandırma seçeneklerini gruplar halinde kaydedebilirsiniz: öncelikle yeni bir yapılandırma ekleyin ve ardından gerekli değerleri yeni yapılandırmaya girin, yani, bu profillere uygulanacak kuralları tanımlayın.

Yapılandırmanın manuel değiştirilmesi veya otomatik değiştirilmesi arasında seçim yapabilirsiniz. Değişikliği otomatik olarak ayarlamak istiyorsanız, uygulanacak kuralları tanımlamanız gerekir.
Size sunulan seçenekler şunlardır: atanmamış bir ağ geçidi kullanıldığında uygulanacak bir varsayılan kural seçmek veya varsayılan ağ geçidini tanımlamak üzere bir IP veya MAC adresi (veya bir IP adresi ve bir ağ maskesi) belirlemek. Bu yapılandırma profilleri tanımlı ağ geçidinin her kullanılışında uygulanır.

Hiçbir geçiş kuralı tanımlanmaz ise, bağlam menüsünde bir yapılandırmaya manuel olarak geçebilirsiniz. Yapılandırma başlığı menüsünü kullanarak yapılandırma profillerini yönetebilirsiniz:

Bağlam menüsü

Kısayol	Bağlam menüsü / açıklama
Ins	**Yeni yapılandırma oluştur** Çeşitli yapılandırma seçenekleri için standart değerlerle yeni bir yapılandırma oluşturur.
F2	**Yapılandırmayı yeniden adlandır** Yapılandırmanın adını düzenler.
Del	**Yapılandırmayı sil** Vurgulanan yapılandırmayı siler: Öncelikle, seçilen yapılandırmayı iptal edebileceğiniz veya onaylayabileceğiniz bir iletişim kutusu açılır.
F4	**Yapılandırmayı kopyala** Vurgulanan yapılandırmayı kopyalar.

F6	**Yapılandırmayı sıfırla** Vurgulanan yapılandırmanın yapılandırma seçeneklerini varsayılan değerlere sıfırlar.
	Kurallar: Yapılandırma profilleri için kural belirlemeye yarayan farklı seçenekleri gösterir: **Hiçbiri** Vurgulanan yapılandırmaya geçiş için geçerli bir kural yoktur. İlgili yapılandırmaya geçiş yapma, el ile yürütülmelidir. **Varsayılan kural** Seçilen yapılandırma, varsayılan yapılandırma olarak kullanılır. Herhangi bir yapılandırmaya atanmamış bir ağ geçidi kullanıldığında, seçilen yapılandırmaya otomatik geçiş gerçekleşir. **Varsayılan ağ geçidi** Vurgulanan yapılandırma için geçiş kuralı olarak varsayılan ağ geçidinin bir IP adresi veya MAC adresi belirtilebilir. Belirtilen varsayılan ağ geçidi kullanıldığında, seçilen yapılandırmaya otomatik geçiş gerçekleşir. **IP adresi** Vurgulanan yapılandırma için geçiş kuralı olarak bir ağ bağdaştırıcının IP adresi ve ağ maskesi belirtilebilir. Belirtilen IP adresi kullanıldığında, seçilen yapılandırmaya otomatik geçiş gerçekleşir.

Not
Sekize kadar yapılandırma kaydedebilirsiniz.

Not
Ağ geçidi değiştirilirken geçerli bir kural bulunmazsa, bulunan son yapılandırma etkin kalır.

Düğmeler

Düğme	Açıklama
Varsayılan değerler	Yapılandırmanın tüm ayarları, varsayılan değerlere geri yüklenir. Varsayılan ayarlar geri yüklendiğinde tüm değişiklikler ve özel girdiler kaybedilir.
Tamam	Yapılan tüm ayarlar kaydedilir. Yapılandırma kapandı. Kullanıcı Hesabı Kontrolü (UAC), Windows Vista'dan itibaren işletim sistemlerinde değişiklik uygulamak için izninizi isteyecektir.
İptal	Yapılandırma, yapılandırmadaki ayarlarınız kaydedilmeden kapatılır.
Uygula	Yapılan tüm ayarlar kaydedilir. Kullanıcı Hesabı Kontrolü (UAC), Windows Vista'dan itibaren işletim sistemlerinde değişiklik uygulamak için izninizi isteyecektir.

8.2 Sistem Tarayıcı

Yapılandırmanın **Sistem Tarayıcı** bölümü, istek üzerine tarama yapılandırmasından sorumludur.

8.2.1 Tara

İstek üzerine taramaya ilişkin tarama yordamının davranışını tanımlayabilirsiniz. İstek üzerine tarama ile taranacak belirli dizinleri seçerseniz, yapılandırmaya bağlı olarak Sistem Tarayıcı taramaları:

- belirli bir tarama önceliği ile gerçekleşir,
- ayrıca önyükleme sektörlerini ve ana belleği de tarar,
- dizindeki tüm veya seçilen dosyaları tarar.

Dosyalar

Sistem Tarayıcı yalnızca belirli bir uzantıya (tür) sahip dosyaları taramak için bir filtre kullanabilir.

Tüm dosyalar

Bu seçenek etkinleştirilirse, içerik ve dosya uzantısına bakılmaksızın tüm dosyalar, virüslere veya istenmeyen programlara karşı taranır. Filtre kullanılmaz.

Not
Tüm dosyalar seçeneği etkinleştirilirse, **Dosya uzantıları** düğmesi seçilemez.

Akıllı uzantılar kullan

Bu seçenek etkinleştirilirse, virüslere veya istenmeyen programlara karşı taranan dosyaların seçimi, program tarafından yapılır. Başka bir deyişle, Avira programınız, dosyaların içeriklerine göre taranıp taranmayacağına karar verir. Taramada yalnızca dosya uzantısı temel alınmadığından bu yordam, Dosya uzantısı listesini kullan yordamından daha yavaş, ancak daha güvenlidir. Bu seçenek, varsayılan ayar olarak etkinleştirilir ve önerilir.

Not
Akıllı uzantılar kullan seçeneği etkinleştirilirse, **Dosya uzantıları** düğmesi seçilemez.

Dosya uzantısı listesini kullan

Bu seçenek etkinleştirilirse, yalnızca belirtilen bir uzantıya sahip dosyalar taranır. Virüs ve istenmeyen programlar içerebilecek tüm dosya türleri önceden ayarlanır. Bu liste, "**Dosya uzantısı**" düğmesi aracılığıyla el ile düzenlenebilir.

Not
Bu seçenek etkinleştirilirse ve dosya uzantılarını içeren listeden tüm girdileri sildiyseniz, bu, **Dosya uzantıları** düğmesinin altında "*Dosya uzantısı yok*" metniyle belirtilir.

Dosya uzantıları

Bu düğmenin yardımıyla, **"Dosya uzantısı listesini kullan"** modunda taranan tüm dosya uzantılarının görüntülendiği bir iletişim kutusu açılır. Uzantılar için varsayılan girdiler ayarlanır, ancak girdiler eklenebilir veya silinebilir.

Not
Lütfen varsayılan listenin sürümden sürüme değişiklik gösterebileceğini unutmayın.

Ek ayarlar

Seçilen sürücülerin önyükleme sektörlerini tara

Bu seçenek etkinleştirilirse, Sistem Tarayıcı, istek üzerine sistem taraması için seçilen sürücülerin önyükleme sektörlerini tarar. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

Ana önyükleme sektörlerini tara

Bu seçenek etkinleştirilirse, Sistem Tarayıcı, sistemde kullanılan sabit disklerin ana önyükleme sektörlerini tarar.

Çevrimdışı dosyaları yoksay

Bu seçenek etkinleştirilirse, doğrudan tarama, çevrimdışı dosyaları bir tarama sırasında tamamen yoksayar. Başka bir deyişle, bu dosyalar, virüs ve istenmeyen programlara karşı taranmaz. Çevrimdışı dosyalar, Hiyerarşik Depolama Yönetimi Sistemi (HSMS) tarafından sabit diskten örneğin, bir banda fiziksel olarak taşınmış dosyalardır. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

Sistem dosyalarının bütünlük denetimi yapılıyor

Bu seçenek etkinleştirildiğinde, en önemli Windows sistem dosyaları her istek üzerine tarama sırasında zararlı yazılımlar tarafından yapılan değişiklikler için özellikle güvenli bir denetimden geçer. Değiştirilmiş bir dosya algılanırsa, bu şüpheli olarak bildirilir. Bu işlev, çok miktarda bilgisayar kapasitesi kullanır. Bu nedenle bu seçenek, varsayılan ayar olarak devre dışı bırakılır.

Not
Bu seçenek yalnızca Windows Vista ve üzeri sürümlerle kullanılabilir. Avira programını AMC altında yönetiyorsanız bu seçenek **kullanılamaz**.

Not
Sistem dosyalarını değiştiren ve önyükleme veya başlatma ekranını kendi gereksinimlerinize uyarlayan üçüncü taraf araçlar kullanıyorsanız, bu seçenek kullanılmamalıdır. Bu araçlara örnek olarak, dış görünüm paketleri, TuneUp yardımcı programları veya Vista Özelleştirmesi verilebilir.

En iyi duruma getirilmiş tarama

Bu seçenek etkinleştirildiğinde, Sistem Tarayıcı taraması sırasında işlemci kapasitesi en iyi şekilde kullanılır. Performans nedenleriyle, en iyi duruma getirilmiş bir tarama yalnızca standart düzeyde günlüğe kaydedilir.

Not
Bu seçenek yalnızca çok işlemcili sistemlerde kullanılabilir. Avira programınız AMC üzerinden yönetiliyorsa, bu seçenek her zaman görüntülenir ve etkinleştirilebilir: Yönetilen sistemde birden fazla işlemci yoksa, Sistem Tarayıcı seçeneği kullanılmaz.

Sembolik bağlantıları izle

Bu seçenek etkinleştirilirse, Sistem Tarayıcı, tarama profilindeki veya seçilen dizindeki tüm sembolik bağlantıları izleyen bir tarama gerçekleştirir ve bağlantılı dosyaları virüslere ve zararlı yazılımlara karşı tarar.

Not
Bu seçenek herhangi bir kısayol içermez, ancak dosya sisteminde saydam olan sembolik bağlantılara (mklink.exe tarafından oluşturulur) veya Birleşim Noktalarına (junction.exe tarafından oluşturulur) özel olarak başvurur.

Taramadan önce Kök kullanıcı takımı ara

Bu seçenek etkinleştirilirse ve bir tarama başlatılırsa, Sistem Tarayıcı, Windows sistem dizinini bir kısayoldaki etkin kök kullanıcı takımlarına karşı tarar. Bu işlem, bilgisayarınızı etkin kök kullanıcı takımlarına karşı tarama profili "**Kök kullanıcı takımlarına karşı tara**" kadar kapsamlı şekilde taramaz ancak çok daha hızlı gerçekleşir. Bu seçenek yalnızca sizin tarafınızdan oluşturulan profillerin ayarlarını değiştirir.

Not
Kök kullanıcı takımı taraması, Windows XP 64 bit

Kayıt Defterini Tara

Bu seçenek etkinleştirilirse, Kayıt Defteri, zararlı yazılım başvurularına karşı taranır. Bu seçenek yalnızca sizin tarafınızdan oluşturulan profillerin ayarlarını değiştirir.

Ağ sürücülerinde dosya ve yolları yoksay

Bu seçenek etkinleştirilirse, bilgisayara bağlı ağ sürücüleri, istek üzerine taramanın dışında bırakılır. Sunucular veya diğer iş istasyonları anti virüs yazılımıyla korunuyorsa bu seçenek önerilir. Bu seçenek, varsayılan ayar olarak devre dışı bırakılır.

İşlemi tara

Tarayıcının durdurulmasına izin ver

Bu seçenek etkinleştirilirse, virüslere veya istenmeyen programlara karşı tarama, "Luke Filewalker" penceresinde "**Durdur**" düğmesi yardımıyla istendiği zaman sonlandırılabilir. Bu ayarı devre dışı bıraktıysanız, "Luke Filewalker" penceresindeki **Durdur** düğmesi gri bir arka plana sahiptir. Tarama işleminin zamanından önce sonlandırılması mümkün değildir! Bu seçenek, varsayılan ayar olarak etkinleştirilir.

Scanner önceliği

İstek üzerine tarama ile Sistem Tarayıcı, öncelik düzeylerini ayırt eder. Bu yalnızca iş istasyonunda birçok işlem aynı anda çalışıyorsa geçerli olur. Seçim, tarama hızını etkiler.

düşük

Başka bir işlem için hesaplama süresi gerekmiyorsa, işletim sistemi tarafından yalnızca Sistem Tarayıcı'ya işlemci süresi ayrılır; başka bir deyişle, yalnızca Sistem Tarayıcı çalıştığı sürece hız maksimumdur. Sonuç olarak, diğer programlar ile birlikte

çalışması optimum düzeydedir: Sistem Tarayıcı arka planda çalışmaya devam ederken başka programlar için hesaplama süresi gerekiyorsa, bilgisayar daha hızlı şekilde yanıt verir.

orta

Sistem Tarayıcı, normal öncelikle yürütülür. İşletim sistemi tarafından tüm işlemlere aynı miktarda işlemci süresi ayrılır. Bu seçenek, varsayılan ayar olarak etkinleştirilir ve önerilir. Belirli koşullar altında başka uygulamalarla çalışma etkilenebilir.

yüksek

Sistem Tarayıcı en yüksek önceliğe sahiptir. Diğer uygulamalarla eşzamanlı çalışma neredeyse olanaksızdır. Ancak Sistem Tarayıcı, taramasını maksimum hızda tamamlar.

Algılama durumunda eylem

Bir virüs veya istenmeyen program algılandığında Sistem Tarayıcı tarafından gerçekleştirilecek eylemleri tanımlayabilirsiniz.

Etkileşimli

Bu seçenek etkinleştirilirse, Sistem Tarayıcı taramasının sonuçları bir iletişim kutusunda görüntülenir. Sistem Tarayıcı ile tarama yürütürken, taramanın sonunda etkilenen dosyaların listesi ile birlikte bir uyarı alırsınız. Çeşitli etkilenen dosyalar için yürütülecek bir eylem seçmek için bağlama duyarlı menüyü kullanabilirsiniz. Tüm etkilenen dosyalar için standart eylemleri yürütebilir veya Sistem Tarayıcı'yı iptal edebilirsiniz.

Not
Sistem Tarayıcı iletişim kutusunda, **Karantina** eylemi varsayılan eylem olarak görüntülenir.

İzin verilen eylemler

Bu kutuda, bir virüs algılaması durumunda bireysel veya uzman bildirim modunda seçilebilen eylemler belirtilebilir. Bunun için karşılık gelen seçenekleri etkinleştirmeniz gerekir.

Onar

Sistem Tarayıcı, olanaklıysa, etkilenen dosyayı onarır.

Yeniden Adlandır

Sistem Tarayıcı, dosyayı yeniden adlandırır. Bu nedenle, bu dosyalara doğrudan (örneğin çift tıklatmayla) erişim artık mümkün değildir. Dosya daha sonra tekrar onarılabilir ve yeniden adlandırılabilir.

Karantina

Sistem Tarayıcı, dosyayı Karantinaya taşır. Dosya, bilgilendirici bir değere sahipse karantina yöneticisinden kurtarılabilir veya gerekirse, Avira Zararlı Yazılım Araştırma Merkezi'ne gönderilir. Dosyaya bağlı olarak, karantina yöneticisinde daha fazla seçenek kullanılabilir.

Sil

Dosya silinecektir. Bu işlem, "üzerine yaz ve sil" işleminden daha hızlıdır.

Yoksay

Dosya yoksayılacaktır.

Üzerine yaz ve sil

Sistem Tarayıcı varsayılan bir desenle dosyanın üzerine yazar ve sonra dosyayı siler. Geri yüklenemez.

Varsayılan

Bu düğme, karşılaşılan dosyaları işlemek üzere Sistem Tarayıcı tarafından gerçekleştirilecek varsayılan bir eylemi tanımlamak için kullanılır. Bir eylemi vurgulayın ve "**Varsayılan"** düğmesini tıklatın. Birleşik bildirim modunda ilgili dosyalar için yalnızca seçilen varsayılan eylem yürütülebilir. İlgili dosyalar için seçilen varsayılan eylem, bireysel ve uzman bildirim modunda önceden seçilir.

Not
Onar eylemi, varsayılan eylem olarak seçilemez.

Not
Varsayılan eylem olarak **Sil** veya **Üzerine yaz ve sil** eylemini seçtiyseniz ve bildirim modunu birleşik olarak ayarladıysanız, lütfen şu hususlara dikkate edin: Buluşsal yöntem isabetlerinde, etkilenen dosyalar silinmez, bunun yerine karantinaya taşınır.

Otomatik

Bu seçenek etkinleştirilirse, bir virüs algılaması oluşması durumunda iletişim kutusu görüntülenmez. Sistem Tarayıcı, bu bölümde birincil ve ikincil eylem olarak önceden tanımladığınız ayarlara göre hareket eder.

Eylemden önce dosyayı karantinaya kopyala

Bu seçenek etkinleştirilirse, Sistem Tarayıcı istenen birincil veya ikincil eylemi gerçekleştirmeden önce bir yedek kopya oluşturur. Yedek kopya Karantina'ya kaydedilir ve burada dosya, bilgilendirici değere sahipse geri yüklenebilir. Daha fazla inceleme için yedek kopyayı, Avira Zararlı Yazılım Araştırma Merkezi'ne de gönderebilirsiniz.

Algılama uyarılarını görüntüle

Bu seçenek etkinleştirilirse, her virüs veya istenmeyen program algılandığında bir uyarı görüntülenerek yürütülmekte olan eylemleri gösterir.

Birincil eylem

Birincil eylem, Sistem Tarayıcı bir virüs veya istenmeyen program bulduğunda gerçekleştirilen eylemdir. "**Onar"** seçeneği belirlenirse ancak etkilenen dosya onarılamazsa, "**İkincil eylem"** konumunda seçilen eylem gerçekleştirilir.

Not
İkincil eylem seçeneği yalnızca **Onar** seçeneği **Birincil eylem** konumunda seçilmişse belirlenebilir.

Onar

Bu seçenek etkinleştirilirse, Sistem Tarayıcı, etkilenen dosyaları otomatik olarak onarır. Sistem Tarayıcı etkilenen bir dosyayı onaramazsa, İkincil eylem konumunda seçilen eylemi gerçekleştirir.

Not
Otomatik onarım önerilir, ancak Sistem Tarayıcı'nın iş istasyonundaki dosyaları değiştireceği anlamına gelir.

Yeniden Adlandır

Bu seçenek etkinleştirilirse, Sistem Tarayıcı, dosyayı yeniden adlandırır. Bu nedenle, bu dosyalara doğrudan (örneğin çift tıklatmayla) erişim artık mümkün değildir. Dosyalar daha sonra tekrar onarılabilir ve özgün adlarıyla adlandırılabilir.

Karantina

Bu seçenek etkinleştirilirse, Sistem Tarayıcı, dosyayı karantinaya taşır. Bu dosyalar daha sonra onarılabilir veya gerekirse Avira Zararlı Yazılım Araştırma Merkezi'ne gönderilebilir.

Sil

Bu seçenek etkinleştirilirse, dosya silinir. Bu işlem, "üzerine yaz ve sil" işleminden daha hızlıdır.

Yoksay

Bu seçenek etkinleştirilirse, dosyaya erişime izin verilir ve dosya olduğu gibi bırakılır.

Uyarı
Etkilenen dosya, iş istasyonunuzda etkin kalır! Bu, iş istasyonunuzda ciddi hasara neden olabilir!

Üzerine yaz ve sil

Bu seçenek etkinleştirilirse, Sistem Tarayıcı varsayılan bir desenle dosyanın üzerine yazar ve sonra dosyayı siler. Geri yüklenemez.

İkincil eylem

"**İkincil eylem"** seçeneği yalnızca **Onar** seçeneği "**Birincil eylem"** konumunda seçilmişse belirlenebilir. Bu seçenek sayesinde, şimdi etkilenen dosya onarılamıyorsa, etkilenen dosyaya ne yapılacağına karar verilebilir.

Yeniden Adlandır

Bu seçenek etkinleştirilirse, Sistem Tarayıcı, dosyayı yeniden adlandırır. Bu nedenle, bu dosyalara doğrudan (örneğin çift tıklatmayla) erişim artık mümkün değildir. Dosyalar daha sonra tekrar onarılabilir ve özgün adlarıyla adlandırılabilir.

Karantina

Bu seçenek etkinleştirilirse, Sistem Tarayıcı, dosyayı Karantinaya taşır. Bu dosyalar daha sonra onarılabilir veya gerekirse Avira Zararlı Yazılım Araştırma Merkezi'ne gönderilebilir.

Sil

Bu seçenek etkinleştirilirse, dosya silinir. Bu işlem, "üzerine yaz ve sil" işleminden daha hızlıdır.

Yoksay

Bu seçenek etkinleştirilirse, dosyaya erişime izin verilir ve dosya olduğu gibi bırakılır.

Uyarı
Etkilenen dosya, iş istasyonunuzda etkin kalır! Bu, iş istasyonunuzda ciddi hasara neden olabilir!

Üzerine yaz ve sil

Bu seçenek etkinleştirilirse, Sistem Tarayıcı varsayılan bir desenle dosyanın üzerine yazar ve sonra dosyayı siler (temizler). Geri yüklenemez.

Not
Birincil veya ikincil eylem olarak **Sil** veya **Üzerine yaz ve sil** eylemini seçtiyseniz ve bildirim modunu birleşik olarak ayarladıysanız, lütfen şu hususlara dikkate edin: Buluşsal yöntem isabetlerinde, etkilenen dosyalar silinmez, bunun yerine karantinaya taşınır.

Daha fazla eylem

Algılamanın ardından programı başlat

En az bir virüs veya istenmeyen program (örneğin, bir e-posta programı) algılandıysa, istek üzerine taramanın ardından Sistem Tarayıcı istediğiniz bir dosyayı (örneğin, bir program) açabilir; böylece diğer kullanıcıları veya yöneticiyi bilgilendirebilirsiniz.

> **Not**
> Güvenlik nedenleriyle yalnızca bir kullanıcı bilgisayarda oturum açtığında algılamadan sonra bir programı başlatabilirsiniz. Daha sonra dosya, oturum açan kullanıcı için geçerli olan haklarla açılır. Bir kullanıcı oturum açmazsa, bu seçenek gerçekleştirilmez.

Program adı

Bu giriş kutusuna, Sistem Tarayıcı'nın bir algılamadan sonra başlatacağı programın adını ve ilgili yolunu girebilirsiniz.

Bu düğme, dosya seçimi iletişim kutusunun yardımıyla istediğiniz programı seçebileceğiniz bir pencereyi açar.

Bağımsız değişkenler

Bu giriş kutusuna, gerekirse başlatılacak program için komut satırı parametrelerini girebilirsiniz.

Olay günlüğü

Olay günlüğü kullan

Bu seçenek etkinleştirilirse, Sistem Tarayıcı taraması tamamlandıktan sonra, tarayıcı sonuçlarını içeren bir olay raporu Windows Olay Günlüğü'ne aktarılır. Olaylar, Windows olay görüntüleyicisinde çağrılabilir. Bu seçenek, varsayılan ayar olarak devre dışı bırakılır.

Arşivler

Arşivler taranırken, Sistem Tarayıcı yinelemeli tarama yöntemini kullanır: Arşivlerdeki arşivler ayrıca paketten çıkarılır ve virüsler ve istenmeyen programlara karşı taranır. Dosyalar taranır, açılır ve yeniden taranır.

Arşivleri tara

Bu seçenek etkinleştirilirse, arşiv listesindeki seçilen arşivler taranır. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

Tüm arşiv türleri

Bu seçenek etkinleştirilirse, arşiv listesindeki tüm arşiv türleri seçilir ve taranır.

Akıllı Uzantılar

Bu seçenek etkinleştirilirse, Sistem Tarayıcı, dosya uzantısı normal uzantılardan farklılık gösterse de, bir dosyanın paketlenmiş dosya biçiminde (arşiv) olup olmadığını algılar ve arşivi tarar. Ancak bunun için her dosya açılmalıdır ve bu da tarama hızını düşürür. Örnek: Bir *.zip arşivi, *.xyz dosya uzantısına sahipse, Sistem Tarayıcı bu arşivi de paketten çıkarır ve tarar. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

Not
Yalnızca arşiv listesinde işaretlenmiş olan arşiv türleri desteklenir.

Yineleme derinliğini sınırla

Paketten çıkarma ve yinelenen arşivleri tarama, çok miktarda bilgisayar süresi ve kaynağı gerektirir. Bu seçenek etkinleştirilirse, çok paketli arşivlerdeki tarama derinliğini belirli sayıda paketleme düzeyine (maksimum yineleme derinliği) sınırlarsınız. Bu da zaman ve bilgisayar kaynağından tasarruf edilmesini sağlar.

Not
Bir arşivde virüs veya istenmeyen program bulmak için, Sistem Tarayıcı, virüs ya da istenmeyen programın bulunduğu yineleme düzeyine kadar tarama yapmalıdır.

Maksimum yineleme derinliği

Maksimum yineleme derinliğini girmek için, Yineleme derinliğini sınırla seçeneği etkinleştirilmelidir.
İstenen yineleme derinliğini doğrudan veya girdi alanındaki sağ ok tuşu yardımıyla girebilirsiniz. İzin verilen değerler, 1 - 99 aralığındadır. Standard değer 20 olup bu değer önerilir.

Varsayılan değerler

Düğme, arşivlerin taranması için önceden tanımlı değerleri geri yükler.

Arşivler

Bu görüntüleme alanında, Sistem Tarayıcı'nın tarayacağı arşivleri ayarlayabilirsiniz. Bunun için ilgili girdileri seçmeniz gerekir.

İstisnalar

Sistem Tarayıcı için atılacak dosya nesneleri

Bu penceredeki liste, virüs veya istenmeyen programlara karşı yapılan taramaya Sistem Tarayıcı tarafından dahil edilmeyecek dosyaları ve yolları içerir.

Lütfen buraya olabildiğince az sayıda istisna ve nedeni ne olursa olsun, yalnızca normal bir taramaya dahil edilmeyecek dosyaları girin. Dosyaları bu listeye dahil etmeden önce her zaman bu dosyaları virüslere veya istenmeyen programlara karşı taramanızı öneririz!

Not
Listedeki girdiler, toplamda 6000 karakterden fazla olmamalıdır.

Uyarı
Bu dosyalar taramaya dahil edilmez!

Not
Bu listeye dahil edilen dosyalar, Rapor dosyasına kaydedilir. Lütfen ara sıra rapor dosyasında taranmamış dosyalar olup olmadığını kontrol edin; belki de bir dosyayı dışarıda bırakma nedeniniz artık yoktur. Bu durumda, bu dosyanın adını yeniden bu listeden kaldırmanız gerekir.

Giriş kutusu

Bu giriş kutusuna, istek üzerine taramaya dahil edilmeyen dosya nesnesinin adını girebilirsiniz. Varsayılan ayar olarak bir dosya nesnesi girilmez.

...

Düğme, gerekli dosyayı veya gerekli yolu seçebileceğiniz bir pencereyi açar.
Tam yoluyla birlikte bir dosya adını girdiğinizde yalnızca bu dosya etkilenmeye karşı taranır. Yol içermeyen bir dosya adı girdiyseniz, bu ada sahip olan tüm dosyalar (yola veya sürücüye bakılmaksızın) taranmaz.

Ekle

Bu düğme ile giriş kutusuna girilen dosya nesnesini görüntüleme penceresine ekleyebilirsiniz.

Sil

Bu düğme, seçilen girdiyi listeden siler. Bir girdi seçilmediyse, bu düğme devre dışıdır.

Not
Avira programını AMC'de yönetiyorsanız, dosya istisnaları için yol ayrıntılarında değişkenler kullanabilirsiniz. Kullanabileceğiniz değişkenler listesini şurada bulabilirsiniz: Değişkenler: Gerçek Zamanlı Koruma ve Sistem Tarayıcı İstisnaları.

Buluşsal yöntem

Bu yapılandırma bölümü, tarama motorunun buluşsal yöntemine ilişkin ayarları içerir.

Avira ürünleri, bilinmeyen zararlı yazılımları proaktif olarak; başka bir deyişle hasarlı öğeyle savaşmak için özel bir virüs imzası oluşturulmadan ve bir virüs koruyucu güncellemesi gönderilmeden önce açığa çıkarabilen çok güçlü bir buluşsal yöntem içerir. Virüs algılama, etkilenen kodların, zararlı yazılımların tipik işlevlerine karşı yoğun bir analizini ve araştırmasını içerir. Taranmakta olan kod bu belirgin nitelikleri sergilerse, şüpheli olarak bildirilir. Bu mutlaka kodun zararlı yazılım olduğu anlamına gelmez. Bazen yanlış pozitifler oluşur. Etkilenen kodun nasıl işleneceğiyle ilgili karar, kod kaynağının güvenilir olup olmadığına ilişkin bilgisine göre kullanıcı tarafından alınır.

Makro virüs buluşsal yöntemi

Makro virüs buluşsal yöntemi

Avira ürününüz son derece güçlü bir makro virüs buluşsal yöntemini içerir. Bu seçenek etkinleştirilirse, bir onarım durumunda ilgili belgedeki tüm makrolar silinir, alternatif olarak şüpheli belgeler yalnızca bildirilir; başka bir deyişle bir uyarı alırsınız. Bu seçenek, varsayılan ayar olarak etkinleştirilir ve önerilir.

Gelişmiş Buluşsal Yöntem Analizi ve Algılaması (AHeAD)

AHeAD etkinleştir

Avira programınız, bilinmeyen (yeni) zararlı yazılımları da algılayabilen, Avira AHeAD teknolojisi şeklinde çok güçlü bir buluşsal yöntem içerir. Bu seçenek etkinleştirilirse, buluşsal yöntemin ne kadar "şiddetli" olacağını tanımlayabilirsiniz. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

Düşük algılama düzeyi

Bu seçenek etkinleştirilirse, daha az bilinen zararlı yazılımlar algılanır; bu durumda yanlış uyarı riski düşüktür.

Orta algılama düzeyi

Bu seçenek güçlü algılama düzeyi ile düşük yanlış uyarı riskinin birleşimidir. Bu buluşsal yöntemin kullanımını seçtiyseniz, orta düzey varsayılan ayar olur.

Yüksek algılama düzeyi

Bu seçenek etkinleştirilirse, çok daha az bilinen zararlı yazılımlar algılanır; ancak yanlış pozitif riski de yüksektir.

8.2.2 Rapor

Sistem Tarayıcı, kapsamlı bir raporlama işlevine sahiptir. Bu nedenle, istek üzerine tarama sonuçları hakkında kesin bilgiler edinirsiniz. Rapor dosyası, tüm sistem girdilerinin yanı sıra, istek üzerine taramanın uyarılarını ve iletilerini de içerir.

Not
Virüs veya istenmeyen programlar algılandığında Sistem Tarayıcı'nın hangi eylemleri gerçekleştirdiğini belirlemenize olanak sağlamak için rapor dosyasını yapılandırmasında etkinleştirmelisiniz.

Raporlama

Kapalı

Bu seçenek etkinleştirilirse, Sistem Tarayıcı, istek üzerine taramanın eylemlerini ve sonuçlarını bildirmez.

Varsayılan

Bu seçenek etkinleştirildiğinde, Sistem Tarayıcı, ilgili dosyaların yolunu ve adlarını günlüğe kaydeder. Ayrıca, geçerli taramanın yapılandırması, sürüm bilgileri ve lisans sahibiyle ilgili bilgiler, rapor dosyasına yazılır.

Genişletilmiş

Bu seçenek etkinleştirildiğinde, Sistem Tarayıcı, varsayılan bilgilere ek olarak uyarıları ve ipuçlarını günlüğe kaydeder. Rapor ayrıca Koruma Bulutu tarafından gerçekleştirilen algılamaları belirtmek amacıyla '(bulut)' sonekini içerir.

Tam

Bu seçenek etkinleştirildiğinde, Sistem Tarayıcı, tüm taranmış dosyaları da günlüğe kaydeder. Ayrıca, uyarılar ve ipuçları da dahil olmak üzere, tüm dosyalar rapor dosyasına dahil edilir.

Not
Bize bir rapor dosyası göndermeniz gerekirse (sorun giderme için), lütfen bu rapor dosyasını bu modda oluşturun.

8.3 Gerçek Zamanlı Koruma

Yapılandırmanın **Gerçek Zamanlı Koruma** bölümü, erişim taramasının yapılandırmasından sorumludur.

8.3.1 Tara

Normalde sisteminizi sürekli olarak izlemek istersiniz. Bu amaçla, Gerçek Zamanlı Koruma'yı (= erişim Sistem Tarayıcı) kullanın. Böylece, bilgisayarda kopyalanan veya açılan tüm dosyaları "anında" virüslere ve istenmeyen programlara karşı tarayabilirsiniz.

Dosyalar

Gerçek Zamanlı Koruma yalnızca belirli bir uzantıya (tür) sahip dosyaları taramak için bir filtre kullanabilir.

Tüm dosyalar

Bu seçenek etkinleştirilirse, içerik ve dosya uzantısına bakılmaksızın tüm dosyalar, virüslere veya istenmeyen programlara karşı taranır.

> **Not**
> **Tüm dosyalar** seçeneği etkinleştirilirse, **Dosya uzantıları** düğmesi seçilemez.

Akıllı uzantılar kullan

Bu seçenek etkinleştirilirse, virüslere veya istenmeyen programlara karşı taranan dosyaların seçimi, program tarafından yapılır. Başka bir deyişle, program, dosyaların içeriklerine göre taranıp taranmayacağına karar verir. Taramada yalnızca dosya uzantısı temel alınmadığından bu yordam, **Dosya uzantısı listesini kullan** yordamından daha yavaş, ancak daha güvenlidir.

> **Not**
> **Akıllı uzantıları kullan** seçeneği etkinleştirilirse, **Dosya uzantıları** düğmesi seçilemez.

Dosya uzantısı listesini kullan

Bu seçenek etkinleştirilirse, yalnızca belirtilen bir uzantıya sahip dosyalar taranır. Virüs ve istenmeyen programlar içerebilecek tüm dosya türleri önceden ayarlanır. Bu liste, "**Dosya uzantıları**" düğmesi aracılığıyla el ile düzenlenebilir. Bu seçenek, varsayılan ayar olarak etkinleştirilir ve önerilir.

> **Not**
> Bu seçenek etkinleştirilirse ve dosya uzantılarını içeren listeden tüm girdileri sildiyseniz, bu, **Dosya uzantıları** düğmesinin altındaki "Dosya uzantısı yok" metniyle belirtilir.

Dosya uzantıları

Bu düğmenin yardımıyla, **"Dosya uzantısı listesini kullan"** modunda taranan tüm dosya uzantılarının görüntülendiği bir iletişim kutusu açılır. Uzantılar için varsayılan girdiler ayarlanır, ancak girdiler eklenebilir veya silinebilir.

> **Not**
> Lütfen dosya uzantısı listesinin sürümden sürüme değişiklik gösterebileceğini unutmayın.

Sürücüler

Ağ sürücülerini izle

Bu seçenek etkinleştirilirse, sunucu birimleri, eş sürücüler, vb. gibi ağ sürücülerindeki (eşlenmiş sürücüler) dosyalar taranır.

Not
Bilgisayarınızın performansını çok düşürmemek için, yalnızca özel durumlarda **Ağ sürücülerini izle** seçeneği etkinleştirilmelidir.

Uyarı
Bu seçenek devre dışı bırakılırsa, ağ sürücüleri **izlenmez**. Artık virüslere veya istenmeyen programlara karşı korunmazlar!

Not
Ağ sürücülerinde dosyalar yürütüldüğünde, bunlar **Ağ sürücülerini izle** seçeneğinin ayarından bağımsız olarak Gerçek Zamanlı Koruma tarafından taranır. Bazı durumlarda, **Ağ sürücülerini izle** seçeneği devre dışı bırakılsa da, ağ sürücülerindeki dosyalar açılırken taranır. Nedeni: Bu dosyalara 'Dosya Yürüt' haklarıyla erişilir. Bu dosyaları veya ağ sürücülerinde yürütülen dosyaları, Gerçek Zamanlı Koruma taraması dışında bırakmak istiyorsanız, dosyaları dışarıda bırakılacak dosya nesneleri listesine girin (bkz: Gerçek Zamanlı Koruma > Tara > İstisnalar).

Önbelleğe almayı etkinleştir

Bu seçenek etkinleştirilirse, ağ sürücülerinde izlenen dosyalar, Gerçek Zamanlı Koruma'nın önbelleğinde kullanılabilir olacaktır. Önbelleğe alma işlevi olmadan ağ sürücülerinin izlenmesi daha güvenlidir; ancak bu, önbelleğe alma işleviyle ağ sürücülerinin izlenmesi kadar iyi performans göstermez.

Arşivler

Arşivleri tara

Bu seçenek etkinleştirilirse, arşivler taranır. Sıkıştırılmış dosyalar taranır, sonra açılır ve yeniden taranır. Bu seçenek, varsayılan olarak devre dışı bırakılır. Arşiv taraması; yineleme derinliği, taranacak dosya sayısı ve arşiv boyutu ile kısıtlanır. Maksimum yineleme derinliğini, taranacak dosya sayısını ve maksimum arşiv boyutunu ayarlayabilirsiniz.

Not
Söz konusu işlem yüksek bilgisayar performansı gerektirdiğinden, bu seçenek

varsayılan olarak devre dışı bırakılır. Genellikle arşivlerin istek üzerine tarama kullanılarak denetlenmesi önerilir.

Maks. yineleme derinliği

Arşivler taranırken, Gerçek Zamanlı Koruma yinelemeli tarama yöntemini kullanır: Arşivlerdeki arşivler ayrıca paketten çıkarılır ve virüsler ve istenmeyen programlara karşı taranır. Yineleme derinliğini tanımlayabilirsiniz. Yineleme derinliği için varsayılan değer 1'dir ve bu değerin kullanılması önerilir: doğrudan ana arşive yerleştirilen tüm dosyalar taranır.

Maks. dosya sayısı

Arşivler taranırken, taramayı arşivdeki maksimum dosya sayısıyla kısıtlayabilirsiniz. Taranacak maksimum dosya numarası için varsayılan değer 10 olup bu değer önerilir.

Maks. boyut (KB)

Arşivler taranırken, taramayı paketten çıkarılacak maksimum arşiv boyutuyla kısıtlayabilirsiniz. Standart değer olan 1000 KB önerilir.

Algılama durumunda eylem

Bir virüs veya istenmeyen program algılandığında Gerçek Zamanlı Koruma tarafından gerçekleştirilecek eylemleri tanımlayabilirsiniz.

Etkileşimli

Bu seçenek etkinleştirilirse, Gerçek Zamanlı Koruma bir virüs veya istenmeyen program algıladığında bir masaüstü bildirimi görüntülenir. "**Ayrıntılar**" düğmesi aracılığıyla, algılanan zararlı yazılımı kaldırma veya diğer olası virüs işleme eylemlerine erişme seçeneğiniz vardır. Eylemler bir iletişim kutusunda görüntülenir. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

İzin verilen eylemler

Bu görüntüleme kutusunda, iletişim kutusunda daha fazla eylem olarak kullanılabilir olacak virüs yönetimi eylemlerini belirtebilirsiniz. Bunun için karşılık gelen seçenekleri etkinleştirmeniz gerekir.

Onar

Gerçek Zamanlı Koruma, olanaklıysa, etkilenen dosyayı onarır.

Yeniden Adlandır

Gerçek Zamanlı Koruma dosyayı yeniden adlandırır. Bu nedenle, bu dosyalara doğrudan (örneğin çift tıklatmayla) erişim artık mümkün değildir. Dosya daha sonra tekrar onarılabilir ve yeniden adlandırılabilir.

Karantina

Gerçek Zamanlı Koruma, dosyayı Karantinaya taşır. Dosya, bilgilendirici bir değere sahipse karantina yöneticisinden kurtarılabilir veya gerekirse, Avira Zararlı Yazılım

Araştırma Merkezi'ne gönderilir. Dosyaya bağlı olarak, Karantina yöneticisinde daha fazla seçenek kullanılabilir.

Sil

Dosya silinecektir. Bu işlem, **Üzerine yaz ve sil** işleminden daha hızlıdır (aşağıya bakınız).

Yoksay

Dosyaya erişime izin verilir ve dosya yoksayılır.

Üzerine yaz ve sil

Gerçek Zamanlı Koruma, dosyayı silmeden önce varsayılan bir desenle dosyanın üzerine yazar. Geri yüklenemez.

Uyarı
Gerçek Zamanlı Koruma **Yazarken tara** olarak ayarlıysa etkilenen dosya yazılmaz.

Varsayılan

Bu düğme, bir virüs algılandığında varsayılan olarak iletişim kutusunda etkinleştirilecek bir eylem seçmenize olanak sağlar. Varsayılan olarak etkinleştirilecek eylemi seçin ve "**Varsayılan**" düğmesini tıklatın.

Not
Onar eylemi, varsayılan eylem olarak seçilemez.

Daha fazla bilgi için burayı tıklatın.

Otomatik

Bu seçenek etkinleştirilirse, bir virüs algılaması oluşması durumunda iletişim kutusu görüntülenmez. Gerçek Zamanlı Koruma, bu bölümde birincil ve ikincil eylem olarak önceden tanımladığınız ayarlara göre hareket eder.

Eylemden önce dosyayı karantinaya kopyala

Bu seçenek etkinleştirilirse, Gerçek Zamanlı Koruma istenen birincil veya ikincil eylemi gerçekleştirmeden önce bir yedek kopya oluşturur. Yedek kopya, karantinaya kaydedilir. Bilgilendirici değere sahipse, Karantina yöneticisi aracılığıyla geri yüklenebilir. Yedek kopyayı, Avira Zararlı Yazılım Araştırma Merkezi'ne de gönderebilirsiniz. Nesneye bağlı olarak, Karantina yöneticisinde daha fazla seçenek kullanılabilir durumdadır.

Algılama uyarılarını görüntüle

Bu seçenek etkinleştirilirse, her virüs veya istenmeyen program algılandığında bir uyarı görüntülenir.

Birincil eylem

Birincil eylem, Gerçek Zamanlı Koruma bir virüs veya istenmeyen program bulduğunda gerçekleştirilen eylemdir. "**Onar**" seçeneği belirlenirse ancak etkilenen dosya onarılamazsa, "**İkincil eylem**" konumunda seçilen eylem gerçekleştirilir.

Not
İkincil eylem seçeneği yalnızca **Onar** seçeneği **Birincil eylem** konumunda seçilmişse belirlenebilir.

Onar

Bu seçenek etkinleştirilirse, Gerçek Zamanlı Koruma, etkilenen dosyaları otomatik olarak onarır. Gerçek Zamanlı Koruma etkilenen bir dosyayı onaramazsa, **İkincil eylem** konumunda seçilen eylemi gerçekleştirir.

Not
Otomatik onarım önerilir, ancak Gerçek Zamanlı Koruma'nın iş istasyonundaki dosyaları değiştireceği anlamına gelir.

Yeniden Adlandır

Bu seçenek etkinleştirilirse, Gerçek Zamanlı Koruma, dosyayı yeniden adlandırır. Bu nedenle, bu dosyalara doğrudan (örneğin çift tıklatmayla) erişim artık mümkün değildir. Dosyalar daha sonra tekrar onarılabilir ve özgün adlarıyla adlandırılabilir.

Karantina

Bu seçenek etkinleştirilirse, Gerçek Zamanlı Koruma, dosyayı Karantinaya taşır. Bu dizindeki dosyalar daha sonra onarılabilir veya gerekirse, Avira Zararlı Yazılım Araştırma Merkezi'ne gönderilebilir.

Sil

Bu seçenek etkinleştirilirse, dosya silinir. Bu işlem, **Üzerine yaz ve sil** işleminden daha hızlıdır.

Yoksay

Bu seçenek etkinleştirilirse, dosyaya erişime izin verilir ve dosya olduğu gibi bırakılır.

Uyarı
Etkilenen dosya, iş istasyonunuzda etkin kalır! Bu, iş istasyonunuzda ciddi hasara neden olabilir!

Üzerine yaz ve sil

Bu seçenek etkinleştirilirse, Gerçek Zamanlı Koruma varsayılan bir desenle dosyanın üzerine yazar ve sonra dosyayı siler. Geri yüklenemez.

Erişimi reddet

Bu seçenek etkinleştirilirse, Gerçek Zamanlı Koruma yalnızca rapor işlevi etkinleştirilmişse algılamayı rapor dosyasına girer. Ayrıca bu seçenek etkinleştirilirse, Gerçek Zamanlı Koruma, Olay günlüğüne de bir girdi yazar.

Uyarı
Gerçek Zamanlı Koruma **Yazarken tara** olarak ayarlıysa etkilenen dosya yazılmaz.

İkincil eylem

İkincil eylem seçeneği yalnızca **Onar** seçeneği **Birincil eylem** konumunda seçilmişse belirlenebilir. Bu seçenek sayesinde, şimdi etkilenen dosya onarılamıyorsa, etkilenen dosyaya ne yapılacağına karar verilebilir.

Yeniden Adlandır

Bu seçenek etkinleştirilirse, Gerçek Zamanlı Koruma, dosyayı yeniden adlandırır. Bu nedenle, bu dosyalara doğrudan (örneğin çift tıklatmayla) erişim artık mümkün değildir. Dosyalar daha sonra tekrar onarılabilir ve özgün adlarıyla adlandırılabilir.

Karantina

Bu seçenek etkinleştirilirse, Gerçek Zamanlı Koruma, dosyayı Karantinaya taşır. Dosyalar daha sonra onarılabilir veya gerekirse Avira Zararlı Yazılım Araştırma Merkezi'ne gönderilebilir.

Sil

Bu seçenek etkinleştirilirse, dosya silinir. Bu işlem, **Üzerine yaz ve sil** işleminden daha hızlıdır.

Yoksay

Bu seçenek etkinleştirilirse, dosyaya erişime izin verilir ve dosya olduğu gibi bırakılır.

Uyarı
Etkilenen dosya, iş istasyonunuzda etkin kalır! Bu, iş istasyonunuzda ciddi hasara neden olabilir!

Üzerine yaz ve sil

Bu seçenek etkinleştirilirse, Gerçek Zamanlı Koruma varsayılan bir desenle dosyanın üzerine yazar ve sonra dosyayı siler. Geri yüklenemez.

Erişimi reddet

Bu seçenek etkinleştirilirse, etkilenen dosya yazılmadıysa; Gerçek Zamanlı Koruma yalnızca rapor işlevi etkinleştirilmişse algılamayı rapor dosyasına girer. Ayrıca bu seçenek etkinleştirilirse, Gerçek Zamanlı Koruma, Olay günlüğüne de bir girdi yazar.

Not
Birincil veya ikincil eylem olarak **Sil** veya **Üzerine yaz ve sil** eylemini seçtiyseniz lütfen şuna dikkate edin: Buluşsal yöntem isabetlerinde, etkilenen dosyalar silinmez, bunun yerine karantinaya taşınır.

Daha fazla eylem

Olay günlüğü kullan

Bu seçenek etkinleştirilirse, her algılama için Windows olay günlüğüne bir girdi eklenir. Olaylar, Windows olay görüntüleyicisinde çağrılabilir. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

İstisnalar

Bu seçeneklerle, Gerçek Zamanlı Koruma (erişim taraması) için istisna nesneleri yapılandırabilirsiniz. İlgili nesneler, erişim taramasına dahil edilmez. Gerçek Zamanlı Koruma, atılacak işlemler listesi aracılığıyla erişim taraması sırasında bu nesnelere dosya erişimlerini yoksayabilir. Bu, örneğin, veritabanları veya yedekleme çözümleri için kullanışlıdır.

Lütfen atılacak işlemleri ve dosya nesnelerini belirtirken aşağıdakileri not edin: Liste, yukarıdan aşağıya doğru işlenir. Liste ne kadar uzun olursa, her bir erişime yönelik listenin işlenmesi için o kadar çok işlemci süresi gerekir. Bu nedenle, listeyi olabildiğince kısa tutun.

Gerçek Zamanlı Koruma tarafından atılacak işlemler

Bu listedeki işlemlerin tüm dosya erişimleri, Gerçek Zamanlı Koruma izlemesinin dışında bırakılır.

Giriş kutusu

Bu alana, gerçek zamanlı tarama tarafından yoksayılacak işlemin adını girin. Varsayılan ayar olarak bir işlem girilmez.

İşlemin belirtilen yolu ve dosya adı maksimum 255 karakterden oluşabilir. 128 adede kadar işlem girebilirsiniz. Listedeki girdiler, toplamda 6000 karakterden fazla olmamalıdır.

İşlem girilirken, Unicode sembolleri kabul edilir. Bu nedenle, özel semboller içeren işlem veya dizin adları girebilirsiniz.

Sürücü bilgileri şu şekilde girilmelidir: [Sürücü harfi]:\

İki nokta sembolü (:) yalnızca sürücüleri belirtmek için kullanılır.

İşlemi belirtirken, joker karakterleri * (herhangi sayıda karakter) ve ? (tek bir karakter) içerebilir.

```
C:\Program Files\Application\application.exe
C:\Program Files\Application\applicatio?.exe
C:\Program Files\Application\applic*.exe
C:\Program Files\Application\*.exe
```

İşlemin genel olarak Gerçek Zamanlı Koruma izlemesi dışında bırakılmasını önlemek için, özel olarak şu karakterleri kapsayan belirtimler geçersizdir: * (yıldız), ? (soru işareti), / (eğik çizgi), \ (ters eğik çizgi), . (nokta), : (iki nokta).

Tam yol ayrıntıları olmadan işlemleri Gerçek Zamanlı Koruma izlemesi dışında bırakma seçeneğiniz vardır. Örnek: `application.exe`

Ancak bu yalnızca yürütülebilir dosyaların sabit disk sürücülerinde bulunduğu işlemler için geçerlidir.

Yürütülebilir dosyaların ağ sürücüleri gibi bağlı sürücülerde bulunduğu işlemler için tam yol ayrıntıları gerekir. Lütfen Bağlı ağ sürücüleriyle ilgili istisnalar gösterimiyle ilgili genel bilgileri dikkate alın.

Yürütülebilir dosyaların dinamik sürücülerde bulunduğu işlemler için herhangi bir istisna belirtmeyin. Dinamik sürücüler; CD'ler, DVD'ler veya USB çubuklar gibi çıkarılabilir diskler için kullanılır.

Uyarı
Lütfen listeye kaydedilen işlemler tarafından tüm dosya erişimlerinin, virüs ve istenmeyen programlara karşı tarama dışında bırakıldığını unutmayın!

Düğme, yürütülebilir bir dosya seçebileceğiniz bir pencereyi açar.

İşlemler

"**İşlemler**" düğmesi, çalışmakta olan işlemlerin görüntülendiği "**İşlem seçimi**" penceresini açar.

Ekle

Bu düğme ile giriş kutusuna girilen işlemi görüntüleme penceresine ekleyebilirsiniz.

Sil

Bu düğme ile, seçilen bir işlemi görüntüleme penceresinden silebilirsiniz.

Gerçek Zamanlı Koruma tarafından atılacak dosya nesneleri

Bu listedeki nesnelere tüm dosya erişimleri, Gerçek Zamanlı Koruma izlemesinin dışında bırakılır.

Giriş kutusu

Bu kutuya, erişim taramasına dahil edilmeyen dosya nesnesinin adını girebilirsiniz. Varsayılan ayar olarak bir dosya nesnesi girilmez.

Listedeki girdiler toplamda 6000'den fazla karakter içermemelidir.

Atılacak dosya nesnelerini belirtirken, joker karakterleri* (herhangi sayıda karakter) ve ? (bir tek karakter) kullanabilirsiniz: Bireysel dosya uzantıları da hariç tutulabilir (joker karakterler dahil).

```
C:\Directory\*.mdb
*.mdb
*.md?
*.xls*
C:\Directory\*.log
```

Dizin adları ters eğik çizgi \ ile bitmelidir.

Bir dizin dışarıda bıkılırsa, tüm alt dizinleri de otomatik olarak dışarıda bırakılır.

Her bir sürücü için, tam yolu girerek (sürücü harfiyle başlayıp) maksimum 20 istisna belirtebilirsiniz. Örnek:

```
C:\Program Files\Application\Name.log
```

Tam yol içermeyen maksimum istisna sayısı 64'tür. Örnek:

```
*.log
\computer1\C\directory1
```

Başka bir sürücüye dizin olarak takılan dinamik sürücüler olması durumunda, istisna listesindeki tümleşik sürücü için işletim sisteminin diğer adı kullanılmalıdır:

```
\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\
```

Takma noktasını kullanıyorsanız, örneğin, `C:\DynDrive`, dinamik sürücü gene de taranır. Gerçek Zamanlı Koruma rapor dosyasından kullanılacak işletim sisteminin diğer adını belirleyebilirsiniz.

Düğme, dışarıda bırakılacak dosya nesnesini seçebileceğiniz bir pencereyi açar.

Ekle

Bu düğme ile giriş kutusuna girilen dosya nesnesini görüntüleme penceresine ekleyebilirsiniz.

Sil

Bu düğme ile, seçilen bir dosya nesnesini görüntüleme penceresinden silebilirsiniz.

Lütfen istisnaları belirtirken daha fazla bilgiyi dikkate alın:

Kısa DOS dosya adları (DOS adı kuralı 8.3) ile erişildiğinde nesneleri de dışarıda bırakmak için, ilgili kısa dosya adı da listeye girilmelidir.

Joker karakterler içeren bir dosya adı, ters eğik çizgiyle sonlandırılamaz. Örnek:
`C:\Program Files\Application\applic*.exe\`
Bu girdi geçerli değildir ve bir istisna olarak işlem görmez!

Lütfen **bağlı ağ sürücüleri ile ilgili istisnalar** konusunda aşağıdakilere dikkat edin: Bağlı ağ sürücüsünün sürücü harfini kullanırsanız, belirtilen dosyalar ve klasörler Gerçek Zamanlı Koruma taraması DIŞINDA BIRAKILMAZ. İstisna listesindeki UNC yolu, ağ sürücüsüne bağlanmak için kullanılan UNC yolundan farklıysa (istisnalar listesindeki IP adresi belirtimi - ağ sürücüsüne bağlantı için bilgisayar adı belirtimi), belirtilen klasörler ve dosyalar, Gerçek Zamanlı Koruma taraması DIŞINDA BIRAKILMAZ. Gerçek Zamanlı Koruma rapor dosyasında ilgili UNC yolunu bulun:
`\\<Bilgisayar adı>\<Etkinleştir>\` - VEYA - `\\<IP adresi>\<Etkinleştir>\`

Gerçek Zamanlı Koruma rapor dosyasında Gerçek Zamanlı Koruma'nın etkilenen dosyalara karşı tarama yapmak için kullandığı yolu bulabilirsiniz. İstisna listesinde tamamen aynı yolu belirtin. Aşağıdaki adımları uygulayın: Gerçek Zamanlı Koruma > Rapor altındaki yapılandırmada Gerçek Zamanlı Koruma'nın protokol işlevini **Tam** olarak ayarlayın. Şimdi etkinleştirilmiş Gerçek Zamanlı Koruma ile dosyalara, klasörlere, takılı sürücülere veya bağlı ağ sürücülerine erişin. Şimdi Gerçek Zamanlı Koruma rapor dosyasından kullanılacak yolu okuyabilirsiniz. Rapor dosyasına, Yerel koruma > Gerçek Zamanlı Koruma altında Kontrol Merkezi'nden erişilebilir.

Avira ürününü AMC'de yönetiyorsanız, işlem ve dosya istisnaları için yol ayrıntılarında değişkenler kullanabilirsiniz. Kullanabileceğiniz değişkenler listesini şurada bulabilirsiniz: Değişkenler: Gerçek Zamanlı Koruma ve Scanner İstisnaları.

Dışarıda bırakılacak işlemler için örnekler:

- `application.exe`
  application.exe işlemi, hangi sabit disk sürücüsünde ve hangi dizinde bulunduğuna bakılmaksızın, Gerçek Zamanlı Koruma taraması dışında bırakılır.
- `C:\Program Files1\Application.exe`
  C:\Program Files1 yolunda bulunan *application.exe* dosyasının işlemi, Gerçek Zamanlı Koruma taraması dışında bırakılır.
- `C:\Program Files1\*.exe`
  C:\Program Files1 yolunda bulunan yürütülebilir dosyaların tüm işlemleri, Gerçek Zamanlı Koruma taraması dışında bırakılır.

Dışarıda bırakılacak dosyalar için örnekler:

- `*.mdb`
  '*mdb*' uzantısına sahip tüm dosyalar, Gerçek Zamanlı Koruma taraması dışında bırakılır.
- `*.xls*`
  '*xls*' ile başlayan bir dosya uzantısına sahip tüm dosyalar, Gerçek Zamanlı Koruma taraması dışında bırakılır; örn. *.xls* ve *.xlsx* uzantılarına sahip dosyalar.
- `C:\Directory\*.log`
  C:\Directory yolunda bulunan, *log*' uzantısına sahip tüm günlük dosyaları, Gerçek Zamanlı Koruma taraması dışında bırakılır.
- `\\Computer name\Shared1\`
  '*Computer name1**Shared1*' bağlantısıyla erişilen tüm dosyalar, Gerçek Zamanlı Koruma taraması dışında bırakılır. Bu genellikle, bilgisayar adı '*Computer name1*' ve paylaşılan adı '*Shared1*' aracılığıyla paylaşılan.klasör içeren başka bir bilgisayara erişen bağlı bir ağ sürücüsüdür.
- `\\1.0.0.0\Shared1\*.mdb`
  '*mdb*' uzantısına sahip tüm dosyalar,*1.0.0.0**Shared1*' bağlantısıyla erişilen Gerçek Zamanlı Koruma taraması dışında bırakılır. Bu genellikle, '1.0.0.0' IP adresi ve '*Shared1*' paylaşılan adı aracılığıyla paylaşılan bir klasör içeren başka bir bilgisayara erişen bağlı bir ağ sürücüsüdür.

Buluşsal yöntem

Bu yapılandırma bölümü, tarama motorunun buluşsal yöntemine ilişkin ayarları içerir.

Avira ürünleri, bilinmeyen zararlı yazılımları proaktif olarak; başka bir deyişle hasarlı öğeyle savaşmak için özel bir virüs imzası oluşturulmadan ve bir virüs koruyucu güncellemesi gönderilmeden önce açığa çıkarabilen çok güçlü bir buluşsal yöntem içerir. Virüs algılama, etkilenen kodların, zararlı yazılımların tipik işlevlerine karşı yoğun bir analizini ve araştırmasını içerir. Taranmakta olan kod bu belirgin nitelikleri sergilerse, şüpheli olarak bildirilir. Bu mutlaka kodun zararlı yazılım olduğu anlamına gelmez. Bazen yanlış pozitifler oluşur. Etkilenen kodun nasıl işleneceğiyle ilgili karar, kod kaynağının güvenilir olup olmadığına ilişkin bilgisine göre kullanıcı tarafından alınır.

Makro virüs buluşsal yöntemi

Makro virüs buluşsal yöntemi

Avira ürününüz son derece güçlü bir makro virüs buluşsal yöntemini içerir. Bu seçenek etkinleştirilirse, bir onarım durumunda ilgili belgedeki tüm makrolar silinir, alternatif olarak şüpheli belgeler yalnızca bildirilir; başka bir deyişle bir uyarı alırsınız. Bu seçenek, varsayılan ayar olarak etkinleştirilir ve önerilir.

Gelişmiş Buluşsal Yöntem Analizi ve Algılaması (AHeAD)

AHeAD etkinleştir

Avira programınız, bilinmeyen (yeni) zararlı yazılımları da algılayabilen, Avira AHeAD teknolojisi şeklinde çok güçlü bir buluşsal yöntem içerir. Bu seçenek etkinleştirilirse, buluşsal yöntemin ne kadar "şiddetli" olacağını tanımlayabilirsiniz. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

Düşük algılama düzeyi

Bu seçenek etkinleştirilirse, daha az bilinen zararlı yazılımlar algılanır; bu durumda yanlış uyarı riski düşüktür.

Orta algılama düzeyi

Bu seçenek güçlü algılama düzeyi ile düşük yanlış uyarı riskinin birleşimidir. Bu buluşsal yöntemin kullanımını seçtiyseniz, orta düzey varsayılan ayar olur.

Yüksek algılama düzeyi

Bu seçenek etkinleştirilirse, çok daha az bilinen zararlı yazılımlar algılanır; ancak yanlış pozitif riski de yüksektir.

8.3.2 Rapor

Gerçek Zamanlı Koruma, kullanıcıya veya yöneticiye, bir algılamanın türü ve yöntemiyle ilgili tam notlar sağlamak için yoğun bir günlük kaydı işlevine sahiptir.

Raporlama

Bu grup, rapor dosyası içeriğinin belirlenmesine olanak sağlar.

Kapalı

Bu seçenek etkinleştirilirse, Gerçek Zamanlı Koruma bir günlük oluşturmaz.
Birden çok virüs veya istenmeyen program içeren deneme sürümlerini yürüttüğünüz zamanlarda olduğu gibi yalnızca özel durumlarda günlük kaydı işlevini kapatmanızı öneririz.

Varsayılan

Bu seçenek etkinleştirilirse, Gerçek Zamanlı Koruma, rapor dosyasında önemli bilgileri (algılamalar, uyarılar ve hatalarla ilgili) kaydederken, daha az önemli bilgiler, gelişmiş netlik için yoksayılır. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

Genişletilmiş

Bu seçenek etkinleştirilirse, Gerçek Zamanlı Koruma, rapor dosyasına daha az önemli bilgileri de dahil eder.

Tam

Bu seçenek etkinleştirilirse, Gerçek Zamanlı Koruma, dosya boyutu, dosya türü, tarih, vb. gibi tüm kullanılabilir bilgileri rapor dosyasına dahil eder.

Rapor dosyasını sınırla

Boyutu n MB ile sınırla

Bu seçenek etkinleştirilirse, rapor dosyası belirli bir boyutla sınırlandırılabilir. İzin verilen değerler, 1 ile 100 MB arasındadır. Sistem kaynakları kullanımını en aza indirgemek için rapor dosyasının boyutu sınırlanırken yaklaşık 50 kilobayt fazladan alana izin verilir. Günlük dosyasının boyutu, belirtilen boyutu 50 kilobayt'tan fazla aşarsa, belirtilen boyutun 50 kilobayt aşağısına ulaşılıncaya kadar eski girdiler silinir.

Kısaltmadan önce rapor dosyasını yedekle

Bu seçenek etkinleştirilirse, kısaltmadan önce rapor dosyası yedeklenir. Kaydetme konumu için bkz. Rapor dizini.

Rapor dosyasına yazma yapılandırması

Bu seçenek etkinleştirilirse, erişim taraması yapılandırması, rapor dosyasına kaydedilir.

Not
Herhangi bir rapor dosyası kısıtlaması belirtmediyseniz, rapor dosyası 100 MB'ye ulaştığında otomatik olarak yeni bir rapor dosyası oluşturulur. Eski rapor dosyasının bir yedeği oluşturulur. Eski rapor dosyasının üç adede kadar yedeği kaydedilir. En eski yedeklemeler en önce silinir.

8.4 Değişkenler: Gerçek Zamanlı Koruma ve Sistem Tarayıcı istisnaları

Avira ürününüz AMC ile yönetiliyorsa, Gerçek Zamanlı Koruma ve Sistem Tarayıcı istisnalarını yapılandırmak için değişkenler kullanabilirsiniz. Yönetilen sistemde yapılandırmayı kaydederken, değişkenler otomatik olarak işletim sistemi ve diline karşılık gelen gerçek değerlerle değiştirilir.

Aşağıdaki değişkenler kullanılabilir:

8.4.1 Windows XP 32 Bit (**İngilizce) için değişkenler

Değişken	Windows XP 32 Bit (**İngilizce)
`%WINDIR%`	*C:\Windows*
`%SYSDIR%`	*C:\Windows\System32*

%ALLUSERSPROFILE%	*C:\Documents and Settings\All Users* **
%PROGRAMFILES%	*C:\Program Files* **
%PROGRAMFILES(x86)%	*C:\Program Files (x86)* **
%SYSTEMROOT%	*C:\Windows*
%INSTALLDIR%	*C:\Program Files\Avira\Antivir Desktop* **
%AVAPPDATA%	*C:\Documents and Settings\All Users\Avira\AntiVir Desktop* **

**** ile işaretli yollar dile bağımlıdır. Yukarıda verilen örnekler İngilizce bir işletim sistemindeki ilgili yolları gösterir.

8.4.2 Windows 7 32-Bit/ 64-Bit (**İngilizce) için değişkenler

Değişken	Windows 7 32-Bit (**İngilizce)	Windows 7 64-Bit (**İngilizce)
%WINDIR%	*C:\Windows*	*C:\Windows*
%SYSDIR%	*C:\Windows\System32*	*C:\Windows\System32*
%ALLUSERSPROFILE%	*C:\ProgramData*	*C:\ProgramData*
%PROGRAMFILES%	*C:\Program Files* **	*C:\Program Files* **
%PROGRAMFILES(x86)%	*C:\Program Files (x86)* **	*C:\Program Files (x86)* **
%SYSTEMROOT%	*C:\Windows*	*C:\Windows*
%INSTALLDIR%	*C:\Program Files\Avira\Antivir Desktop* **	*C:\Program Files (x86)\Avira\Antivir Desktop* **
%AVAPPDATA%	*C:\ProgramData\Avira\AntiVir Desktop*	*C:\ProgramData\Avira\AntiVir Desktop*

** ile işaretli yollar dile bağımlıdır. Yukarıda verilen örnekler İngilizce bir işletim sistemindeki ilgili yolları gösterir.

8.5 Güncelle

Güncelle bölümünde, güncellemelerin otomatik alınmasını ve karşıdan yükleme sunucularıyla bağlantıyı yapılandırabilirsiniz. Çeşitli güncelleme aralıklarını belirtebilir ve otomatik güncellemeyi etkinleştirebilir veya devre dışı bırakabilirsiniz.

> **Not**
> Avira Güvenlik Konsolu'nda Avira ürününüzü yapılandırırsanız, otomatik güncellemeler kullanılamaz.

Otomatik güncelle

Etkinleştir

Bu seçenek etkinleştirilirse, etkinleştirilen olaylar için belirtilen aralıkta otomatik güncellemeler gerçekleştirilir.

Tüm n Gün / Saat / Dakika

Bu kutuda, otomatik güncellemenin gerçekleştirilme aralığını belirtebilirsiniz. Güncelleme aralığını değiştirmek için, kutudaki zaman seçeneklerinden birini vurgulayın ve giriş kutusunun sağındaki ok tuşlarını kullanarak değiştirin.

Ayrica Internet baglantisi kuruldugunda is baslat

Bu seçenek etkinleştirilirse, belirtilen güncelleme aralığına ek olarak, her Internet bağlantısı kurulduğunda güncelleme işi gerçekleştirilir.

Süre önceden dolduysa işi yinele

Bu seçenek etkinleştirilirse, örneğin, bilgisayar kapatıldığı için belirtilen zamanda gerçekleştirilemeyen geçmiş güncelleme işleri gerçekleştirilir.

> Bir web sunucusu aracılığıyla güncelleme için daha fazla ayara şuradan erişebilirsiniz: .
> Bu seçenek etkinleştirilirse, Web sunucusunu ve gerekirse proxy sunucuyu yapılandırabilirsiniz.

dosya sunucusu / paylaşılan klasörler aracılığıyla

Güncelleme, Internet'teki özel bir karşıdan yükleme sunucusundan güncelleme dosyalarını alan, Intranet'te bir dosya sunucusu aracılığıyla gerçekleştirilir.

Not
Not Bir web sunucusu aracılığıyla güncelleme için daha fazla ayara şuradan erişebilirsiniz: Yapılandırma > PC Korumasi > Güncelle > Web sunucusu.
Bu seçenek etkinleştirilirse, kullandığınız dosya sunucusunu yapılandırabilirsiniz.

8.5.1 Dosya sunucusu

Bir ağda birden çok iş istasyonu olması durumunda, Intranet'te bir dosya sunucusundan güncellemeyi karşıdan yükleyebilir ve bunun sonucunda Avira ürününüz Internet'teki özel bir karşıdan yükleme sunucusundan güncelleme dosyalarını alır. Böylece, Avira ürününüzün tüm iş istasyonlarında güncel olması sağlanır.

Not
Yapılandırma başlığı yalnızca Yapılandırma > PC Koruma > Güncelle altında **Dosya Sunucusu / Paylaşılan klasörler aracılığıyla** seçeneği belirlendiyse etkinleştirilir.

Karşıdan yükle

Avira ürününüzün güncelleme dosyalarının ve '/release/update/' gerekli dizinlerinin bulunduğu dosya sunucusunun adını girin. Şu belirtilmelidir: *file:// <dosya sunucusunun IP adresi>/release/update/*. 'release' dizini, tüm kullanıcılar tarafından erişilebilen bir dizin olmalıdır.

...

Düğme, gerekli karşıdan yükleme dizinini seçebileceğiniz bir pencereyi açar.

Sunucu oturumu açma

Oturum açma adı

Sunucuda oturum açmak için bir kullanıcı adı girin. Sunucuda kullanılan paylaşılan klasörlere erişim hakları olan bir kullanıcı hesabı kullanın.

Oturum açma parolası

Kullanıcı hesabının parolasını girin. Girilen karakterler * ile maskelenir.

Not
Sunucu oturum açma bölümünde herhangi bir veri belirtmezseniz, dosya sunucusuna erişilirken kimlik doğrulaması gerçekleştirilmez. Bu durumda kullanıcının dosya sunucusuna ilişkin yeterli haklara sahip olması gerekir.

8.5.2 Web sunucusu

Web sunucusu

Güncelleme, doğrudan Internet'te veya Intranet'te bir web sunucusu aracılığıyla gerçekleştirilebilir.

Web sunucusu bağlantısı

Varolan bağlantıyı kullan (ağ)

Bağlantınız bir ağ aracılığıyla kullanılıyorsa bu ayar görüntülenir.

Aşağıdaki bağlantıyı kullan

Bağlantınızı bireysel olarak tanımlarsanız bu ayar görüntülenir.

Güncelleyici, hangi bağlantı seçeneklerinin kullanılabilir olduğunu otomatik olarak algılar. Kullanılabilir olmayan bağlantı seçenekleri grileşir ve etkinleştirilemez. Örneğin, Windows'da bir telefon rehberi girdisi aracılığıyla el ile bir çevirmeli bağlantı kurulabilir.

Kullanıcı

Seçilen hesabın kullanıcı adını girin.

Parola

Bu hesabın parolasını girin. Güvenlik nedenleriyle, bu alana yazdığınız gerçek karakterlerin yerini yıldız işaretleri (*) alır.

> **Not**
> Varolan bir Internet hesap adını veya parolasını unuttuysanız, Internet Hizmet Sağlayıcınız ile görüşün.

> **Not**
> Çevirmeli araçlar (örn. SmartSurfer, Oleco, vb.) aracılığıyla güncelleyicinin otomatik çevirme işlevi şu anda kullanılamaz.

Güncelleme için ayarlanmış bir çevirmeli bağlantıyı sonlandır

Bu seçenek etkinleştirilirse, karşıdan yükleme başarıyla gerçekleştirildiğinde hemen güncelleme için yapılan çevirmeli bağlantı otomatik olarak yeniden kesintiye uğrar.

> **Not**
> Bu seçenek yalnızca Windows XP'de kullanılabilir. Daha güncel işletim sistemlerinde güncelleme için açılan çevirmeli bağlantı her zaman karşıdan yükleme gerçekleştirildiği anda sonlandırılır.

Karşıdan yükle

Öncelikli sunucu

Bu alana, güncelleme sağlamak için ilk istenecek web sunucusunun güncelleme dizinini ve URL'sini girin. Bu sunucuya ulaşılamazsa, belirtilen standart sunucular kullanılır. Web sunucusu adresinin biçimi şu şekildedir: `http://<hostname veya IP>[:port]/update`. Bir bağlantı noktası belirtmezseniz, 80 numaralı bağlantı noktası kullanılır.

Varsayılan sunucu

Güncellemelerin yükleneceği web sunucularının güncelleme dizinini ve URL'sini girin. Birden çok girdi virgülle ayrılır. Web sunucusu adresinin biçimi şu şekildedir: `http://<hostname veya IP>[:port]/update`. Bir bağlantı noktası belirtmezseniz, 80 numaralı bağlantı noktası kullanılır. Varsayılan olarak, erişilebilir Avira web sunucuları güncelleme için belirtilir. Ancak, şirket Intranet'inde kendi web sunucularınızı kullanabilirsiniz. Bir web sunucusu sayısı belirtilirse, her birini virgülle ayırın.

Varsayılan

Düğme, önceden tanımlı adresleri geri yükler.

Proxy ayarları

Proxy sunucu

Proxy sunucu kullanma

Bu seçenek etkinleştirilirse, web sunucusuyla bağlantınız bir proxy sunucu aracılığıyla kurulmaz.

Proxy sistem ayarlarını kullan

Seçenek etkinleştirildiğinde, proxy sunucu aracılığıyla web sunucusuyla bağlantı için geçerli Windows sistem ayarları kullanılır. Proxy sunucu kullanmak için **Denetim masası > Internet seçenekleri > Bağlantılar > LAN ayarları** konumunda Windows sistem ayarlarını yapılandırın. Ayrıca Internet Explorer'da **Ekstralar** menüsünde Internet seçeneklerine erişebilirsiniz.

Uyarı
Kimlik doğrulama gerektiren bir proxy sunucu kullanıyorsanız, **Bu proxy sunucuyu kullan** seçeneğinin altına tüm gerekli verileri girin. **Proxy sistem ayarlarını kullan** seçeneği yalnızca kimlik doğrulama olmadan proxy sunucular için kullanılabilir.

Bu proxy sunucuyu kullan

Web sunucusu bağlantınız bir proxy sunucu aracılığıyla kurulursa, ilgili bilgileri buraya girebilirsiniz.

Adres

Web sunucusuna bağlanmak için kullanmak istediğiniz proxy sunucunun bilgisayar adını veya IP adresini girin.

Bağlantı noktası

Lütfen web sunucusuna bağlanmak için kullanmak istediğiniz proxy sunucunun bağlantı noktası numarasını girin.

Oturum açma adı

Proxy sunucuda oturum açmak için bir kullanıcı adı girin.

Oturum açma parolası

Proxy sunucuda oturum açmak için ilgili günlük kaydı parolasını buraya girin. Güvenlik nedenleriyle, bu alana yazdığınız gerçek karakterlerin yerini yıldız işaretleri (*) alır.

Örnekler:

Adres: `proxy.domain.com` Bağlantı noktası: `8080`

Adres: `192.168.1.100` Bağlantı noktası: `3128`

8.6 Güvenlik Duvari

8.6.1 Güvenlik Duvarını Yapılandırma

Avira Professional Security Avira Güvenlik Duvarını yapılandırmanıza veya Windows Güvenlik Duvarını (Windows 8'den itibaren) yönetmenize izin verir:

- Avira Güvenik Duvarı
- AMC altında Avira Güvenlik Duvarı
- Windows Güvenlik Duvarı

8.6.2 Avira Güvenlik Duvari

Yapılandırma > Internet Koruması altındaki **Güvenlik Duvarı** Avira Güvenlik Duvarının (Windows 7'ye kadar işletim sistemleri).

Bağdaştırıcı kuralları

Avira Güvenlik Duvarı'nda bir bağdaştırıcı, yazılım benzetimli donanım aygıtını (örn. mini bağlantı noktası, köprü bağlantısı, vb.) veya gerçek bir donanım aygıtını (örn. ağ kartı) temsil eder.

Avira Güvenlik Duvarı, bir sürücünün kurulu olduğu bilgisayarınızdaki tüm varolan bağdaştırıcıların bağdaştırıcı kurallarını görüntüler.

- ICMP protokolü
- TCP Bağlantı Noktası Taraması

- UDP Bağlantı Noktası Taraması
- Gelen Kurallar
- Giden Kurallar
- Kuralları yönetme düğmeleri

Önceden tanımlı bir bağdaştırıcı kuralı, güvenlik düzeyine bağlıdır. Kontrol Merkezinde **İnternet koruması > Güvenlik Duvarı** seçeneklerinin altında *Güvenlik düzeyini* değiştirebilir veya kendi bağdaştırıcı kurallarınızı tanımlayabilirsiniz. Kendi bağdaştırıcı kurallarınızı tanımladıysanız, Kontrol Merkezi'nin Güvenlik Duvarı bölümündeki *Güvenlik düzeyi* **Özel** olarak ayarlanır.

> **Not**
> Avira Güvenlik Duvarı'nın tüm önceden tanımlı kuralları için varsayılan *Güvenlik düzeyi* ayarı, **Orta'dır.**

ICMP protokolü

Internet Kontrol İletisi Protokolü (ICMP), ağlar üzerinde hata ve bilgi iletilerinin alışverişini yapmak için kullanılır. Bu protokol ayrıca ping veya izleyici ile durum iletileri için de kullanılır.
Bu kuralla, gelen ve giden engellenmiş ileti türlerini, baskın durumundaki davranışı ve parçalanmış ICMP paketlerine yanıtı tanımlayabilirsiniz. Bu kural, her pakete yanıt verilirken, saldırılan makinenin CPU yükünde artışla sonuçlanan, ICMP baskın saldırılarının önlenmesi görevini görür.

ICMP protokolü için önceden tanımlı kurallar

Ayar	Kurallar
Düşük	Gelen engellenen türler:**tür yok**. Giden engellenen türler: **tür yok**. Paketler arasındaki gecikme **50** ms'den azsa baskın olduğunu varsayın. Parçalanmış ICMP paketlerini **Reddet**.
Orta	Düşük düzey kuralıyla aynı kural.

Yüksek	Gelen engellenen türler: **çeşitli türler** Giden engellenen türler: **çeşitli türler** Paketler arasındaki gecikme **50** ms'den azsa baskın olduğunu varsayın. Parçalanmış ICMP paketlerini **Reddet**.

Gelen engellenen türler: tür yok/çeşitli türler

Bağlantı fareyle tıklatıldığında, ICMP paket türlerinin bir listesi görüntülenir. Bu listeden, engellemek istediğiniz gelen ICMP ileti türlerini belirtebilirsiniz.

Giden engellenen türler: tür yok/çeşitli türler

Bağlantı fareyle tıklatıldığında, ICMP paket türlerinin bir listesi görüntülenir. Bu listeden, engellemek istediğiniz giden ICMP ileti türlerini seçebilirsiniz.

Baskın Olduğunu Varsay

Bağlantı fareyle tıklatıldığında, izin verilen maksimum ICMP gecikmesini girebileceğiniz bir iletişim kutusu görüntülenir. Örnek: `50` milisaniye.

Parçalanmış ICMP paketleri

Bağlantı fareyle tıklatıldığında, parçalanmış ICMP paketlerini **Reddet** veya **Reddetme** seçeneğiniz vardır.

TCP bağlantı noktası taraması

Bu kural ile, ne zaman Güvenlik Duvarı tarafından bir TCP bağlantı noktası taramasının varsayılacağını ve bu durumda ne yapılması gerektiğini tanımlayabilirsiniz. Bu kural, bilgisayarınızdaki açık TCP bağlantı noktalarının algılanmasıyla sonuçlanan TCP bağlantı noktası tarama saldırılarının önlenmesi görevini görür. Bu saldırı türü, bir bilgisayardaki zayıf noktaları aramak için kullanılır ve bunu genellikle tehlikeli saldırı türleri takip eder.

TCP bağlantı noktası taraması için önceden tanımlı kurallar

Ayar	Kurallar
Düşük	**5.000** milisaniyede **50** veya daha fazla bağlantı noktası tarandıysa bir TCP bağlantı noktası taraması olduğunu varsayın. Algılandığında, saldırganın IP'sini **günlüğe kaydedin** ve saldırıyı engelleme kuralı **eklemeyin**.
Orta	**5.000** milisaniyede **50** veya daha fazla bağlantı noktası tarandıysa bir TCP bağlantı noktası taraması olduğunu varsayın. Algılandığında, saldırganın IP'sini **günlüğe kaydedin** ve saldırıyı engelleme kuralı **ekleyin**.
Yüksek	Orta düzey kuralıyla aynı kural.

Bağlantı noktaları

Bağlantı fareyle tıklatıldığında, TCP bağlantı noktası taramasının varsayılması için taranmış olması gereken bağlantı noktası sayısını girebileceğiniz bir iletişim kutusu görüntülenir.

Bağlantı noktası tarama süresi penceresi

Bu bağlantı fareyle tıklatıldığında, TCP bağlantı noktası taramasının varsayılması için belirli sayıda bağlantı noktası taramasına ilişkin zaman aralığını girebileceğiniz bir iletişim kutusu görüntülenir.

Olay veritabanı

Bağlantı fareyle tıklatıldığında, saldırganın IP adresini **günlüğe kaydet** veya **kaydetme** seçeneğiniz vardır.

Kural

Bağlantı fareyle tıklatıldığında, TCP bağlantı noktası tarama saldırısını engelleme kuralı **ekle** veya **ekleme** seçeneğiniz vardır.

UDP Bağlantı Noktası Taraması

Bu kural ile, ne zaman Güvenlik Duvarı tarafından bir UDP bağlantı noktası taramasının varsayılacağını ve bu durumda ne yapılması gerektiğini tanımlayabilirsiniz. Bu kural, bilgisayarınızdaki açık UDP bağlantı noktalarının algılanmasıyla sonuçlanan UDP bağlantı noktası tarama saldırılarını önler. Bu saldırı türü, bir bilgisayardaki zayıf noktaları aramak için kullanılır ve bunu genellikle tehlikeli saldırı türleri takip eder.

UDP Bağlantı Noktası Taraması için önceden tanımlı kurallar

Ayar	Kurallar
Düşük	**50** milisaniyede **5.000** veya daha fazla bağlantı noktası tarandıysa bir UDP bağlantı noktası taraması olduğunu varsayın. Algılandığında, saldırganın IP'sini **günlüğe kaydedin** ve saldırıyı engelleme kuralı **eklemeyin**.
Orta	**50** milisaniyede **5.000** veya daha fazla bağlantı noktası tarandıysa bir UDP bağlantı noktası taraması olduğunu varsayın. Algılandığında, saldırganın IP'sini **günlüğe kaydedin** ve saldırıyı engelleme kuralı **ekleyin**.
Yüksek	Orta düzey kuralıyla aynı kural.

Bağlantı noktaları

Bağlantı fareyle tıklatıldığında, UDP bağlantı noktası taramasının varsayılması için taranmış olması gereken bağlantı noktası sayısını girebileceğiniz bir iletişim kutusu görüntülenir.

Bağlantı noktası tarama süresi penceresi

Bu bağlantı fareyle tıklatıldığında, UDP bağlantı noktası taramasının varsayılması için belirli sayıda bağlantı noktası taramasına ilişkin zaman aralığını girebileceğiniz bir iletişim kutusu görüntülenir.

Olay veritabanı

Bağlantı fareyle tıklatıldığında, saldırganın IP adresini **günlüğe kaydet** veya **kaydetme** seçeneğiniz vardır.

Kural

Bağlantı fareyle tıklatıldığında, UDP bağlantı noktası tarama saldırısını engelleme kuralı **ekle** veya **ekleme** seçeneğiniz vardır.

Gelen Kurallar

Gelen kurallar, Avira Güvenlik Duvarı tarafından gelen veri trafiğini denetlemek için tanımlanır.

Uyarı
Bir paket filtrelendiğinde, karşılık gelen kurallar ard arda uygulanır; bu nedenle

kural sırası çok önemlidir. Yalnızca ne yaptığınızın tamamen farkındaysanız kural sırasını değiştirin.

TCP trafik verisi izleyicisi için Önceden tanımlı kurallar

Ayar	Kurallar
Düşük	Avira Güvenlik Duvarı tarafından herhangi bir gelen veri trafiği engellenmez.
Orta	**135 üzerinden kurulan TCP bağlantılarına izin ver** Yerel bağlantı noktası **{135}** ve uzak bağlantı noktası **{0-65535}** içinde olursa, **0.0.0.0** maskesi ile **0.0.0.0** adresinden gelen TCP paketlerine izin ver. **Varolan bağlantıların paketleri** için uygula. Paket kuralla eşleştiğinde **günlüğe kaydetme**. Gelişmiş: **<0>** göreli konumunda **<boş>** maske ile şu **<boş>** baytları içeren paketleri at. **135 üzerindeki TCP paketlerini reddet** Yerel bağlantı noktası **{135}** ve uzak bağlantı noktası **{0-65535}** içinde olursa, **0.0.0.0** maskesi ile **0.0.0.0** adresinden TCP paketlerini **Reddet**. **Tüm paketler** için uygula. Paket kuralla eşleştiğinde **günlüğe kaydetme**. Gelişmiş: **<0>** göreli konumunda **<boş>** maske ile şu **<boş>** baytları içeren paketleri at. **TCP sağlıklı veri trafiğini denetle** Yerel bağlantı noktası **{0-65535}** içinde ve uzak bağlantı noktası **{0-65535}** içinde olursa, **0.0.0.0** maskesi ile **0.0.0.0** adresinden TCP paketlerine **izin ver**. **Bağlantı başlatma ve var olan bağlantı paketleri** için uygula. Paket kuralla eşleştiğinde **günlüğe kaydetme.** **Gelişmiş: 0 göreli konumunda <boş> maske ile şu <boş> baytları içeren paketleri seç.** **TCP trafiğini at** **Yerel bağlantı noktası {0-65535} içinde ve uzak bağlantı noktası {0-65535} içinde olursa, 0.0.0.0 maskesi ile 0.0.0.0 adresinden TCP paketlerini reddet.** **Tüm paketler için uygula.** **Paket kuralla eşleştiğinde günlüğe kaydetme.** **Gelişmiş: 0 göreli konumunda <boş> maske ile şu <boş> baytları içeren paketleri seç.**

Yüksek	**Kurulmuş TCP veri trafiğini denetle** **Yerel bağlantı noktası {0-65535} içinde ve uzak bağlantı noktası {0-65535} içinde olursa, 0.0.0.0 maskesi ile 0.0.0.0 adresinden TCP paketlerine izin ver.** **Varolan bağlantıların paketleri için uygula.** **Paket kuralla eşleştiğinde günlüğe kaydetme.** **Gelişmiş: 0 göreli konumunda <boş> maske ile şu <boş> baytları içeren paketleri seç.**

Tüm TCP paketlerini onayla/reddet

Bağlantı fareyle tıklatıldığında, özel tanımlanmış gelen TCP paketlerine izin verme veya bunları reddetme seçeneğiniz vardır.

IP adresi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 adresini girebileceğiniz bir iletişim kutusu açılır.

IP maskesi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 maskesini girebileceğiniz bir iletişim kutusu açılır.

Yerel bağlantı noktaları

Bu bağlantı fareyle tıklatıldığında, yerel bağlantı noktası numaralarını veya eksiksiz bağlantı noktası aralıklarını tanımlayabileceğiniz bir iletişim kutusu görüntülenir.

Uzak bağlantı noktaları

Bu bağlantı fareyle tıklatıldığında, uzak bağlantı noktası numaralarını veya eksiksiz bağlantı noktası aralıklarını tanımlayabileceğiniz bir iletişim kutusu görüntülenir.

Uygulama yöntemi

Bu bağlantı fareyle tıklatıldığında, "**bağlantı başlatma ve var olan bağlantı paketleri**" için veya yalnızca "**varolan bağlantıların paketleri**" ya da "**tüm paketler**" için kuralı uygulama seçeneğiniz vardır.

Olay veritabanı

Bağlantıyı fareyle tıklatarak, paket kurala uyuyorsa bir olayı veritabanına "**yazma**" veya "**yazmama**" kararı verebilirsiniz.

Gelişmiş

Gelişmiş özellik, içerik filtrelemesini etkinleştirir. Örneğin, paketler belirli bir göreli konumda belirli veriler içeriyorsa, reddedilebilir. Bu seçeneği kullanmak istemiyorsanız, bir dosya seçmeyin veya boş bir dosya seçin.

Filtrelenen içerik: baytlar

Bağlantı fareyle tıklatıldığında, belirli arabelleği içeren bir dosya seçebileceğiniz bir iletişim kutusu görüntülenir.

Filtrelenen içerik: maske

Bağlantı fareyle tıklatıldığında, belirli maskeyi seçebileceğiniz bir iletişim kutusu görüntülenir.

Filtrelenen içerik: göreli konum

Bağlantı fareyle tıklatıldığında, filtrelenen içerik göreli konumunu tanımlayabileceğiniz bir iletişim kutusu görüntülenir. Göreli konum, TCP üstbilgisinin bittiği yerden itibaren hesaplanır.

UDP veri trafiği izleyicisi için önceden tanımlı kurallar

Ayar	Kurallar
Düşük	-
Orta	**UDP kabul edilmiş veri trafiğini denetle** Yerel bağlantı noktası **{0-66535}** içinde ve uzak bağlantı noktası **{0-66535}** içinde olursa, **0.0.0.0** maskesi ile **0.0.0.0** adresinden UDP paketlerine **izin ver**. **Tüm akışlarda açılan bağlantı noktalarına** kural uygula. Paket kuralla eşleştiğinde **günlüğe kaydetme**. Gelişmiş: **0** göreli konumunda **<boş>** maske ile şu **<boş>** baytları içeren paketleri at. **UDP trafiğini at** Yerel bağlantı noktası **{0-65535}** içinde ve uzak bağlantı noktası **{0-65535}** içinde olursa, **0.0.0.0** maskesi ile **0.0.0.0** adresinden UDPP paketlerini **reddet**. **Tüm akışlarda tüm bağlantı noktalarına** kural uygula. Paket kuralla eşleştiğinde **günlüğe kaydetme**. Gelişmiş: **0** göreli konumunda **<boş>** maske ile şu **<boş>** baytları içeren paketleri seç.

Yüksek	**Kurulmuş UDP trafiğini denetle** Yerel bağlantı noktası **{0-65535}** içinde ve uzak bağlantı noktası **{53, 67, 68, 123}** içinde olursa, **0.0.0.0** maskesi ile **0.0.0.0** adresinden UDP paketlerine **izin ver.** **Tüm akışlar** için **açık bağlantı noktalarına** kuralıuygula. Paket kuralla eşleştiğinde **günlüğe kaydetme**. Gelişmiş: **0** göreli konumunda **<boş>** maske ile şu **<boş>** baytları içeren paketleri at.

UDP paketlerini onayla/reddet

Bağlantı fareyle tıklatıldığında, özel tanımlanmış genel UDP paketlerine izin verme veya bunları reddetme seçeneğiniz vardır.

IP adresi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 adresini girebileceğiniz bir iletişim kutusu açılır.

IP maskesi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 maskesini girebileceğiniz bir iletişim kutusu açılır.

Yerel bağlantı noktaları

Bu bağlantı fareyle tıklatıldığında, yerel bağlantı noktası numaralarını veya eksiksiz bağlantı noktası aralıklarını tanımlayabileceğiniz bir iletişim kutusu görüntülenir.

Uzak bağlantı noktaları

Bu bağlantı fareyle tıklatıldığında, uzak bağlantı noktası numaralarını veya eksiksiz bağlantı noktası aralıklarını tanımlayabileceğiniz bir iletişim kutusu görüntülenir.

Uygulama yöntemi

Bağlantı noktaları

Bu bağlantı fareyle tıklatıldığında, bu kuralı tüm bağlantı noktalarına veya yalnızca tüm açık bağlantı noktalarına uygulama seçeneğiniz vardır.

Akışlar

Bu bağlantı fareyle tıklatıldığında, bu kuralı tüm akışlara veya yalnızca giden akışlara uygulama seçeneğiniz vardır.

Olay veritabanı

Bağlantıyı fareyle tıklatarak, paket kurala uyuyorsa bir olayı veritabanına "**yazma**" veya "**yazmama**" kararı verebilirsiniz.

Gelişmiş

Gelişmiş özellik, içerik filtrelemesini etkinleştirir. Örneğin, paketler belirli bir göreli konumda belirli veriler içeriyorsa, reddedilebilir. Bu seçeneği kullanmak istemiyorsanız, bir dosya seçmeyin veya boş bir dosya seçin.

Filtrelenen içerik: baytlar

Bağlantı fareyle tıklatıldığında, belirli arabelleği içeren bir dosya seçebileceğiniz bir iletişim kutusu görüntülenir.

Filtrelenen içerik: maske

Bağlantı fareyle tıklatıldığında, belirli maskeyi seçebileceğiniz bir iletişim kutusu görüntülenir.

Filtrelenen içerik: göreli konum

Bağlantı fareyle tıklatıldığında, filtrelenen içerik göreli konumunu tanımlayabileceğiniz bir iletişim kutusu görüntülenir. Göreli konum, UDP üstbilgisinin bittiği yerden itibaren hesaplanır.

ICMP trafik izleyicisi için Önceden tanımlı kurallar

Ayar	Kurallar
Düşük	-
Orta	**IP adresine dayalı ICMP'yi atma** **0.0.0.0** maskesi ile **0.0.0.0** adresinden gelen ICMP paketlerine **izin ver**. Paket kuralla eşleştiğinde **günlüğe kaydetme**. Gelişmiş: **0** göreli konumunda **<boş>** maske ile şu **<boş>** baytları içeren paketleri at.
Yüksek	Orta düzey kuralıyla aynı kural.

ICMP paketlerini onayla/reddet

Bağlantı fareyle tıklatıldığında, özel tanımlanmış genel ICMP paketlerine izin verme veya bunları reddetme seçeneğiniz vardır.

IP adresi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 adresini girebileceğiniz bir iletişim kutusu açılır.

IP maskesi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 maskesini girebileceğiniz bir iletişim kutusu açılır.

Olay veritabanı

Bağlantıyı fareyle tıklatarak, paket kurala uyuyorsa bir olayı veritabanına "**yazma**" veya "**yazmama**" kararı verebilirsiniz.

Gelişmiş

Gelişmiş özellik, içerik filtrelemesini etkinleştirir. Örneğin, paketler belirli bir göreli konumda belirli veriler içeriyorsa, reddedilebilir. Bu seçeneği kullanmak istemiyorsanız, bir dosya seçmeyin veya boş bir dosya seçin.

Filtrelenen içerik: baytlar

Bağlantı fareyle tıklatıldığında, belirli arabelleği içeren bir dosya seçebileceğiniz bir iletişim kutusu görüntülenir.

Filtrelenen içerik: maske

Bağlantı fareyle tıklatıldığında, belirli maskeyi seçebileceğiniz bir iletişim kutusu görüntülenir.

Filtrelenen içerik: göreli konum

Bağlantı fareyle tıklatıldığında, filtrelenen içerik göreli konumunu tanımlayabileceğiniz bir iletişim kutusu görüntülenir. Göreli konum, ICMP üstbilgisinin bittiği yerden itibaren hesaplanır.

IP paketleri için önceden tanımlı kurallar

Ayar	Kurallar
Düşük	-
Orta	-
Yüksek	**Tüm IP paketlerini reddet** **0.0.0.0** maskesi ile **0.0.0.0** adresinden gelen **IPv4 paketlerini reddet**. Paket kuralla eşleştiğinde **günlüğe kaydetme**.

İzin ver/Reddet

Bağlantıyı fareyle tıklatarak, özel olarak tanımlanmış IP paketlerini kabul etmek mi yoksa reddetmek mi istediğinize karar verebilirsiniz.

IPv4/IPv6

Bağlantıyı fareyle tıklatarak, IPv4 veya IPv6 seçimi yapabilirsiniz.

IP adresi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 adresini girebileceğiniz bir iletişim kutusu açılır.

IP maskesi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 maskesini girebileceğiniz bir iletişim kutusu açılır.

Olay veritabanı

Bağlantıyı fareyle tıklatarak, bir olay veritabanına yazıp yazmamaya veya paketin kurala uyup uymadığına karar verebilirsiniz.

Giden Kurallar

Giden kurallar, Avira Güvenlik Duvarı tarafından giden veri trafiğini denetlemek için tanımlanır. Şu protokollerden biri için giden kural tanımlayabilirsiniz: IP, ICMP, UDP, TCP. Bkz. Yeni kural ekle.

Uyarı
Bir paket filtrelendiğinde, karşılık gelen kurallar ard arda uygulanır; bu nedenle kural sırası çok önemlidir. Yalnızca ne yaptığınızın tamamen farkındaysanız kural sırasını değiştirin.

Kuralları yönetme düğmeleri

Düğme	Açıklama
Kural ekle	Yeni bir kural oluşturmanıza olanak sağlar. Bu düğmeye basarsanız, **Yeni kural ekle** iletişim kutusu açılır. Bu iletişim kutusunda yeni kurallar seçebilirsiniz.
Kuralı kaldır	Seçilen kuralı kaldırır.
Kural yukarı	Seçilen kuralı bir satır yukarı taşır; başka bir deyişle, kural önceliğini yükseltir.
Kural aşağı	Seçilen kuralı bir satır aşağı taşır; başka bir deyişle, kural önceliğini düşürür.

Kuralı yeniden adlandır	Seçilen kurala başka bir ad vermenize olanak sağlar.

Not
Bireysel bağdaştırıcılar için veya bilgisayarda bulunan tüm bağdaştırıcılar için yeni kurallar ekleyebilirsiniz. Tüm bağdaştırıcılara ilişkin bir bağdaştırıcı kuralı eklemek için görüntülenen bağdaştırıcı hiyerarşisinden **Bilgisayarım**'ı seçin ve **Kural ekle** düğmesini tıklatın. Bkz. Yeni kural ekle.

Not
Bir kuralın konumunu değiştirmek için, fareyi kullanarak ta kuralı istediğiniz konuma sürükleyebilirsiniz.

Yeni kural ekle

Bu pencerede yeni gelen ve giden kurallar seçebilirsiniz. Seçilen kural, **Bağdaştırıcı kuralları** penceresindeki varsayılan bilgilere dahil edilir ve bu konumda daha ayrıntılı olarak tanımlanabilir. Gelen ve giden kurallara ek olarak daha fazla kural kullanılabilir.

Olası kurallar

Eşler Arası ağa izin ver

Eşler arası bağlantılara izin verir: 4662 Numaralı Bağlantı Noktasında gelen TCP iletişimleri ve 4672 Numaralı Bağlantı Noktasında gelen UDP iletişimleri

TCP bağlantı noktası

Bağlantı fareyle tıklatıldığında, izin verilen TCP bağlantı noktasını girebileceğiniz bir iletişim kutusu görüntülenir.

UDP bağlantı noktası

Bağlantı fareyle tıklatıldığında, izin verilen UDP bağlantı noktasını girebileceğiniz bir iletişim kutusu görüntülenir.

VMWARE bağlantılarına izin ver

VMWare sistemleri arasında iletişime izin verir

IP'yi engelle

Belirtilen bir IP adresinden gelen tüm trafiği engeller

Internet Protokolü sürümü

Bağlantıyı fareyle tıklatarak, IPv4 veya IPv6 seçebilirsiniz.

IP adresi

Bağlantı fareyle tıklatıldığında, gerekli IP adresini girebileceğiniz bir iletişim penceresi açılır.

Alt ağı engelle

Belirtilen bir IP adresinden ve alt ağ maskesinden gelen tüm trafiği engeller

Internet Protokolü sürümü

Bağlantıyı fareyle tıklatarak, IPv4 veya IPv6 seçebilirsiniz.

IP adresi

Bağlantı fareyle tıklatıldığında, gerekli IP adresini girebileceğiniz bir iletişim penceresi açılır.

Alt ağ maskesi

Bağlantı fareyle tıklatıldığında, gerekli alt ağ maskesini girebileceğiniz bir iletişim penceresi açılır.

IP'ye izin ver

Belirtilen bir IP adresinden gelen tüm trafiğe izin verir

Internet Protokolü sürümü

Bağlantıyı fareyle tıklatarak, IPv4 veya IPv6 seçebilirsiniz.

IP adresi

Bağlantı fareyle tıklatıldığında, gerekli IP adresini girebileceğiniz bir iletişim penceresi açılır.

Alt ağa izin ver

Belirtilen bir IP adresinden ve alt ağ maskesinden gelen tüm trafiğe izin verir

Internet Protokolü sürümü

Bağlantıyı fareyle tıklatarak, IPv4 veya IPv6 seçebilirsiniz.

IP adresi

Bağlantı fareyle tıklatıldığında, gerekli IP adresini girebileceğiniz bir iletişim penceresi açılır.

Alt ağ maskesi

Bağlantı fareyle tıklatıldığında, gerekli alt ağ maskesini girebileceğiniz bir iletişim penceresi açılır.

Web sunucusuna izin ver

80 Numaralı Bağlantı Noktası üzerindeki bir web sunucusuna izin verir: 80 Numaralı Bağlantı Noktası üzerinde gelen TCP iletişimi

Bağlantı noktası

Bağlantı fareyle tıklatıldığında, web sunucusu tarafından kullanılan bağlantı noktasını girebileceğiniz bir iletişim kutusu görüntülenir.

VPN bağlantılarına izin ver

VPN (Sanal Özel Ağ) bağlantılarına belirli bir IP ile izin verir: x bağlantı noktalarında gelen UDP veri trafiği, x bağlantı noktalarında gelen TCP veri trafiği, ESP(50), GRE(47) protokolleri ile gelen IP veri trafiği

Internet Protokolü sürümü

Bağlantıyı fareyle tıklatarak, IPv4 veya IPv6 seçebilirsiniz.

IP adresi

Bağlantı fareyle tıklatıldığında, gerekli IP adresini girebileceğiniz bir iletişim penceresi açılır.

Uzak Masaüstü bağlantısına izin ver

3389 Numaralı Bağlantı Noktasında "Uzak Masaüstü" bağlantılarına (Uzak Masaüstü Protokolü) izin verir

Bağlantı noktası

Bağlantı fareyle tıklatıldığında, izin verilen uzak masaüstü bağlantısı için kullanılacak bağlantı noktasını girebileceğiniz bir iletişim kutusu görüntülenir.

VNC bağlantısına izin ver

5900 Numaralı Bağlantı Noktasında VNC (Sanal Ağ Bilgi İşlem) bağlantılarına izin verir

Bağlantı noktası

Bağlantı fareyle tıklatıldığında, izin verilen uzak masaüstü bağlantısı için kullanılacak bağlantı noktasını girebileceğiniz bir iletişim kutusu görüntülenir.

Dosya ve Yazıcı paylaşımına izin ver.

Yazıcı ve dosya onaylarına erişime izin verir: Belirtilen bir IP adresinden 137, 139 Numaralı Bağlantı Noktalarında gelen TCP veri trafiği ve 445 Numaralı Bağlantı Noktasında gelen UDP veri trafiği.

Olası gelen kurallar

- **Gelen IP kuralı**
- **Gelen ICMP kuralları**
- **Gelen UDP kuralları**
- **Gelen TCP kuralları**
- **Gelen IP Protokolü kuralı**

Olası giden kurallar

- **Giden IP kuralı**
- **Giden ICMP kuralları**
- **Giden UDP kuralları**
- **Giden TCP kuralları**
- **Giden IP Protokolü kuralı**

> **Not**
> Olası gelen ve giden kurallara ilişkin sözdizimi, ilgili protokollerin önceden tanımlı kurallarına ilişkin sözdizimiyle aynıdır, bkz. Güvenlik Duvarı > Bağdaştırıcı kuralları.

Düğmeler

Düğme	Açıklama
Tamam	Vurgulanan kural, yeni bir bağdaştırıcı kuralı olarak dahil edilir.
İptal	Yeni bir kural eklenmeden pencere kapatılır.

Uygulama kuralları

Kullanıcı için uygulama kuralları

Bu liste, sistemdeki tüm kullanıcıları içerir. Yönetici olarak oturum açarsanız, kuralların uygulanmasını istediğiniz kullanıcıyı seçebilirsiniz. Ayrıcalıklı bir kullanıcı değilseniz, yalnızca şu anda oturum açmış olan kullanıcıyı görebilirsiniz.

Uygulama

Bu tablo, kuralların tanımlandığı uygulamaların listesini gösterir. Uygulama listesi, yürütülen ve Avira Güvenlik Duvarı'nın kurulmasından itibaren kaydedilmiş bir kuralı olan her bir uygulamanın ayarlarını içerir.

Normal görünüm

Sütun	Açıklama
Uygulama	Uygulamanın adı.
Etkin Bağlantılar	Uygulama tarafından açılan etkin bağlantı sayısı.
Eylem	Ağ kullanım türü ne olursa olsun, uygulama, ağı kullanırken Avira Güvenlik Duvarı'nın otomatik olarak uygulayacağı eylemi gösterir. Bağlantı fareyle tıklatıldığında, başka bir eylem türüne geçiş yapabilirsiniz. Eylem türleri; **Sor**, **İzin Ver** veya **Reddet** şeklindedir. **Sor**, varsayılan eylemdir.

Gelişmiş yapılandırma

Bir uygulamanın ağ erişimleri bireysel kurallar gerektirirse, bağdaştırıcı kuralları oluşturduğunuz şekilde paket filtrelerine dayalı uygulama kuralları oluşturabilirsiniz.

- Ardından **Yapılandırma > İnternet koruması > Güvenlik Duvarı > Ayarlar**'a gidin ve **Uygulama kuralları** altındaki *Gelişmiş ayarlar*'ı etkinleştirin.
- **Uygula** veya **Tamam**'ı seçerek ayarı kaydedin.
  - ↳ **Yapılandırma > İnternet koruması > Güvenlik Duvarı > Uygulama kuralları** bölümünde uygulama kuralları listesinde, her bir uygulama için **Temel** girdisini içeren **Filtreleme** başlıklı ek bir sütun görüntülenir.

Sütun	Açıklama
Uygulama	Uygulamanın adı.
Etkin Bağlantılar	Uygulama tarafından açılan etkin bağlantı sayısı.

Eylem	Ağ kullanım türü ne olursa olsun, uygulama, ağı kullanırken Avira Güvenlik Duvarı'nın otomatik olarak uygulayacağı eylemi gösterir. **Filtreleme** sütununda **Temel** seçeneğini belirlerseniz, başka bir eylem türünü seçmek için bağlantıyı tıklatabilirsiniz. Değerler; **Sor**, **İzin Ver** veya **Reddet** şeklindedir. **Filtreleme** sütununda **Gelişmiş** seçeneğini belirlerseniz, **Kurallar** eylem türü görüntülenir. **Kurallar** bağlantısı, uygulamaya ilişkin belirli kuralları girebileceğiniz **Gelişmiş uygulama kuralları** penceresini açar.
Filtreleme	Filtreleme türünü gösterir. Bağlantıyı tıklatarak başka bir filtreleme türü seçebilirsiniz. **Temel**: Temel filtreleme durumununda, yazılım uygulaması tarafından gerçekleştirilen tüm ağ etkinliklerinde belirtilen eylem gerçekleştirilir. **Gelişmiş**: Bu filtreleme türüyle, genişletilmiş yapılandırmaya eklenen kurallar uygulanır.

- Bir uygulama için belirli kurallar oluşturmak istiyorsanız, **Filtreleme** seçeneğinin altında **Gelişmiş** girdisini seçin.
  - ↪ Daha sonra **Eylem** sütununda **Kurallar** girdisi görüntülenir.
- Belirli uygulama kuralları oluşturma penceresini açmak için **Kurallar**'ı tıklatın.

Gelişmiş yapılandırmada belirtilen uygulama kuralları

Belirtilen uygulama kurallarını kullanarak, uygulama için belirtilen veri trafiğine izin verebilir veya veri trafiğini reddedebilir ya da bireysel bağlantı noktalarının pasif dinlenmesine izin verebilir ya da bunu reddedebilirsiniz. Aşağıdaki seçenekler kullanılabilir:

Kod eklemeye izin ver / Kod eklemeyi reddet

Kod ekleme, eylemleri yürüterek dinamik bağlantı kitaplığı (DLL) yüklemek üzere bu işlemi zorlamak için başka bir işlemin adres alanına kod sunma tekniğidir. Kod ekleme, başka bir programın kapsamı altında kodu yürütmek için diğer şeyler arasında zararlı yazılımlar tarafından kullanılır. Bu şekilde, Güvenlik Duvarı'nın önünde Internet'e erişim gizlenebilir. Varsayılan modda, tüm imzalanmış uygulamalar için kod ekleme etkinleştirilmiştir.

Bağlantı noktaları uygulamasının pasif dinlenmesine izin ver / reddet

Trafiğe İzin ver/Reddet

Gelen ve/veya giden IP paketlerine izin ver ya da bunları reddet

Gelen ve/veya giden TCP paketlerine izin ver ya da bunları reddet

Gelen ve/veya giden UDP paketlerine izin ver ya da bunları reddet

Her bir uygulama için istediğiniz kadar uygulama kuralı oluşturabilirsiniz. Uygulama kuralları, gösterilen sırayla yürütülür (Daha fazla bilgiyi Gelişmiş uygulama kuralları altında bulabilirsiniz).

> **Not**
> Bir uygulama kuralının **Gelişmiş** filtrelemesini **Temel** ile değiştirirseniz, gelişmiş yapılandırmada önceden varolan uygulama kuralları devre dışı bırakılır, geri döndürülemez şekilde silinmez. **Gelişmiş** filtrelemeyi yeniden seçerseniz, önceden varolan gelişmiş uygulama kuralları yeniden etkinleştirilir ve **Uygulama kuralları** yapılandırma penceresinde görüntülenir.

Uygulama ayrıntıları

Bu kutuda, uygulama liste kutusunda seçilen uygulamanın ayrıntılarını görebilirsiniz.

- *Ad* - Uygulamanın adı.
- *Yol* - Yürütülebilir dosyanın tam yolu.

Düğmeler

Düğme	Açıklama
Uygulama ekle	Yeni bir uygulama kuralı oluşturmanıza olanak sağlar. Bu düğmeye basarsanız, bir iletişim kutusu açılır. Burada, yeni bir kural oluşturmak için gerekli uygulamayı seçebilirsiniz.
Kuralı kaldır	Seçilen uygulama kuralını kaldırır.
Ayrıntıları göster	"**Ayrıntıları göster"** penceresi uygulama listesi kutusunda seçili ayrıntıları gösterir.
Yeniden yükle	Uygulamaların listesini yeniden yükler ve yapılan değişiklikleri aynı anda atar.

Gelişmiş uygulama kuralları

Gelişmiş uygulama kuralları penceresi, uygulamaların veri trafiği ve bağlantı noktalarının dinlenmesi için belirtilen kurallar oluşturmanıza olanak sağlar. **Kural ekle** düğmesiyle yeni bir kural oluşturulabilir. Pencerenin alt kısmında daha fazla kural belirtebilirsiniz. Bir uygulama için istediğiniz kadar kural oluşturabilirsiniz. Kurallar, görüntülenme sırasıyla

yürütülür. Kuralların sırasını değiştirmek için **Kural yukarı** ve **Kural aşağı** düğmelerini kullanabilirsiniz.

> **Not**
> Bir uygulamanın konumunu değiştirmek için, fareyi kullanarak kuralı istediğiniz konuma da sürükleyebilirsiniz.

Uygulama ayrıntıları

Seçilen uygulamayla ilgili bilgiler, *Uygulama ayrıntıları* alanında görüntülenir.

- *Ad* - Uygulamanın adı.
- *Yol* - Uygulama için yürütülebilir dosyanın yolu.

Kural seçenekleri

Kod eklemeyi reddet / Kod eklemeye izin ver

Bağlantıyı fareyle tıklatarak, seçilen uygulama için kod eklemeye izin vermek mi yoksa kod eklemeyi reddetmek mi istediğinize karar verebilirsiniz.

Kural Türü: Trafik/ Dinle

Bağlantıyı fareyle tıklatarak, trafik izleme için mi yoksa bağlantı noktalarının dinlenmesi için mi bir kural oluşturmak istediğinize karar verebilirsiniz.

Eylemi reddet / Eyleme izin ver

Bağlantıyı fareyle tıklatarak, kuralla hangi eylemin yürütüleceğine karar verebilirsiniz.

Bağlantı noktası

Bağlantı fareyle tıklatıldığında, Dinleme kuralının geçerli olduğu yerel bağlantı noktasını girebileceğiniz bir iletişim kutusu görüntülenir. Ayrıca birkaç bağlantı noktası veya bağlantı noktası alanı da girebilirsiniz.

Giden, gelen, tüm paketler

Bu bağlantı fareyle tıklatıldığında, Trafik kuralının yalnızca giden paketleri mi yoksa gelen paketleri mi izleyeceğine karar verebilirsiniz.

IP paketleri / TCP paketleri / UDP paketleri

Bağlantıyı fareyle tıklatarak, hangi protokolün Trafik kuralını izlediğine karar verebilirsiniz.

IP paketleri seçenekleri:

IP adresi

Bağlantı fareyle tıklatıldığında, gerekli IP adresini girebileceğiniz bir iletişim kutusu açılır.

IP maskesi

Bağlantı fareyle tıklatıldığında, gerekli IP maskesini girebileceğiniz bir iletişim kutusu açılır.

TCP paketleri / UDP paketi seçenekleri:

Yerel IP adresi

Bağlantı fareyle tıklatıldığında, yerel IP adresini girebileceğiniz bir iletişim kutusu açılır.

Yerel IP maskesi

Bağlantı fareyle tıklatıldığında, gerekli yerel IP maskesini girebileceğiniz bir iletişim kutusu açılır.

Uzak IP adresi

Bağlantı fareyle tıklatıldığında, gerekli uzak IP adresini girebileceğiniz bir iletişim kutusu açılır.

Uzak IP maskesi

Bağlantı fareyle tıklatıldığında, gerekli uzak IP maskesini girebileceğiniz bir iletişim kutusu açılır.

Yerel bağlantı noktası

Bağlantı fareyle tıklatıldığında, yerel bağlantı noktalarını veya eksiksiz bağlantı noktası aralıklarını tanımlayabileceğiniz bir iletişim kutusu görüntülenir.

Uzak bağlantı noktası

Bağlantı fareyle tıklatıldığında, bir veya daha fazla gerekli uzak bağlantı noktasını veya eksiksiz bağlantı noktası aralıklarını tanımlayabileceğiniz bir iletişim kutusu görüntülenir.

Rapor dosyası

Bağlantı fareyle tıklatıldığında, bir kural yerine getirildiğinde programın rapor dosyasına "**kaydet**" ve "**kaydetme**" seçeneklerinden birini seçebilirsiniz.

Düğmeler

Düğme	Açıklama
Kural ekle	Yeni bir uygulama kuralı oluşturulur.
Kuralı kaldır	Seçilen uygulama kuralı silinir.

Kural yukarı	Seçilen kural bir satır yukarı taşınır; başka bir deyişle, kural önceliği yükseltilir.
Kural aşağı	Seçilen uygulama kuralı bir satır aşağı taşınır; başka bir deyişle, kural önceliği düşürülür.
Kuralı yeniden adlandır	Yeni bir kural adı girilebilmesi için, seçilen kural düzenlenir.
Uygula	Yapılan değişiklikler kabul edilir ve Avira Güvenlik Duvarı tarafından hemen uygulanır.
Tamam	Yapılan değişiklikler uygulanır. Uygulama kuralları yapılandırma penceresi kapatılır.
İptal	Yapılan değişiklikler uygulanmadan, uygulama kuralları yapılandırma penceresi kapatılır.

Güvenilen üreticiler

Güvenilen yazılım üreticilerinin bir listesi, **Güvenilen üreticiler** altında görüntülenir.

Ağ Olayı açılır penceresinde **Her zaman bu sağlayıcıya güven** seçeneğini kullanarak listeye üreticiler ekleyebilir veya listeden üreticileri kaldırabilirsiniz. **Güvenilen üreticilerin oluşturduğu uygulamalara otomatik olarak izin ver** seçeneğini etkinleştirerek, varsayılan olarak listelenen sağlayıcıların imzaladığı uygulamalardan ağ erişimine izin verebilirsiniz.

Kullanıcı için güvenilen üreticiler

Bu liste, sistemdeki tüm kullanıcıları içerir. Yönetici olarak oturum açarsanız, güvenilen üreticilerin listesini görüntülemek veya güncellemek istediğiniz kullanıcıyı seçebilirsiniz. Ayrıcalıklı bir kullanıcı değilseniz, yalnızca şu anda oturum açmış olan kullanıcıyı görebilirsiniz.

Güvenilen üreticilerin oluşturduğu uygulamalara otomatik olarak izin ver

Bu seçenek etkinleştirilirse, bilinen ve güvenilen bir sağlayıcının imzası sağlanan uygulamanın otomatik olarak ağa erişmesine izin verilir. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

Üreticiler

Bu liste, güvenilen olarak sınıflandırılan tüm üreticileri gösterir.

Düğmeler

Düğme	Açıklama
Kaldır	Vurgulanan girdi, güvenilen üreticiler listesinden kaldırılır. Seçilen sağlayıcıyı listeden kalıcı olarak kaldırmak için, yapılandırma penceresinde **Uygula** veya **Tamam** seçeneğine tıklayın.
Yeniden yükle	Yapılan değişiklikler geri alınır. Kaydedilen son liste yüklenir.

Not
Listeden üreticileri kaldırır ve **Uygula** seçeneğini işaretlerseniz, üreticiler listeden kalıcı olarak kaldırılır. **Yeniden Yükle** seçeneği ile değişiklik geri alınamaz. Ancak güvenilen üreticiler listesine yeniden bir üretici eklemek için **Ağ Olayı** açılır penceresinde **Her zaman bu üreticiye güven** seçeneğini kullanabilirsiniz.

Not
Avira FireWall güvenilen üreticiler listesine girdi eklemeden önce uygulama kurallarını öncelik sırasına koyar: Bir uygulama kuralı oluşturmuş iseniz ve uygulama sağlayıcı güvenilen üreticiler listesinde yer alıyorsa, uygulama kuralı yürütülür.

Ayarlar

Gelişmiş seçenekler

Güvenlik Duvarı'nı Aç

Seçenek etkinleştirilirse, Avira Güvenlik Duvarı etkinleştirilir ve bilgisayarınızı Internet ve diğer ağlardan kaynaklanan risklere karşı korur.

Başlangıçta Windows Güvenlik Duvarını durdur

Bu seçenek etkinleştirilirse, bilgisayar yeniden başlatıldığında Windows Güvenlik Duvarı devre dışı bırakılır. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

Otomatik kural zaman aşımı

Devamlı engelle

Bu seçenek etkinleştirilirse, otomatik olarak oluşturulmuş bir kural örneğin, bir bağlantı noktası taraması sırasında korunur.

n saniye sonra kuralı kaldır

Bu seçenek etkinleştirilirse, otomatik olarak oluşturulmuş bir kural örneğin, bir bağlantı noktası taraması sırasında, tanımladığınız süreden sonra yeniden kaldırılır. Bu seçenek, varsayılan ayar olarak etkinleştirilir. Bu kutuda, kuralların kaldırılacağı saniye sayısını belirleyebilirsiniz.

Bildirimler

Bildirimler, Avira FireWall'ndan masaüstü bildirimi almak istediğiniz olayları tanımlar.Bildirimler, Güvenlik Duvarı'ndan masaüstü bildirimi almak istediğiniz olayları tanımlar.

Bağlantı noktası taraması

Seçenek etkinleştirilirse, bir bağlantı noktası taramasının Avira FireWall tarafından algılanması durumunda bir masaüstü bildirimi alırsınız.

Baskın

Seçenek etkinleştirilirse, bir baskın saldırısının Avira FireWall tarafından algılanması durumunda bir masaüstü bildirimi alırsınız.

Engellenen uygulamalar

Seçenek etkinleştirilirse, Avira FireWall'nın bir uygulamanın ağ etkinliğini reddetmesi, başka bir deyişle engellemesi durumunda bir masaüstü bildirimi alırsınız.

Engellenen IP

Seçenek etkinleştirilirse, Avira FireWall'nın bir IP adresinden gelen veri trafiğini reddetmesi, başka bir deyişle engellemesi durumunda bir masaüstü bildirimi alırsınız.

Uygulama kuralları

Güvenlik Duvarı > Uygulama kuralları bölümünde uygulama kurallarına yönelik yapılandırma seçeneklerini ayarlamak için uygulama kuralları seçenekleri kullanılır.

Gelişmiş ayarlar

Bu seçenek etkinleştirilirse, bir uygulamanın farklı ağ erişimlerini tek tek düzenleyebilirsiniz.

Temel ayarlar

Bu seçenek etkinleştirilirse, uygulamanın farklı ağ erişimleri için yalnızca bir eylem ayarlanabilir.

Açılır pencere ayarları

İşlem başlatma yığınını incele

Bu seçenek etkinleştirilirse, işlem yığını incelemesi daha doğru bir denetime olanak sağlar. Avira FireWall, yığındaki güvenilir olmayan tüm işlemlerin gerçekte alt işlemleri üzerinden ağa erişmekte olabileceğini varsayar. Bu nedenle, işlem yığınındaki güvenilir olmayan her işlem için farklı bir açılır pencere açılacaktır. Bu seçenek, varsayılan ayar olarak devre dışı bırakılır.

İşlem başına birden çok açılır pencereye izin ver

Bu seçenek etkinleştirilirse, bir uygulama her ağ bağlantısı yaptığında bir açılır pencere tetiklenir. Alternatif olarak, yalnızca birinci bağlantı girişiminde bilgilendirilirsiniz. Bu seçenek, varsayılan ayar olarak devre dışı bırakılır.

Bu uygulama için eylemi hatırla

Her zaman etkin

Bu seçenek etkinleştirildiğinde, "**Ağ olayı**" iletişim kutusunun "**Bu uygulama için eylemi hatırla**" seçeneği, varsayılan ayar olarak etkinleştirilir.

Her zaman devre dışı

Bu seçenek etkinleştirildiğinde, "**Ağ olayı**" iletişim kutusunun "**Bu uygulama için eylemi hatırla**" seçeneği, varsayılan ayar olarak devre dışı bırakılır.

İmzalanan uygulamalar için etkin

Bu seçenek etkinleştirildiğinde, "**Ağ olayı**" iletişim kutusunun "**Bu uygulama için eylemi hatırla**" seçeneği, imzalanan uygulamalar tarafından ağ erişimi sırasında otomatik olarak etkinleştirilir. İmzalanmış uygulamalar "güvenilen üreticiler" tarafından dağıtılır (bkz. Güvenilen Üreticiler).

Son kullanılan durumu hatırla

Bu seçenek etkinleştirildiğinde, "**Ağ olayı**" iletişim kutusunun "**Bu uygulama için eylemi hatırla**" seçeneği, son ağ olayıyla aynı şekilde etkinleştirilir. "**Bu uygulama için eylemi hatırla**" seçeneği etkinleştirilmişse, aşağıdaki ağ olayı için bu seçenek etkinleştirilir. Son ağ olayı için "**Bu uygulama için eylemi hatırla**" seçeneği devre dışı bırakılmışsa, aşağıdaki ağ olayı için de bu seçenek devre dışı bırakılır.

Ayrıntıları göster

Bu yapılandırma seçenekleri grubunda, **Ağ olayı** penceresinde ayrıntılı bilgilerin görüntüsünü ayarlayabilirsiniz.

İstek üzerine ayrıntıları göster

Bu seçenek etkinleştirilirse, ayrıntılı bilgiler yalnızca istek üzerine "**Ağ olayı**" penceresinde görüntülenir; başka bir deyişle ayrıntılı bilgiler, "**Ağ olayı**" penceresinde "**Ayrıntıları göster**" düğmesi tıklatılarak görüntülenir.

Her zaman ayrıntıları göster

Bu seçenek etkinleştirilirse, ayrıntılı bilgiler her zaman "**Ağ olayı**" penceresinde görüntülenir.

Son kullanılan durumu hatırla

Bu seçenek etkinleştirilirse, ayrıntılı bilgilerin görünümü, önceki ağ olayıyla aynı şekilde yönetilir. Son ağ olayı sırasında ayrıntılı bilgiler görüntülendiyse veya ayrıntılı bilgilere erişildiyse, aşağıdaki ağ olayı için ayrıntılı bilgiler görüntülenir. Son ağ olayı sırasında ayrıntılı bilgiler gizlendiyse ve görüntülenmediyse, aşağıdaki ağ olayı için ayrıntılı bilgiler görüntülenmez.

8.6.3 AMC kapsamında Avira Güvenlik Duvarı

Güvenlik Duvarı, Avira Yönetim Konsolu aracılığıyla belirli yönetim gereksinimlerini karşılamak üzere yapılandırılmıştır. Bireysel yapılandırma seçenekleri için genişletilmiş seçenekler ve kısıtlamalar vardır:

- İstemci bilgisayarın tüm kullanıcıları için Güvenlik Duvarı ayarları geçerlidir
- Bağdaştırıcı kuralları: Bireysel bağdaştırıcılara yönelik güvenlik düzeyleri, bağlam menüleri kullanılarak ayarlanabilir
- Uygulama kuralları: Uygulamaların ağ erişimine izin verilebilir veya ağ erişimi reddedilebilir. Belirli uygulama kuralları oluşturmanın yolu yoktur.

Avira ürününüz Avira Yönetim Konsolu tarafından yönetiliyorsa, Kontrol Merkezi'ndeki aşağıdaki Güvenlik Duvarı ayarı seçenekleri istemci bilgisayarlarda devre dışı bırakılır:

- Güvenlik Duvarı güvenlik düzeylerinin ayarlanması
- Bağdaştırıcı ve uygulama kurallarının ayarlanması

Genel ayarlar

Gelişmiş seçenekler

Güvenlik Duvarı'nı etkinleştir

Seçenek etkinleştirilirse, Avira Güvenlik Duvarı etkinleştirilir ve bilgisayarınızı Internet ve diğer ağlardan kaynaklanan risklere karşı korur.

Başlangıçta Windows Güvenlik Duvarını durdur

Bu seçenek etkinleştirilirse, bilgisayar yeniden başlatıldığında Windows Güvenlik Duvarı devre dışı bırakılır. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

Öğrenme modu

Bu seçenek etkinleştirildiyse, Avira Güvenlik Duvarı'nın öğrenme modu etkindir.

Otomatik kural zaman aşımı

Devamlı engelle

Bu seçenek etkinleştirilirse, otomatik olarak oluşturulmuş bir kural örneğin, bir bağlantı noktası taraması sırasında korunur.

n saniye sonra kuralı kaldır

Bu seçenek etkinleştirilirse, otomatik olarak oluşturulmuş bir kural örneğin, bir bağlantı noktası taraması sırasında, tanımladığınız süreden sonra yeniden kaldırılır. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

Genel bağdaştırıcı kuralları

Kurulan ağ bağlantıları, belirtilmiş bağdaştırıcılardır. Şu İstemci ağ bağlantıları için bağdaştırıcı kuralları hazırlanabilir:

- **Varsayılan** bağdaştırıcı: LAN veya yüksek hızlı Internet
- **Kablosuz**
- **Çevirmeli** bağlantı

Bağdaştırıcı içerik menüsünden (**Genel bağdaştırıcı kuralları** penceresinde, **Bilgisayarım** veya **Varsayılan, Kablosuz, Çevirmeli,** seçeneklerinden birini sağ tıklatın) mevcut her bağdaştırıcı için önceden tanımlı bağdaştırıcı kurallarını belirleyebilirsiniz:

- **Güvenlik düzeyini Düşük olarak ayarla**
- **Güvenlik düzeyini Orta olarak ayarla**
- **Güvenlik düzeyini Yüksek olarak ayarla**

Ayrıca bireysel bağdaştırıcı kurallarını kendi gereksinimlerinize uyacak şekilde değiştirme seçeneğiniz de vardır.

> **Not**
> Avira Güvenlik Duvarı'nın tüm önceden tanımlı kuralları için varsayılan Güvenlik düzeyi ayarı, **Orta**'dır.

- ICMP protokolü
- TCP Bağlantı Noktası Taraması
- UDP Bağlantı Noktası Taraması
- Gelen kurallar
- Gelen IP protokolü kuralı

- Giden kurallar
- Kuralları yönetme düğmeleri

ICMP protokolü

Internet Kontrol İletisi Protokolü (ICMP), ağlar üzerinde hata ve bilgi iletilerinin alışverişini yapmak için kullanılır. Bu protokol ayrıca ping veya izleyici ile durum iletileri için de kullanılır.
Bu kuralla, gelen ve giden engellenmiş ileti türlerini, baskın durumundaki davranışı ve parçalanmış ICMP paketlerine yanıtı tanımlayabilirsiniz. Bu kural, her pakete yanıt verilirken, saldırılan makinenin CPU yükünde artışla sonuçlanan, ICMP baskın saldırılarının önlenmesi görevini görür.

ICMP protokolü için önceden tanımlı kurallar

Ayar	Kurallar
Düşük	Gelen engellenen türler: **tür yok**. Giden engellenen türler: **tür yok**. Paketler arasındaki gecikme **50** ms'den azsa baskın olduğunu varsayın. Parçalanmış ICMP paketlerini **Reddet**.
Orta	Düşük düzey kuralıyla aynı kural.
Yüksek	Gelen engellenen türler: **çeşitli türler** Giden engellenen türler: **çeşitli türler** Paketler arasındaki gecikme **50** ms'den azsa baskın olduğunu varsayın. Parçalanmış ICMP paketlerini **Reddet**.

Gelen engellenen türler: tür yok/çeşitli türler

Bağlantı fareyle tıklatıldığında, ICMP paket türlerinin bir listesi görüntülenir. Bu listeden, engellemek istediğiniz gelen ICMP ileti türlerini belirtebilirsiniz.

Giden engellenen türler: tür yok/çeşitli türler

Bağlantı fareyle tıklatıldığında, ICMP paket türlerinin bir listesi görüntülenir. Bu listeden, engellemek istediğiniz giden ICMP ileti türlerini seçebilirsiniz.

Baskın

Bağlantı fareyle tıklatıldığında, izin verilen maksimum ICMPA gecikmesini girebileceğiniz bir iletişim kutusu görüntülenir.

Parçalanmış ICMP paketleri

Bağlantı fareyle tıklatıldığında, parçalanmış ICMP paketlerini reddetme veya reddetmeme seçeneğiniz vardır.

TCP bağlantı noktası taraması

Bu kural ile, ne zaman Güvenlik Duvarı tarafından bir TCP bağlantı noktası taramasının varsayılacağını ve bu durumda ne yapılması gerektiğini tanımlayabilirsiniz. Bu kural, bilgisayarınızdaki açık TCP bağlantı noktalarının algılanmasıyla sonuçlanan TCP bağlantı noktası tarama saldırılarının önlenmesi görevini görür. Bu saldırı türü, bir bilgisayardaki zayıf noktaları aramak için kullanılır ve bunu genellikle tehlikeli saldırı türleri takip eder.

TCP bağlantı noktası taraması için önceden tanımlı kurallar

Ayar	Kurallar
Düşük	**5.000** milisaniyede **50** veya daha fazla bağlantı noktası tarandıysa bir TCP bağlantı noktası taraması olduğunu varsayın. Algılandığında, saldırganın IP'sini **günlüğe kaydedin** ve saldırıyı engelleme kuralı **eklemeyin**.
Orta	**5.000** milisaniyede **50** veya daha fazla bağlantı noktası tarandıysa bir TCP bağlantı noktası taraması olduğunu varsayın. Algılandığında, saldırganın IP'sini **günlüğe kaydedin** ve saldırıyı engelleme kuralı **ekleyin**.
Yüksek	Orta düzey kuralıyla aynı kural.

Bağlantı noktaları

Bağlantı fareyle tıklatıldığında, TCP bağlantı noktası taramasının varsayılması için taranmış olması gereken bağlantı noktası sayısını girebileceğiniz bir iletişim kutusu görüntülenir.

Bağlantı noktası tarama süresi penceresi

Bu bağlantı fareyle tıklatıldığında, TCP bağlantı noktası taramasının varsayılması için belirli sayıda bağlantı noktası taramasına ilişkin zaman aralığını girebileceğiniz bir iletişim kutusu görüntülenir.

Rapor dosyası

Bağlantı fareyle tıklatıldığında, saldırganın IP adresini günlüğe kaydetme veya kaydetmeme seçeneğiniz vardır.

Kural

Bağlantı fareyle tıklatıldığında, TCP bağlantı noktası tarama saldırısını engelleme kuralı ekleme veya eklememe seçeneğiniz vardır.

UDP bağlantı noktası taraması

Bu kural ile, ne zaman Güvenlik Duvarı tarafından bir UDP bağlantı noktası taramasının varsayılacağını ve bu durumda ne yapılması gerektiğini tanımlayabilirsiniz. Bu kural, bilgisayarınızdaki açık UDP bağlantı noktalarının algılanmasıyla sonuçlanan UDP bağlantı noktası tarama saldırılarını önler. Bu saldırı türü, bir bilgisayardaki zayıf noktaları aramak için kullanılır ve bunu genellikle tehlikeli saldırı türleri takip eder.

UDP bağlantı noktası taraması için önceden tanımlı kurallar

Ayar	Kurallar
Düşük	**50** milisaniyede **5.000** veya daha fazla bağlantı noktası tarandıysa bir UDP bağlantı noktası taraması olduğunu varsayın. Algılandığında, saldırganın IP'sini **günlüğe kaydedin** ve saldırıyı engelleme kuralı **eklemeyin**.
Orta	**50** milisaniyede **5.000** veya daha fazla bağlantı noktası tarandıysa bir UDP bağlantı noktası taraması olduğunu varsayın. Algılandığında, saldırganın IP'sini **günlüğe kaydedin** ve saldırıyı engelleme kuralı **ekleyin**.
Yüksek	Orta düzey kuralıyla aynı kural.

Bağlantı noktaları

Bağlantı fareyle tıklatıldığında, UDP bağlantı noktası taramasının varsayılması için taranmış olması gereken bağlantı noktası sayısını girebileceğiniz bir iletişim kutusu görüntülenir.

Bağlantı noktası tarama süresi penceresi

Bu bağlantı fareyle tıklatıldığında, UDP bağlantı noktası taramasının varsayılması için belirli sayıda bağlantı noktası taramasına ilişkin zaman aralığını girebileceğiniz bir iletişim kutusu görüntülenir.

Rapor dosyası

Bağlantı fareyle tıklatıldığında, saldırganın IP adresini günlüğe kaydetme veya kaydetmeme seçeneğiniz vardır.

Kural

Bağlantı fareyle tıklatıldığında, UDP bağlantı noktası tarama saldırısını engelleme kuralı ekleme veya eklememe seçeneğiniz vardır.

Gelen Kurallar

Gelen kurallar, Avira Güvenlik Duvarı tarafından gelen veri trafiğini denetlemek için tanımlanır.

> **Uyarı**
> Bir paket filtrelendiğinde, karşılık gelen kurallar art arda uygulanır; bu nedenle kural sırası çok önemlidir. Yalnızca ne yaptığınızın tamamen farkındaysanız kural sırasını değiştirin.

TCP trafik verisi izleyicisi için Önceden tanımlı kurallar

Ayar	Kurallar
Düşük	Avira Güvenlik Duvarı tarafından herhangi bir gelen veri trafiği engellenmez.
Orta	• 135 üzerinden Kurulan TCP bağlantılarına izin ver Yerel bağlantı noktaları **{135}** içinde ve uzak bağlantı noktaları **{0-65535}** içinde olursa, **0.0.0.0** maskesi ile **0.0.0.0** adresinden gelen TCP paketlerine **izin ver**. **Varolan bağlantıların paketleri** için uygula. Paket kuralla eşleştiğinde **günlüğe kaydetme**. Gelişmiş: **0** göreli konumunda **<boş>** maske ile şu **<boş>** baytları içeren paketleri at • 135 üzerindeki TCP paketlerini reddet Yerel bağlantı noktası **{135}** içinde ve uzak bağlantı noktası **{0-65535}** içinde olursa, **0.0.0.0** maskesi ile **0.0.0.0** adresinden TCP paketlerini reddet. **Tüm paketler** için uygula. Paket kuralla eşleştiğinde **günlüğe kaydetme**. Gelişmiş: **0** göreli konumunda **<boş>** maske ile şu **<boş>** baytları içeren paketleri at. • TCP sağlıklı veri trafiğini denetle Yerel bağlantı noktası **{0-65535}** içinde ve uzak bağlantı noktası **{0-65535}** içinde olursa, **0.0.0.0** maskesi ile **0.0.0.0** adresinden TCP paketlerine **izin ver**. **Bağlantı başlatma ve var olan bağlantı paketleri** için uygula. Paket kuralla eşleştiğinde **günlüğe kaydetme**. Gelişmiş: **0** göreli konumunda **<boş>** maske ile şu **<boş>** baytları içeren paketleri seç. • TCP trafiğini at Yerel bağlantı noktası **{0-65535}** içinde ve uzak bağlantı noktası **{0-65535}** içinde olursa, **0.0.0.0** maskesi ile **0.0.0.0** adresinden TCP paketlerini **reddet**. **Tüm paketler** için uygula. Paket kuralla eşleştiğinde **günlüğe kaydetme**. Gelişmiş: **0** göreli konumunda **<boş>** maske ile şu **<boş>** baytları içeren paketleri seç.

Yüksek	Kurulmuş TCP veri trafiğini denetle Yerel bağlantı noktası **{0-65535}** içinde ve uzak bağlantı noktası **{0-65535}** içinde olursa, **0.0.0.0** maskesi ile **0.0.0.0** adresinden TCP paketlerine i**zin ver**. **Varolan bağlantıların paketleri** için uygula. Paket kuralla eşleştiğinde **günlüğe kaydetme**. Gelişmiş: **0** göreli konumunda **<boş>** maske ile şu **<boş>** baytları içeren paketleri seç.

TCP paketlerini kabul et / reddet

Bağlantı fareyle tıklatıldığında, özel tanımlanmış gelen TCP paketlerine izin verme veya bunları reddetme seçeneğiniz vardır.

IP adresi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 adresini girebileceğiniz bir iletişim kutusu açılır.

IP maskesi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 maskesini girebileceğiniz bir iletişim kutusu açılır.

Yerel bağlantı noktaları

Bu bağlantı fareyle tıklatıldığında, yerel bağlantı noktası numaralarını veya eksiksiz bağlantı noktası aralıklarını tanımlayabileceğiniz bir iletişim kutusu görüntülenir.

Uzak bağlantı noktaları

Bu bağlantı fareyle tıklatıldığında, uzak bağlantı noktası numaralarını veya eksiksiz bağlantı noktası aralıklarını tanımlayabileceğiniz bir iletişim kutusu görüntülenir.

Uygulama yöntemi

Bu bağlantı fareyle tıklatıldığında, bağlantı başlatma ve var olan bağlantı paketleri için veya yalnızca varolan bağlantıların paketleri ya da tüm paketler için kuralı uygulama seçeneğiniz vardır.

Rapor dosyası

Bağlantıyı fareyle tıklatarak, bir rapor dosyasına yazıp yazmamaya veya paketin kurala uyup uymadığına karar verebilirsiniz.

Gelişmiş özellik, içerik filtrelemesini etkinleştirir. Örneğin, paketler belirli bir göreli konumda belirli veriler içeriyorsa, reddedilebilir. Bu seçeneği kullanmak istemiyorsanız, bir dosya seçmeyin veya boş bir dosya seçin.

Filtrelenen içerik: Veri

Bağlantı fareyle tıklatıldığında, belirli arabelleği içeren bir dosya seçebileceğiniz bir iletişim kutusu görüntülenir.

Filtrelenen içerik: Maske

Bağlantı fareyle tıklatıldığında, belirli maskeyi seçebileceğiniz bir iletişim kutusu görüntülenir.

Filtrelenen içerik: Göreli konum

Bağlantı fareyle tıklatıldığında, filtrelenen içerik göreli konumunu tanımlayabileceğiniz bir iletişim kutusu görüntülenir. Göreli konum, TCP üstbilgisinin bittiği yerden itibaren hesaplanır.

UDP trafik verisi izleyicisi için önceden tanımlı kurallar

Ayar	Kurallar
Düşük	-
Orta	• UDP kabul edilmiş veri trafiğini denetle Yerel bağlantı noktası **{0-66535}** içinde ve uzak bağlantı noktası **{0-66535}** içinde olursa, **0.0.0.0** maskesi ile **0.0.0.0** adresinden UDP paketlerine **izin ver**. **Tüm akışlarda açılan bağlantı noktalarına** kural uygula. Paket kuralla eşleştiğinde **günlüğe kaydetme**. Gelişmiş: **0** göreli konumunda **<boş>** maske ile şu **<boş>** baytları içeren paketleri at. • UDP trafiğini at Yerel bağlantı noktası **{0-65535}** içinde ve uzak bağlantı noktası **{0-65535}** içinde olursa, **0.0.0.0** maskesi ile **0.0.0.0** adresinden UDPP paketlerini **reddet**. **Tüm akışlarda tüm bağlantı noktalarına** kural uygula. Paket kuralla eşleştiğinde **günlüğe kaydetme**. Gelişmiş: **0** göreli konumunda **<boş>** maske ile şu **<boş>** baytları içeren paketleri seç.

Yüksek	Kurulmuş UDP trafiğini denetle Yerel bağlantı noktası **{0-65535}** içinde ve uzak bağlantı noktası {53, 67, 68, 123} içinde olursa, **0.0.0.0** maskesi ile **0.0.0.0** adresinden UDP paketlerine **izin ver.Tüm akışlarda açılan bağlantı noktalarına kural uygula.** **Paket kuralla eşleştiğinde günlüğe kaydetme.** **Gelişmiş: 0 göreli konumunda <boş> maske ile şu <boş> baytları içeren paketleri at.**

UDP paketlerini kabul et / reddet

Bağlantı fareyle tıklatıldığında, özel tanımlanmış genel UDP paketlerine izin verme veya bunları reddetme seçeneğiniz vardır.

IP adresi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 adresini girebileceğiniz bir iletişim kutusu açılır.

IP maskesi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 maskesini girebileceğiniz bir iletişim kutusu açılır.

Yerel bağlantı noktaları

Bu bağlantı fareyle tıklatıldığında, yerel bağlantı noktası numaralarını veya eksiksiz bağlantı noktası aralıklarını tanımlayabileceğiniz bir iletişim kutusu görüntülenir.

Uzak bağlantı noktaları

Bu bağlantı fareyle tıklatıldığında, uzak bağlantı noktası numaralarını veya eksiksiz bağlantı noktası aralıklarını tanımlayabileceğiniz bir iletişim kutusu görüntülenir.

Uygulama yöntemi

Bu bağlantı fareyle tıklatıldığında, bu kuralı tüm bağlantı noktalarına veya yalnızca tüm açık bağlantı noktalarına uygulama seçeneğiniz vardır.

Rapor dosyası

Bağlantıyı fareyle tıklatarak, bir rapor dosyasına yazıp yazmamaya veya paketin kurala uyup uymadığına karar verebilirsiniz.

Gelişmiş özellik, içerik filtrelemesini etkinleştirir. Örneğin, paketler belirli bir göreli konumda belirli veriler içeriyorsa, reddedilebilir. Bu seçeneği kullanmak istemiyorsanız, bir dosya seçmeyin veya boş bir dosya seçin.

Filtrelenen içerik: Veri

Bağlantı fareyle tıklatıldığında, belirli arabelleği içeren bir dosya seçebileceğiniz bir iletişim kutusu görüntülenir.

Filtrelenen içerik: Maske

Bağlantı fareyle tıklatıldığında, belirli maskeyi seçebileceğiniz bir iletişim kutusu görüntülenir.

Filtrelenen içerik: Göreli konum

Bağlantı fareyle tıklatıldığında, filtrelenen içerik göreli konumunu tanımlayabileceğiniz bir iletişim kutusu görüntülenir. Göreli konum, UDP üstbilgisinin bittiği yerden itibaren hesaplanır.

ICMP trafik verisi izleyicisi için önceden tanımlı kurallar

Ayar	Kurallar
Düşük	-
Orta	IP adresine dayalı ICMP'yi atma **0.0.0.0** maskesi ile **0.0.0.0** adresinden gelen ICMP paketlerine **izin ver**. Paket kuralla eşleştiğinde **günlüğe kaydetme**. Gelişmiş: **0** göreli konumunda **<boş>** maske ile şu **<boş>** baytları içeren paketleri at.
Yüksek	Orta düzey kuralıyla aynı kural.

ICMP paketlerini kabul et / reddet

Bağlantı fareyle tıklatıldığında, özel tanımlanmış genel ICMP paketlerine izin verme veya bunları reddetme seçeneğiniz vardır.

IP adresi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 adresini girebileceğiniz bir iletişim kutusu açılır.

IP maskesi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 maskesini girebileceğiniz bir iletişim kutusu açılır.

Rapor dosyası

Bağlantıyı fareyle tıklatarak, bir rapor dosyasına yazıp yazmamaya veya paketin kurala uyup uymadığına karar verebilirsiniz.

Gelişmiş özellik, içerik filtrelemesini etkinleştirir. Örneğin, paketler belirli bir göreli konumda belirli veriler içeriyorsa, reddedilebilir. Bu seçeneği kullanmak istemiyorsanız, bir dosya seçmeyin veya boş bir dosya seçin.

Filtrelenen içerik: Veri

Bağlantı fareyle tıklatıldığında, belirli arabelleği içeren bir dosya seçebileceğiniz bir iletişim kutusu görüntülenir.

Filtrelenen içerik: Maske

Bağlantı fareyle tıklatıldığında, belirli maskeyi seçebileceğiniz bir iletişim kutusu görüntülenir.

Filtrelenen içerik: Göreli konum

Bağlantı fareyle tıklatıldığında, filtrelenen içerik göreli konumunu tanımlayabileceğiniz bir iletişim kutusu görüntülenir. Göreli konum, ICMP üstbilgisinin bittiği yerden itibaren hesaplanır.

IP paketleri için önceden tanımlı kurallar

Ayar	Kurallar
Düşük	-
Orta	-
Yüksek	Tüm IP paketlerini reddet **0.0.0.0 maskesi ile 0.0.0.0 adresinden gelen IP paketlerini reddet.** **Paket kuralla eşleştiğinde günlüğe kaydetme.**

IP paketlerini kabul et / reddet

Bağlantıyı fareyle tıklatarak, özel olarak tanımlanmış IP paketlerini kabul etmek mi yoksa reddetmek mi istediğinize karar verebilirsiniz.

IP adresi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 adresini girebileceğiniz bir iletişim kutusu açılır.

IP maskesi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 maskesini girebileceğiniz bir iletişim kutusu açılır.

Rapor dosyası

Bağlantıyı fareyle tıklatarak, bir rapor dosyasına yazıp yazmamaya veya paketin kurala uyup uymadığına karar verebilirsiniz.

Gelen IP Protokolü kuralı

IP paketleri

Bağlantıyı fareyle tıklatarak, özel olarak tanımlanmış IP paketlerini kabul etmek mi yoksa reddetmek mi istediğinize karar verebilirsiniz.

IP adresi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 adresini girebileceğiniz bir iletişim kutusu açılır.

IP maskesi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 maskesini girebileceğiniz bir iletişim kutusu açılır.

Protokol

Bu bağlantı fareyle tıklatıldığında, gerekli IP protokolünü girebileceğiniz bir iletişim kutusu açılır.

Rapor dosyası

Bağlantıyı fareyle tıklatarak, bir rapor dosyasına yazıp yazmamaya veya paketin kurala uyup uymadığına karar verebilirsiniz.

Giden Kurallar

Giden kurallar, Avira Güvenlik Duvarı tarafından giden veri trafiğini denetlemek için tanımlanır. Şu protokollerden biri için giden kural tanımlayabilirsiniz: IP, ICMP, UDP ve TCP. Bkz. Yeni kural ekle.

Uyarı
Bir paket filtrelendiğinde, karşılık gelen kurallar art arda uygulanır; bu nedenle kural sırası çok önemlidir. Yalnızca ne yaptığınızın tamamen farkındaysanız kural sırasını değiştirin.

Kuralları yönetme düğmeleri

Düğme	Açıklama
Kural ekle	Yeni bir kural oluşturmanıza olanak sağlar. Bu düğmeye basarsanız "**Yeni kural ekle**" iletişim kutusu açılır. Bu iletişim kutusunda yeni kurallar seçebilirsiniz.
Kuralı kaldır	Seçilen kuralı kaldırır.
Kural yukarı	Seçilen kuralı bir satır yukarı taşır; başka bir deyişle, kural önceliğini yükseltir.
Kural aşağı	Seçilen kuralı bir satır aşağı taşır; başka bir deyişle, kural önceliğini düşürür.
Kuralı yeniden adlandır	Seçilen kurala başka bir ad vermenize olanak sağlar.

Not
Bireysel bağdaştırıcılar için veya bilgisayarda bulunan tüm bağdaştırıcılar için yeni kurallar ekleyebilirsiniz. Tüm bağdaştırıcılara ilişkin bir bağdaştırıcı kuralı eklemek için görüntülenen bağdaştırıcı hiyerarşisinden **Bilgisayarım**'ı seçin ve **Kural ekle** düğmesini tıklatın. Bkz. Yeni kural ekle.

Not
Bir kuralın konumunu değiştirmek için, fareyi kullanarak ta kuralı istediğiniz konuma sürükleyebilirsiniz.

Uygulama listesi

Uygulamaların ağlara nasıl erişeceğini belirten kurallar oluşturmak için uygulama listesini kullanabilirsiniz. Listelere uygulamalar ekleyebilir ve bağlam menüsü kullanarak seçilen uygulama için **İzin Ver** ve **Reddet** kurallarını ayarlayın:

- **İzin Ver** kuralına izin verilen uygulamalar tarafından ağlara erişin.
- **Reddet** kuralının reddedildiği uygulamalar tarafından ağlara erişin.

Uygulamalar eklendiğinde, **İzin Ver** kuralı ayarlanır.

Uygulama listesi

Bu tablo, kuralların tanımlandığı uygulamaların listesini gösterir. Semboller, uygulamalar tarafından ağ erişimine izin mi verildiğini yoksa red mi edildiğini belirtir. Uygulamalar için kurallar, bir bağlam menüsü kullanılarak değiştirilebilir.

Düğmeler

Düğme	Açıklama
Yola göre ekle	Bu düğme, uygulamaları seçebileceğiniz bir iletişim kutusunu açar. "**İzin ver**" kuralı ile uygulama listesine uygulama eklenir. "**Yola göre ekle**" seçeneğini kullanırsanız, eklenen Güvenlik Duvarı uygulaması, yol ve dosya adıyla tanımlanır.
md5 öğesine göre ekle	Bu düğme, uygulamaları seçebileceğiniz bir iletişim kutusunu açar. "**İzin ver**" kuralı ile uygulama listesine uygulama eklenir. "**md5 kullanarak ekle**" seçeneğini kullanırsanız, tüm eklenen uygulamalar, MD5 sağlama toplamı kullanılarak benzersiz şekilde tanımlanır. Bu, Güvenlik Duvarı'nın dosya içeriği üzerindeki değişiklikleri tanımlamasına olanak sağlar. Bir güncellemenin ardından uygulama değişirse, örneğin, söz konusu kuralı içeren uygulama otomatik olarak uygulama listesinden kaldırılır. Bir değişikliğin ardından, uygulama yeniden listeye eklenmelidir ve istenen kural yeniden uygulanır.
Grup ekle	Bu düğme, bir dizin seçebileceğiniz bir iletişim kutusunu açar. Seçilen yoldaki tüm uygulamalar, "**İzin ver**" kuralı ile uygulama listesine eklenir.
Kaldır	Seçilen uygulama kuralı kaldırıldı.
Tümünü kaldır	Tüm uygulama kuralları kaldırılır.

Güvenilen üreticiler

Güvenilen yazılım üreticilerinin bir listesi, **Güvenilen üreticiler** altında görüntülenir. Listelenen yazılım üreticilerinin uygulamalarına, ağ erişimi verilir. Listeye üretici ekleyebilir ve listeden üreticileri kaldırabilirsiniz.

Üreticiler

Bu liste, güvenilen olarak sınıflandırılan tüm üreticileri gösterir.

Düğmeler

Düğme	Açıklama
Ekle	Bu düğme, uygulamaları seçebileceğiniz bir iletişim kutusunu açar. Uygulama üreticisi oluşturulur ve güvenilen üreticiler listesine eklenir.
Grup ekle	Bu düğme, bir dizin seçebileceğiniz bir iletişim kutusunu açar. Seçilen yoldaki tüm uygulamaların üreticileri oluşturulur ve güvenilen üreticiler listesine eklenir.
Kaldır	Vurgulanan girdi, güvenilen üreticiler listesinden kaldırılır. Seçilen sağlayıcıyı listeden kalıcı olarak kaldırmak için, yapılandırma penceresinde "**Uygula**" veya "**Tamam**" seçeneğini tıklatın.
Tümünü kaldır	Tüm girdiler, güvenilen üreticiler listesinden kaldırılır.
Yeniden yükle	Yapılan değişiklikler geri alınır. Kaydedilen son liste yüklenir.

Not
Listeden üreticileri kaldırır ve **Uygula** seçeneğini işaretlerseniz, üreticiler listeden kalıcı olarak kaldırılır. **Yeniden Yükle** seçeneği ile değişiklik geri alınamaz.

Not
Güvenlik Duvarı güvenilen üreticiler listesine girdi eklemeden önce uygulama kurallarını öncelik sırasına koyar: Bir uygulama kuralı oluşturmuş iseniz ve uygulama sağlayıcı güvenilen üreticiler listesinde yer alıyorsa, uygulama kuralı yürütülür.

Diğer ayarlar

Bildirimler

Bildirimler, Güvenlik Duvarı'ndan masaüstü bildirimi almak istediğiniz olayları tanımlar.

Bağlantı noktası taraması

Seçenek etkinleştirilirse, bir bağlantı noktası taramasının Güvenlik Duvarı tarafından algılanması durumunda bir masaüstü bildirimi alırsınız.

Baskın

Seçenek etkinleştirilirse, bir baskın saldırısının Güvenlik Duvarı tarafından algılanması durumunda bir masaüstü bildirimi alırsınız.

Engellenen uygulamalar

Seçenek etkinleştirilirse, Güvenlik Duvarı'nın bir uygulamanın ağ etkinliğini reddetmesi, başka bir deyişle engellemesi durumunda bir masaüstü bildirimi alırsınız.

Engellenen IP

Seçenek etkinleştirilirse, Güvenlik Duvarı'nın bir IP adresinden gelen veri trafiğini reddetmesi, başka bir deyişle engellemesi durumunda bir masaüstü bildirimi alırsınız.

Açılır pencere ayarları

İşlem başlatma yığınını incele

Bu seçenek etkinleştirilirse, işlem yığını incelemesi daha doğru bir denetime olanak sağlar. Güvenlik Duvarı, yığındaki güvenilir olmayan tüm işlemlerin gerçekte alt işlemleri üzerinden ağa erişmekte olabileceğini varsayar. Bu nedenle, işlem yığınındaki güvenilir olmayan her işlem için farklı bir açılır pencere açılacaktır. Bu seçenek, varsayılan ayar olarak devre dışı bırakılır.

İşlem başına birden çok açılır pencereye izin ver

Bu seçenek etkinleştirilirse, bir uygulama her ağ bağlantısı yaptığında bir açılır pencere tetiklenir. Alternatif olarak, yalnızca birinci bağlantı girişiminde bilgilendirilirsiniz. Bu seçenek, varsayılan ayar olarak devre dışı bırakılır.

Görüntü ayarları

Bu uygulama için eylemi hatırla

Her zaman etkin

Bu seçenek etkinleştirildiğinde, "**Ağ olayı**" iletişim kutusunun "**Bu uygulama için eylemi hatırla**" seçeneği, varsayılan ayar olarak etkinleştirilir. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

Her zaman devre dışı

Bu seçenek etkinleştirildiğinde, "**Ağ olayı**" iletişim kutusunun "**Bu uygulama için eylemi hatırla**" seçeneği, varsayılan ayar olarak devre dışı bırakılır.

İmzalanan uygulamalar için etkin

Bu seçenek etkinleştirildiğinde, "**Ağ olayı**" iletişim kutusunun "**Bu uygulama için eylemi hatırla**" seçeneği, imzalanan uygulamalar tarafından ağ erişimi sırasında otomatik olarak etkinleştirilir. Uygulama üreticileri şunlardır: Microsoft, Mozilla, Opera, Yahoo, Google, Hewlet Packard, Sun, Skype, Adobe, Lexmark, Creative Labs, ATI, nVidia.

Son kullanılan durumu hatırla

Bu seçenek etkinleştirildiğinde, "**Ağ olayı**" iletişim kutusunun "**Bu uygulama için eylemi hatırla**" seçeneği, son ağ olayıyla aynı şekilde etkinleştirilir. "**Bu uygulama için eylemi hatırla**" seçeneği etkinleştirilmişse, aşağıdaki ağ olayı için bu seçenek etkinleştirilir. Son ağ olayı için "**Bu uygulama için eylemi hatırla**" seçeneği devre dışı bırakılmışsa, aşağıdaki ağ olayı için de bu seçenek devre dışı bırakılır.

Ayrıntıları göster

Bu yapılandırma seçenekleri grubunda, **Ağ olayı** penceresinde ayrıntılı bilgilerin görüntüsünü ayarlayabilirsiniz.

İstek üzerine ayrıntıları göster

Bu seçenek etkinleştirilirse, ayrıntılı bilgiler yalnızca istek üzerine "**Ağ olayı**" penceresinde görüntülenir; başka bir deyişle ayrıntılı bilgiler, "**Ağ olayı**" penceresinde "**Ayrıntıları göster**" düğmesi tıklatılarak görüntülenir.

Her zaman ayrıntıları göster

Bu seçenek etkinleştirilirse, ayrıntılı bilgiler her zaman "**Ağ olayı**" penceresinde görüntülenir.

Son kullanılan durumu hatırla

Bu seçenek etkinleştirilirse, ayrıntılı bilgilerin görünümü, önceki ağ olayıyla aynı şekilde yönetilir. Son ağ olayı sırasında ayrıntılı bilgiler görüntülendiyse veya ayrıntılı bilgilere erişildiyse, aşağıdaki ağ olayı için ayrıntılı bilgiler görüntülenir. Son ağ olayı sırasında ayrıntılı bilgiler gizlendiyse ve görüntülenmediyse, aşağıdaki ağ olayı için ayrıntılı bilgiler görüntülenmez.

Yeni kural ekle

Bu pencerede yeni gelen ve giden kurallar seçebilirsiniz. Seçilen kural, Bağdaştırıcı kuralları penceresindeki varsayılan bilgilere dahil edilir ve bu konumda daha ayrıntılı olarak tanımlanabilir. Gelen ve giden kurallara ek olarak daha fazla kural kullanılabilir.

Olası kurallar

Eşler Arası ağa izin ver

Eşler arası bağlantılara izin verir: 4662 Numaralı Bağlantı Noktasında gelen TCP iletişimleri ve 4672 Numaralı Bağlantı Noktasında gelen UDP iletişimleri.

TCP bağlantı noktası

Bağlantı fareyle tıklatıldığında, izin verilen TCP bağlantı noktasını girebileceğiniz bir iletişim kutusu görüntülenir.

UDP bağlantı noktası

Bağlantı fareyle tıklatıldığında, izin verilen UDP bağlantı noktasını girebileceğiniz bir iletişim kutusu görüntülenir.

VMWARE bağlantılarına izin ver

VMWare sistemleri arasında iletişime izin verir.

IP'yi engelle

Belirtilen bir IP adresinden gelen tüm trafiği engeller.

Internet Protokolü sürümü

Bağlantıyı fareyle tıklatarak, IPv4 veya IPv6 seçebilirsiniz.

IP adresi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 adresini girebileceğiniz bir iletişim kutusu açılır.

Alt ağı engelle

Belirtilen bir IP adresinden ve alt ağ maskesinden gelen tüm trafiği engeller.

Internet Protokolü sürümü

Bağlantıyı fareyle tıklatarak, IPv4 veya IPv6 seçebilirsiniz.

IP adresi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 adresini girebileceğiniz bir iletişim kutusu açılır.

Alt ağ maskesi

Bağlantı fareyle tıklatıldığında, gerekli alt ağ maskesini girebileceğiniz bir iletişim kutusu açılır.

IP'ye izin ver

Belirtilen bir IP adresinden gelen tüm trafiğe izin verir.

Internet Protokolü sürümü

Bağlantıyı fareyle tıklatarak, IPv4 veya IPv6 seçebilirsiniz.

IP adresi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 adresini girebileceğiniz bir iletişim kutusu açılır.

Alt ağa izin ver

Belirtilen bir IP adresinden ve alt ağ maskesinden gelen tüm trafiğe izin verir.

Internet Protokolü sürümü

Bağlantıyı fareyle tıklatarak, IPv4 veya IPv6 seçebilirsiniz.

IP adresi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 adresini girebileceğiniz bir iletişim kutusu açılır.

Alt ağ maskesi

Bağlantı fareyle tıklatıldığında, gerekli alt ağ maskesini girebileceğiniz bir iletişim kutusu açılır.

Web sunucusuna izin ver

80 Numaralı Bağlantı Noktası üzerindeki bir web sunucusuna izin verir: 80 Numaralı Bağlantı Noktası üzerinde gelen TCP iletişimi.

Bağlantı noktası

Bağlantı fareyle tıklatıldığında, web sunucusu tarafından kullanılan bağlantı noktasını girebileceğiniz bir iletişim kutusu görüntülenir.

VPN bağlantılarına izin ver

VPN (Sanal Özel Ağ) bağlantılarına belirli bir IP ile izin verir: x bağlantı noktalarında gelen UDP veri trafiği, x bağlantı noktalarında gelen TCP veri trafiği, ESP(50), GRE(47) protokolleri ile gelen IP veri trafiği

Internet Protokolü sürümü

Bağlantıyı fareyle tıklatarak, IPv4 veya IPv6 seçebilirsiniz.

IP adresi

Bu bağlantı fareyle tıklatıldığında, gerekli IPv4 veya IPv6 adresini girebileceğiniz bir iletişim kutusu açılır.

Uzak Masaüstü bağlantısına izin ver

3389 Numaralı Bağlantı Noktasında "Uzak Masaüstü" bağlantılarına (Uzak Masaüstü Protokolü) izin verir

Bağlantı noktası

Bağlantı fareyle tıklatıldığında, izin verilen uzak masaüstü bağlantısı için kullanılacak bağlantı noktasını girebileceğiniz bir iletişim kutusu görüntülenir.

VNC bağlantısına izin ver

5900 Numaralı Bağlantı Noktasında VNC (Sanal Ağ Bilgi İşlem) bağlantılarına izin verir.

Bağlantı noktası

Bağlantı fareyle tıklatıldığında, izin verilen uzak masaüstü bağlantısı için kullanılacak bağlantı noktasını girebileceğiniz bir iletişim kutusu görüntülenir.

Dosya ve Yazıcı paylaşımına izin ver

Yazıcı ve dosya onaylarına erişime izin verir: Belirtilen bir IP adresinden 137, 139 Numaralı Bağlantı Noktalarında gelen TCP veri trafiği ve 445 Numaralı Bağlantı Noktasında gelen UDP veri trafiği.

Olası gelen kurallar

- Gelen IP kuralı
- Gelen ICMP kuralı
- Gelen UDP kuralı
- Gelen TCP kuralı
- Gelen IP Protokolü kuralı

Olası giden kurallar

- Giden IP kuralı
- Giden ICMP kuralı
- Giden UDP kuralı
- Giden TCP kuralı
- Giden IP Protokolü kuralı

Not
Olası gelen ve giden kurallara ilişkin seçenekler, ilgili protokollerin önceden tanımlı kurallarına ilişkin seçeneklerle aynıdır (bkz. Güvenlik Duvarı > Bağdaştırıcı kuralları).

Düğmeler

Düğme	Açıklama
Tamam	Vurgulanan kural, yeni bir bağdaştırıcı kuralı olarak dahil edilir.
İptal	Yeni bir kural eklenmeden pencere kapatılır.

8.6.4 Windows Güvenlik Duvarı

Windows 7'den itibaren **İnternet Koruması > Yapılandırma** altındaki **Güvenlik Duvarı** bölümü, Windows Güvenlik Duvarı'nın yapılandırmasından sorumludur.

Windows Güvenlik Duvarı

Etkinleştir Avira tarafından yönetilen Windows Güvenlik Duvarını

Bu seçenek etkinse, Avira Windows Güvenlik Duvarını yönetir.

Ağ profilleri

Ağ profilleri

Windows Güvenlik Duvarı, program ve uygulamaların bilgisayarınıza yetkisiz erişimini üç ağ konumu profiline dayalı olarak engeller:

- Özel ağ: ev veya şirket ağları için
- Genel ağ: kamusal alan ağları için
- Etki alanı ağı: etki alanı kontrol birimi olan ağlar için

Bu profilleri, Avira ürününüzün **İnternet koruması > Windows Güvenlik Duvarı > Ağ profilleri** altındaki yapılandırmasından yönetebilirsiniz.

Bu ağ profilleri hakkında daha ayrıntılı bilgiler için lütfen resmi Microsoft web sitesini ziyaret edin.

> **Uyarı**
> Windows Güvenlik Duvarı aynı kuralları, aynı ağ konumuna ait olan tüm ağlarda kullanır, bu ise, bir program veya uygulamanın çalışmasına izin verdiğinizde, bu program veya uygulamanın aynı profildeki tüm ağlara da erişim kazanacağı anlamına gelir.

Özel ağ

Özel ağ ayarları

Özel ağ ayarları, ev veya şirket ağınızda diğer bilgisayar veya cihazların bilgisayarınıza olan erişimini yönetir. Bu ayarlar varsayılan olarak, özel ağ kullanıcılarının bilgisayarınızı görmesine ve erişmesine izin verir.

Etkinleştir

Bu seçenek etkinse, Windows Güvenlik Duvarı Avira ürünü üzerinden etkinleştirilir ve çalışır.

Gelen tüm bağlantıları engelle

Bu seçenek etkinse, Windows Güvenlik Duvarı, izin verilen tüm uygulamalardan gelen bağlantılar da dahil, bilgisayarınıza bağlanmak için istenmeyen tüm denemeleri reddeder.

Yeni bir uygulama engellendiğinde beni bilgilendir

Bu seçenek etkinse, Windows Güvenlik Duvarı yeni bir program veya uygulamayı engellediği her defasında bir bildirim alırsınız.

Devre dışı bırak (önerilmez)

Bu seçenek etkinse, Windows Güvenlik Duvarı devre dışıdır. Bu seçenek önerilmez, bilgisayarınızı riske sokar.

Genel ağ

Genel ağ ayarları

Genel ağ ayarları, kamusal alan ağlarında diğer bilgisayar veya cihazların bilgisayarınıza olan erişimini yönetir. Bu ayarlar varsayılan olarak, genel ağ kullanıcılarının bilgisayarınızı görmesine ve erişmesine izin vermez.

Etkinleştir

Bu seçenek etkinse, Windows Güvenlik Duvarı Avira ürünü üzerinden etkinleştirilir ve çalışır.

Gelen tüm bağlantıları engelle

Bu seçenek etkinse, Windows Güvenlik Duvarı, izin verilen tüm uygulamalardan gelen bağlantılar da dahil, bilgisayarınıza bağlanmak için istenmeyen tüm denemeleri reddeder.

Yeni bir uygulama engellendiğinde beni bilgilendir

Bu seçenek etkinse, Windows Güvenlik Duvarı yeni bir program veya uygulamayı engellediği her defasında bir bildirim alırsınız.

Devre dışı bırak (önerilmez)

Bu seçenek etkinse, Windows Güvenlik Duvarı devre dışıdır. Bu seçenek önerilmez, bilgisayarınızı riske sokar.

Etki alanı ağı

Etki alanı ağ ayarları

Etki alanı ağ ayarları, bir etki alanı kontrol birimiyle doğrulayan bir ağda diğer bilgisayar veya cihazların bilgisayarınıza olan erişimini yönetir. Bu ayarlar varsayılan olarak, etki alanının doğrulanmış kullanıcılarının bilgisayarınızı görmesine ve erişmesine izin verir.

Etkinleştir

BU seçenek etkinse, Windows Güvenlik Duvarı Avira ürünü üzerinden etkinleştirilir ve çalışır.

Gelen tüm bağlantıları engelle

Bu seçenek etkinse, Windows Güvenlik Duvarı, izin verilen tüm uygulamalardan gelen bağlantılar da dahil, bilgisayarınıza bağlanmak için istenmeyen tüm denemeleri reddeder.

Yeni bir uygulama engellendiğinde beni bilgilendir

Bu seçenek etkinse, Windows Güvenlik Duvarı yeni bir program veya uygulamayı engellediği her defasında bir bildirim alırsınız.

Devre dışı bırak (önerilmez)

Bu seçenek etkinse, Windows Güvenlik Duvarı devre dışıdır. Bu seçenek önerilmez, bilgisayarınızı riske sokar.

> **Not**
> Bu seçenek ancak bilgisayarınız bir ağa bir etki alanı kontrol birimiyle bağlandığında kullanılabilir.

Uygulama kuralları

Windows Güvenlik Duvarı > Uygulama kuralları altındaki bağlantıyı tıklarsanız, yeniden Windows Güvenlik Duvarı yapılandırmasının **İzin verilen uygulamalar ve özellikler** menüsüne yönlendirilirsiniz.

Gelişmiş ayarlar

Windows Güvenlik Duvarı > Gelişmiş ayarlar seçeneğini tıklattığınızda, yeniden Windows Güvenlik Duvarı yapılandırmasının **Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı** menüsüne yönlendirilirsiniz.

8.7 Web Koruması

Yapılandırma > İnternet Koruması altındaki **Web Koruması** bölümü Web Koruması'nın yapılandırmasından sorumludur.

8.7.1 Tara

Web Koruması, Internet'te web tarayıcınızda yüklediğiniz web sayfalarından bilgisayarınıza ulaşan virüslere veya zararlı yazılımlara karşı sizi korur. Web Koruması bileşeninin davranışını ayarlamak için **Tara** seçeneği kullanılabilir.

Tara

Web Koruması'nı etkinleştir

Bu seçenek etkinleştirilirse, Web Koruması işlevi etkindir.

IPv6 desteğini etkinleştir

Bu seçenek etkinleştirilirse, Internet Protokolü sürüm 6, Web Koruması tarafından desteklenir. Bu seçenekler Windows 8'in yeni ya da değiştirilen kurulumları için geçerli değildir.

Sürücü koruması

Sürücü koruması, satır içi çerçeveler olarak da bilinen I-Frames uygulamalarını engellemek için ayar yapmanıza olanak sağlar. I-Frame uygulamaları, HTML öğeleridir; başka bir deyişle, Internet sayfalarının bir web sayfası alanını sınırlayan öğeleridir. I-Frame uygulamaları, farklı web içeriklerini (genellikle diğer URL'leri) tarayıcının alt penceresinde bağımsız belgeler olarak yüklemek ve görüntülemek için kullanılabilir. I-Frame uygulamaları daha çok başlık sayfası reklamları için kullanılır. Bazı durumlarda, zararlı yazılımları gizlemek için I-Frame uygulamaları kullanılır. Bu durumlarda, I-Frame alanı tarayıcıda genellikle görünmez veya neredeyse görünmez olur. **Şüpheli I-Frame uygulamalarını engelle** seçeneği, I-Frame uygulamalarının yüklenmesini denetlemenize ve engellemenize olanak sağlar.

Şüpheli I-frame uygulamalarını engelle

Bu seçenek etkinleştirilirse, istediğiniz web sayfalarındaki I-Frame uygulamaları, belirli ölçütlere göre taranır. İstenen bir web sayfasında şüpheli I-Frame çerçeveleri varsa, I-Frame engellenir. I-Frame penceresinde bir hata iletisi görüntülenir.

Algılama durumunda eylem

Bir virüs veya istenmeyen program algılandığında Web Koruması tarafından gerçekleştirilecek eylemleri tanımlayabilirsiniz.

Etkileşimli

Bu seçenek etkinleştirilirse, istek üzerine tarama sırasında bir virüs veya istenmeyen program algılandığında etkilenen dosyaya ne yapılacağını seçebileceğiniz bir iletişim kutusu görüntülenir. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

İlerleme çubuğunu göster

Bu seçenek etkinleştirilirse, web sitesi içeriğinin karşıdan yüklenmesinin 20 saniyelik zaman aşımını geçmesi durumunda bir karşıdan yükleme ilerleme çubuğuyla birlikte masaüstü bildirimi görüntülenir. Bu masaüstü bildirimi özellikle geniş veri hacimlerine sahip web sitelerinin karşıdan yüklenmesi için tasarlanmıştır: Web Koruması ile geziniyorsanız, web sitesi içerikleri Internet tarayıcısında görüntülenmeden önce virüs ve zararlı yazılımlara karşı tarandığından, Internet tarayıcısına artımlı olarak karşıdan yüklenmez. Bu seçenek, varsayılan ayar olarak devre dışı bırakılır.

İzin verilen eylemler

Bu kutuda, bir virüs algılaması durumunda görüntülenmesi seçilebilen eylemler belirtilebilir. Bunun için karşılık gelen seçenekleri etkinleştirmeniz gerekir.

Erişimi reddet

Web sunucusundan istenen web sitesi ve/veya aktarılan veri ya da dosyalar, web tarayıcınıza gönderilmez. Web tarayıcısında, erişimin reddedildiğini bildiren bir hata iletisi görüntülenir. rapor işlevi etkinleştirilirse, Web Koruması, algılamayı rapor dosyasına kaydeder.

Karantinaya taşı

Bir virüs veya zararlı yazılım algılanması durumunda, web sunucusundan istenen web sitesi ve/veya aktarılan veri ve dosyalar, karantinaya taşınır. Etkilenen dosya, bilgilendirici bir değere sahipse karantina yöneticisinden kurtarılabilir veya gerekirse, Avira Zararlı Yazılım Araştırma Merkezi'ne gönderilir.

Yoksay

Web sunucusundan istenen web sitesi ve/veya aktarılan veri ve dosyalar, Web Koruması tarafından web tarayıcınıza iletilir.

Varsayılan

Bu düğme, bir virüs algılandığında varsayılan olarak iletişim kutusunda etkinleştirilecek bir eylem seçmenize olanak sağlar. Varsayılan olarak etkinleştirilecek eylemi seçin ve "Varsayılan" düğmesini tıklatın.

Daha fazla bilgi için burayı tıklatın.

Otomatik

Bu seçenek etkinleştirilirse, bir virüs algılaması oluşması durumunda iletişim kutusu görüntülenmez. Web Koruması, bu bölümde birincil ve ikincil eylem olarak önceden tanımladığınız ayarlara göre hareket eder.

Algılama uyarılarını görüntüle

Bu seçenek etkinleştirilirse, her virüs veya istenmeyen program algılandığında bir uyarı görüntülenerek yürütülmekte olan eylemleri gösterir.

Birincil eylem

Birincil eylem, Web Koruması bir virüs veya istenmeyen program bulduğunda gerçekleştirilen eylemdir.

Erişimi reddet

Web sunucusundan istenen web sitesi ve/veya aktarılan veri ya da dosyalar, web tarayıcınıza gönderilmez. Web tarayıcısında, erişimin reddedildiğini bildiren bir hata iletisi görüntülenir. rapor işlevi etkinleştirilirse, Web Koruması, algılamayı rapor dosyasına kaydeder.

Karantinaya taşı

Bir virüs veya zararlı yazılım algılanması durumunda, web sunucusundan istenen web sitesi ve/veya aktarılan veri ve dosyalar, karantinaya taşınır. Etkilenen dosya, bilgilendirici bir değere sahipse karantina yöneticisinden kurtarılabilir veya gerekirse, Avira Zararlı Yazılım Araştırma Merkezi'ne gönderilir.

Yoksay

Web sunucusundan istenen web sitesi ve/veya aktarılan veri ve dosyalar, Web Koruması tarafından web tarayıcınıza iletilir. Dosyaya erişime izin verilir ve dosya yoksayılır.

Uyarı
Etkilenen dosya, iş istasyonunuzda etkin kalır! Bu, iş istasyonunuzda ciddi hasara neden olabilir!

Engellenen istekler

Engellenen istekler bölümünde, Web Koruması tarafından engellenecek dosya türlerini ve MIME türlerini (aktarılan verilerin içerik türleri) belirtebilirsiniz. Web filtresi bilinen kimlik avı ve zararlı yazılım URL'lerini engellemenizi sağlar. Web Koruması, Internet'ten bilgisayar sisteminize veri aktarımını önler.

Web Koruması aşağıdaki dosya türlerini / MIME Türlerini engeller

Listedeki tüm dosya türleri ve MIME türleri (aktarılan veriler için içerik türleri), Web Koruması tarafından engellenir.

Giriş kutusu

Bu kutuya, Web Koruması'nın engellemesini istediğiniz MIME türlerinin ve dosya türlerinin adlarını girin. Dosya türleri için, dosya uzantısını girin; örn. **.htm**. MIME türleri için, ortam türünü ve gerekirse alt türü belirtin. İki deyim, tek eğik çizgiyle birbirinden ayrılır; örn. **video/mpeg** veya **audio/x-wav**.

Not
Ancak önceden bilgisayar sisteminizde geçici Internet dosyaları olarak depolanan ve Web Koruması tarafından engellenen dosyalar, bilgisayarınızın Internet tarayıcısı tarafından yerel olarak Internet'ten karşıdan yüklenebilir. Geçici Internet dosyaları, web sitelerine daha hızlı erişilebilmesi için Internet tarayıcısı tarafından bilgisayarınıza kaydedilen dosyalardır.

Not
Web Koruması > Tara > İstisnalar konumundaki dışarıda bırakılan dosya ve MIME türleri listesine girilmişse, engellenmiş dosya ve MIME türlerinin listesi yok sayılır.

Not
Dosya türleri ve MIME türleri girilirken, joker karakterler (herhangi sayıda karakter için * veya tek bir karakter için ?) kullanılamaz.

MIME türleri: Ortam türü örnekleri:

- `text` = metin dosyaları için
- `image` = grafik dosyaları için
- `video` = video dosyaları için
- `audio` = ses dosyaları için
- `application` = belirli bir programa bağlantılı dosyalar için

Dışarıda bırakılan dosya ve MIME türleri örnekleri

- `application/octet-stream` = application/octet-stream MIME türü dosyalar (yürütülebilir dosyalar *.bin, *.exe, *.com, *dll, *.class), Web Koruması tarafından engellenir.
- `application/olescript` = application/olescript MIME türü dosyalar (ActiveX komut dosyaları *.axs), Web Koruması tarafından engellenir.
- `.exe` = .exe uzantısına sahip tüm dosyalar (yürütülebilir dosyalar) Web Koruması tarafından engellenir.
- `.msi` = .msi uzantısına sahip tüm dosyalar (Windows Installer dosyaları) Web Koruması tarafından engellenir.

Ekle

Bu düğme, giriş alanından görüntüleme penceresine MIME ve dosya türlerini kopyalamanıza olanak sağlar.

Sil

Bu düğme, seçilen girdiyi listeden siler. Bir girdi seçilmediyse, bu düğme devre dışıdır.

Web filtresi

Web filtresi bir iç veritabanını temel alır, her gün güncellenir ve böylece içeriğe göre URL'ler sınıflandırılır.

Web filtresini etkinleştir

Bu seçenek etkinleştirildiğinde, Web filtresi listesindeki seçili kategorilerle eşleşen tüm URL'ler engellenir.

Web filtresi listesi

Web filtresi listesinde, URL'leri Web Koruması tarafından engellenecek içerik kategorilerini seçebilirsiniz.

Not
Web filtresi Web Koruması > Tara > İstisnalar altındaki dışarıda bırakılan URL'ler listesindeki girdiler için yoksayılır.

Not
İstenmeyen posta URL'leri istenmeyen e-postalarla gönderilen URL'lerdir. **Sahtekarlık / Dolandırıcılık** kategorisi, "Abonelik Süresi Dolan" web sayfalarını ve maliyetleri sağlayıcı tarafından gizlenen diğer hizmet tekliflerini içerir.

İstisnalar

Bu seçenekler, Web Koruması taraması için MIME türlerini (aktarılan veriler için içerik türleri) ve URL'lerin (Internet adresleri) dosya türlerini temel alarak istisnalar ayarlamanıza olanak sağlar. Belirtilen MIME türleri ve URL'ler, Web Koruması tarafından yoksayılır; başka bir deyişle, bu veriler bilgisayar sisteminize aktarılırken virüs ve zararlı yazılımlara karşı taranmaz.

Web Koruması tarafından atlanan MIME türleri

Bu alanda, tarama sırasında Web Koruması tarafından yok sayılacak MIME türlerini (aktarılan veriler için içerik türleri) seçebilirsiniz.

Web Koruması tarafından atlanan dosya türleri/MIME türleri (kullanıcı tanımlı)

Listedeki tüm MIME türleri (aktarılan veriler için içerik türleri), tarama sırasında Web Koruması tarafından yok sayılır.

Giriş kutusu

Bu kutuya, tarama sırasında Web Koruması tarafından yoksayılacak MIME türlerinin ve dosya türlerinin adını girebilirsiniz. Dosya türleri için, dosya uzantısını girin; örn. **.htm**. MIME türleri için, ortam türünü ve gerekirse alt türü belirtin. İki deyim, tek eğik çizgiyle birbirinden ayrılır; örn. **video/mpeg** veya **audio/x-wav**.

Not
Dosya türleri ve MIME türleri girilirken, joker karakterler (herhangi sayıda karakter için * veya tek bir karakter için ?) kullanılamaz.

Uyarı
Dışlama listesindeki tüm dosya türleri ve içerik türleri Internet tarayıcıya engellenmiş isteklerde başka tarama yapılmadan indirilir (Web Koruması > Tara > Engellenen istekler konumunda engellenecek dosya ve MIME türlerinin listesi) veya Web Koruması ile: Dışlama listesindeki tüm girdilerde, dosya ve

MIME türleri listesindeki engellenecek girdiler yoksayılır. Virüs ve zararlı yazılım taraması yapılmaz.

MIME türleri: Ortam türü örnekleri:

- `text` = metin dosyaları için
- `image` = grafik dosyaları için
- `video` = video dosyaları için
- `audio` = ses dosyaları için
- `application` = belirli bir programa bağlantılı dosyalar için

Dışarıda bırakılan dosya ve MIME türleri örnekleri:

- `audio/` = Tüm ses ortam türündeki dosyalar, Web Koruması taramaları dışında bırakılır
- `video/quicktime` = Tüm Quicktime alt türündeki video dosyaları (*.qt, *.mov), Web Koruması taramaları dışında bırakılır
- `.pdf` = Tüm Adobe PDF dosyaları, Web Koruması taramaları dışında bırakılır.

Ekle

Bu düğme, giriş alanından görüntüleme penceresine MIME ve dosya türlerini kopyalamanıza olanak sağlar.

Sil

Bu düğme, seçilen girdiyi listeden siler. Bir girdi seçilmediyse, bu düğme devre dışıdır.

Web Koruması tarafından atlanan URL'ler

Bu listedeki tüm URL'ler, Web Koruması taramaları dışında bırakılır.

Giriş kutusu

Bu kutuya, Web Koruması taramaları dışında bırakılacak URL'leri (Internet adresleri) (örn. `www.domainname.com`) girebilirsiniz. Etki alanı düzeyini belirtmek için başta veya sonda noktalar kullanarak URL'nin bölümlerini belirtebilirsiniz: etki alanının tüm sayfaları ve tüm alt etki alanları için `.domainname.com`. Üst düzey etki alanını (`.com` veya `.net`) içeren web sitelerini, sonuna nokta koyarak belirtin: `domainname.`. Bir dizeyi başında veya sonunda nokta ile belirtirseniz, dize bir üst düzey etki alanı olarak yorumlanır; örn. tüm NET etki alanları için `net` (`www.domain.net`).

Not
URL'leri belirtirken herhangi sayıda karakter için * joker karakterini de kullanabilirsiniz. Etki alanı düzeyini belirtmek için başta veya sonda noktalar ile birlikte joker karakterler kullanabilirsiniz:
`.domainname.*`

`*.domainname.com`
`.*name*.com` (geçerli ancak tavsiye edilmez)
`name`, gibi nokta içermeyen gösterimler bir üst düzey etki alanına aittir ve tavsiye edilmez.

Uyarı
Dışarıda bırakılan URL'ler listesindeki tüm web sayfaları Internet tarayıcıya engellenmiş isteklerde web filtresi ile veya Web Koruması ile başka tarama yapılmadan indirilir: Dışarıda bırakılan URL'ler listesindeki tüm girdilerde, web filtresindeki girdiler (bkz. Web Koruması > Tara > Engellenen istekler) yoksayılır. Virüs ve zararlı yazılım taraması yapılmaz. Virüs ve zararlı yazılım taraması yapılmaz. Bu nedenle yalnızca güvenilen URL'ler, Web Koruması taramaları dışında bırakılır.

Ekle

Bu düğme, giriş alanına girilen URL'yi (Internet adresi), görüntüleyici penceresine kopyalamanıza olanak sağlar.

Sil

Bu düğme, seçilen girdiyi listeden siler. Bir girdi seçilmediyse, bu düğme devre dışıdır.

Örnekler: Atlanan URL'ler

- `www.avira.com` -VEYA- `www.avira.com/*`
  = `www.avira.com` etki alanına sahip tüm URL'ler Web Koruması taraması dışında bırakılır: *www.avira.com/en/pages/index.php*, *www.avira.com/en/support/index.html*, *www.avira.com/en/download/index.html*, vb.
  `www.avira.de` etki alanını içeren tüm URL'ler, Web Koruması taramaları dışında bırakılmaz.
- `avira.com` -VEYA- `*.avira.com`
  = İkinci ve üst düzey etki alanına `avira.com` sahip tüm URL'ler are Web Koruması taramaları dışında bırakılır: Gösterim tüm mevcut `.avira.com` alt etki alanlarına işaret eder: *www.avira.com*, *forum.avira.com* vb.
- `avira.` -VEYA- `*.avira.*`
  = İkinci düzey etki alanına `avira` sahip tüm URL'ler Web Koruması taramaları dışında bırakılır: Gösterim mevcut `.avira` üst düzey etki alanlarına veya alt etki alanlarına işaret eder: *www.avira.com*, *www.avira.de*, *forum.avira.com*, vb.
- `.*domain*.*`
  `domain` dizesine sahip bir ikinci düzey etki alanı içeren tüm URL'ler Web Koruması taramaları dışında bırakılır: *www.domain.com*, *www.new-domain.de*, *www.sample-domain1.de*, ...
- `net` -VEYA- `*.net`
  = Üst düzey etki alanına `net` sahip tüm URL'ler Web Koruması taramaları dışında bırakılır: *www.name1.net*, *www.name2.net*, vb.

Uyarı
Web Koruması taraması dışında bırakmak istediğiniz URL'leri olabildiğince belirgin şekilde girin. Zararlı yazılım ve istenmeyen programlar dağıtan Internet sayfalarının, dışarıda bırakmalar konumundaki genel belirtimler aracılığıyla Web Koruması taraması dışında bırakılma riski olduğundan, tüm üst düzey etki alanını veya ikinci düzey etki alanının bölümlerini belirtmekten kaçının. En azından eksiksiz ikinci düzey etki alanını ve üst düzey etki alanını belirtmeniz önerilir: `domainname.com`

Buluşsal yöntem

Bu yapılandırma bölümü, tarama motorunun buluşsal yöntemine ilişkin ayarları içerir.

Avira ürünleri, bilinmeyen zararlı yazılımları proaktif olarak; başka bir deyişle hasarlı öğeyle savaşmak için özel bir virüs imzası oluşturulmadan ve bir virüs koruyucu güncellemesi gönderilmeden önce açığa çıkarabilen çok güçlü bir buluşsal yöntem içerir. Virüs algılama, etkilenen kodların, zararlı yazılımların tipik işlevlerine karşı yoğun bir analizini ve araştırmasını içerir. Taranmakta olan kod bu belirgin nitelikleri sergilerse, şüpheli olarak bildirilir. Bu mutlaka kodun zararlı yazılım olduğu anlamına gelmez. Bazen yanlış pozitifler oluşur. Etkilenen kodun nasıl işleneceğiyle ilgili karar, kod kaynağının güvenilir olup olmadığına ilişkin bilgisine göre kullanıcı tarafından alınır.

Makro virüs buluşsal yöntemi

Avira ürününüz son derece güçlü bir makro virüs buluşsal yöntemini içerir. Bu seçenek etkinleştirilirse, bir onarım durumunda ilgili belgedeki tüm makrolar silinir, alternatif olarak şüpheli belgeler yalnızca bildirilir; başka bir deyişle bir uyarı alırsınız. Bu seçenek, varsayılan ayar olarak etkinleştirilir ve önerilir.

Gelişmiş Buluşsal Yöntem Analizi ve Algılaması (AHeAD)

AHeAD etkinleştir

Avira programınız, bilinmeyen (yeni) zararlı yazılımları da algılayabilen, Avira AHeAD teknolojisi şeklinde çok güçlü bir buluşsal yöntem içerir. Bu seçenek etkinleştirilirse, buluşsal yöntemin ne kadar "şiddetli" olacağını tanımlayabilirsiniz. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

Düşük algılama düzeyi

Bu seçenek etkinleştirilirse, daha az bilinen zararlı yazılımlar algılanır; bu durumda yanlış uyarı riski düşüktür.

Orta algılama düzeyi

Bu seçenek güçlü algılama düzeyi ile düşük yanlış uyarı riskinin birleşimidir. Bu buluşsal yöntemin kullanımını seçtiyseniz, orta düzey varsayılan ayar olur.

Yüksek algılama düzeyi

Bu seçenek etkinleştirilirse, çok daha az bilinen zararlı yazılımlar algılanır; ancak yanlış pozitif riski de yüksektir.

8.7.2 Rapor

Web Koruması, kullanıcıya veya yöneticiye, bir algılamanın türü ve yöntemiyle ilgili tam notlar sağlamak için yoğun bir günlük kaydı işlevine sahiptir.

Raporlama

Bu grup, rapor dosyası içeriğinin belirlenmesine olanak sağlar.

Kapalı

Bu seçenek etkinleştirilirse, Web Koruması bir günlük oluşturmaz.
Birden çok virüs veya istenmeyen program içeren deneme sürümlerini yürüttüğünüz zamanlarda olduğu gibi yalnızca özel durumlarda günlük kaydı işlevini kapatmanızı öneririz.

Varsayılan

Bu seçenek etkinleştirilirse, Web Koruması, rapor dosyasında önemli bilgileri (algılamalar, uyarılar ve hatalarla ilgili) kaydederken, daha az önemli bilgiler, gelişmiş netlik için yoksayılır. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

Gelişmiş

Bu seçenek etkinleştirilirse, Web Koruması, rapor dosyasına daha az önemli bilgileri de dahil eder.

Tam

Bu seçenek etkinleştirilirse, Web Koruması, dosya boyutu, dosya türü, tarih, vb. gibi tüm kullanılabilir bilgileri rapor dosyasına dahil eder.

Rapor dosyasını sınırla

Boyutu n MB ile sınırla

Bu seçenek etkinleştirilirse, rapor dosyası belirli bir boyutla sınırlandırılabilir; olası değerler: İzin verilen değerler, 1 ile 100 MB arasındadır. Sistem kaynakları kullanımını en aza indirgemek için rapor dosyasının boyutu sınırlanırken yaklaşık 50 kilobayt fazladan alana izin verilir. Günlük dosyasının boyutu, belirtilen boyutu 50 kilobayt'tan fazla aşarsa, belirtilen boyut %20 küçülünceye kadar eski girdiler silinir.

Rapor dosyasında yazma yapılandırması

Bu seçenek etkinleştirilirse, erişim taraması yapılandırması, rapor dosyasına kaydedilir.

Not
Herhangi bir rapor dosyası kısıtlaması belirtmediyseniz, rapor dosyası 100 MB'ye ulaştığında otomatik olarak eski girdiler silinir. Rapor dosyasının boyutu 80 MB'ye ulaşıncaya kadar girdiler silinir.

8.8 EPosta Koruması

Yapılandırma'nın **EPosta Koruması** bölümü, EPosta Koruması yapılandırmasından sorumludur.

8.8.1 Tara

EPosta Koruması'nı kullanarak gelen e-postaları virüs ve zararlı yazılımlara karşı tarayın. Giden e-postalar virüs ve zararlı yazılımlara karşı EPosta Koruması ile taranabilir. Bilgisayarınız üzerinden bilinmeyen bir bot'tan gönderilen istenmeyen e-postaları türündeki giden e-postalar EPosta Koruması tarafından engellenerek istenmeyen e-postalar önlenebilir.

EPosta Koruması'nı etkinleştir

Bu seçenek etkinleştirilirse, e-posta trafiği EPosta Koruması tarafından izlenir. EPosta Koruması, kullandığınız e-posta sunucusu ile bilgisayar sisteminizdeki e-posta istemci programı arasındaki veri trafiğini denetleyen bir proxy sunucudur: gelen e-postalar varsayılan olarak zararlı yazılımlara karşı taranır. Bu seçenek devre dışı bırakılırsa, EPosta Koruması hizmeti yine başlatılır ancak EPosta Koruması izlemesi devre dışı bırakılır.

Gelen e-postaları tara

Bu seçenek etkinleştirilirse, gelen e-postalar, virüslere, zararlı yazılımlarakarşı taranır. EPosta Koruması, POP3 ve IMAP protokollerini destekler. EPosta Koruması izlemesine ilişkin e-posta almak için e-posta istemcinizin kullandığı gelen kutusu hesabını etkinleştirin.

POP3 hesaplarını izle

Bu seçenek etkinleştirilirse, POP3 hesapları belirtilen bağlantı noktalarında izlenir.

İzlenen bağlantı noktaları

Bu alana, POP3 protokolü tarafından gelen kutusu olarak kullanılacak bağlantı noktasını girmeniz gerekir. Birden çok bağlantı noktaları virgülle ayrılır.

Varsayılan

Bu düğme, belirtilen bağlantı noktasını varsayılan POP3 bağlantı noktasına sıfırlar.

IMAP hesaplarını izle

Bu seçenek etkinleştirilirse, IMAP hesapları belirtilen bağlantı noktalarında izlenir.

İzlenen bağlantı noktaları

Bu alana, IMAP protokolü tarafından gelen kutusu olarak kullanılacak bağlantı noktasını girmeniz gerekir. Birden çok bağlantı noktaları virgülle ayrılır.

Varsayılan

Bu düğme, belirtilen bağlantı noktasını varsayılan IMAP bağlantı noktasına sıfırlar.

Giden e-postaları tara (SMTP)

Bu seçenek etkinleştirilirse, giden e-postalar, virüslere ve zararlı yazılımlara karşı taranır. Bilinmeyen bot'ların gönderdiği istenmeyen posta niteliğindeki e-postalar engellenir.

İzlenen bağlantı noktaları

Bu alana, SMTP protokolü tarafından giden kutusu olarak kullanılacak bağlantı noktasını girmeniz gerekir. Birden çok bağlantı noktaları virgülle ayrılır.

Varsayılan

Bu düğme, belirtilen bağlantı noktasını varsayılan SMTP bağlantı noktasına sıfırlar.

Not
Kullanılan protokolleri ve bağlantı noktalarını doğrulamak için, e-posta istemci programınızda e-posta hesaplarınızın özelliklerini anımsayın. Varsayılan bağlantı noktaları en çok kullanılır.

IPv6 desteğini etkinleştir

Bu seçenek etkinleştirilmişse, Internet Protokol sürümü 6 EPosta Koruması tarafından desteklenmektedir. (Seçenekler Windows 8'in yeni ya da değiştirilen kurulumları için geçerli değildir.)

Algılama durumunda eylem

Bu yapılandırma bölümü, EPosta Koruması bir e-postada veya ekte virüs ya da istenmeyen program bulduğunda gerçekleştirilecek eylemlerin diğer ayarlarını içerir.

Not
Bu eylemler hem gelen e-postalarda bir virüs algılandığında hem de giden e-postalarda bir virüs algılandığında gerçekleştirilir.

Etkileşimli

Bu seçenek etkinleştirilirse, bir e-postada veya ekte virüs ya da istenmeyen program algılandığında, ilgili e-posta veya ekle ne yapılacağını seçebileceğiniz bir iletişim kutusu görüntülenir. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

İlerleme çubuğunu göster

Bu seçenek etkinleştirilirse, EPosta Koruması, e-postaların karşıdan yüklenmesi sırasında bir ilerleme çubuğu gösterir. Bu seçenek yalnızca "**Etkileşimli**" seçeneği belirlenmişse etkinleştirilebilir.

İzin verilen eylemler

Bu kutuda, bir virüs algılaması durumunda görüntülenmesi seçilebilen eylemler belirtilebilir. Bunun için karşılık gelen seçenekleri etkinleştirmeniz gerekir.

Karantinaya taşı

Bu seçenek etkinleştirildiğinde, tüm ekleri içeren e-posta, karantinaya taşınır. Daha sonra karantina yöneticisi aracılığıyla gönderilebilir. Etkilenen e-posta silinir. E-posta metninin gövdesi ve ekler, bir varsayılan metin ile değiştirilir.

Postayı sil

Bu seçenek etkinleştirilirse, bir virüs veya istenmeyen program algılandığında etkilenen e-posta silinir. E-posta metninin gövdesi ve ekler, bir varsayılan metin ile değiştirilir.

Eki sil

Bu seçenek etkinleştirildiyse, etkilenen ek, varsayılan bir metinle değiştirilir. E-posta gövdesi etkilendiyse, silinir ve yerine varsayılan bir metin gelir. E-posta teslim edilir.

Eki karantinaya taşı

Bu seçenek etkinleştirildiyse, etkilenen ek, karantinaya taşınır ve sonra silinir (varsayılan bir metinle değiştirilir). E-posta gövdesi teslim edilir. Etkilenen ek daha sonra karantina yöneticisi aracılığıyla gönderilebilir.

Yoksay

Bu seçenek etkinleştirilirse, bir virüs veya istenmeyen program algılanmasına rağmen etkilenen e-posta teslim edilir.

Varsayılan

Bu düğme, bir virüs algılandığında varsayılan olarak iletişim kutusunda etkinleştirilecek bir eylem seçmenize olanak sağlar. Varsayılan olarak etkinleştirilecek eylemi seçin ve "**Varsayılan"** düğmesini tıklatın.

Otomatik

Bu seçenek etkinleştirilirse, artık bir virüs veya istenmeyen program bulunduğunda size bildirim gönderilmez. EPosta Koruması, bu bölümde tanımladığınız ayarlara göre hareket eder.

Etkilenen e-postalar

"*Etkilenen e-postalar*" için seçilen eylem, EPosta Koruması bir e-postada virüs veya istenmeyen program bulduğunda gerçekleştirilen eylemdir. "Yoksay" seçeneği belirlenirse, bir ekte algılanan virüs ya da istenmeyen program ile ilgili işlemin "*Etkilenen ekler*" konumunda seçilmesi mümkündür.

Sil

Bu seçenek etkinleştirilirse, bir virüs veya istenmeyen program bulunduğunda etkilenen e-posta otomatik olarak silinir. E-posta gövdesi, aşağıda verilen varsayılan metin ile değiştirilir. Aynı şey, e-postanın tüm ekleri için de geçerlidir; bunlar da bir varsayılan metin ile değiştirilir.

Yoksay

Bu seçenek etkinleştirilirse, bir virüs veya istenmeyen program algılanmasına rağmen etkilenen e-posta yoksayılır. Ancak, etkilenen ek ile ne yapılacağına siz karar verebilirsiniz.

Karantinaya taşı

Bu seçenek etkinleştirilirse, bir virüs veya istenmeyen program bulunması durumunda tüm ekler de dahil olmak üzere, e-postanın tamamı Karantinaya yerleştirilir. Gerekirse, daha sonra geri yüklenebilir. Etkilenen e-posta silinir. E-posta gövdesi, aşağıda verilen varsayılan metin ile değiştirilir. Aynı şey, e-postanın tüm ekleri için de geçerlidir; bunlar da bir varsayılan metin ile değiştirilir.

Etkilenen ekler

"*Etkilenen ekler*" seçeneği yalnızca "**Yoksay**" ayarı "*Etkilenen e-postalar*" altında seçildiyse belirlenebilir. Bu seçenek sayesinde şimdi bir ekte virüs veya istenmeyen program bulunması durumunda ne yapılacağına karar verilmesi mümkündür.

Sil

Bu seçenek etkinleştirilirse, bir virüs veya istenmeyen program bulunması durumunda etkilenen ek silinir ve bir varsayılan metin ile değiştirilir.

Yoksay

Bu seçenek etkinleştirilirse, bir virüs veya istenmeyen program algılanmasına rağmen ek yoksayılır ve teslim edilir.

Uyarı
Bu seçeneği belirlerseniz, virüslere ve istenmeyen programlara karşı EPosta Koruması tarafından korunmazsınız. Yalnızca ne yaptığınızdan eminseniz bu öğeyi seçin. E-posta programınızda önizlemeyi devre dışı bırakın, asla ekleri çift tıklatarak açmayın!

Karantinaya taşı

Bu seçenek etkinleştirilirse, etkilenen ek, Karantinaya yerleştirilir ve sonra silinir (bir varsayılan metin ile değiştirilir). Gerekirse, etkilenen ek(ler) daha sonra geri yüklenebilir.

Daha fazla eylem

Bu yapılandırma bölümü, EPosta Koruması bir e-postada veya ekte virüs ya da istenmeyen program bulduğunda gerçekleştirilecek eylemlerin diğer ayarlarını içerir.

Not
Bu eylemler yalnızca gelen e-postalarda bir virüs algılandığında gerçekleştirilir.

Silinen ve taşınan e-postalar için varsayılan metin

Bu kutudaki metin, etkilenen e-posta yerine bir ileti olarak e-postaya eklenir. Bu iletiyi düzenleyebilirsiniz. Bir metin maksimum 500 karakter içerebilir.

Biçimlendirme için aşağıdaki tuş birleşimlerini kullanabilirsiniz:

Ctrl + Enter = bir satır sonu ekler.

Varsayılan

Düğme, düzenleme kutusuna önceden tanımlanmış bir varsayılan metin ekler.

Silinen ve taşınan ekler için varsayılan metin

Bu kutudaki metin, etkilenen ek yerine bir ileti olarak e-postaya eklenir. Bu iletiyi düzenleyebilirsiniz. Bir metin maksimum 500 karakter içerebilir.

Biçimlendirme için aşağıdaki tuş birleşimlerini kullanabilirsiniz:

Ctrl + Enter = bir satır sonu ekler.

Varsayılan

Düğme, düzenleme kutusuna önceden tanımlanmış bir varsayılan metin ekler.

Buluşsal yöntem

Bu yapılandırma bölümü, tarama motorunun buluşsal yöntemine ilişkin ayarları içerir.

Avira ürünleri, bilinmeyen zararlı yazılımları proaktif olarak; başka bir deyişle hasarlı öğeyle savaşmak için özel bir virüs imzası oluşturulmadan ve bir virüs koruyucu güncellemesi gönderilmeden önce açığa çıkarabilen çok güçlü bir buluşsal yöntem içerir. Virüs algılama, etkilenen kodların, zararlı yazılımların tipik işlevlerine karşı yoğun bir analizini ve araştırmasını içerir. Taranmakta olan kod bu belirgin nitelikleri sergilerse, şüpheli olarak bildirilir. Bu mutlaka kodun zararlı yazılım olduğu anlamına gelmez. Bazen yanlış pozitifler oluşur. Etkilenen kodun nasıl işleneceğiyle ilgili karar, kod kaynağının güvenilir olup olmadığına ilişkin bilgisine göre kullanıcı tarafından alınır.

Makro virüs buluşsal yöntemi

Avira ürününüz son derece güçlü bir makro virüs buluşsal yöntemini içerir. Bu seçenek etkinleştirilirse, bir onarım durumunda ilgili belgedeki tüm makrolar silinir, alternatif olarak şüpheli belgeler yalnızca bildirilir; başka bir deyişle bir uyarı alırsınız. Bu seçenek, varsayılan ayar olarak etkinleştirilir ve önerilir.

Gelişmiş Buluşsal Yöntem Analizi ve Algılaması (AHeAD)

AHeAD etkinleştir

Avira programınız, bilinmeyen (yeni) zararlı yazılımları da algılayabilen, Avira AHeAD teknolojisi şeklinde çok güçlü bir buluşsal yöntem içerir. Bu seçenek etkinleştirilirse, buluşsal yöntemin ne kadar "şiddetli" olacağını tanımlayabilirsiniz. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

Düşük algılama düzeyi

Bu seçenek etkinleştirilirse, daha az bilinen zararlı yazılımlar algılanır; bu durumda yanlış uyarı riski düşüktür.

Orta algılama düzeyi

Bu seçenek güçlü algılama düzeyi ile düşük yanlış uyarı riskinin birleşimidir. Bu buluşsal yöntemin kullanımını seçtiyseniz, orta düzey varsayılan ayar olur.

Yüksek algılama düzeyi

Bu seçenek etkinleştirilirse, çok daha az bilinen zararlı yazılımlar algılanır; ancak yanlış pozitif riski de yüksektir.

8.8.2 Genel

İstisnalar

İstisnalar taranıyor

Bu tabloda, EPosta Koruması taramasının dışında bırakılan e-posta adreslerinin listesi gösterilir (beyaz liste).

> **Not**
> Bu istisna listesi, EPosta Koruması tarafından yalnızca gelen e-postalarla ilgili olarak kullanılır.

İstisnalar taranıyor

Giriş kutusu

Bu kutuya, taranmayacak e-posta adresleri listesine eklemek istediğiniz e-posta adresini girersiniz. Ayarlarınıza bağlı olarak, e-posta adresi artık EPosta Koruması tarafından gelecekte taranmaz.

Ekle

Bu düğme ile, giriş kutusuna girilen e-posta adresini, taranmayacak e-posta adresleri listesine ekleyebilirsiniz.

Sil

Bu düğme, vurgulanan bir e-posta adresini listeden siler.

E-posta adresi

Artık taranmayacak e-posta.

Zararlı yazılım

Bu seçenek etkinleştirildiğinde, e-posta adresi artık zararlı yazılıma karşı taranmaz.

Yukarı

Vurgulanan bir e-posta adresini daha yüksek bir konuma taşımak için bu düğmeyi kullanabilirsiniz. Bir girdi vurgulanmadıysa veya vurgulanan adres, listenin birinci konumundaysa, bu düğme etkinleştirilmez.

Aşağı

Vurgulanan bir e-posta adresini daha düşük bir konuma taşımak için bu düğmeyi kullanabilirsiniz. Bir girdi vurgulanmadıysa veya vurgulanan adres, listenin son konumundaysa, bu düğme etkinleştirilmez.

Önbellek

EPosta Koruması önbelleği, taranan e-postalarla ilgili verileri, **EPosta Koruması** altında Kontrol Merkezi'nde istatistiksel veriler olarak görüntüler.

Önbellekteki maksimum e-posta sayisi

Bu alan, EPosta Koruması tarafından önbellekte depolanan maksimum e-posta sayısını ayarlamak için kullanılır. En eski e-postalar en önce silinir.

Bir e-postanın depolanacağı maksimum gün sayısı

Bu kutuya bir e-postanın maksimum depolanacağı süre gün olarak girilir. Bu süreden sonra, e-posta önbellekten kaldırılır.

Önbelleği Boşalt

Önbellekte depolanan e-postaları silmek için bu düğmeyi tıklatın.

Altbilgi

Altbilgi konumunda, gönderdiğiniz e-postalarda görüntülenecek bir e-posta altbilgisi yapılandırabilirsiniz.

Bu işlev, giden e-postaların EPosta Koruması taramasının etkinleştirilmesini gerektirir (**Yapılandırma > EPosta Koruması > Tara**konumundaki **Giden e-postaları tara (SMTP)** seçeneğine bakın). Gönderilen e-postanın bir virüs koruma programı tarafından tarandığını onaylamak için tanımlanmış Avira EPosta Koruması altbilgisini kullanabilirsiniz. Ayrıca kullanıcı tanımlı altbilgi için istediğiniz metni ekleme seçeneğiniz vardır. Her iki altbilgi seçeneğini kullanırsanız, kullanıcı tanımlı metnin önüne Avira EPosta Koruması altbilgisi gelir.

Gönderilecek e-postalar için altbilgi

EPosta Koruması altbilgisi ekle

Bu seçenek etkinleştirilirse, Avira EPosta Koruması altbilgisi, gönderilen e-postanın ileti metninin altında görüntülenir. Avira EPosta Koruması altbilgisi, gönderilen e-postanın virüslere ve istenmeyen programlara karşı Avira EPosta Koruması tarafından tarandığını ve bilinmeyen bir bot'tan gelmediğini onaylar. Avira EPosta Koruması altbilgisi aşağıdaki metni içerir: "*Avira EPosta Koruması [ürün sürümü] [arama motorunun ilk harfleri ve sürüm numarası] [virüs tanım dosyasının ilk harfleri ve sürüm numarası]*" ile taranmıştır.

Aşağıdaki altbilgiyi ekle

Bu seçenek etkinleştirilirse, giriş kutusuna eklediğiniz metin, gönderilen e-postalarda altbilgi olarak görüntülenir.

Giriş kutusu

Bu giriş kutusuna, gönderilen e-postalarda altbilgi olarak görüntülenen bir metin ekleyebilirsiniz.

8.8.3 Rapor

EPosta Koruması, kullanıcıya veya yöneticiye, bir algılamanın türü ve yöntemiyle ilgili tam notlar sağlamak için yoğun bir günlük kaydı işlevine sahiptir.

Raporlama

Bu grup, rapor dosyası içeriğinin belirlenmesine olanak sağlar.

Kapalı

Bu seçenek etkinleştirilirse, EPosta Koruması bir günlük oluşturmaz.
Birden çok virüs veya istenmeyen program içeren deneme sürümlerini yürüttüğünüz zamanlarda olduğu gibi yalnızca özel durumlarda günlük kaydı işlevini kapatmanızı öneririz.

Varsayılan

Bu seçenek etkinleştirilirse, EPosta Koruması, rapor dosyasında önemli bilgileri (algılamalar, uyarılar ve hatalarla ilgili) kaydederken, daha az önemli bilgiler, gelişmiş netlik için yoksayılır. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

Genişletilmiş

Bu seçenek etkinleştirilirse, EPosta Koruması, rapor dosyasına daha az önemli bilgileri de dahil eder.

Tam

Bu seçenek etkinleştirilirse, EPosta Koruması, rapor dosyasına tüm bilgileri dahil eder.

Rapor dosyasını sınırla

Boyutu n MB ile sınırla

Bu seçenek etkinleştirilirse, rapor dosyası belirli bir boyutla sınırlandırılabilir; olası değerler: İzin verilen değerler, 1 ile 100 MB arasındadır. Sistem kaynakları kullanımını en aza indirgemek için rapor dosyasının boyutu sınırlanırken yaklaşık 50 kilobayt fazladan alana izin verilir. Günlük dosyasının boyutu, belirtilen boyutu 50 kilobayt'tan fazla aşarsa, belirtilen boyutun 50 kilobayt aşağısına ulaşılıncaya kadar eski girdiler silinir.

Kısaltmadan önce rapor dosyasını yedekle

Bu seçenek etkinleştirilirse, kısaltmadan önce rapor dosyası yedeklenir. Kaydetme konumu için bkz. Yapılandırma > Genel > Dizinler > Rapor dizini.

Rapor dosyasında yazma yapılandırması

Bu seçenek etkinleştirilirse, EPosta Koruması yapılandırması, rapor dosyasına kaydedilir.

Not
Herhangi bir rapor dosyası kısıtlaması belirtmediyseniz, rapor dosyası 100 MB'ye ulaştığında otomatik olarak yeni bir rapor dosyası oluşturulur. Eski rapor dosyasının bir yedeği oluşturulur. Eski rapor dosyasının üç adede kadar yedeği kaydedilir. En eski yedeklemeler en önce silinir.

8.9 Genel

8.9.1 Tehdit kategorileri

Genişletilmiş tehdit kategorilerinin seçimi

Avira ürününüz sizi bilgisayar virüslerine karşı korur. Ayrıca, aşağıdaki genişletilmiş tehdit kategorilerine göre tarama yapabilirsiniz.

- Reklam Yazılımı
- Reklam Yazılımı/Casus Yazılım
- Uygulamalar
- Arka Kapı İstemcileri
- Numara Çevirici
- Çift Uzantı Dosyaları
- Sahte yazılım
- Oyunlar
- Şakalar

- Kimlik Avı
- Özel etki alanını ihlal eden programlar
- Olağandışı çalışma zamanı paketleyicileri

İlgili kutu tıklatılarak, seçilen tür etkinleştirilir (onay işareti ayarlanır) veya devre dışı bırakılır (onay işareti yoktur).

Tümünü seç

Bu seçenek etkinleştirilirse, tüm türler etkinleştirilir.

Varsayılan değerler

Bu düğme, önceden tanımlı varsayılan değerleri geri yükler.

> **Not**
> Bir tür devre dışı bırakılırsa, ilgili program türü olarak tanınan dosyalar artık belirtilmez. Rapor dosyasına bir girdi yapılmaz.

8.9.2 Gelişmiş koruma

Proaktif

Proaktif'i etkinleştir

Bu seçenek etkinleştirilirse, sisteminizdeki programlar şüpheli eylemlere karşı izlenir ve denetlenir. Tipik zararlı yazılım davranışı algılanırsa, bir ileti alırsınız. Programı engelleyebilir veya programı kullanmaya devam etmek için "**Yoksay**" seçeneğini belirleyebilirsiniz. İzleme işlemine şunlar dahil değildir: Güvenilir olarak sınıflandırılan programlar, izin verilen uygulamalar filtresine varsayılan olarak dahil edilen güvenilir ve imzalanmış programlar ve izin verilen programlar için uygulama filtresine eklediğiniz tüm programlar.

Proaktif, kullanılabilir bir virüs tanımı veya buluşsal yöntemi olmayan yeni ve bilinmeyen tehditlere karşı sizi korur. Proaktif teknolojisi, Gerçek Zamanlı Koruma bileşenine tümleşik olup gerçekleştirilen program eylemlerini izler ve analiz eder. Program davranışı, tipik zararlı yazılım eylem desenlerine karşı denetlenir: Eylem türü ve eylem sıraları. Bir program tipik bir zararlı yazılım davranışı sergilerse, bu bir virüs algılama olarak işlem görür : Programı engelleyebilir ya da bildirimi yoksayarak programı kullanmaya devam edebilirsiniz. Programı güvenilir olarak sınıflandırabilir ve izin verilen programlar için uygulama filtresine ekleyebilirsiniz. **Her zaman engelle** komutunu kullanarak programı, engellenen programlar için uygulama filtresine ekleme seçeneğiniz vardır.

Proaktif bileşeni, şüpheli davranışı tanımlamak için Avira Zararlı Yazılım Araştırma Merkezi tarafından geliştirilen kural kümelerini kullanır. Kural kümeleri Avira veritabanları tarafından sağlanır. Proaktif herhangi bir şüpheli programa ilişkin bilgileri günlük kaydı için Avira

veritabanlarına gönderir. Avira'nın kurulumu sırasında, Avira veritabanlarına veri iletimini devre dışı bırakma seçeneğiniz bulunmaktadır.

> **Not**
> Proaktif teknolojisi henüz 64 bit sistemler için kullanılabilir değildir!

Koruma Bulutu

Koruma Bulutu'nu etkinleştir

Tüm şüpheli dosyaların parmak izleri dinamik çevrimiçi inceleme için Koruma Bulutu'na gönderilir. Yürütülebilir dosyalar anında temiz, etkilenmiş veya bilinmeyen olarak tanımlanır.

Koruma Bulutu kullanıcı tabanımız genelinde meydana gelen siber saldırı girişimlerinin izlendiği bir merkezi konum işlevi görür. Bilgisayarınız üzerinden erişilen dosyalar bulutta kayıtlı dosyaalrın parmak izleri ile karşılaştırılır. Bulutta daha çok tarama yapıldıkça, antivirüs uygulaması işlem yapmak için daha az güce ihtiyaç duyar.

Hızlı sistem tarama görevi yürütüldüğünde zararlı yazılımlar tarafından sık olarak hedeflenen dosya konumlarının listesi oluşturulur. Bu liste yürütülen işlemleri, başlangıçta çalışan programları ve hizmetleri içerir. Her dosyanın "temiz" veya "zararlı yazılım" olarak sınıflandırılacak parmak izi oluşturulur ve Koruma Bulutu'na gönderilir. Bilinmeyen program dosyaları analiz için Koruma Bulutu'na yüklenir.

Şüpheli dosyaları Avira'ya gönderirken manüel olarak onayla

Koruma Bulutu'na gönderilmesi gereken şüpheli dosyaların bir listesini görebilir ve göndermek istediğiniz dosyaları seçebilirsiniz.

Gerçek zamanlı dosya tarama

Bu seçenek etkinleştirilirse bilinmeyen dosyalar kendilerine erişilir erişilmez analiz için Koruma Bulutuna gönderilir.

Avira Koruma Bulutuna yapılan yüklemelerdeki ilerlemeyi göster

Bir pencerede, karşıya yüklenen dosya(lar) ile ilgili aşağıdaki bilgiler, bir ilerleme çubuğu şeklinde görüntülenir:

- dosya kaydetme konumu
- dosya adı
- durum (yükleniyor/inceleniyor)
- durum (temiz/virüslü)

Engellenen uygulamalar

Engellenecek uygulamalar konumuna, zararlı olarak sınıflandırdığınız ve Avira Proaktif'in varsayılan olarak engellemesini istediğiniz uygulamaları girebilirsiniz. Eklenen uygulamalar, bilgisayar sisteminizde yürütülemez. Ayrıca **Bu programı her zaman engelle** seçeneğini belirleyerek, şüpheli program davranışıyla ilgili Gerçek Zamanlı Koruma bildirimleri aracılığıyla engelleme için uygulama filtresine programlar da ekleyebilirsiniz.

Engellenecek uygulamalar

Uygulama

Bu liste, yapılandırma aracılığıyla veya Proaktif bileşeninin bildirimi yoluyla zararlı olarak sınıflandırdığınız tüm uygulamaları içerir. Listedeki uygulamalar, Avira Proaktif tarafından engellenir ve bilgisayar sisteminizde yürütülemez. Engellenen bir program başlatıldığında bir işletim sistemi iletisi görüntülenir. Engellenecek uygulamalar, belirtilen yol ve dosya adı temel alınarak Avira Proaktif tarafından tanımlanır ve içeriklerinden bağımsız olarak engellenir.

Giriş kutusu

Bu kutuya engellemek istediğiniz uygulamayı girin. Uygulamayı tanımlamak için, tam yol, dosya adı ve dosya uzantısı belirtilmelidir. Yol, uygulamanın bulunduğu sürücüyü göstermeli veya bir ortam değişkeniyle başlamalıdır.

Düğme, engellenecek uygulamayı seçebileceğiniz bir pencereyi açar.

Ekle

"**Ekle**" düğmesiyle, giriş kutusunda belirtilen uygulamayı, engellenecek uygulamalar listesine aktarabilirsiniz.

> **Not**
> İşletim sisteminin düzgün çalışması için gerekli uygulamalar eklenemez.

Sil

"**Sil**" düğmesi, vurgulanan uygulamayı, engellenecek uygulamalar listesinden kaldırmanıza olanak sağlar.

İzin verilen uygulamalar

Atlanacak uygulamalar bölümü Proaktif bileşenin izlemesinden muaf tutulacak uygulamaları listeler: güvenilir olarak sınıflandırılan ve varsayılan olarak listeye dahil edilen imzalanmış programlar, güvenilir olarak sınıflandırılan ve uygulama filtresine eklenen tüm uygulamalar: İzin verilen uygulamaları Yapılandırma'daki listeye ekleyebilirsiniz. Ayrıca Gerçek Zamanlı Koruma bildiriminde **Güvenilen program** seçeneğini kullanarak Gerçek

Zamanlı Koruma bildirimleri aracılığıyla şüpheli program davranışına uygulamalar ekleme seçeneğiniz de vardır.

Atlanacak uygulamalar

Uygulama

Bu liste, Proaktif bileşeninin izlemesi dışında bırakılan uygulamaları içerir. Varsayılan kurulum ayarlarında liste, güvenilen üreticilerin imzalanmış uygulamalarını içerir. Yapılandırma aracılığıyla veya Gerçek Zamanlı Koruma bildirimleri aracılığıyla güvenilir olduğunu düşündüğünüz uygulamaları ekleme seçeneğiniz de vardır. Proaktif bileşeni, yolu, dosya adını ve içeriği kullanarak uygulamaları tanımlar. Güncelleme gibi değişiklikler yoluyla bir programa zararlı yazılım eklenebileceğinden, içeriğin denetlenmesini öneririz. Belirtilen **Tür** için bir içerik denetimi yapılıp yapılmayacağına karar verebilirsiniz: "*İçerik*" türü için, yola ve dosya adına göre belirtilen uygulamalar, Proaktif bileşeninin izlemesi dışında bırakılmadan önce dosya içeriği üzerindeki değişikliklere karşı denetlenir. Dosya içerikleri değiştirilmişse, uygulama yeniden Proaktif bileşeni tarafından izlenir. *Yol* türü için, uygulama, Gerçek Zamanlı Koruma izlemesi dışında bırakılmadan önce bir içerik denetimi gerçekleştirilmez. Dışlama türünü değiştirmek için, görüntülenen türü tıklatın.

Uyarı
Yalnızca özel durumlarda *Yol* türünü kullanın. Güncelleme yoluyla bir uygulamaya zararlı kod eklenebilir. Başlangıçta zararsız olan uygulama şimdi zararlı yazılım olmuştur.

Not
Örneğin, Avira ürününüzün tüm uygulama bileşenleri de dahil olmak üzere, bazı güvenilen uygulamalar, listeye dahil edilmemiş olsalar da, varsayılan olarak Proaktif bileşeninin izlemesi dışında bırakılır.

Giriş kutusu

Bu kutuya, Proaktif bileşeninin izlemesi dışında bırakılacak uygulamayı girersiniz. Uygulamayı tanımlamak için, tam yol, dosya adı ve dosya uzantısı belirtilmelidir. Yol, uygulamanın bulunduğu sürücüyü göstermeli veya bir ortam değişkeniyle başlamalıdır.

Düğme, dışarıda bırakılacak uygulamayı seçebileceğiniz bir pencereyi açar.

Ekle

"Ekle" düğmesiyle, giriş kutusunda belirtilen uygulamayı, dışarıda bırakılacak uygulamalar listesine aktarabilirsiniz.

Sil

"**Sil**" düğmesi, vurgulanan uygulamayı, dışarıda bırakılacak uygulamalar listesinden kaldırmanıza olanak sağlar.

8.9.3 Parola

Avira ürününüzü farklı alanlarda bir parola ile koruyabilirsiniz. Bir parola verildiyse, korumalı alanı her açmak istediğinizde sizden bu parola istenir.

Parola

Parola girin

Gerekli parolanızı buraya girin. Güvenlik nedenleriyle, bu alana yazdığınız gerçek karakterlerin yerini yıldız işaretleri (*) alır. Parola yalnızca maksimum 20 karakterden oluşabilir. Parola verildikten sonra, yanlış bir parola girilirse program erişimi reddeder. Boş bir kutu, "Parola yok" anlamına gelir.

Onay

Yukarıya girilen parolayı buraya yeniden girerek onaylayın. Güvenlik nedenleriyle, bu alana yazdığınız gerçek karakterlerin yerini yıldız işaretleri (*) alır.

Not
Parola büyük küçük harfe duyarlıdır!

Parolayla korunan alanlar

Avira ürününüz, bir parolayla tek tek alanları koruyabilir. İlgili kutu tıklatılarak gerektiği şekilde tek tek alanlar için parola isteği devre dışı bırakılabilir veya yeniden etkinleştirilebilir.

Parola korumalı alan	İşlev
Kontrol Merkezi	Bu seçenek etkinleştirilirse, Kontrol Merkezi'ni başlatmak için önceden tanımlı parola gerekir.
Gerçek Zamanlı Koruma'yı etkinleştir / devre dışı bırak	Bu seçenek etkinleştirilirse, Avira Gerçek Zamanlı Koruma'yı etkinleştirmek veya devre dışı bırakmak için önceden tanımlı parola gerekir.

EPosta Koruması'nı etkinleştir/devre dışı bırak	Bu seçenek etkinleştirilirse, EPosta Koruması'nı etkinleştirmek/devre dışı bırakmak için önceden tanımlı parola gerekir.
Güvenlik Duvarı etkinleştir/devre dışı bırak	Bu seçenek etkinleştirilirse, Güvenlik Duvarı'nı etkinleştirmek/devre dışı bırakmak için önceden tanımlı parola gerekir.
Web Koruması'nı etkinleştir / devre dışı bırak	Bu seçenek etkinleştirilirse, Web Koruması'nı etkinleştirmek/devre dışı bırakmak için önceden tanımlı parola gerekir.
Karantina	Bu seçenek etkinleştirilirse, parolayla korunan tüm karantina yöneticisi alanları etkinleştirilir. İlgili kutu tıklatılarak tek tek alanlar için parola sorgusu istek üzerine yeniden devre dışı bırakılabilir veya etkinleştirilebilir.
Etkilenen nesneleri geri yükle	Bu seçenek etkinleştirilirse, bir nesneyi geri yüklemek için önceden tanımlı parola gerekir.
Etkilenen nesneleri yeniden tara	Bu seçenek etkinleştirilirse, bir nesneyi yeniden taramak için önceden tanımlı parola gerekir.
Etkilenen nesne özellikleri	Bu seçenek etkinleştirilirse, bir nesnenin özelliklerini görüntülemek için önceden tanımlı parola gerekir.
Etkilenen nesneleri sil	Bu seçenek etkinleştirilirse, bir nesneyi silmek için önceden tanımlı parola gerekir.

Avira'ya e-posta gönder	Bu seçenek etkinleştirilirse, incelenmek üzere Avira Zararlı Yazılım Araştırma Merkezi'ne bir nesne göndermek için önceden tanımlı parola gerekir.
Etkilenen nesneler kopyalanıyor	Bu seçenek etkinleştirilirse, etkilenen nesneyi kopyalamak için önceden tanımlı parola gerekir.
İş ekle ve değiştir	Bu seçenek etkinleştirilirse, Zamanlayıcı'da işler eklemek ve değiştirmek için önceden tanımlı parola gerekir.
Internet'ten kurtarma CD'sini karşıdan yükle	Bu seçenek etkinleştirilirse, Avira Kurtarma CD'si karşıdan yüklemesini başlatmak için önceden tanımlı parola gerekir.
Yapılandırma	Bu seçenek etkinleştirilirse, program yapılandırması yalnızca önceden tanımlı parola girildikten sonra mümkündür.
Yapılandırmayı el ile değiştir	Bu seçenek etkinleştirilirse, farklı bir yapılandırma profiline el ile geçiş yapmak için önceden tanımlı parola gerekir.
Kurulum / kaldırma	Bu seçenek etkinleştirilirse, programı kurmak veya kaldırmak için önceden tanımlı parola gerekir.

8.9.4 Güvenlik

Autorun

Autorun işlevini engelle

Bu seçenek etkinleştirildiğinde, USB çubuklar, CD ve DVD sürücüleri ve ağ sürücüleri de dahil olmak üzere tüm bağlı sürücülerde Windows autorun işlevinin yürütülmesi engellenir. Windows autorun işlevi sayesinde, veri ortamındaki veya ağ sürücülerindeki dosyalar yükleme ya da bağlantı anında hemen okunur ve böylece dosyalar otomatik olarak başlatılıp kopyalanabilir. Ancak autorun ile birlikte zararlı yazılım ve istenmeyen programlar kurulabileceğinden, bu işlev yüksek bir güvenlik riskini de beraberinde getirir. USB çubuklardaki veriler her an değiştirilebildiğinden, autorun işlevi özellikle, USB çubuklar için kritiktir.

CD ve DVD'leri hariç tut

Bu seçenek etkinleştirildiğinde, CD ve DVD sürücülerde autorun işlevine izin verilir.

Uyarı
Yalnızca güvenilir veri ortamı kullandığınızdan eminseniz CD ve DVD sürücüler için autorun işlevini devre dışı bırakın.

Sistem koruması

Windows ana bilgisayar dosyalarını koru

Bu seçenek etkin olarak ayarlanırsa, Windows ana bilgisayar dosyaları yazmaya karşı korumalıdır. Artık değişiklik mümkün değildir. Örneğin, zararlı yazılımlar sizi istenmeyen web sitelerine yeniden yönlendiremez. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

Ürün koruma

Not
Gerçek Zamanlı Koruma, kullanıcı tanımlı kurulum seçeneği kullanılarak kurulmadıysa, ürün koruma seçenekleri kullanılamaz.

İstenmeyen sonlandırmaya karşı işlemleri koru

Bu seçenek etkinleştirilirse, programın tüm işlemleri, virüsler ve zararlı yazılımlar tarafından istenmeyen sonlandırmaya karşı veya Görev Yöneticisi gibi bir kullanıcı tarafından 'kontrolsüz' sonlandırmaya karşı korunur. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

Gelişmiş işlem koruma

Bu seçenek etkinleştirilirse, programın tüm işlemleri, istenmeyen sonlandırmaya karşı gelişmiş seçeneklerle korunur. Gelişmiş işlem koruması, basit işlem korumasından daha fazla bilgisayar kaynağı gerektirir. Bu seçenek, varsayılan ayar olarak etkinleştirilir. Bu seçeneği devre dışı bırakmak için, bilgisayarınızı yeniden başlatmanız gerekir.

Not
Windows XP 64 bit !

Uyarı
İşlem koruması etkinleştirilirse, diğer yazılım ürünleriyle etkileşim sorunları oluşabilir. Bu durumlarda işlem korumayı devre dışı bırakın.

Değişikliğe karşı dosyaları ve kayıt defteri girdilerini koru

Bu seçenek etkinleştirilirse, programın tüm kayıt defteri girdileri ve tüm program dosyaları (ikili ve yapılandırma dosyaları) değişikliğe karşı korunur. Değişikliğe karşı koruma; kayıt defteri girdilerine veya program dosyalarına kullanıcılar ya da dış programlar tarafından yazma, silme ve bazı durumlarda okuma erişiminin engellenmesini gerektirir. Bu seçeneği etkinleştirmek için, bilgisayarınızı yeniden başlatmanız gerekir.

Uyarı
Bu seçenek devre dışı bırakılırsa, belirli zararlı yazılım türlerinden etkilenen bilgisayarların onarımının başarısız olabileceğini unutmayın.

Not
Bu seçenek etkinleştirildiğinde, yalnızca tarama veya güncelleme istekleri üzerindeki değişiklikler de dahil olmak üzere kullanıcı arabirimi aracılığıyla yapılandırma üzerinde değişiklik yapılabilir.

Not
Windows XP 64 bit !

8.9.5 WMI

Windows Yönetim Araçları desteği

Windows Yönetim Araçları, Windows sistemindeki ayarlara hem yerel hem de uzak okuma ve yazma erişimine olanak sağlamak için komut dosyası ve programlama dillerini kullanan temel bir Windows yönetim teknolojisidir. Avira ürününüz WMI'yı destekler ve arabirim aracılığıyla verilerin (durum bilgileri, istatistiksel veriler, raporlar, planlanmış istekler, vb.) yanı sıra olaylar ve yöntemler de (durdurma ve başlatma işlemleri)sağlar. WMI, size programdan işletim verilerini karşıdan yükleme ve programı kontrol etme seçeneğini sunar. Üreticiden WMI arabirimine ilişkin tam bir başvuru kılavuzu isteyebilirsiniz. Gizlilik sözleşmesini imzaladığınızda, başvuru dosyası PDF biçiminde mevcuttur.

WMI desteğini etkinleştir

Bu seçenek etkinleştirildiğinde, WMI aracılığıyla programdan işletim verilerini karşıdan yükleyebilirsiniz.

Hizmetlerin etkinleştirilmesine/devre dışı bırakılmasına izin ver

Bu seçenek etkinleştirildiğinde, WMI aracılığıyla program hizmetlerini etkinleştirebilir ve devre dışı bırakabilirsiniz.

8.9.6 Olaylar

Olay veritabanının boyutunu sınırla

Boyutu maksimum n girdi ile sınırla

Bu seçenek etkinleştirilirse, olay veritabanında listelenen maksimum olay sayısı, belirli bir boyutla sınırlandırılabilir; olası değerler: 100 - 10000 girdi. Girilen girdilerin sayısı aşılırsa, en eski girdiler silinir.

n günden daha eski tüm olayları sil

Bu seçenek etkinleştirilirse, olay veritabanında listelenen olaylar, belirli bir süre sonra silinir; olası değerler: 1 - 90 gün. Bu seçenek, 30 gün değeri ile varsayılan ayar olarak etkinleştirilir.

Sınır yok

Bu seçenek etkinleştirildiğinde, olay veritabanının boyutu sınırlandırılmaz. Ancak, program arabiriminde Olaylar'ın altında maksimum 20.000 girdi görüntülenir.

8.9.7 Raporlar

Raporları sınırla

Sayıyı maks. n adet ile sınırla

Bu seçenek etkinleştirildiğinde, maksimum rapor sayısı belirli bir miktarla sınırlandırılabilir. 1 ile 300 arasında değerlere izin verilir. Belirtilen sayı aşılırsa, o andaki en eski rapor silinir.

n günden daha eski tüm raporları sil

Bu seçenek etkinleştirilirse, belirli bir gün sayısından sonra raporlar otomatik olarak silinir. İzin verilebilir değerler şunlardır: 1 - 90 gün. Bu seçenek, 30 gün değeri ile varsayılan ayar olarak etkinleştirilir.

Sınır yok

Bu seçenek etkinleştirilirse, rapor sayısı kısıtlanmaz.

8.9.8 Dizinler

Geçici yol

Varsayılan sistem ayarlarını kullan

Bu seçenek etkinleştirilirse, sistemin ayarları, geçici dosyaları işlemek için kullanılır.

Not
Sisteminizin geçici dosyaları nereye kaydettiğini görebilirsiniz - örneğin Windows XP'de, **Başlat > Ayarlar > Denetim Masası > Sistem > Dizin kartı** altında: "**Gelişmiş**" Düğmesi "**Ortam Değişkenleri**". Şu anda kayıtlı kullanıcının ve sistem değişkenlerinin (`TEMP`, `TMP`) geçici değişkenleri (`TEMP`, `TMP`) burada ilgili değerleriyle birlikte gösterilir.

Aşağıdaki dizini kullan

Bu seçenek etkinleştirilirse, giriş kutusunda görüntülenen yol kullanılır.

Giriş kutusu

Bu giriş kutusuna, programın geçici dosyalarını saklayacağı yolu girin.

Düğme, gerekli geçici yolu seçebileceğiniz bir pencereyi açar.

Varsayılan

Düğme, geçici yol için önceden tanımlı dizini geri yükler.

Rapor dizini

Giriş kutusu

Bu giriş kutusu, rapor dizinine giden tam yolu içerir.

Düğme, gerekli dizini seçebileceğiniz bir pencereyi açar.

Varsayılan

Düğme, rapor dizinine önceden tanımlı yolu geri yükler.

Karantina dizini

Giriş kutusu

Bu kutu, karantina dizininin yolunu içerir.

Düğme, gerekli dizini seçebileceğiniz bir pencereyi açar.

Varsayılan

Düğme, önceden tanımlı yolu karantina dizinine geri yükler.

8.9.9 Sesli uyarılar

Sistem Tarayıcı veya Gerçek Zamanlı Koruma tarafından bir virüs veya zararlı yazılım algılandığında, etkileşimli eylem modunda bir sesli uyarı duyulur. Şimdi sesli uyarıyı etkinleştirmeyi veya devre dışı bırakmayı seçebilir ve uyarı için alternatif bir WAVE dosyası seçebilirsiniz.

> **Not**
> System Scanner'ın eylem modu, System Scanner > Tara > Algılama durumunda eylem konumundaki yapılandırmada ayarlanır. Gerçek Zamanlı Koruma eylem modu, Gerçek Zamanlı Koruma > Tara > Algılama durumunda eylem konumundaki yapılandırmada ayarlanır.

Uyarı yok

Bu seçenek etkinleştirildiğinde, Sistem Tarayıcı veya Gerçek Zamanlı Koruma tarafından bir virüs algılandığında, sesli bir uyarı verilmez.

PC hoparlörlerini kullan (yalnızca etkileşimli modda)

Bu seçenek etkinleştirildiğinde, Sistem Tarayıcı veya Gerçek Zamanlı Koruma tarafından bir virüs algılandığında, varsayılan sinyal ile sesli bir uyarı verilir. Sesli uyarı, PC'nin dahili hoparlöründen verilir.

Aşağıdaki WAVE dosyasını kullan (yalnızca etkileşimli modda)

Bu seçenek etkinleştirildiğinde, Sistem Tarayıcı veya Gerçek Zamanlı Koruma tarafından bir virüs algılandığında, seçilen WAVE dosyasıyla sesli bir uyarı verilir. Seçilen WAVE dosyası, bağlı bir harici hoparlör üzerinden yürütülür.

WAVE dosyası

Bu giriş kutusuna, seçtiğiniz ses dosyasının adını ve ilişkilendirilmiş yolunu girebilirsiniz. Programın varsayılan sesli sinyali standart olarak girilir.

Düğme, dosya gezgininin yardımıyla gerekli dosyayı seçebileceğiniz bir pencereyi açar.

Sınama

Bu düğme, seçilen WAVE dosyasını sınamak için kullanılır.

8.9.10 Uyarılar

Ağ

Ağınızdaki herhangi bir iş istasyonuna Sistem Tarayıcı 'dan veya Gerçek Zamanlı Koruma 'dan tek tek yapılandırılabilir uyarılar gönderebilirsiniz.

Not
Lütfen "İleti hizmetinin" başlatılıp başlatılmadığını kontrol edin. Hizmeti (başka bir deyişle, örneğin, Windows XP'de) **Başlat > Ayarlar > Sistem denetimi > Yönetim > Hizmetler** konumunda bulabilirsiniz.

Not
Her zaman belirli bir kullanıcıya **değil** , bilgisayarlara bir uyarı gönderilir.

Uyarı
Bu fonksiyon aşağıdaki işletim sistemleri tarafından **artık desteklenmemektedir** :
Windows Server 2008 ve üzeri sürümleri
Windows Vista ve üzeri sürümleri

İleti gönderme hedefi

Bu penceredeki listede, bir virüs veya istenmeyen program bulunduğunda ileti alan bilgisayarların adları gösterilir.

Not
Bir bilgisayar yalnızca bir defa bu listeye girilebilir.

Ekle

Bu düğme ile daha fazla bilgisayar ekleyebilirsiniz. Yeni bilgisayarların adlarını girebileceğiniz bir pencere açılır. Bir bilgisayar adı maksimum 15 karakter uzunluğunda olabilir.

Bu düğme, alternatif olarak doğrudan bilgisayar ortamınızdan bir bilgisayar seçebileceğiniz bir pencereyi açar.

Sil

Bu düğme ile, şu anda seçili olan girdiyi listeden silebilirsiniz.

Gerçek Zamanlı Koruma ağ uyarıları

Ağ uyarıları

Bu seçenek etkinleştirilirse, ağ uyarıları gönderilir. Bu seçenek, varsayılan ayar olarak devre dışı bırakılır.

Not
Bu seçeneği etkinleştirebilmek için, şu konuma en az bir alıcı girilmelidir Yapılandırma > Genel > Uyarılar > Ağ.

Gönderilecek ileti

Pencerede, bir virüs veya istenmeyen program algılandığında seçilen iş istasyonuna gönderilen ileti gösterilir. Bu iletiyi düzenleyebilirsiniz. Bir metin maksimum 500 karakter içerebilir.

İleti biçimlendirmesi için aşağıdaki tuş birleşimlerini kullanabilirsiniz:

Kısayol	Açıklama
Ctrl + Tab	Bir sekme ekler Geçerli satır, sağda birkaç karakterle girintilendirilir.
Ctrl + Enter	Bir satır sonu ekler

İleti, arama sırasında bulunan bilgiler için joker karakterler içerebilir. Gönderim sırasında bu joker karakterlerin yerini gerçek metin alır.

Aşağıdaki joker karakterler kullanılabilir:

Joker karakter	Açıklama
%VIRUS%	Algılanan virüsün veya istenmeyen programın adını içerir
%FILE%	Etkilenen dosyanın yolunu ve dosya adını içerir
%COMPUTER%	Gerçek Zamanlı Koruma'nın çalışmakta olduğu bilgisayarın adını içerir
%NAME%	Etkilenen dosyaya erişen kullanıcının adını içerir
%ACTION%	Virüs algılamasından sonra gerçekleştirilen eylemi içerir
%MACADDR%	Gerçek Zamanlı Koruma'nın çalışmakta olduğu bilgisayarın MAC adresini içerir

Varsayılan

Düğme, bir uyarı için önceden tanımlı varsayılan metni geri yükler.

Sistem Tarayıcı ağ uyarıları

Ağ uyarılarını etkinleştir

Bu seçenek etkinleştirilirse, ağ uyarıları gönderilir. Bu seçenek, varsayılan ayar olarak devre dışı bırakılır.

> **Not**
> Bu seçeneği etkinleştirebilmek için, şu konuma en az bir alıcı girilmelidir Yapılandırma > Genel > Uyarılar > Ağ.

Gönderilecek ileti

Pencerede, bir virüs veya istenmeyen program algılandığında seçilen iş istasyonuna gönderilen ileti gösterilir. Bu iletiyi düzenleyebilirsiniz. Bir metin maksimum 500 karakter içerebilir.

İleti biçimlendirmesi için aşağıdaki tuş birleşimlerini kullanabilirsiniz:

Kısayollar	Açıklama
Ctrl + Tab	Bir sekme ekler Geçerli satır, sağda birkaç karakterle girintilendirilir
Ctrl + Enter	Bir satır sonu ekler

İleti, arama sırasında bulunan bilgiler için joker karakterler içerebilir. Gönderim sırasında bu joker karakterlerin yerini gerçek metin alır.

Aşağıdaki joker karakterler kullanılabilir:

Joker karakter	Açıklama
`%VIRUS%`	Algılanan virüsün veya istenmeyen programın adını içerir
`%NAME%`	Sistem Tarayıcı'yı kullanan, oturum açmış kullanıcının adını içerir
`%COMPUTER%`	Sistem Tarayıcı'nın çalışmakta olduğu bilgisayarın adını içerir

Varsayılan

Düğme, bir uyarı için önceden tanımlı varsayılan metni geri yükler.

E-posta

Belirli olaylarda Avira ürünü, bir veya daha fazla alıcıya e-postayla uyarılar ve iletiler gönderebilir. Bu, Basit İleti Aktarım Protokolü (SMTP) ile yapılır.

İletiler çeşitli olaylar tarafından tetiklenebilir. Aşağıdaki bileşenler, e-posta gönderimini destekler:

- Gerçek Zamanlı Koruma e-posta uyarıları
- Sistem Tarayıcı e-posta uyarıları
- Güncelleyici e-posta uyarıları

> **Not**
> Lütfen ESMTP'nin desteklenmediğini unutmayın. Ayrıca şu anda TLS (Taşıma Katmanı Güvenliği) veya SSL (Güvenli Yuva Katmanı) aracılığıyla şifrelenmiş bir aktarım mümkün değildir.

E-posta iletileri

SMTP Sunucusu

Buraya kullanılacak ana bilgisayarı adını (IP adresini veya doğrudan ana bilgisayar adını) girin.
Ana bilgisayar adının olası maksimum uzunluğu 127 karakterdir.

Örneğin*:*

`192.168.1.100` or `mail.samplecompany.com`.

Bağlantı noktası

Kullanılacak bağlantı noktasını buraya girin.

Gönderen adresi

Bu giriş kutusuna, gönderenin e-posta adresini girin. Gönderen adresinin maksimum uzunluğu 127 karakterdir.

Kimlik doğrulama

Bazı posta sunucuları, bir e-posta gönderilmeden önce programın sunucuya kendini doğrulatmasını (oturum açmasını) bekler. E-posta aracılığıyla bir SMTP sunucusuna kimlik doğrulaması ile uyarılar iletilebilir.

Kimlik doğrulama kullan

Bu seçenek etkinleştirilirse, oturum açma (kimlik doğrulama) için ilgili kutulara bir kullanıcı adı ve parola girilebilir.

Oturum açma adı:
Buraya kullanıcı adınızı girin.

Parola:
İlgili parolayı buraya girin. Parola, şifrelenmiş şekilde kaydedilir. Güvenlik nedenleriyle, bu alana yazdığınız gerçek karakterlerin yerini yıldız işaretleri (*) alır.

Sınama e-postası gönder

Düğmeyi tıklattığınızda, program girilen verileri denetlemek için gönderen adresine bir sınama e-postası göndermeye çalışır.

Gerçek Zamanlı Koruma e-posta uyarıları

Avira Gerçek Zamanlı Koruma, belirli olaylar için bir veya daha fazla alıcıya e-postayla uyarılar gönderebilir.

E-posta uyarıları

Bu seçenek etkinleştirilirse, Avira Gerçek Zamanlı Koruma, belirli olaylar gerçekleştiğinde en önemli bilgileri içeren e-posta iletileri gönderir. Bu seçenek, varsayılan ayar olarak devre dışı bırakılır.

Aşağıdaki olaylar için iletileri e-posta ile gönder

Erişim taraması bir virüs veya istenmeyen program algıladı

Bu seçenek etkinleştirilirse, erişim taraması bir virüs veya istenmeyen program algıladığında her zaman virüs veya istenmeyen programın ve etkilenen dosyanın adını içeren bir e-posta alırsınız.

Düzenle

"**Düzenle**" düğmesi, bir "Erişim algılaması" olayına ilişkin bildirimi yapılandırabileceğiniz "**E-posta şablonu**" penceresini açar. Konu satırı ve e-posta gövdesi için metin ekleme seçeneğiniz vardır. Değişkenleri bu amaçla kullanabilirsiniz. (Bkz. E-posta Şablonu)

Gerçek Zamanlı Koruma'da kritik bir hata oluştu

Bu seçenek etkinleştirilirse, her iç hata algılandığında bir e-posta alırsınız.

Not
Bu durumda, lütfen teknik desteğimizi bilgilendirin ve verilen verileri e-postaya dahil edin. Belirtilen dosyanın da inceleme için gönderilmesi gerekir.

Düzenle

"**Düzenle**" düğmesi, "Gerçek Zamanlı Koruma'da kritik hata" olayına ilişkin bildirimi yapılandırabileceğiniz "**E-posta şablonu**" penceresini açar. Konu satırı ve e-posta gövdesi için metin ekleme seçeneğiniz vardır. Değişkenleri bu amaçla kullanabilirsiniz. (Bkz. E-posta Şablonu)

Alıcılar

Bu kutuya alıcıların e-posta adreslerini girin. Bireysel adresler, virgülle ayrılır. Tüm adreslerin birlikte maksimum uzunluğu (başka bir deyişle, toplam karakter dizesi) 260 karakterdir.

Sistem Tarayıcı e-posta uyarıları

Belirli olaylarda, istek üzerine tarama, e-posta yoluyla bir veya daha fazla alıcıya uyarı ve iletiler gönderebilir.

E-posta uyarıları

Bu seçenek etkinleştirilirse, program, belirli olaylar gerçekleştiğinde en önemli bilgileri içeren e-posta iletileri gönderir. Bu seçenek, varsayılan ayar olarak devre dışı bırakılır.

Aşağıdaki olaylar için iletileri e-posta ile gönder

İstek üzerine tarama bir virüs veya istenmeyen program algıladı

Bu seçenek etkinleştirilirse, istek üzerine tarama bir virüs veya istenmeyen program algıladığında her zaman virüs veya istenmeyen programın ve etkilenen dosyanın adını içeren bir e-posta alırsınız.

Düzenle

"**Düzenle**" düğmesi, bir "Tarama algılaması" olayına ilişkin bildirimi yapılandırabileceğiniz "**E-posta şablonu**" penceresini açar. Konu satırı ve e-posta gövdesi için metin ekleme seçeneğiniz vardır. Değişkenleri bu amaçla kullanabilirsiniz. (Bkz. E-posta Şablonu)

Zamanlanmış tarama sonu

Seçenek etkinleştirildiğinde, bir tarama işi gerçekleştirildiğinde e-posta gönderilir. E-posta; tarama işi noktası ve süresi, taranan klasörler ve dosyalar ile bulunan virüsler ve uyarılar hakkında veriler içerir.

Düzenle

"**Düzenle**" düğmesi, bir "Tarama sonu" olayına ilişkin bildirimi yapılandırabileceğiniz "**E-posta şablonu**" penceresini açar. Konu satırı ve e-posta gövdesi için metin ekleme seçeneğiniz vardır. Değişkenleri bu amaçla kullanabilirsiniz. (Bkz. E-posta Şablonu)

Rapor dosyasını ek olarak ekle

Seçenek etkinleştirilirse, Sistem Tarayıcı bileşeninin geçerli rapor dosyası, Sistem Tarayıcı bildirimleri gönderilirken ek olarak e-postaya eklenir.

Alıcı(lar)

Bu kutuya alıcı(lar)nın e-posta adres(ler)ini girin. Bireysel adresler, virgülle ayrılır. Tüm adreslerin birlikte maksimum uzunluğu (başka bir deyişle, toplam karakter dizesi) 260 karakterdir.

Güncelleyici e-posta uyarıları

Güncelleyici bileşeni, belirli olaylar için bir veya daha fazla alıcıya e-postayla bildirimler gönderebilir.

E-posta uyarıları

Bu seçenek etkinleştirilirse, Güncelleme bileşeni, belirli olaylar gerçekleştiğinde en önemli verileri içeren e-posta iletileri gönderir. Bu seçenek, varsayılan ayar olarak devre dışı bırakılır.

Aşağıdaki olaylar için iletileri e-posta ile gönder

Güncelleme gerekli değil. Programınız güncel

Bu seçenek etkinleştirildiğinde, Güncelleyici karşıdan yükleme sunucusuyla başarılı şekilde bağlantı kurduysa ancak sunucuda kullanılabilir yeni bir dosya yoksa, bir e-posta gönderilir. Başka bir deyişle, Avira ürününüz günceldir.

Düzenle

"**Düzenle**" düğmesi, bir "Güncelleme gerekli değil" olayına ilişkin bildirimi yapılandırabileceğiniz "**E-posta şablonu**" penceresini açar. Konu satırı ve e-posta gövdesi için metin ekleme seçeneğiniz vardır. Değişkenleri bu amaçla kullanabilirsiniz. (Bkz. E-posta Şablonu)

Güncelleme başarıyla tamamlandı. Yeni dosyalar kuruldu

Bu seçenek etkinleştirilirse, gerçekleştirilen tüm güncellemeler için e-posta gönderilir: Bu bir ürün güncellemesi veya bir virüs tanımı dosyası ya da tarama motoru güncellemesi olabilir.

Düzenle

"**Düzenle**" düğmesi, bir "Güncelleme başarılı oldu - yeni dosyalar kuruldu" olayına ilişkin bildirimi yapılandırabileceğiniz "**E-posta şablonu**" penceresini açar. Konu satırı ve e-posta gövdesi için metin ekleme seçeneğiniz vardır. Değişkenleri bu amaçla kullanabilirsiniz. (Bkz. E-posta Şablonu)

Güncelleme başarısız oldu

Bu seçenek etkinleştirilirse, bir hata nedeniyle güncelleme başarısız olduğunda bir e-posta gönderilir.

Düzenle

"**Düzenle**" düğmesi, bir "Güncelleme başarısız oldu" olayına ilişkin bildirimi yapılandırabileceğiniz "**E-posta şablonu**" penceresini açar. Konu satırı ve e-posta gövdesi için metin ekleme seçeneğiniz vardır. Değişkenleri bu amaçla kullanabilirsiniz. (Bkz. E-posta Şablonu)

Rapor dosyasını ek olarak ekle

Seçenek etkinleştirilirse, Güncelleyici bileşeninin geçerli rapor dosyası, Güncelleyici bildirimleri gönderilirken ek olarak e-postaya eklenir.

Alıcılar

Bu kutuya alıcıların e-posta adreslerini girin. Bireysel adresler, virgülle ayrılır. Tüm adreslerin birlikte maksimum uzunluğu (başka bir deyişle, toplam karakter dizesi) 260 karakterdir.

E-posta şablonu

E-posta şablonu penceresinde, etkinleştirilmiş olaylara yönelik bireysel bileşenlerle ilgili e-posta bildirimlerini yapılandırabilirsiniz. Konu satırına maksimum 128 karakterlik ve ileti alanına maksimum 1024 karakterlik metin ekleyebilirsiniz.

Aşağıdaki değişkenler, e-posta konusunda ve e-posta iletisinde kullanılabilir:

Genel olarak kabul edilebilir değişkenler

Değişken	Değer
Windows ortam değişkenleri	E-posta bildirimleri bileşeni tüm Windows ortam değişkenlerini destekler.
%SYSTEM_IP%	Bilgisayarın IP adresi
%FQDN%	Tam nitelendirilmiş etki alanı adı
%TIMESTAMP%	Olay zaman damgası: İşletim sisteminin dil ayarlarına göre saat ve tarih biçimi

%COMPUTERNAME%	NetBIOS bilgisayar adı
%USERNAME%	Bileşene erişen kullanıcının adı
%PRODUCTVER%	Ürün sürümü
%PRODUCTNAME%	Ürün adı
%MODULENAME%	E-posta gönderen bileşenin adı
%MODULEVER%	E-posta gönderen bileşenin sürümü

Belirli bileşen değişkenleri

Değişken	Değer	Bileşen e-postaları
%ENGINEVER%	Kullanılan tarama motorunun sürümü	Gerçek Zamanlı Koruma Sistem Tarayıcı
%VDFVER%	Kullanılan virüs tanımı dosyasının sürümü	Gerçek Zamanlı Koruma Sistem Tarayıcı
%SOURCE%	Tam nitelendirilmiş dosya adı	Gerçek Zamanlı Koruma
%VIRUSNAME%	Virüs veya istenmeyen programın adı	Gerçek Zamanlı Koruma

%ACTION%	Algılamadan sonra gerçekleştirilen eylem	Gerçek Zamanlı Koruma
%MACADDR%	İlk kaydedilen ağ kartının MAC adresi	Gerçek Zamanlı Koruma
%UPDFILESLIST%	Güncellenen dosyaların listesi	Güncelleyici
%UPDATETYPE%	Güncelleme türü: Tarama motoru ve virüs tanımı dosyasının güncellemesi veya tarama motoru ve virüs tanımı dosyasının güncellemesi ile ürün güncellemesi	Güncelleyici
%UPDATEURL%	Güncelleme için kullanılan karşıdan yükleme sunucusunun URL'si	Güncelleyici
%UPDATE_ERROR%	Sözcüklerde güncelleme hatası	Güncelleyici
%DIRCOUNT%	Taranan dizinlerin sayısı	Sistem Tarayıcı
%FILECOUNT%	Taranan dosyaların sayısı	Sistem Tarayıcı
%MALWARECOUNT%	Algılanan virüslerin veya istenmeyen programların sayısı	Sistem Tarayıcı
%REPAIREDCOUNT%	Onarılan etkilenmiş dosyaların sayısı	Sistem Tarayıcı
%RENAMEDCOUNT%	Yeniden adlandırılan etkilenmiş dosyaların sayısı	Sistem Tarayıcı
%DELETEDCOUNT%	Silinen etkilenmiş dosyaların sayısı	Sistem Tarayıcı

%WIPECOUNT%	Üzerine yazılan ve silinen etkilenmiş dosyaların sayısı	Sistem Tarayıcı
%MOVEDCOUNT%	Karantinaya taşınan etkilenmiş dosyaların sayısı	Sistem Tarayıcı
%WARNINGCOUNT%	Uyarı sayısı	Sistem Tarayıcı
%ENDTYPE%	Tarama durumu: Sonlandırıldı/Başarıyla tamamlandı	Sistem Tarayıcı
%START_TIME%	Tarama başlangıç zamanı: Güncelleme başlangıç zamanı	Sistem Tarayıcı, Güncelleyici
%END_TIME%	Tarama sonu Güncelleme sonu	Sistem Tarayıcı, Güncelleyici
%TIME_TAKEN%	Tarama süresi, dakika Güncelleme süresi, dakika	Sistem Tarayıcı, Güncelleyici
%LOGFILEPATH%	Rapor dosyasının yolu ve dosya adı	Sistem Tarayıcı, Güncelleyici

Sesli uyarılar

Sistem Tarayıcı veya Gerçek Zamanlı Koruma tarafından bir virüs veya zararlı yazılım algılandığında, etkileşimli eylem modunda bir sesli uyarı duyulur. Şimdi sesli uyarıyı etkinleştirmeyi veya devre dışı bırakmayı seçebilir ve uyarı için alternatif bir WAVE dosyası seçebilirsiniz.

Not
System Scanner'ın eylem modu, System Scanner > Tara > Algılama durumunda eylem konumundaki yapılandırmada ayarlanır. Gerçek Zamanlı Koruma eylem modu, Gerçek Zamanlı Koruma > Tara > Algılama durumunda eylem konumundaki yapılandırmada ayarlanır.

Uyarı yok

Bu seçenek etkinleştirildiğinde, Sistem Tarayıcı veya Gerçek Zamanlı Koruma tarafından bir virüs algılandığında, sesli bir uyarı verilmez.

PC hoparlörlerini kullan (yalnızca etkileşimli modda)

Bu seçenek etkinleştirildiğinde, Sistem Tarayıcı veya Gerçek Zamanlı Koruma tarafından bir virüs algılandığında, varsayılan sinyal ile sesli bir uyarı verilir. Sesli uyarı, PC'nin dahili hoparlöründen verilir.

Aşağıdaki WAVE dosyasını kullan (yalnızca etkileşimli modda)

Bu seçenek etkinleştirildiğinde, Sistem Tarayıcı veya Gerçek Zamanlı Koruma tarafından bir virüs algılandığında, seçilen WAVE dosyasıyla sesli bir uyarı verilir. Seçilen WAVE dosyası, bağlı bir harici hoparlör üzerinden yürütülür.

WAVE dosyası

Bu giriş kutusuna, seçtiğiniz ses dosyasının adını ve ilişkilendirilmiş yolunu girebilirsiniz. Programın varsayılan sesli sinyali standart olarak girilir.

...

Düğme, dosya gezgininin yardımıyla gerekli dosyayı seçebileceğiniz bir pencereyi açar.

Sınama

Bu düğme, seçilen WAVE dosyasını sınamak için kullanılır.

Uyarılar

Avira ürününüz, güncelleme gibi başarılı veya başarısız program dizileriyle ilgili bilgi veren, belirli olaylara ilişkin masaüstü bildirimleri niteliğinde "slide-up"lar oluşturur. **Uyarılar** bölümünde, belirli olaylara yönelik bildirimleri etkinleştirebilir veya devre dışı bırakabilirsiniz.

Masaüstü bildirimleri ile, bildirimi doğrudan "slide-up"ta devre dışı bırakma seçeneğiniz vardır. **Uyarılar** yapılandırma penceresinde, bildirimi yeniden etkinleştirebilirsiniz.

Güncelle

Son güncelleme n günden eskiyse uyar

Bu kutuya, son güncellemeden sonra geçmesine izin verilen maksimum gün sayısını girebilirsiniz. Bu gün sayısı geçtiyse, Kontrol Merkezi'nde **Durum** altında güncelleme durumu için kırmızı bir simge görüntülenir .

Virüs tanımı dosyası güncel değilse bildirim göster

Bu seçenek etkinleştirilirse, virüs tanımı dosyasının güncel olmaması durumunda bir uyarı alırsınız. Uyarı seçeneğinin yardımıyla, son güncelleme n günden daha eskiyse, bir uyarı için geçici aralığı yapılandırabilirsiniz.

Uyarılar / Aşağıdaki durumlarla ilgili notlar

Çevirmeli bağlantı kullanılıyor

Bu seçenek etkinleştirilirse, numara çeviricinin telefon veya ISDN ağı aracılığıyla bilgisayarınızda bir çevirmeli bağlantı oluşturması durumunda bir masaüstü bildirimi uyarısı alırsınız. Bağlantının bilinmeyen ve istenmeyen bir numara çevirici tarafından oluşturulmuş olma ve bağlantının ücretli olma tehlikesi vardır. (bkz. Virüsler ve daha fazlası > Tehdit kategorileri: Numara çevirici

Dosyalar başarıyla güncellendi

Bu seçenek etkinleştirilirse, her başarılı şekilde bir güncelleme gerçekleştirildiğinde ve dosyalar güncellendiğinde bir masaüstü bildirimi alırsınız.

Güncelleme başarısız oldu

Bu seçenek etkinleştirilirse, bir güncelleme başarısız olduğunda bir masaüstü bildirimi alırsınız: Karşıdan yükleme sunucusu ile bağlantı kurulamadı veya güncelleme dosyaları yüklenemedi.

Güncelleme gerekli değil

Bu seçenek etkinleştirilirse, güncelleme her başlatıldığında ancak programınız güncel olduğundan dosyaların kurulumu gerekli olmadığında bir masaüstü bildirimi alırsınız.

9. Tepsi Simgesi

Görev çubuğunun sistem tepsisindeki tepsi simgesi, Gerçek Zamanlı Koruma ve Güvenlik Duvarı hizmetinin durumunu görüntüler.

Simge	Açıklama
	Avira Gerçek Zamanlı Koruma etkin ve Güvenlik Duvarı etkin
	Avira Gerçek Zamanlı Koruma devre dışı veya Güvenlik Duvarı devre dışı

Bağlam menüsündeki girdiler

- **Gerçek Zamanlı Koruma'yı etkinleştir**: Avira Gerçek Zamanlı Koruma'yı etkinleştirir veya devre dışı bırakır.
- **EPosta Koruması'nı etkinleştir**: Avira EPosta Koruması'nı etkinleştirir veya devre dışı bırakır.
- **Web Koruması'nı etkinleştir**: Avira Web Koruması'nı etkinleştirir veya devre dışı bırakır.
- **Güvenlik Duvarı**:
  - **Güvenlik Duvarı'nı etkinleştir**: Avira Güvenlik Duvarı'nı etkinleştirir veya devre dışı bırakır
  - **Güvenlik Duvarı'nı etkinleştir**: Windows Güvenlik Duvarı'nı etkinleştirir veya devre dışı bırakır (bu özellik Windows 8'den itibaren sunulmaktadır).
  - **Tüm trafiği engelle**: Etkin: Ana bilgisayar sistemine yapılan aktarımlar dışında tüm veri aktarımlarını engeller (Yerel Ana Bilgisayar/IP 127.0.0.1).
- **Avira Professional Security'i başlat**: Kontrol Merkezi'ni açar.
- **Avira Professional Security'i yapılandır**: Yapılandırma'yı açar.
- **Güncellemeyi başlat** Bir güncelleme başlatır.
- **Yapılandırmayı seç**:
  Kullanılabilir yapılandırma profillerini içeren bir alt menü açar. Bu yapılandırmayı etkinleştirmek için bir yapılandırmayı tıklatın. Önceden bir yapılandırmaya otomatik geçiş yapma kuralı tanımladıysanız, menü komutu devre dışı bırakılır.
- **Yardım**: Online Yardım'ı açar.
- **Avira Professional Security hakkında**: Avira ürününüz hakkında bilgiler içeren bir iletişim kutusu açar: Ürün bilgileri, Sürüm bilgileri, Lisans bilgileri.
- **Internet'te Avira**: Internet'te Avira web portalını açar. Bunun koşulu, etkin bir Internet bağlantısının olmasıdır.

10. Güvenlik Duvari

10.1 Güvenlik Duvarı

Avira Professional Security bilgisayar ayarlarınıza bağlı olarak gelen ve giden veri trafiğini yönetmenize izin verir:

- Avira Güvenlik Duvarı

Windows 7'ye kadar olan işletim sistemlerinde, Avira Professional Security Avira Güvenlik Duvarını içermektedir.

- AMC kapsamında Avira Güvenlik Duvarı

Avira Yönetim Konsolu üzerinden yönetiliyorsa, Avira Professional Security Avira Güvenlik Duvarını da içerir.

- Windows Güvenlik Duvarı

Windows 7'den başlayarak, Avira Professional Security Avira Güvenlik Duvarı içermemektedir. Windows Güvenlik Duvarı artık Avira ürünü üzerinden yönetilmektedir.

10.2 Avira Güvenlik Duvarı

10.2.1 Güvenlik Duvarı

Avira Güvenlik Duvarı, bilgisayar sisteminizdeki gelen ve giden veri trafiğini izleyip düzenler ve Internet'ten gelebilecek çok çeşitli saldırılara ve tehditlere karşı sizi korur: Gelen veya giden veri trafiğine veya bağlantı noktalarını dinlemeye, güvenlik kurallarına bağlı olarak izin verilir veya reddedilir. Avira Güvenlik Duvarı, ağ etkinliğini reddedip ağ bağlantılarını engellerse bir masaüstü bildirimi alırsınız. Aşağıdaki seçenekler, Avira Güvenlik Duvarı ayarları için kullanılabilir:

Kontrol Merkezi'nde bir güvenlik düzeyi ayarlayarak

Kontrol Merkezi'nde bir güvenlik düzeyi tanımlayabilirsiniz. *Düşük*, *orta* ve *yüksek* güvenlik düzeylerinin her biri, paket filtrelerini temel alan birçok tamamlayıcı güvenlik kuralları içerir. Bu güvenlik kuralları, Güvenlik Duvarı > Bağdaştırıcı kuralları konumundaki Yapılandırma'da önceden tanımlı bağdaştırıcı kuralları olarak kaydedilir

Ağ olayı penceresinde eylemleri kaydederek

Bir uygulama önce bir ağ veya Internet bağlantısı oluşturmaya çalıştığında, *Ağ Olayı* açılır penceresi görüntülenir. *Ağ Olayı* penceresi, kullanıcının, uygulamanın ağ etkinliğine izin verilmesini veya ağ etkinliğini reddetmesini seçmesine olanak sağlar. **Bu uygulama için Eylemi kaydet** seçeneği etkinleştirilirse, eylem bir uygulama kuralı olarak oluşturulur ve **Güvenlik Duvarı > Uygulama Kuralları** konumundaki yapılandırmaya kaydedilir. Ağ olayı penceresindeki eylemlerin kaydedilmesi, size uygulamaların ağ etkinlikleri için kural kümesi sunar.

Not
Güvenilen üreticilerin uygulamaları için, bir bağdaştırıcı kuralı ağ erişimini yasaklamadığı sürece varsayılan olarak ağ erişimine izin verilir. Güvenilen üreticiler listesinden sağlayıcıları kaldırma seçeneğiniz vardır.

Yapılandırma'da bağdaştırıcı ve uygulama kuralları oluşturarak

Yapılandırma'da önceden tanımlı bağdaştırıcı kurallarını değiştirebilir veya yeni bağdaştırıcı kuralları oluşturabilirsiniz. Bağdaştırıcı kuralları eklerseniz veya değiştirirseniz, Güvenlik Duvarı'nın güvenlik düzeyi otomatik olarak *Özel* değerine ayarlanır.
Uygulama kuralları, uygulamalar için belirlenen izleme kurallarını tanımlamanızı sağlar:
Bir yazılım uygulamasının tüm ağ etkinliklerinin reddedileceğini veya bunlara izin verileceğini ya da bunların *Ağ Olayı* açılan penceresi aracılığıyla işlenip işlenmeyeceğini tanımlamak için basit uygulama kuralları kullanabilirsiniz.
Uygulama kuralları ayarı gelişmiş yapılandırmasında, bir uygulama için, belirtilen uygulama kuralları olarak yürütülen farklı paket filtreleri tanımlayabilirsiniz.

10.2.2 Ağ olayı

Avira Güvenlik Duvarı bileşeninin Ağ olayı penceresinde, ağ erişiminin yazılım uygulamasının veri göndermesine veya başka ağ etkinlikleri gerçekleştirmesine izin verilip verilmeyeceğini seçebilirsiniz: Veri trafiğine veya bağlantı noktalarını pasif dinlemeye izin verebilir veya reddedebilirsiniz. Ağ etkinliklerinin reddedilmesi bir bağlantının iptal edilmesine neden olabilir.

Ağ üzerinden uygulamalara erişildiğinde aşağıdaki durumlarda ağ olayı penceresi açılır:

- Bu uygulama için henüz bir uygulama kuralı oluşturulmamıştır. Avira Güvenlik Duvarı kurulduktan sonra bir uygulama ağa ilk kez bağlandığında bu durum söz konusudur. Ancak, üreticileri güvenilen olarak sınıflandırılan ve ağ erişimine otomatik olarak izin verilen uygulamalar dışarıda bırakılır (bkz. Bölüm Yapılandırma > Güvenlik Duvarı > Güvenilen üreticiler).
- **Sor** eylem türünde basit bir uygulama kuralı oluşturulmuştur.
- Genişletilmiş yapılandırmadaki paket filtreleri temel alınarak uygulama için belirtilen uygulama kuralları oluşturulmuştur; ancak oluşan ağ olayı için bir kural algılanmamıştır. Bu durumda, varolan uygulama kurallarını çağırmak ve yeni bir kural olarak ağ erişimi eklemek için *Genişletilmiş* düğmesini kullanabilirsiniz.

Ağ olayı

Görüntülenen bilgi

Uygulamanın adı.

Uygulamanın adı.

Dosya adı

Yürütülebilir dosyanın adı.

İmza denetimi ve öneri

İmza denetimi ve önerilen eylem sonucu.
Uygulama, güvenilen bir sağlayıcı sertifikasıyla imzalanırsa, veri trafiğine izin verilmesi önerilir.

Ayrıntılı bilgi

Yerel adres

Kaynak adres ve kaynak bağlantı noktası.

Uzak adres

Hedef adres ve hedef bağlantı noktası

Kullanıcı

Uygulamanın yürütüldüğü kayıtlı kullanıcı.

İşlem Kimliği

Uygulamanın işlem kimliği.

Yol

Uygulama için yürütülebilir dosyanın yolu.

Şirket

Uygulama sağlayıcısı (sürüm bilgileri).

Sürüm

Uygulamanın sürümü.

İmzalayan

Uygulama sağlayıcısı (imza).

Eylemler ve düğmeler

Her zaman bu üreticiye güven

Bu seçenek etkinleştirilirse, *Ağ Olayı* isteği yürütülürken, yazılım sağlayıcısı güvenilen üreticiler listesine eklenir. Bu seçeneği etkinleştirdiğiniz anda hemen Reddet düğmesi devre dışı bırakılır.

> **Not**
> Bu eylem yalnızca imzalanmış uygulamalarla kullanılabilir.

Bu uygulama için eylemi hatırla

Bu seçenek etkinleştirilirse, yürütülen eylem bir uygulama kuralı olarak kaydedilir. Güvenlik Duvarı > Açılır pencere ayarları konumundaki yapılandırmada uygulama kuralı çağrılabilir.

Bu uygulama için eylemi hatırla seçeneği etkinleştirilirse ve uygulama için paket filtrelerini temel alan belirtilmiş uygulama kuralları varsa, **İzin Ver** veya **Reddet** düğmesini tıklattığınızda uygulama kurallarının gelişmiş yapılandırması açılır. Oluşan veri trafiği, belirtilen bir uygulama kuralı olarak listenin en üstüne otomatik olarak eklenmiştir. *Güvenlik Duvarı > Uygulama Kuralları* penceresinde, eklenen uygulama kurallarının konumunu değiştirebilir veya eklenen uygulama kurallarını kaldırabilirsiniz.

Düğmeler	Açıklama
Gelişmiş	Uygulama kurallarının gelişmiş yapılandırma penceresi açılır. **Not** Bu düğme yalnızca uygulama kuralları için genişletilmiş ayarlar etkinleştirilmişse kullanılabilir (bkz. Yapılandırma > Güvenlik Duvarı > Ayarlar).
İzin ver	İlgili ağ etkinliğine izin verilir.
Reddet	İlgili ağ etkinliği reddedilir.
Ayrıntıları Göster/Gizle	Uygulamayla ilgili ayrıntılı bilgiler görüntülenir veya gizlenir.

10.3 Windows Güvenlik Duvarı

Avira Professional Security artık Avira Güvenlik Duvarı içermez, ancak size Windows Güvenlik Duvarını doğrudan Avira Kontrol ve Yapılandırma Merkezi üzerinden yönetme seçeneği verir. Windows Güvenlik Duvarı ayarları için aşağıdaki seçenekler mevcuttur:

Kontrol Merkezi üzerinden Windows Güvenlik Duvarını etkinleştirme

Durum > *Internet Koruması* altındaki **Güvenlik Duvarı** seçeneği **AÇIK/KAPALI** düğmesine tıklayarak Windows Güvenlik Duvarını etkinleştirmenizi veya devre dışı bırakmanızı sağlar.

Kontrol Merkezinden Windows Güvenlik Duvarının durumunu kontrol etme

Windows Güvenlik Duvarının durumunu **INTERNET KORUMASI > Güvenlik Duvarı** bölümü altından kontrol edebilir ve önerilen ayarları **Sorunu onar** düğmesine tıklayarak geri yükleyebilirsiniz.

11. Güncellemeler

11.1 Güncellemeler

Anti virüs yazılımının verimliliği, programın, özellikle de virüs tanımı dosyasının ve tarama motorunun ne kadar güncel olduğuna bağlıdır. Düzenli güncellemeler gerçekleştirmek için Güncelleyici bileşeni Avira ürününüzle tümleştirilir. Güncelleyici, Avira ürününüzün her zaman güncel olmasını sağlar ve her gün ortaya çıkan yeni virüslerle mücadele edebilir. Güncelleyici şu bileşenleri günceller:

- Virüs tanımı dosyası:

  Virüs tanımı dosyası, virüs ve zararlı yazılımlara karşı tarama yapmak ve etkilenen nesneleri onarmak için Avira ürününüz tarafından kullanılan zararlı programların virüs desenlerini içerir.

- Tarama motoru:

  Tarama motoru, virüs ve zararlı yazılımlara karşı tarama yapmak için Avira ürününüz tarafından kullanılan yöntemleri içerir.

- Program dosyaları (ürün güncellemesi):

  Ürün güncellemelerine yönelik güncelleme paketleri, tek tek program bileşenleri için ekstra işlevleri kullanılabilir duruma getirir.

Güncelleme, virüs tanımı dosyası, tarama motoru ve ürünün güncel olup olmadığını denetler ve gerekirse bir güncelleme uygular. Bir ürün güncellemesinden sonra, bilgisayar sisteminizi yeniden başlatmanız gerekebilir. Yalnızca virüs tanımı dosyası ve tarama motoru güncellenirse bilgisayarın yeniden başlatılması gerekmez.

Bir ürün güncellemesi yeniden başlatma gerektiriyorsa, güncellemeye devam etme veya güncellemenin daha sonra hatırlatılmasına karar verebilirsiniz. Ürün güncellemeye heman devam etmek isterseniz, yeniden başlatmanın ne zaman gerçekleşeceğini seçebilirsiniz.

Güncellemenin daha sonra hatırlatılmasını istiyorsanız, virüs tanımı dosyası ve tarama motoru güncellenir, ancak ürün güncellemesi gerçekleştirilmez.

Not
Ürün güncellemesi yeniden başlatmaya kadar tamamlanmaz.

Not
Güvenlik nedenleriyle Güncelleyici, bilgisayarınızın Windows barındırma dosyasının değiştirilip değiştirilmediğini, örneğin, Güncelleme URL'sinin zararlı yazılım tarafından değiştirilip değiştirilmediğini ve Güncelleyici'yi istenmeyen karşıdan yükleme sitelerine yönlendirip yönlendirmediğini denetler. Windows barındırma dosyası değiştirilmişse, Güncelleyici rapor dosyasında bu gösterilir.

Şu aralıkta otomatik olarak bir güncelleme gerçekleştirilir: 60 dakika. Yapılandırma yoluyla otomatik güncellemeyi düzenleyebilir veya devre dışı bırakabilirsiniz (Yapılandırma > Güncelle).

Kontrol Merkezi'nde **Zamanlayıcı** altında Güncelleyici tarafından belirtilen aralıklarda uygulanan ek güncelleme işleri oluşturabilirsiniz. Bir güncellemeyi el ile de başlatabilirsiniz:

- Kontrol Merkezi'nde: **Güncelleme** menüsünde ve **Durum** bölümünde
- tepsi simgesinin bağlam menüsü aracılığıyla

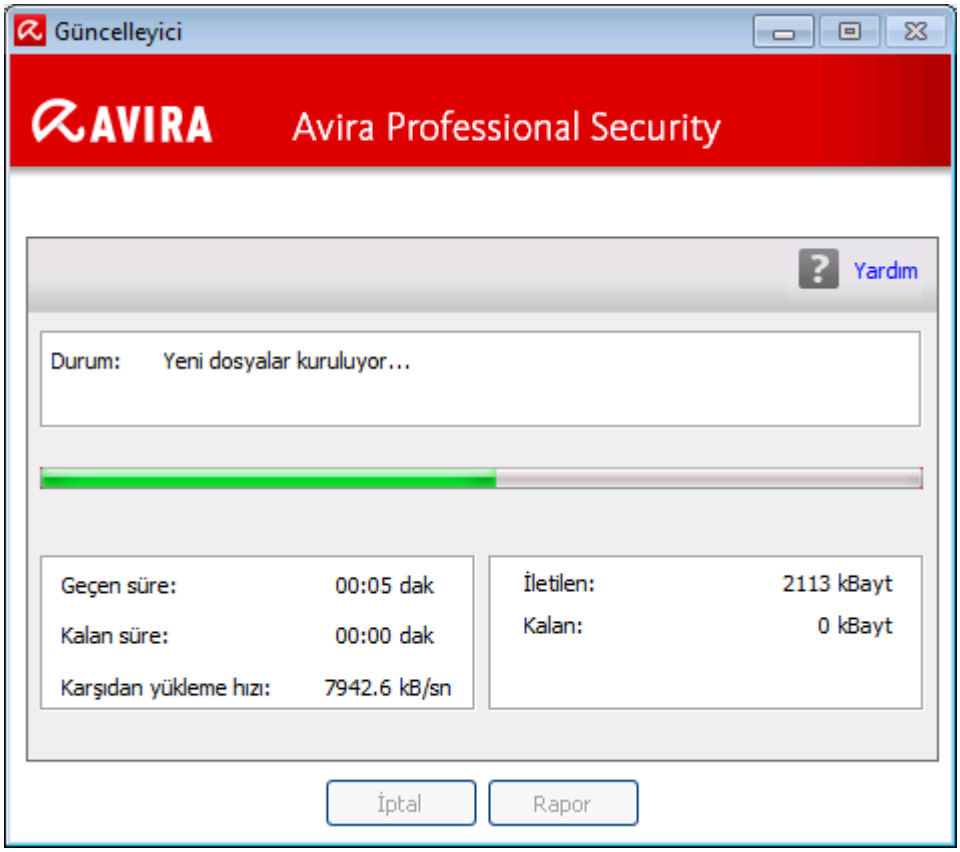
Güncellemeler, Internet'ten özel bir web sunucusu aracılığıyla veya intranet'te bir web ya da dosya sunucusu aracılığıyla edinilebilir; bu sunucular, Internet'ten güncelleme dosyalarını karşıdan yükler ve bunları ağdaki diğer bilgisayarlar için kullanılabilir duruma getirir. Ağdaki birden çok bilgisayarda Avira ürünlerini güncellemek istiyorsanız bu kullanışlıdır. Intranet'teki bir karşıdan yükleme sunucusu, minimum kaynak kullanarak korumalı bilgisayarlarda Avira ürünlerinin güncel olduğundan emin olmak için kullanılabilir. İntranet'te çalışan bir karşıdan yükleme sunucusu kurmak için, Avira ürününün güncel yapısıyla uyumlu olan bir sunucuya ihtiyacınız vardır.

Not
Intranet'te bir web sunucusu veya dosya sunucusu olarak Avira Güncelleme Yöneticisi'ni (Windows'da dosya sunucusu ya da web sunucusu) kullanabilirsiniz. Avira Güncelleme Yöneticisi, Avira ürünlerinin karşıdan yükleme sunucularını yansıtır ve Internet'te Avira web sitesinden edinilebilir. http://www.avira.com/tr

Bir web sunucusu kullanıldığında, karşıdan yükleme için HTTP protokolü kullanılır. Dosya sunucusu kullanılırken, ağ aracılığıyla güncelleme dosyasına erişim sağlanır. Şu konumdaki Yapılandırma'da web sunucusu veya dosya sunucusu bağlantısını yapılandırabilirsiniz: Yapılandırma > Güncelle. Varsayılan yapılandırma, Avira web sunucuları bağlantısı olarak varolan Internet bağlantısını kullanır.

11.2 Güncelleyici

Güncelleyici penceresi bir güncellemenin başlangıcında açılır.



Not
Zamanlayıcı'da oluşturulan güncelleme işleri için, güncelleme penceresinin görüntü modunu tanımlayabilirsiniz: **Gizle**, **Simge durumuna küçült** veya **Ekranı kapla** seçeneklerini belirleyebilirsiniz.

Not
Bir programı tam ekran modunda (örn. oyunlar) kullanıyorsanız ve güncelleyicinin görüntü modu, ekranı kaplayan veya simge durumuna küçültülen olarak ayarlanırsa, güncelleyici masaüstüne geçiş yapar. Bunu önlemek için, görüntü modu gizle olarak ayarlanmış şekilde güncelleyiciyi başlatın. Bu modda artık size güncelleme penceresi tarafından güncellemelerle ilgili bildirim gönderilmez.

Durum: Güncelleyicinin ilerleme durumunu gösterir.

Geçen süre: Karşıdan yükleme başlatıldığından itibaren geçen süre.

Kalan süre: Karşıdan yükleme bitinceye kadar kalan süre.

Karşıdan yükleme hızı: Karşıdan yükleme hızı.

İletilen: Önceden karşıdan yüklenen bayt sayısı.

Kalan: Karşıdan yüklemenin bitmesine kadar kalan baytlar.

Düğmeler ve bağlantılar

Düğme / bağlantı	Açıklama
	Online yardımın bu sayfası, bu düğme veya bağlantı aracılığıyla açılır.
Azalt	Güncelleyicinin görüntüleme penceresi, küçültülmüş boyutta görüntülenir.
Büyüt	Güncelleyicinin görüntüleme penceresi, özgün boyutuna yeniden getirilir.
Durdur	Güncelleme yordamı iptal edilir. Güncelleyici kapatılır.
Kapat	Güncelleme yordamı tamamlanır. Görüntüleme penceresi şimdi kapatılır.
Rapor	Güncellemenin rapor dosyası görüntülenir.

12. SSS, İpuçları

Bu bölümde sorun gidermeyle ilgili önemli bilgiler ve Avira ürününü kullanmaya yönelik daha fazla ipucu bulunur.

- Bkz. Bölüm Sorun olması durumunda yardım
- Bkz. Bölüm Kısayollar
- Bkz. Bölüm Windows Güvenlik Merkezi (Windows XP) veya Windows Eylem Merkezi (Windows 7'den itibaren)

12.1 Sorun olması durumunda yardım

Burada, olası sorunların nedenleri ve çözümleriyle ilgili bilgiler bulursunuz.

- *Lisans dosyası açılamıyor* hata iletisi görüntülenir.
- Bir güncelleme başlatılmaya çalışılırken *Dosya karşıdan yüklenirken bağlantı başarısız oldu*... hata iletisi görüntülenir.
- Virüsler ve zararlı yazılımlar taşınamaz veya silinemez.
- Tepsi simgesinin durumu devre dışı bırakılır.
- Veri yedeklemesi gerçekleştirdiğimde bilgisayar çok yavaşlıyor.
- Güvenlik duvarım, etkinleştirmeden hemen sonra Avira Gerçek Zamanlı Koruma'yı ve Avira EPosta Koruması'nı bildirir.
- Avira EPosta Koruması çalışmaz.
- Avira Güvenlik Duvarı, ana bilgisayara kurulursa ve Avira Güvenlik Duvarı'nın güvenlik düzeyi *orta* veya *yüksek* olarak ayarlanırsa, sanal makinede (örn. VMWare, Sanal PC, ...) kullanılabilir bir ağ bağlantısı yoktur.
- Avira Güvenlik Duvarı'nın güvenlik düzeyi *orta* veya *yüksek* olarak ayarlanırsa, Sanal Özel Ağ (VPN) Bağlantısı engellenir.
- TLS bağlantısı yoluyla gönderilen bir e-posta, EPosta Koruması tarafından engellendi.
- Web sohbeti çalışmıyor: Sohbet iletileri görüntülenmeyecek

***Lisans dosyası açılamıyor* hata iletisi görüntülenir.**

Nedeni: Dosya şifrelidir.

- Lisansı etkinleştirmek için, dosyayı açmanız gerekmez ancak dosyayı program dizinine kaydedersiniz. Ayrıca zamanda Lisans Yöneticisine de bakın.

Bir güncelleme başlatılmaya çalışılırken *Dosya karşıdan yüklenirken bağlantı başarısız oldu...* hata iletisi görüntülenir.

Nedeni: Internet bağlantınız etkin değil. Bu nedenle Internet'te web sunucusuna bağlantı kurulamaz.

- WWW veya e-posta çalışması gibi diğer Internet hizmetlerini sınayın. Aksi takdirde, Internet bağlantısını yeniden kurun.

Nedeni: Proxy sunucuya ulaşılamıyor.

- Proxy sunucu için oturum açma adının değişim değişmediğini denetleyin ve gerekirse bunu yapılandırmanıza göre uyarlayın.

Nedeni: *update.exe* dosyası, kişisel güvenlik duvarınız tarafından tamamen onaylanmıyor.

- *update.exe* dosyasının, kişisel güvenlik duvarınız tarafından onaylandığından emin olun.

Aksi takdirde:

- PC Koruma > Güncelle konumundaki Yapılandırma'da ayarlarınızı denetleyin.

Virüsler ve zararlı yazılımlar taşınamaz veya silinemez.

Nedeni: Dosya windows tarafından yüklenmiş ve etkin.

- Avira ürününüzü güncelleyin.
- Windows XP işletim sistemini kullanıyorsanız, Sistem Geri Yüklemesi'ni devre dışı bırakın.
- Bilgisayarı Güvenli Modda başlatın.
- Avira ürününüzün Yapılandırma'sını başlatın.
- **Sistem Tarayıcı > Tara > Dosyalar > Tüm dosyalar** öğesini seçin ve **Tamam** seçeneği ile pencereyi onaylayın.
- Tüm yerel sürücülerin taramasını başlatın.
- Bilgisayarı Normal Modda başlatın.
- Normal Modda bir tarama gerçekleştirin.
- Başka bir virüs veya zararlı yazılım bulunmadıysa, kullanılabilir durumdaysa Sistem Geri Yüklemesini etkinleştirin.

Tepsi simgesinin durumu devre dışı bırakılır.

Nedeni: Avira Gerçek Zamanlı Koruma devre dışı.

- Kontrol Merkezi'nde **Durum** seçeneğine tıklayın ve **PC Koruma** alanında *Gerçek Zamanlı Koruma* seçeneğini etkinleştirin.

-VEYA-

- Sağ fare düğmesiyle Tepsi Simgesini tıklayarak bağlam menüsünü açın. **Gerçek Zamanlı Koruma etkinleştir** seçeneğine tıklayın.

Nedeni: Avira Gerçek Zamanlı Koruma bir güvenlik duvarı tarafından engelleniyor.

- Güvenlik duvarınızın yapılandırmasında Avira Gerçek Zamanlı Koruma için genel bir onay tanımlayın. Avira Gerçek Zamanlı Koruma yalnızca 127.0.0.1 adresiyle (yerel ana bilgisayar) çalışır. Bir internet bağlantısı kurulmaz. Aynı durum Avira EPosta Koruması için de geçerlidir.

Aksi takdirde:

- Avira Gerçek Zamanlı Koruma hizmetinin başlatma türünü denetleyin. Gerekiyorsa, hizmeti etkinleştirin: Görev çubuğunda **Başlat > Ayarlar > Denetim Masası** seçeneklerini belirleyin. Çift tıklatarak **Hizmetler** yapılandırma panelini başlatın (Windows XP'de hizmetler uygulaması, *Yönetimsel Araçlar* alt dizininde bulunur). *Avira Gerçek Zamanlı Koruma* girdisini bulun. Başlatma türü olarak Otomatik ve durum olarak Başlatıldı girilmelidir. Gerekirse, ilgili satırı ve **Başlat** düğmesini seçerek hizmeti el ile başlatın. Bir hata iletisi görüntülenirse, lütfen olay görüntüsünü denetleyin.

Veri yedeklemesi gerçekleştirdiğimde bilgisayar çok yavaşlıyor.

Nedeni: Yedekleme yordamı sırasında Avira Gerçek Zamanlı Koruma, yedekleme yordamı tarafından kullanılmakta olan tüm dosyaları tarar.

- Yapılandırma'da **Gerçek Zamanlı Koruma > Tara > İstisnalar** seçeneklerini belirleyin ve yedekleme yazılımının işlem adlarını girin.

Güvenlik duvarım, etkinleştirmeden hemen sonra Avira Gerçek Zamanlı Koruma'yı ve Avira EPosta Koruması'nı bildirir.

Nedeni: Avira Gerçek Zamanlı Koruma ve Avira EPosta Koruması ile iletişim, TCP/IP Internet protokolü aracılığıyla gerçekleşir. Bir güvenlik duvarı, bu protokol aracılığıyla tüm bağlantıları izler.

- Güvenlik duvarınızın yapılandırmasında Avira Gerçek Zamanlı Koruma ve Avira EPosta Koruması için genel bir onay tanımlayın. Avira Gerçek Zamanlı Koruma yalnızca 127.0.0.1 adresiyle (yerel ana bilgisayar) çalışır. Bir internet bağlantısı kurulmaz. Aynı durum Avira EPosta Koruması için de geçerlidir.

Avira EPosta Koruması çalışmaz.

Avira EPosta Koruması ile ilgili bir sorun oluşursa, lütfen aşağıdaki kontrol listelerinin yardımıyla Avira EPosta Koruması'nın düzgün çalışıp çalışmadığını kontrol edin.

Kontrol listesi

- Posta istemcinizin Kerberos, APOP veya RPA aracılığıyla sunucuda oturum açıp açmadığını kontrol edin. Bu doğrulama yöntemleri şu anda desteklenmemektedir.
- Posta istemcinizin, SSL (TLS -Taşıma Katmanı Güvenliği olarak da adlandırılır) üzerinden sunucuya rapor verip vermediğini kontrol edin. Avira EPosta Koruması, SSL'yi desteklemez ve bu nedenle şifrelenmiş SSL bağlantılarını sonlandırır. Şifrelenmiş SSL bağlantılarını EPosta Koruması olmadan kullanmak istiyorsanız, bağlantı için EPosta Koruması tarafından izlenmeyen bir bağlantı noktası kullanmanız gerekir. EPosta Koruması tarafından izlenen bağlantı noktaları, **EPosta Koruması > Tara** konumundaki yapılandırmada yapılandırılabilir.
- Avira EPosta Koruması hizmeti etkin mi? Gerekiyorsa, hizmeti etkinleştirin: Görev çubuğunda **Başlat > Ayarlar > Denetim Masası** seçeneklerini belirleyin. Çift tıklatarak **Hizmetler** yapılandırma panelini başlatın (Windows XP'de hizmetler uygulaması, *Yönetimsel Araçlar* alt dizininde bulunur). *Avira EPosta Koruması* girdisini bulun. Başlatma türü olarak Otomatik ve durum olarak Başlatıldı girilmelidir. Gerekirse, ilgili satırı ve **Başlat** düğmesini seçerek hizmeti el ile başlatın. Bir hata iletisi görüntülenirse, lütfen olay görüntüsünü denetleyin. Bu başarılı olmazsa, **Başlat > Ayarlar > Denetim Masası > Program Ekle veya Kaldır** seçeneklerini kullanarak Avira ürününüzü tamamen kaldırmanız, bilgisayarı yeniden başlatmanız ve sonra Avira ürününüzü yeniden kurmanız gerekebilir.

Genel

SSL (Güvenli Yuva Katmanı, ayrıca sık sık TLS (Taşıma Katmanı Güvenliği) olarak da ifade edilir) aracılığıyla şifrelenmiş POP3 bağlantıları şu anda korunamaz ve yoksayılır.

Posta sunucusu doğrulaması şu anda "parolalar" ile desteklenmez. "Kerberos" ve "RPA" şu anda desteklenmemektedir.

Avira ürününüz, giden e-postaları virüs ve istenmeyen programlara karşı denetlemez.

> **Not**
> Güvenlikteki boşlukları doldurmak için düzenli olarak Microsoft güncellemelerinin yüklenmesini öneririz.

Avira Güvenlik Duvarı, ana bilgisayara kurulursa ve Avira Güvenlik Duvarı'nın güvenlik düzeyi *orta* veya *yüksek* olarak ayarlanırsa, sanal makinede (örn. VMWare, Sanal PC, ...) kullanılabilir bir ağ bağlantısı yoktur.

Avira Güvenlik Duvarı, sanal makinenin de (örneğin, VMWare, sanal PC, vb.) çalışmakta olduğu bir bilgisayara kurulursa, Avira Güvenlik Duvarı'nın güvenlik düzeyi *orta* veya *yüksek* olarak ayarlandığında, Avira Güvenlik Duvarı, sanal makinenin tüm ağ bağlantılarını engeller. Güvenlik düzeyi *düşük* olarak ayarlanmış ise, Güvenlik Duvarı ağ bağlantılarına izin verir.

Nedeni: Sanal makine, yazılım aracılığıyla bir ağ kartına öykünür. Bu öykünme, konuk sistemin veri paketlerini özel paketlerde (UDP paketleri) kapsüller ve dış ağ geçidi aracılığıyla bunları ana bilgisayar sistemine yönlendirir. Avira Güvenlik Duvarı, *orta* güvenlik düzeyinden başlayarak, dışarıdan gelen bu paketleri reddeder.

Bu davranışı önlemek için aşağıdakileri yapın:

- Kontrol Merkezi'ne gidin ve *İNTERNET KORUMASI* **> Güvenlik Duvarı** bölümünü seçin.
- **Yapılandırma** düğmesini tıklatın.

  Yapılandırma iletişim kutusu görüntülenir. *Uygulama kuralları* yapılandırma bölümünde olursunuz.
- **Bağdaştırıcı kuralları** yapılandırma bölümünü seçin.
- **Kural ekle**'yi tıklatın.
- **Gelen kurallar** bölümünde *UDP* seçeneğini belirleyin.
- Kuralın Bölüm Adı alanına kuralın **adını** yazın.
- **Tamam**'ı tıklatın.
- Kuralın doğrudan **Tüm IP paketlerini reddet** kuralının yukarısında olup olmadığını kontrol edin.

Uyarı
Bu kural, filtreleme olmadan UDP paketlerine izin vereceğinden, tehlikeli olabilir! Sanal makine ile çalıştıktan sonra, önceki güvenlik düzeyine geçiş yapın.

Avira Güvenlik Duvarı'nın güvenlik düzeyi *orta* veya *yüksek* olarak ayarlanırsa, Sanal Özel Ağ (VPN) Bağlantısı engellenir.

Nedeni: Varsayılan olarak, önceden belirlenen kurallara uymayan tüm paketler atılır. VPN yazılımı tarafından gönderilen paketler (GRE paketleri), diğer kategorilere uymaz ve dolayısıyla bu kurallar tarafından filtrelenir.

Avira FireWall Yapılandırma'da **Bağdaştırıcı kuralları** seçeneğinde **VPN bağlantılarına izin ver** kuralını ekleyin. Bu kural VPN ile ilgili tüm paketlere izin verecektir.

TLS bağlantısı yoluyla gönderilen bir e-posta, EPosta Koruması tarafından engellendi.

Nedeni: Taşıma Katmanı Güvenliği (TLS: Internet üzerinde veri aktarımları için şifreleme protokolü), şu anda EPosta Koruması tarafından desteklenmemektedir. Aşağıdaki seçenekler, e-posta gönderme için kullanılabilir:

- SMTP tarafından kullanılan 25 numaralı bağlantı noktasından farklı bir bağlantı noktası kullanın. Bu, EPosta Koruması izlemesini atlar.
- E-posta istemcinizde TLS şifreli bağlantıyı kapatın ve TLS desteğini devre dışı bırakın.

- **EPosta Koruması > Tara** konumundaki yapılandırmada EPosta Koruması tarafından gönderilen giden e-postaların izlenmesini devre dışı bırakın (geçici olarak).

Web sohbeti çalışmıyor: Sohbet iletileri görüntülenmiyor; tarayıcıda veriler yükleniyor.

'transfer-encoding: chunked' ile HTTP protokolünü temel alan sohbetler sırasında bu durum oluşabilir.

Nedeni: Web Koruması, veriler web tarayıcısına yüklenmeden önce, gönderilen verileri virüslere ve istenmeyen programlara karşı tamamen denetler. 'transfer-encoding: chunked' ile veri aktarımı sırasında Web Koruması, ileti uzunluğunu veya veri hacmini belirleyemez.

- Bir istisna olarak web sohbetleri URL'sinin yapılandırmasını girin: (bkz. Yapılandırma: **Web Koruması > Tara > İstisnalar**).

12.2 Kısayollar

Kısayollar olarak da ifade edilen klavye komutları, programda gezinmek, tek tek modülleri almak ve eylemler başlatmak için hızlı bir olanak sunar.

Aşağıda, sizin için kullanılabilir klavye komutlarına genel bakış sağlamaktayız. Lütfen ilgili yardım bölümünde işlevselliğe ilişkin diğer göstergeleri bulun.

12.2.1 İletişim kutularında

Kısayol	Açıklama
Ctrl + Tab **Ctrl + Page down**	Kontrol Merkezi'nde gezinti Bir sonraki bölüme gidin.
Ctrl + Shift + Tab **Ctrl + Page up**	Kontrol Merkezi'nde gezinti Bir önceki bölüme gidin.
← ↑ → ↓	Yapılandırma bölümlerinde gezinti Öncelikle, bir yapılandırma bölümüne odaklanmak için fareyi kullanın. İşaretlenmiş açılan bir listedeki seçenekler arasında veya bir seçenek grubundaki birçok seçenek arasında geçiş yapın.
Sekme	Sonraki seçeneğe veya seçenekler grubuna geçiş yapın.

Shift + Sekme	Önceki seçeneğe veya seçenekler grubuna geçiş yapın.
Boşluk	Etkin seçenek bir onay kutusuysa, onay kutusunu etkinleştirin veya devre dışı bırakın.
Alt + altı çizili harf	Seçeneği belirleyin veya komutu başlatın.
Alt + ↓ **F4**	Seçili açılan listeyi açın.
Esc	Seçili açılan listeyi kapatın. Komutu iptal edin ve iletişim kutusunu kapatın.
Enter	Etkin seçenek veya düğme için komutu başlatın.

12.2.2 Yardımda

Kısayol	Açıklama
Alt + Boşluk	Sistem menüsünü görüntüleyin.
Alt + Sekme	Yardım ve diğer açılan pencereler arasında geçiş yapın.
Alt + F4	Yardımı kapatın.
Shift + F10	Yardımın bağlam menüsünü görüntüleyin.
Ctrl + Tab	Gezinti penceresinde bir sonraki bölüme gidin.
Ctrl + Shift + Sekme	Gezinti penceresinde bir önceki bölüme gidin.
Page up	Dizinde veya arama sonuçları listesinde, içindekilerin yukarısında görüntülenen konuya geçiş yapın.
Page down	Dizinde veya arama sonuçları listesinde, içindekilerdeki geçerli konunun aşağısında görüntülenen konuya geçiş yapın.

Page up **Page down**	Bir konuya göz atın.

12.2.3 Kontrol Merkezi'nde

Genel

Kısayol	Açıklama
F1	Yardımı görüntüle
Alt + F4	Kontrol Merkezi'ni kapat
F5	Yenile
F8	Yapılandırmayı aç
F9	Güncellemeyi başlat

Tarama bölümü

Kısayol	Açıklama
F2	Seçilen profili yeniden adlandır
F3	Seçilen profille tarama başlat
F4	Seçilen profil için masaüstü bağlantısı oluştur
Ins	Yeni profil oluştur

Del	Seçilen profili sil

Güvenlik Duvarı bölümü

Kısayol	Açıklama
Return	Özellikler

Karantina bölümü

Kısayol	Açıklama
F2	Nesneyi yeniden tara
F3	Nesneyi geri yükle
F4	Nesneyi gönder
F6	Nesneyi şuraya geri yükle...
Return	Özellikler
Ins	Dosya ekle
Del	Nesneyi sil

Zamanlayıcı bölümü

Kısayol	Açıklama
F2	İşi düzenle
Return	Özellikler

Ins	Yeni iş ekle
Del	İşi sil

Raporlar bölümü

Kısayol	Açıklama
F3	Rapor dosyasını görüntüle
F4	Rapor dosyasını yazdır
Return	Raporu görüntüle
Del	Raporları sil

Olaylar bölümü

Kısayol	Açıklama
F3	Olay(lar)ı dışarı ver
Return	Olayı göster
Del	Olay(lar)ı sil

12.3 Windows Güvenlik Merkezi

- Windows XP Service Pack 2 -

12.3.1 Genel

Windows Güvenlik Merkezi, önemli güvenlik yönleri için bir bilgisayarın durumunu denetler.

Bu önemli noktalardan (örn. tarihi geçmiş bir anti virüs programı) biriyle ilgili sorun algılanırsa, Güvenlik Merkezi bir uyarı verir ve bilgisayarınızın nasıl daha iyi korunacağına ilişkin öneriler sunar.

12.3.2 Windows Güvenlik Merkezi ve Avira ürününüz

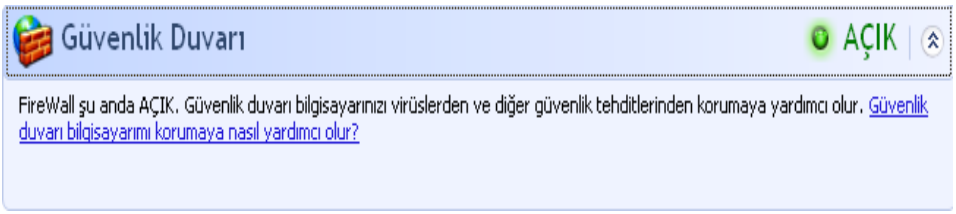
Güvenlik Duvarı

Güvenlik Merkezi'nden güvenlik duvarınızla ilgili aşağıdaki bilgileri alabilirsiniz:

- Güvenlik Duvarı ETKİN / Güvenlik Duvarı açık
- Güvenlik Duvarı DEVRE DIŞI / Güvenlik Duvarı kapalı

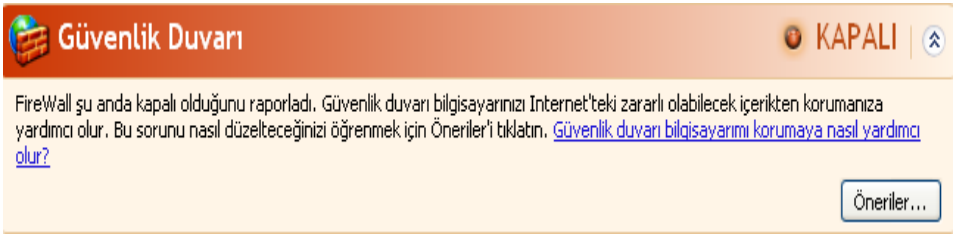
Güvenlik Duvarı ETKİN / Güvenlik Duvarı açık

Avira ürününüzü kurup Windows Güvenlik Duvarı'nı kapattıktan sonra aşağıdaki iletiyi alırsınız:



Güvenlik Duvarı DEVRE DIŞI / Güvenlik Duvarı kapalı

Avira Güvenlik Duvarı'nı devre dışı bıraktığınızda hemen aşağıdaki iletiyi alırsınız:



Not
Avira Güvenlik Duvarı'nı Kontrol Merkezi içindeki Durum sekmesi aracılığıyla etkinleştirebilir veya devre dışı bırakabilirsiniz.

Uyarı
Avira Güvenlik Duvarı'nı kapatırsanız, yetkisiz kullanıcılar ağ veya Internet üzerinden bilgisayarınıza erişim sağlayabilir.

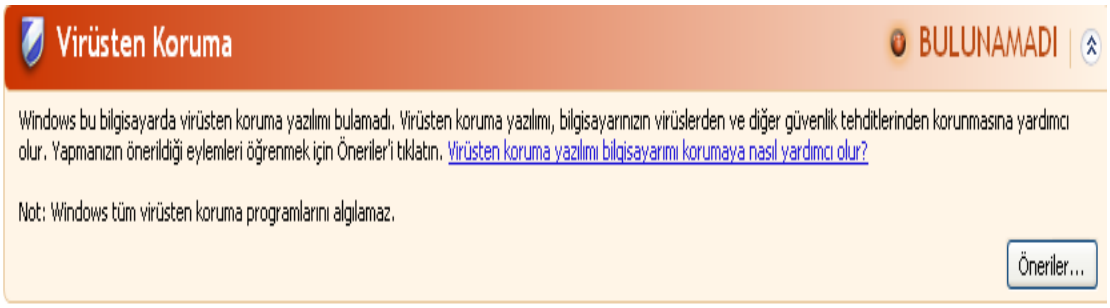
Virüs koruması yazılımı / Zararlı yazılımlara karşı koruma

Windows Güvenlik Merkezi'nden virüs korumanızla ilgili aşağıdaki bilgileri alabilirsiniz:

- Virüs koruması BULUNAMADI
- Virüs korumasının TARİHİ GEÇMİŞ
- Virüs koruması AÇIK
- Virüs koruması KAPALI
- Virüs koruması İZLENMİYOR

Virüs koruması BULUNAMADI

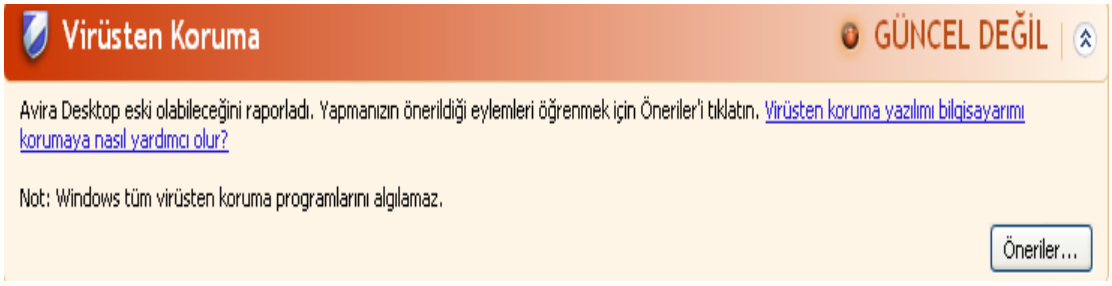
Windows Güvenlik Merkezi bilgisayarınızda herhangi bir anti virüs yazılımı bulmadığında, Windows Güvenlik Merkezi'nin bilgileri görüntülenir.



> **Not**
> Bilgisayarınızı virüslere ve diğer istenmeyen programlara karşı korumak için bilgisayarınıza Avira ürününüzü kurun!

Virüs korumasının TARİHİ GEÇMİŞ

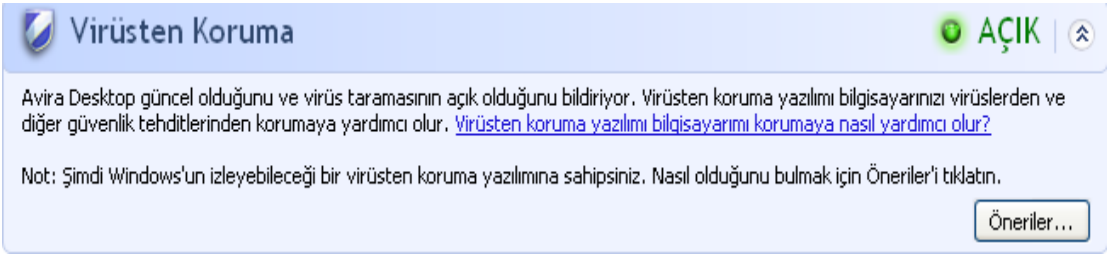
Önceden Windows XP Service Pack 2 kurduysanız ve daha sonra Avira ürününüzü kurarsanız veya Avira ürününün önceden kurulu olduğu bir sisteme Windows XP Service Pack 2 kurarsanız, aşağıdaki iletiyi alırsınız:



> **Not**
> Windows Güvenlik Merkezi'nin, Avira ürününüzü güncel olarak tanıması için, kurulumdan sonra bir güncelleme gerçekleştirilmelidir. Bir güncelleme gerçekleştirerek sisteminizi güncelleyin.

Virüs koruması AÇIK

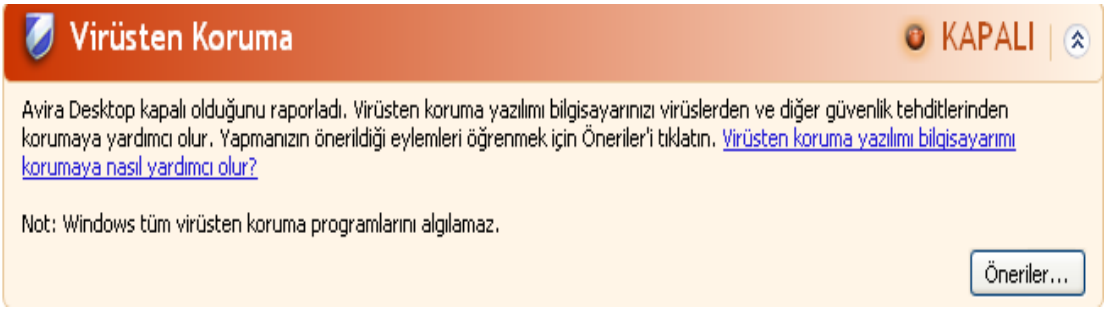
Avira ürününüzü kurduktan ve ardından bir güncelleme gerçekleştirdikten sonra, aşağıdaki iletiyi alırsınız:



Avira ürününüz artık güncel ve Avira Gerçek Zamanlı Koruma etkin.

Virüs koruması KAPALI

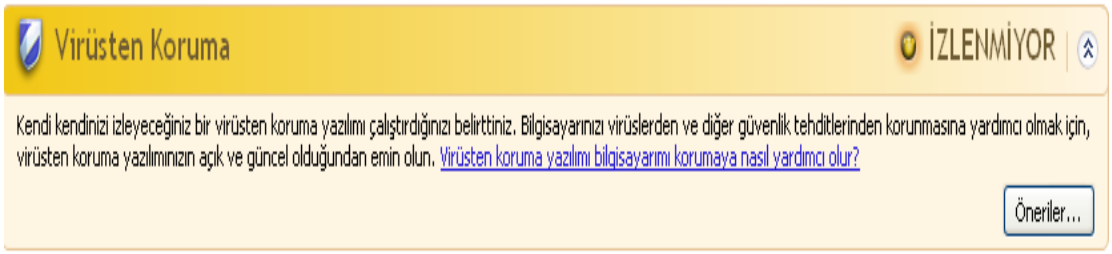
Avira Gerçek Zamanlı Koruma'yı devre dışı bırakırsanız veya Gerçek Zamanlı Koruma hizmetini durdurursanız, aşağıdaki iletiyi alırsınız.



> **Not**
> Avira Gerçek Zamanlı Koruma'yı **Kontrol Merkezi**'nin Durum bölümünde etkinleştirebilir veya devre dışı bırakabilirsiniz. Görev çubuğunuzdaki kırmızı şemsiye açıksa, Avira Gerçek Zamanlı Koruma'nın etkinleştirildiğini görebilirsiniz.

Virüs koruması İZLENMİYOR

Windows Güvenlik Merkezi'nden aşağıdaki iletiyi alırsanız, anti virüs yazılımınızı izlemek istediğinize karar vermişsinizdir.



Not
Windows Güvenlik Merkezi, Avira ürününüz tarafından desteklenir. İstediğiniz zaman **Öneriler** düğmesiyle bu seçeneği etkinleştirebilirsiniz.

Not
Windows XP Service Pack 2 kurmuş olsanız da bir virüs koruma çözümü gerekir. Windows anti virüs yazılımınızı izlese de, herhangi bir anti virüs işlevi içermez. Bu nedenle, ek bir anti virüs çözümü olmadan virüslere ve diğer zararlı yazılımlara karşı korunamazsınız!

12.4 Windows Eylem Merkezi

- Windows 7 ve Windows 8 -

12.4.1 Genel

Not:
Windows 7'den itibaren **Windows Güvenlik Merkezi Windows Eylem Merkezi** adını almıştır. Bu bölümde, tüm güvenlik seçeneklerinizin durumunu göreceksiniz.

Windows Eylem Merkezi, önemli güvenlik yönleri için bir bilgisayarın durumunu denetler. Görev çubuğunuzdaki küçük bayrağa tıklayarak veya **Denetim Masası > Eylem Merkezi** seçeneği ile bu uygulamaya doğrudan erişebilirsiniz.

Bu önemli noktalardan (örn. tarihi geçmiş bir anti virüs programı) biriyle ilgili sorun algılanırsa, Eylem Merkezi bir uyarı verir ve bilgisayarınızın nasıl daha iyi korunacağına ilişkin öneriler sunar. Yani, herşey düzgün çalışıyorsa, bu iletiler ile rahatsız edilmezsiniz. İstediğiniz zaman **Windows Eylem Merkezi**, **Güvenlik** öğesi altında bilgisayar güvenliğinizin durumuna göz atabilirsiniz.
Windows Eylem Merkezi ayrıca size kurulu programları yönetme ve bunlar arasında seçim yapma olanağı sunar (örn. *Kurulu casus yazılım önleme programlarını görüntüle*).

Eylem Merkezi ayarları değiştir seçeneği altında uyarı iletilerini kapatabilirsiniz (örn. *Casus yazılımlar ve bunlara karşı koruma ile ilgili iletileri kapat*).

12.4.2 Windows Eylem Merkezi ve Avira ürününüz

Ağ güvenlik duvarı

Windows Eylem Merkezi'nden Avira Güvenlik Duvarı ile ilgili aşağıdaki bilgileri alabilirsiniz:

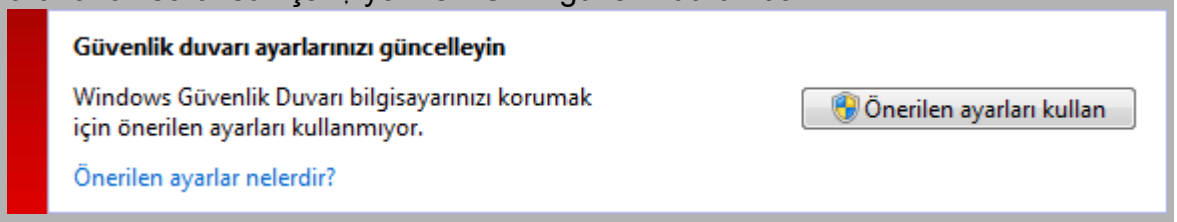
- Avira Güvenlik Duvarı açık olduğunu bildiriyor
- Windows Güvenlik Duvarı ve Avira Güvenlik Duvarı'nın her ikisi de kapalı olduklarını bildiriyor.
- Windows Güvenlik Duvarı kapatılmış veya yanlış ayarlanmış

Avira Güvenlik Duvarı açık olduğunu bildiriyor

Avira ürününüzü kurup Windows Güvenlik Duvarı'nı kapattıktan sonra, **Eylem Merkezi > Güvenlik > Ağ güvenlik duvarı** altında aşağıdaki iletiyi alırsınız: *Avira Güvenlik Duvarı açık olduğunu bildiriyor*. Bu ileti, Avira Güvenlik Duvarı'nı güvenlik duvarı çözümü olarak seçtiğinizi gösterir. (Lütfen Windows Güvenlik Duvarı ve Avira Güvenlik Duvarı, büyük W ile, arasındaki farka dikkat edin).

Uyarı

Denetim Masası > Windows Güvenlik Duvarı seçeneği altında, **bahsedilen tek ürün Windows Güvenlik Duvarı olup, Avira Güvenlik Duvarı değildir**. Bunun için iletide herşey kırmızı olarak gösterilir: *Güvenlik Duvarı ayarlarınızı güncelleyin* ve ***Windows Güvenlik Duvarı bilgisayarınızın korunması için önerilen ayarları kullanmıyor***. Sizin hiçbir şey yapmanız gerekmez, Avira ürününüz sorunsuz çalışıyor ve PC'niz güvenli durumda.

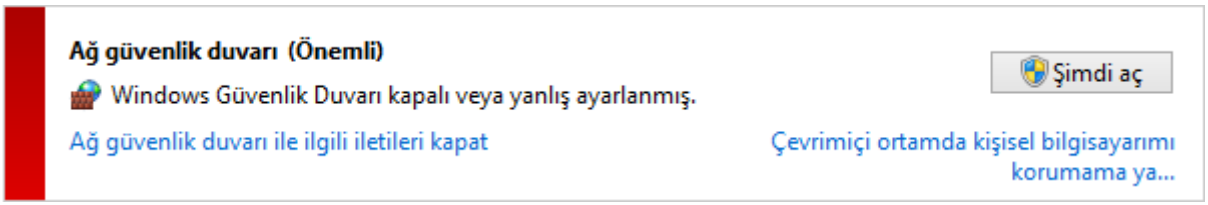


Windows Güvenlik Duvarı ve Avira Güvenlik Duvarı'nın her ikisi de kapalı olduklarını bildiriyor

Avira Güvenlik Duvarı'nı devre dışı bıraktığınızda hemen aşağıdaki iletiyi alırsınız:

Uyarı
Avira Güvenlik Duvarı'nı kapatırsanız, yetkisiz kullanıcılar ağ veya Internet üzerinden bilgisayarınıza erişim sağlayabilir.

Windows Güvenlik Duvarı kapalı veya yanlış ayarlanmış



Yani ne Windows Güvenlik Duvarı ne de Avira'nın Güvenlik Duvarı aktif değil. Bu mesajı iki farklı durumda alabilirsiniz:

- **Avira Güvenlik Duvarı**

  Avira Güvenlik Duvarı yanlış ayarlanmış veya doğru şekilde kurulmamış. Avira Güvenlik Duvarı Windows Eylem Merkezi tarafından hemen agılanmalıdır. Lütfen bilgisayarınızı yeniden başlatmayı deneyin ve eğer bu işe yararsa Avira'yı yeniden kurun.

- **Avira tarafından yönetilen Windows Güvenlik Duvarı**

  Windows 7'den itibaren, Avira Professional Security Avira Güvenlik Duvarı içermez, ancak size Windows Güvenlik Duvarını doğrudan Avira Kontrol ve Yapılandırma Merkezinden yönetme seçeneği verir.

Virüs koruması

Windows Eylem Merkezi'nden virüs korumanızla ilgili aşağıdaki bilgileri alabilirsiniz:

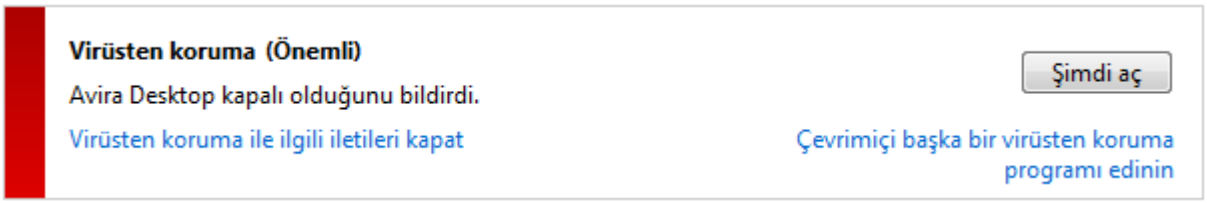
- Avira Desktop güncel olduğunu ve virüs taramasının açık olduğunu bildiriyor.
- Avira Desktop kapalı olduğunu bildiriyor.
- Avira Desktop güncel olmadığını bildiriyor.
- Windows bu bilgisayarda antivirüs yazılımı bulamadı.
- Avira Desktop süresi doldu.

Avira Desktop güncel olduğunu ve virüs taramasının açık olduğunu bildiriyor

Avira ürününüzün kurulumundan ve ardından yapılan güncelleme işleminden sonra Windows Eylem Merkezi'nden herhangi bir ileti almazsınız. Ancak, **Eylem Merkezi > Güvenlik** seçeneğine giderseniz, şu iletiyi görebilirsiniz: *Avira Desktop güncel olduğunu ve virüs taramasının açık olduğunu bildiriyor.* Bu durum, Avira ürününüzün güncel ve Avira Gerçek Zamanlı Koruma'nın etkin olduğu anlamına gelir.

Avira Desktop kapalı olduğunu bildiriyor

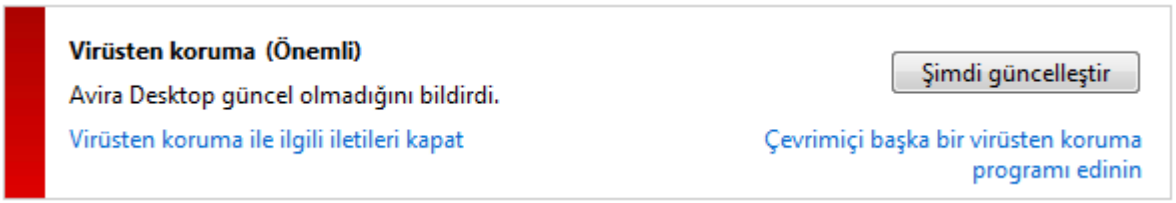
Avira Gerçek Zamanlı Koruma'ı devre dışı bırakırsanız veya Gerçek Zamanlı Koruma hizmetini durdurursanız, aşağıdaki iletiyi alırsınız.



Not
Avira Gerçek Zamanlı Koruma'yı **Avira Kontrol Merkezi'nin Durum** bölümünde etkinleştirebilir veya devre dışı bırakabilirsiniz. Avira Gerçek Zamanlı Koruma'nın görev çubuğunuzdaki açık kırmızı şemsiye aracılığıyla da etkinleştirildiğini görebilirsiniz. Avira ürününü Windows Eylem Merkezi iletisindeki *Şimdi aç* düğmesine tıklayarak da etkinleştirmek mümkündür. Avira'yı çalıştırmak için izninizi isteyen bir bildirim alırsınız. *Evet, yayıncıya güveniyorum ve bu programı çalıştırmak istiyorum* seçeneğine tıkladığınızda Gerçek Zamanlı Koruma tekrar etkinleşir.

Avira Desktop güncel olmadığını bildiriyor

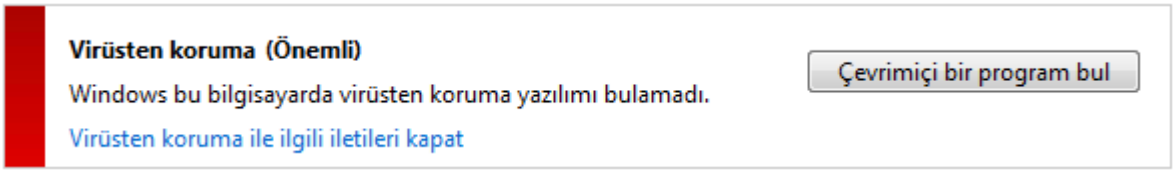
Avira ürününüzü yeni kurduğunuzda veya Avira ürününüzün virüs tanımı dosyası, tarama motoru veya program dosyaları herhangi bir nedenle otomatik olarak güncellenmediği takdirde (örn. Avira ürününüzün önceden kurulu olduğu eski Windows işletim sisteminizi yeni bir sürüme güncellediğinizde, aşağıdaki iletiyi alırsınız:



Not
Windows Eylem Merkezi'nin, Avira ürününüzü güncel olarak tanıması için, kurulumdan sonra bir güncelleme gerçekleştirilmelidir. Bir güncelleme gerçekleştirerek Avira Ürününüzü güncelleyin.

Windows bu bilgisayarda antivirüs yazılımı bulamadı

Windows Eylem Merkezi bilgisayarınızda herhangi bir anti virüs yazılımı bulmadığında, Windows Eylem Merkezi'nin bilgileri görüntülenir.

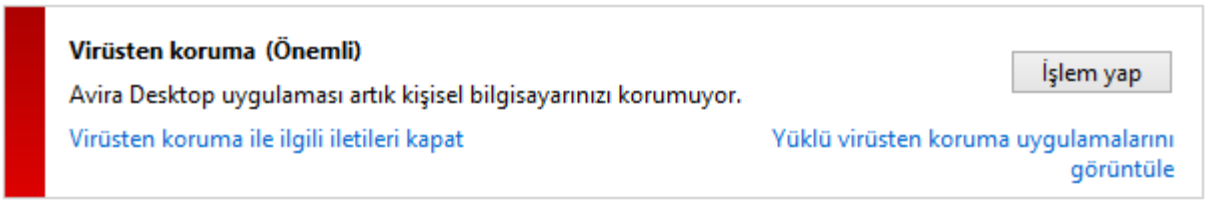


Not
Windows Defender önceden tanımlı virüs koruma uygulaması olduğundan, bu seçenek Window 8'de görüntülenmez.

Not
Bilgisayarınızı virüslere ve diğer istenmeyen programlara karşı korumak için bilgisayarınıza Avira ürününüzü kurun!

Avira Desktop süresi doldu

Avira ürününbüzün lisans süresi sona erdiğinde, Windows Eylem Merkezi'nin bilgileri görüntülenir.
Aboneliği yenile düğmesine tıkladığınızda, yeni bir lisans alabileceğiniz Avira web sitesine yönlendirilirsiniz.



Not
Bu seçenek yalnızca Windows 8'de kullanılabilir.

Casus yazılım ve istenmeyen yazılım koruması

Windows Eylem Merkezi'nden casus yazılım korumanızla ilgili aşağıdaki bilgileri alabilirsiniz:

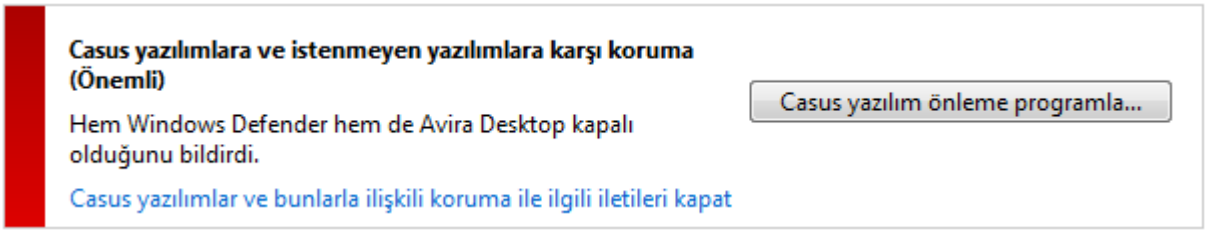
- Avira Desktop açık olduğunu bildiriyor.
- Windows Defender ve Avira Güvenlik Duvarı'nın her ikisi de kapalı olduklarını bildiriyor.
- Avira Desktop güncel olmadığını bildiriyor.
- Windows Defender güncel değil.
- Windows Defender kapalı.

Avira Desktop açık olduğunu bildiriyor

Avira ürününüzün kurulumundan ve ardından yapılan güncelleme işleminden sonra Windows Eylem Merkezi'nden herhangi bir ileti almazsınız. Ancak, **Eylem Merkezi > Güvenlik** seçeneğine giderseniz, şu iletiyi görebilirsiniz: *Avira Desktop güncel olduğunu ve virüs taramasının açık olduğunu bildiriyor*. Bu durum, Avira ürününüzün güncel ve Avira Gerçek Zamanlı Koruma'nın etkin olduğu anlamına gelir.

Windows Defender ve Avira Güvenlik Duvarı'nın her ikisi de kapalı olduklarını bildiriyor

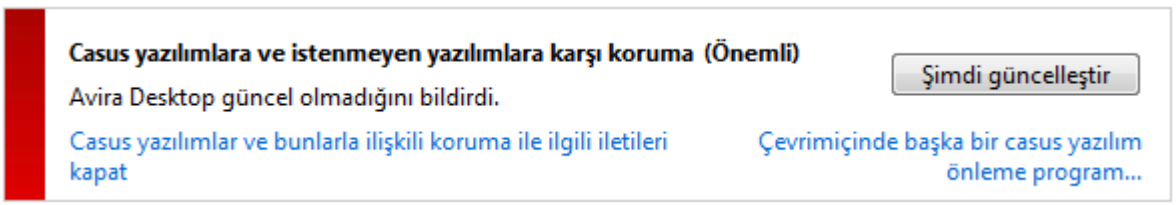
Avira Gerçek Zamanlı Koruma'yı devre dışı bırakırsanız veya Gerçek Zamanlı Koruma hizmetini durdurursanız, aşağıdaki iletiyi alırsınız.



Not
Avira Gerçek Zamanlı Koruma'yı **Avira Kontrol Merkezi'nin Durum** bölümünde etkinleştirebilir veya devre dışı bırakabilirsiniz. Avira Gerçek Zamanlı Koruma'nın görev çubuğunuzdaki açık kırmızı şemsiye aracılığıyla da etkinleştirildiğini görebilirsiniz. Avira ürününü Windows Eylem Merkezi iletisindeki *Şimdi aç* düğmesine tıklayarak ta etkinleştirmek mümkündür. Avira'yı çalıştırmak için izninizi isteyen bir bildirim alırsınız. *Evet, yayıncıya güveniyorum ve bu programı çalıştırmak istiyorum* seçeneğine tıkladığınızda Gerçek Zamanlı Koruma tekrar etkinleşir.

Avira Desktop güncel olmadığını bildiriyor

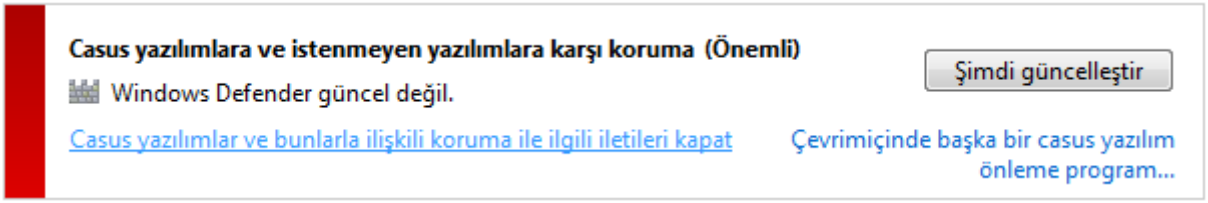
Avira ürününüzü yeni kurduğunuzda veya Avira ürününüzün virüs tanımı dosyası, tarama motoru veya program dosyaları herhangi bir nedenle otomatik olarak güncellenmediği takdirde (örn. Avira ürününüzün önceden kurulu olduğu eski Windows işletim sisteminizi yeni bir sürüme güncellediğinizde, aşağıdaki iletiyi alırsınız:



Not
Windows Eylem Merkezi'nin, Avira ürününüzü güncel olarak tanıması için, kurulumdan sonra bir güncelleme gerçekleştirilmelidir. Bir güncelleme gerçekleştirerek Avira Ürününüzü güncelleyin.

Windows Defender güncel değil

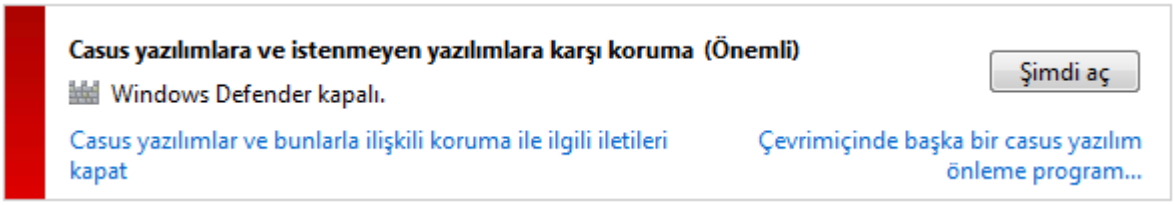
Windows Defender etkin durumdaysa aşağıdaki iletiyi alabilirsiniz. Avira ürünü zaten kuruluysa, bu iletinin görüntülenmemesi beklenir. Lütfen kurulumun Tamam olup olmadığını kontrol edin.



Not
Windows Defender Windows tarafından sunulan önceden tanımlı bir casus yazılım ve virüs koruma çözümüdür.

Windows Defender kapalı

Windows Eylem Merkezi bilgisayarınızda işletim sisteminin varsayılan olarak içerdiği Windows Defender dışında başka herhangi bir anti virüs yazılımı bulmadığında, Windows Eylem Merkezi'nin bilgileri görüntülenir. Bilgisayarınızda yüklü başka antivirüs yazılımları varsa, bu uygulama devre dışı bırakılır. Avira ürünü zaten kuruluysa, bu iletinin görüntülenmemesi beklenir: Avira otomatik olarak algılanmalıdır. Lütfen kurulumun Tamam olup olmadığını kontrol edin.



13. Virüsler ve daha fazlası

Avira Professional Security yalnızca virüs ve zararlı yazılımları algılamakla kalmaz, sizi diğer tehditlere karşı da koruyabilir. Bu kısımda farklı zararlı yazılım türlerinin ve diğer tehditlerin geçmişlerinin, davranışlarının ve beraberinde getirdikleri hoş olmayan sürprizlerinin açıklandığı bir genel bakışını bulabilirsiniz.

İlgili konular:

- Tehdit kategorileri
- Virüsler ve diğer zararlı yazılımlar

13.1 Tehdit kategorileri

Reklam Yazılımı

Reklam yazılımı, bilgisayar ekranında görüntülenen bir çubuk aracılığıyla başlık sayfası reklamlarını veya açılır pencereleri sunan yazılımlardır. Bu reklamlar genellikle kaldırılamaz ve sonuçta her zaman görünür olur. Bağlantı verileri, kullanım davranışıyla ilgili birçok sonuca olanak sağlar ve veri güvenliği açısından sorunludur.

Avira ürününüz reklam yazılımını algılar. **Reklam Yazılımı** seçeneği, Tehdit kategorileri konumundaki yapılandırmada bir onay işaretiyle etkinleştirilmişse, Avira ürününüz bir reklam yazılımı algıladığında, karşılık gelen bir uyarı alırsınız.

Reklam Yazılımı/Casus Yazılım

Genellikle kullanıcının bilgisi veya izni olmaksızın kullanıcının kişisel verilerini üçüncü bir tarafa gönderen ve bu nedenle istenmeyen reklam veya yazılımları görüntüleyen yazılım.

Avira ürününüz "Reklam Yazılımlarını/Casus Yazılımları" tanır. **Reklam Yazılımı/Casus Yazılım** seçeneği, Tehdit kategorileri konumundaki yapılandırmada bir onay işaretiyle etkinleştirilmişse, Avira ürününüz bir reklam yazılımı veya casus yazılım algıladığında, karşılık gelen bir uyarı alırsınız.

Uygulama

APPL, ilgili uygulama terimi, kullanıldığında risk oluşturabilen veya şüpheli kaynaktan gelmiş olabilen bir uygulamayı ifade eder.

Avira ürününüz "Uygulamayı (APPL)" tanır. **Uygulama** seçeneği, Tehdit kategorileri konumundaki yapılandırmada bir onay işaretiyle etkinleştirilmişse, Avira ürününüz böyle bir davranış algıladığında, karşılık gelen bir uyarı alırsınız.

Arka Kapı İstemcileri

Veri çalmak veya bilgisayarları manipüle etmek için, kullanıcının bilgisi dışında bir arka kapı sunucu programı kaçak olarak bilgisayara sokulur. Bu program, İnternet veya ağ üzerinden arka kapı denetim yazılımı (istemci) kullanılarak üçüncü tarafça denetlenebilir.

Avira ürününüz, "Arka kapı denetim yazılımını" tanır. **Arka kapı denetim yazılımı** seçeneği, Tehdit kategorileri konumundaki yapılandırmada bir onay işaretiyle etkinleştirilmişse, Avira ürününüz böyle bir yazılım algıladığında, karşılık gelen bir uyarı alırsınız.

Numara Çevirici

Internet'te kullanılabilir olan belirli hizmetler ücretlidir. Almanya'da 0190/0900 numarası ile numara çeviriciler aracılığıyla faturalandırılır (veya Avusturya ve İsviçre'de 09x0 numaraları aracılığıyla; Almanya'da bu numara orta vadede 09x0 olarak değişecek şekilde ayarlanmıştır). Bilgisayara kurulduktan sonra bu programlar, ücret ölçeği büyük ölçüde değişiklik gösterebilen uygun bir ücretli numara aracılığıyla bağlantıyı garantiler.

Telefon faturanız aracılığıyla çevrimiçi içeriğin pazarlanması yasal olup kullanıcı için avantaj niteliğinde olabilir. Orijinal çeviriciler, kullanıcı tarafından bilerek ve kasten kullanıldıkları konusunda şüpheye yer vermez. Bunlar tamamen net ve açıkça görünür etiketleme veya istek yoluyla verilmesi gereken kullanıcı iznine tabi olarak kullanıcının bilgisayarına kurulur. Orijinal çeviricilerin çevirme işlemi net olarak görüntülenir. Ayrıca, orijinal çeviriciler oluşan maliyetleri tam ve hatasız olarak size bildirir.

Ne yazık ki bildirimde bulunmaksızın, belirsiz yollarla veya aldatıcı amaçlarla bilgisayarlara kurulan çeviriciler de vardır. Örneğin, bunlar Internet kullanıcısının ISP (Internet Hizmet Sağlayıcısı) ile varsayılan veri iletişimi bağlantısının yerini alır ve her bağlantı kurulduğunda maliyetli ve genellikle son derece pahalı olan 0190/0900 numarasını çevirir. Etkilenen kullanıcı bilgisayarında istenmeyen bir 0190/0900 numara çevirici programının her bağlantıda ücretli bir numara çevirdiğini büyük ihtimalle bir sonraki telefon faturasına kadar fark etmez ve bu da büyük ölçüde yüksek maliyetlerle sonuçlanır.

Telefon sağlayıcınızdan, istenmeyen çeviricilere karşı anında koruma için doğrudan bu numara aralığını engellemesini istemenizi öneririz (0190/0900 çeviriciler).

Avira ürününüz varsayılan olarak benzer numara çeviricileri algılayabilir.

Numara Çeviriciler seçeneği, Tehdit kategorileri konumundaki yapılandırmada bir onay işaretiyle etkinleştirilmişse, bir çevirici algılandığında, karşılık gelen bir uyarı alırsınız. Şimdi, istenmiyor olabilecek 0190/0900 numara çeviricisini silebilirsiniz. Ancak bu istenen bir çevirme programıysa, bunu özel bir dosyada bildirebilirsiniz; böylece bu dosya gelecekte taranmaz.

Çift Uzantı Dosyaları

Gerçek dosya uzantısını şüpheli şekilde gizleyen yürütülebilir dosyalar. Bu kamuflaj yöntemi genellikle zararlı yazılımlar tarafından kullanılır.

Avira ürününüz, "Çift Uzantı Dosyalarını" tanır. **Çift Uzantı dosyaları** seçeneği, Tehdit kategorileri konumundaki yapılandırmada bir onay işaretiyle etkinleştirilmişse, Avira ürününüz böyle dosyaları algıladığında, karşılık gelen bir uyarı alırsınız.

Sahte yazılım

"Faydasız yazılım" veya "sahte antivirüs yazılımı" olarak da bilinen yazılım, bilgisayarınızı virüs veya zararlı yazılımdan etkilenmiş gibi gösteren sahte bir yazılımdır. Bu yazılımlar profesyonel antivirüs yazılımlarına benzer görünse de, asıl amacı belirsizlik yaratmak ve kullanıcıyı korkutmaktır. Amacı kişileri olmayan (gerçek dışı) tehlikelere karşı tehdit altında hissettirmek ve bu tehlikeyi yok etmek için para almaktır. Kişilerin saldırı altında olduklarına inandırıldıkları ve aslında gerçek saldırıya yol açacak bazı eylemler yapmaları istenen durumlar da olmaktadır.

Avira ürününüz faydasız yazılımı algılar. **Sahte yazılım** seçeneği, Tehdit kategorileri konumundaki yapılandırmada bir onay işaretiyle etkinleştirilmişse, Avira ürününüz böyle dosyaları algıladığında, karşılık gelen bir uyarı alırsınız.

Oyunlar

Bilgisayar oyunları için bir yer vardır - ancak bu, işte gerekli değildir (belki öğle yemeği molası dışında). Yine de, Internet'ten karşıdan yüklenebilen çok çeşitli oyunlar sayesinde, şirket çalışanları ve devlet memurları arasında mayın tarlası ve Sabır oyunları yaygındır. Internet aracılığıyla çok çeşitli oyunları karşıdan yükleyebilirsiniz. E-posta oyunları da daha popüler bir hale geldi: basit satranç oyunundan "filo alıştırmaları"na uzanan (torpido saldırıları dahil) çok sayıda varyant dolaşmaktadır: İlgili hareketler, e-posta programları ile ortaklara gönderilmekte ve onlar tarafından yanıtlanmaktadır.

Çalışmalar, bilgisayar oyunlarına ayrılan çalışma saati süresinin, ekonomik olarak önemli düzeylere ulaştığını göstermiştir. Bu nedenle, gittikçe daha fazla şirketin, işyeri bilgisayarlarından bilgisayar oyunlarını yasaklamanın yollarını düşünmekte olması hiç de şaşırtıcı değildir.

Avira ürününüz, bilgisayar oyunlarını tanır. **Oyunlar** seçeneği, Tehdit kategorileri konumundaki yapılandırmada bir onay işaretiyle etkinleştirilmişse, Avira ürününüz bir oyun algıladığında, karşılık gelen bir uyarı alırsınız. Oyun şimdi tam anlamıyla bitmiştir, silebilirsiniz.

Şakalar

Şakalar, zarara veya çoğaltmaya neden olmadan birisini korkutmak veya eğlendirmek için tasarlanmıştır. Bir şaka programı yüklendiğinde bilgisayar genellikle bir noktada bir melodi çalmaya başlar ve ekranda olağandışı bir şeyler görüntüler. Şaka örnekleri olarak, disk sürücüsünde çamaşır makinesi (DRAIN.COM) veya ekran yiyicisi (BUGSRES.COM) verilebilir.

Ancak unutmayın! Şaka programlarının tüm belirtileri bir virüs veya Truva atından da kaynaklanabilir. En azından kullanıcılar şok olup yaşadıkları panikle kendileri gerçek bir zarara neden olabilir.

Tarama ve tanımlama yordamlarının uzantısı sayesinde Avira ürününüz şaka programlarını algılayabilir ve gerekirse bunları istenmeyen programlar olarak ortadan kaldırabilir. **Şakalar** seçeneği, Tehdit kategorileri konumundaki yapılandırmada bir onay işaretiyle etkinleştirilmişse, bir şaka programı algılandığında, karşılık gelen bir uyarı verilir.

Kimlik Avı

"Marka sahtekarlığı" olarak da bilinen kimlik avı, Internet hizmeti sağlayıcılarının, bankaların, çevrimiçi bankacılık hizmetlerinin, kayıt yetkililerinin müşterilerini veya olası müşterilerini hedefleyen, akıllıca bir veri hırsızlığı biçimidir.
Internet üzerinden e-posta adresinizi gönderirken, çevrimiçi formları doldururken, haber gruplarına veya web sitelerine erişirken verileriniz "Internet'te gezinen veri toplayıcılar" tarafından çalınabilir ve sonra sahtekarlık veya diğer suçlara girişimde bulunmak için izniniz olmadan kullanılır.

Avira ürününüz, "Kimlik avını" tanır. **Kimlik Avı** seçeneği, Tehdit kategorileri konumundaki yapılandırmada bir onay işaretiyle etkinleştirilmişse, Avira ürününüz böyle bir davranış algıladığında, karşılık gelen bir uyarı alırsınız.

Özel etki alanını ihlal eden programlar

Sisteminizin güvenliğine zarar verebilecek, istenmeyen program etkinlikleri başlatabilecek, gizliliğinize saldırabilecek veya kullanıcı davranışınıza casusluk yapabilecek ve bu nedenle istenmeyen olabilecek yazılımlar.

Avira ürününüz, "Güvenlik Gizlilik Riski" yazılımını algılar. **Özel etki alanını ihlal eden programlar** seçeneği, Tehdit kategorileri konumundaki yapılandırmada bir onay işaretiyle etkinleştirilmişse, Avira ürününüz böyle bir yazılım algıladığında, karşılık gelen bir uyarı alırsınız.

Olağandışı Çalışma Zamanı Paketleyicileri

Olağandışı çalışma zamanı paketleyicisi ile sıkıştırılmış ve bu nedenle şüpheli olarak sınıflandırılabilen dosyalar.

Avira ürününüz, "Olağandışı çalışma zamanı paketleyicilerini" tanır. **Olağandışı çalışma zamanı paketleyicileri** seçeneği, Tehdit kategorileri konumundaki yapılandırmada bir onay işaretiyle etkinleştirilmişse, Avira ürününüz böyle paketleyicileri algıladığında, karşılık gelen bir uyarı alırsınız.

13.2 Virüsler ve diğer zararlı yazılımlar

Reklam Yazılımı

Reklam yazılımı, bilgisayar ekranında görüntülenen bir çubuk aracılığıyla başlık sayfası reklamlarını veya açılır pencereleri sunan yazılımlardır. Bu reklamlar genellikle

kaldırılamaz ve sonuçta her zaman görünür olur. Bağlantı verileri, kullanım davranışıyla ilgili birçok sonuca olanak sağlar ve veri güvenliği açısından sorunludur.

Arka Kapılar

Arka kapı, bilgisayar erişimi güvenlik mekanizmalarını atlayarak bir bilgisayara erişim elde edebilir.

Arka planda yürütülmekte olan bir program genellikle saldırgana neredeyse sınırsız haklar sağlar. Kullanıcının kişisel verilerine, arka kapının yardımı ile casusluk yapılabilir. Ancak asıl olarak ilgili sisteme daha fazla bilgisayar virüsü veya solucanlar kurmak için kullanılır.

Önyükleme virüsleri

Sabit disklerin önyükleme veya ana önyükleme sektörü asıl olarak önyükleme sektörü virüslerinden etkilenir. Bunlar, sistem yürütüme için gerekli olan önemli bilgilerin üzerine yazar. Tuhaf sonuçlardan biri: bilgisayar sistemi artık yüklenemez…

Bot Ağı

Bot ağı, birbiriyle iletişim kuran bot'lardan oluşan uzak kişisel bilgisayarlar ağı (Internet'te) olarak tanımlanır. Bot ağı, ortak bir komut ve denetim altyapısı altında programlar (genellikle solucan, Truva atı olarak ifade edilir) çalıştıran çökmüş makineler koleksiyonundan oluşabilir. Bot ağları, genellikle etkilenen kişisel bilgisayar kullanıcısının bilgisi olmadan hizmet reddi saldırıları, vb. gibi çeşitli amaçlara hizmet eder. Bot ağlarının gerçekleştirebileceği ana olasılık, binlerce bilgisayara kadar büyümeyi başarabilmesi ve bunların toplam bant genişliklerinin en geleneksel Internet erişimlerini aşmasıdır.

Güvenlik Açığı

Güvenlik açığı, bilgisayar sisteminde ayrıcalık artırmaya veya hizmet reddine yol açan bir hata, arıza ya da güvenlik açığından yararlanan bir bilgisayar programı veya komut dosyasıdır. Güvenlik açığı biçimine örnek olarak, manipüle edilen veri paketleri yardımıyla Internet'ten gelen bir saldırı verilebilir. Daha yüksek erişim elde etmek için programlar bilgisayara sızabilir.

Sahte yazılım

"Faydasız yazılım" veya "sahte antivirüs yazılımı" olarak da bilinen yazılım, bilgisayarınızı virüs veya zararlı yazılımdan etkilenmiş gibi gösteren sahte bir yazılımdır. Bu yazılımlar profesyonel antivirüs yazılımlarına benzer görünse de, asıl amacı belirsizlik yaratmak ve kullanıcıyı korkutmaktır. Amacı kişileri olmayan (gerçek dışı) tehlikelere karşı tehdit altında hissettirmek ve bu tehlikeyi yok etmek için para almaktır. Kişilerin saldırı altında olduklarına inandırıldıkları ve aslında gerçek saldırıya yol açacak bazı eylemler yapmaları istenen durumlar da olmaktadır.

Sahtekarlıklar

Yıllardır, Internet ve diğer ağ kullanıcıları, e-postayla yayıldığı söylenen virüslerle ilgili uyarılar almıştır. Bu uyarılar, herkesi "tehlikeye" karşı uyarmak için, mümkün olan en çok sayıda iş arkadaşına ve diğer kullanıcılara gönderilmesi isteğiyle e-posta aracılığıyla yayılır.

Sanal Sunucu

Sanal sunucu, ağa kurulu bir hizmettir (program veya sunucu). İşlevi, bir ağı ve günlük saldırılarını izlemektir. Bu hizmet, geçerli kullanıcı tarafından bilinmez - bu nedenle asla geçerli kullanıcının adresine yönlendirilmez. Bir saldırgan, bir ağda zayıf noktalar olup olmadığını inceler ve sanal sunucu tarafından sunulan hizmetleri kullanırsa, bu günlüğe kaydedilir ve bir uyarı tetiklenir.

Makro virüsler

Makro virüsler, bir uygulamanın makro dilinde (örn. WinWord 6.0 altında WordBasic) yazılan ve normalde yalnızca bu uygulamanın belgeleri içinde yayılabilen küçük programlardır. Bu nedenle, belge virüsleri olarak da adlandırılır. Etkin olması için, karşılık gelen uygulamaların etkinleştirilmesi ve etkilenen makrolardan birinin yürütülmesi gerekir. "Normal" virüslerden farklı olarak makro virüsler, yürütülebilir dosyalara saldırmaz, ancak karşılık gelen barındırma uygulamasının belgelerine saldırır.

Websitesini başka siteye yöneltme

Websitesini başka siteye yöneltme, sahtekar web sitelerine sorguları yönlendirmek için web tarayıcılarının barındırma dosyasının bir manipülasyonudur. Bu, klasik kimlik avının daha ileri bir modelidir. Websitesini başka siteye yöneltme dolandırıcıları, sahte web sitelerinin depolandığı kendi büyük sunucu gruplarını çalıştırır. Websitesini başka siteye yöneltme çeşitli DNS saldırısı türleri için bir kapsayıcı terim olarak ortaya çıkmıştır. Barındırma dosyasının manipülasyonu durumunda, Truva atı veya virüs yardımıyla sistemin belirli bir manipülasyonu gerçekleştirilir. Sonuçta, doğru web adresi girilse de sistem şimdi yalnızca sahte web sitelerine erişebilir.

Kimlik Avı

Kimlik avı, Internet kullanıcısının kişisel ayrıntılarının avlanması anlamına gelir. Kimlik avcıları genellikle kurbanlarına iyi niyetle gizli bilgilerini, özellikle de çevrimiçi bankacılık hesaplarının kullanıcı adı ve parolalarını veya PIN ve TAN'larını saldırgana ifşa etmelerini sağlamak için tasarlanmış e-postalar gibi, resmiymiş gibi görünen mektuplar gönderir. Çalınmış erişim ayrıntıları ile kimlik avcıları, kurbanların kimliklerini üstlenebilir ve onların adlarıyla işlemler gerçekleştirebilir. Bir durum açıktır: bankalar ve sigorta şirketleri asla kredi kartı numaralarını, PIN, TAN veya diğer erişim ayrıntılarını e-posta, SMS ya da telefon yoluyla sormaz.

Çok biçimli virüsler

Çok biçimli virüsler, gerçek kimliğe bürünme uzmanlarıdır. Kendi programlama kodlarını değiştirir ve bu nedenle çok zor algılanır.

Program virüsleri

Bilgisayar virüsü, yürütüldükten sonra diğer programlara kendiliğinden eklenip virüse neden olur. Virüsler, mantıksal bombalar ve Truva atlarından farklı olarak kendi kendilerine çoğalır. Solucanın tersine virüs, her zaman zararlı kodunu yerleştirdiği ana bilgisayar olarak bir program gerektirir. Ana bilgisayarın program yürütmesi, kural olarak değiştirilmez.

Kök kullanıcı takımı

Kök kullanıcı takımı, casusun oturum açma işlemlerini gizlemek, işlemleri gizlemek ve verileri kaydetmek; genel olarak konuşmak gerekirse, kendilerini görünmez yapmak için bir bilgisayar sistemine sızıldıktan sonra: kendilerini görünmez hale getirmektir. Önceden kurulmuş casus programları güncellemeye ve silinen casus yazılımları yeniden kurmaya çalışır.

Komut dosyası virüsleri ve solucanlar

Bu virüsler son derece kolayca programlanır ve e-posta aracılığıyla birkaç saat içinde tüm dünyaya yayılabilir (gerekli teknoloji el altındaysa).

Komut dosyası virüsleri ve solucanlar, diğer komut dosyalarına, yeni komut dosyalarına kendilerini eklemek veya işletim sistemi işlevlerini çağırarak yayılmak için Javascript, VBScript, vb. gibi komut dosyası dillerinden birini kullanır. Bu genellikle e-posta aracılığıyla veya dosya (belge) alışverişi yoluyla gerçekleşir.

Solucan, kendi kendine çoğalan, ancak ana bilgisayarı etkilemeyen bir programdır. Solucanlar sonuçta diğer program dizilerinin parçasını oluşturamaz. Solucanlar genellikle kısıtlı güvenlik önlemlerine sahip sistemlere her türlü hasar veren programları sızdırma olanağıdır.

Casus yazılım

Casus yazılım, kullanıcının izni olmadan bilgisayarın çalışmasını kesintiye uğratan veya kısmi olarak denetimini ele geçiren casus programlardır. Casus yazılım, ticari kazanç için etkilenen bilgisayarların güvenlik açığından yararlanmak üzere tasarlanmıştır.

Truva atları (kısa Truva atları)

Truva atları şu günlerde oldukça yaygındır. Truva atları, belirli bir işleve sahipmiş gibi hareket eden, ancak yürütme işleminden sonra gerçek yüzünü gösteren ve farklı bir işlev gerçekleştiren, hatta çoğu zamanlarda yıkıcı olan programları içerir. Truva atları kendi kendine çoğalamaz ve bu yönüyle virüs ve solucanlardan ayrılır. Çoğu, kullanıcıyı Truva atını başlatmaya teşvik etmek amacıyla ilgi çekici bir ada (SEX.EXE veya STARTME.EXE) sahiptir. Yürütmeden hemen sonra bunlar etkin olur ve örneğin, sabit diski biçimlendirebilir. Dosya yükleyen (dropper); virüsleri 'yükleyen', başka bir deyişle bilgisayar sistemine virüsleri gömen özel bir Truva atı biçimidir.

Zombi

Zombi kişisel bilgisayar, zararlı programlardan etkilenen ve bilgisayar korsanlarının suç amacıyla uzaktan kumanda aracılığıyla bilgisayarları kötü niyetle kullanmasına olanak sağlayan bir bilgisayardır. Etkilenen kişisel bilgisayar, örneğin, komut üzerine hizmet reddi (DoS) saldırılarını başlatır veya istenmeyen posta ve kimlik avı e-postaları gönderir.

14. Bilgi ve Hizmet

Bu bölüm Avira Bilgi ve Hizmetleri ile ilgili bilgiler içerir.

14.1 İletişim adresi

Avira ürün yelpazesiyle ilgili sorularınız veya istekleriniz varsa size yardımcı olmaktan mutluluk duyarız. İletişim adreslerimiz için lütfen **Yardım > Avira Professional Security Hakkında** altında Kontrol Merkezi konumuna bakın.

14.2 Teknik destek

Avira desteği, sorularınızın yanıtlanması ve teknik bir sorunun çözülmesi konusunda güvenilir yardım sağlar.

Kapsamlı destek hizmetimizdeki tüm gerekli bilgiler web sitemizden edinilebilir:

http://www.avira.com/tr/professional-support

Size hızlı ve güvenilir yardım sağlayabilmemiz için şu bilgileri hazır bulundurmanız gerekir:

- **Lisans bilgileri**. Bu bilgileri **Yardım > Avira Professional Security hakkında > Lisans bilgileri** menü öğesinin altındaki program arabiriminde bulabilirsiniz. Bkz. Lisans bilgileri.
- **Sürüm bilgileri**. Bu bilgileri **Yardım > Avira Professional Security hakkında > Sürüm bilgileri**. menü öğesinin altındaki program arabiriminde bulabilirsiniz.Bkz. Sürüm bilgileri.
- **İşletim sistemi sürümü** ve kurulu Hizmet Paketleri.
- **Kurulu yazılım paketleri**, örn. diğer satıcıların anti virüs yazılımları.
- Programın veya rapor dosyasının **tam iletileri**.

14.3 Şüpheli dosya

Ürünlerimiz tarafından algılanmayabilen veya kaldırılmayabilen ya da şüpheli dosyalar bize gönderilebilir. Bunu yapmak için size birçok yol sağlarız.

- Avira Sunucu Güvenlik Konsolu Kontrol Merkezi karantina yöneticisinde dosyayı tanımlayın ve bağlam menüsü ya da karşılık gelen düğme aracılığıyla **Dosya gönder** öğesini seçin.
- Bir e-postanın ekinde gerekli olan dosyayı (WinZIP, PKZip, Arj vb.) şu adrese gönderin: virus-professional-tr@avira.com
  Bazı e-posta ağ geçitleri anti virüs yazılımı ile birlikte çalıştığından, dosyalara bir parola sağlamanız gerekir (lütfen bize parolayı söylemeyi unutmayın).

- Ayrıca web sitemiz aracılığıyla şüpheli dosyayı bize gönderebilirsiniz: http://www.avira.com/tr/sample-upload

14.4 Yanlış pozitifleri bildirme

Avira Professional Security ürününüzün bir dosyada "temiz" olma olasılığı yüksek bir algılama bildirdiğine inanıyorsanız, paketlenmiş (WinZIP, PKZip, Arj, vb.) ilgili dosyayı şu adrese bir e-posta eki olarak gönderin:

virus-professional-tr@avira.com

Bazı e-posta ağ geçitleri anti virüs yazılımı ile birlikte çalıştığından, dosyalara bir parola sağlamanız gerekir (lütfen bize parolayı söylemeyi unutmayın).

14.5 Daha fazla güvenlik için geribildiriminiz

Avira 'da müşterilerimizin güvenliği çok önemlidir. Bu nedenle, yalnızca ürün yayınlanmadan önce her Avira çözümünün kalite ve güvenliğini sınayan şirket içi bir uzman ekibe sahip olmakla kalmayız. Gelişebilecek güvenlikle ilgili boşluklara yönelik göstergelere de çok önem verir ve bunlara ciddiyetle yaklaşırız.

Ürünlerimizden birinde bir güvenlik boşluğu algıladığınızı düşünüyorsanız, lütfen şu adresi kullanarak bize bir e-posta gönderin:

vulnerabilities@avira.tr

Avira

Sürüm: 4 çeyrek 2013

Avira | Kaplaneiweg 1 | 88069 Tettnang | Almanya | Telefon: +49 7542-500 0
www.avira.com