



# Avira

Antivirus Suite

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. Korunmalı ticari markalar bu kılavuzda bu şekilde işaretlenmemiştir. Ancak bu, söz konusu markaların serbestçe kullanılabilceği anlamına gelmez.

### Telif hakkı bilgileri

Avira Antivirus Suite için üçüncü taraf sağlayıcıların sunduğu kod kullanılmıştır. Kodu kullanımımıza sundukları için telif hakkı sahiplerine teşekkür ederiz.

Telif hakkıyla ilgili ayrıntılı bilgi için lütfen Avira Antivirus Suite 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

<b>1. Giriş.....</b>	<b>7</b>
1.1 Simgeler ve vurgular .....	7
<b>2. Ürün bilgileri .....</b>	<b>9</b>
2.1 Teslim kapsamı .....	9
2.2 Sistem gereksinimleri.....	10
2.2.1 Sistem gereksinimleri Avira Antivirus Suite.....	10
2.2.2 Sistem gereksinimleri Avira SearchFree Araç Çubuğu.....	11
2.2.3 Yönetici hakları (Windows Vista'dan itibaren).....	11
2.3 Lisanslama ve Yükseltme .....	12
2.3.1 Lisanslama .....	12
2.3.2 Bir lisansın süresini uzatma .....	12
2.3.3 Yükseltme.....	13
2.3.4 Lisans yöneticisi.....	13
<b>3. Kurulum ve kaldırma.....</b>	<b>15</b>
3.1 Ön Kurulum.....	16
3.2 Ekspres bir kurulum yapma .....	17
3.3 Özel bir Kurulum Yapma .....	18
3.4 Ürünü sına kurulumu.....	18
3.5 Kurulumu yapılandırma.....	20
3.6 Windows 7'de bir kurulumu değiştirme.....	20
3.7 Kurulum bileşenlerinin seçilmesi.....	20
3.8 Kaldırma .....	22
<b>4. Avira Antivirus Suite ürününe genel bakış .....</b>	<b>24</b>
4.1 Kullanıcı arabirimi ve çalışma .....	24
4.1.1 Kontrol Merkezi.....	24
4.1.2 Oyun Modu.....	27
4.1.3 Yapılandırma .....	28
4.1.4 Tepsi simgesi.....	31
4.2 Avira SearchFree Araç Çubuğu .....	32
4.2.1 Kullanım .....	33

4.2.2	Seçenekler .....	36
4.2.3	Windows 7'de Avira SearchFree Araç Çubuğu 'nu kaldırma.....	39
4.3	Nasıl yapılır...? .....	40
4.3.1	Lisans etkinleştirme .....	40
4.3.2	Ürün etkinleştir .....	41
4.3.3	Otomatik güncelleme gerçekleştir .....	42
4.3.4	El ile güncelleme başlat .....	43
4.3.5	Virüslere ve zararlı yazılımlara karşı tarama yapmak için bir tarama profili kullanma.....	44
4.3.6	Sürükleyip Bırak yöntemini kullanarak virüslere ve zararlı yazılımlara karşı tarama yapma .....	46
4.3.7	Bağlam menüsü aracılığıyla virüslere ve zararlı yazılımlara karşı tarama yapma .....	46
4.3.8	Virüslere ve zararlı yazılımlara karşı otomatik olarak tarama yapma .....	46
4.3.9	Kök kullanıcı takımına ve etkin zararlı yazılımlara karşı hedeflenmiş tarama.....	48
4.3.10	Algılanan virüslere ve zararlı yazılımlara yanıt verme .....	48
4.3.11	Karantinaya alınan dosyaları (*.qua) işleme .....	53
4.3.12	Karantinadaki dosyaları geri yükleme.....	55
4.3.13	Şüpheli dosyaları karantinaya taşıma.....	57
4.3.14	Bir tarama profilinde dosya türünü değiştirme veya silme.....	57
4.3.15	Tarama profili için masaüstü kısayolu oluşturma .....	58
4.3.16	Olayları filtreleme .....	58
4.3.17	E-posta adreslerini tarama dışında bırakma.....	59
<b>5.</b>	<b>Sistem Tarayıcı.....</b>	<b>60</b>
<b>6.</b>	<b>Güncellemeler .....</b>	<b>61</b>
<b>7.</b>	<b>Güvenlik Duvarı.....</b>	<b>63</b>
<b>8.</b>	<b>SSS, İpuçları .....</b>	<b>64</b>
8.1	Sorun olması durumunda yardım .....	64
8.2	Kısayollar.....	68
8.2.1	İletişim kutularında.....	68
8.2.2	Yardımda .....	69
8.2.3	Kontrol Merkezi'nde.....	70
8.3	Windows Güvenlik Merkezi .....	72
8.3.1	Genel.....	72
8.3.2	Windows Güvenlik Merkezi ve Avira ürününüz.....	72
8.4	Windows Eylem Merkezi.....	75
8.4.1	Genel.....	75

8.4.2	Windows Eylem Merkezi ve Avira ürününüz .....	76
<b>9.</b>	<b>Virüsler ve daha fazlası .....</b>	<b>81</b>
9.1	Tehdit kategorileri .....	81
9.2	Virüsler ve diğer zararlı yazılımlar.....	84
<b>10.</b>	<b>Bilgi ve Hizmet .....</b>	<b>89</b>
10.1	İletişim adresi .....	89
10.2	Teknik destek .....	89
10.3	Şüpheli dosya .....	89
10.4	Yanlış pozitifleri bildirme .....	90
10.5	Daha fazla güvenlik için geribildiriminiz.....	90
<b>11.</b>	<b>Başvuru: Yapılandırma seçenekleri .....</b>	<b>91</b>
11.1	Sistem Tarayıcı .....	91
11.1.1	Tara .....	91
11.1.2	Rapor .....	100
11.2	Gerçek Zamanlı Koruma.....	101
11.2.1	Tara .....	101
11.2.2	Rapor .....	112
11.3	Güncelle .....	113
11.3.1	Web sunucusu .....	113
11.4	Güvenlik Duvarı .....	115
11.4.1	Güvenlik Duvarını Yapılandırma .....	115
11.4.2	Windows Güvenlik Duvarı.....	115
11.5	Web Koruması .....	118
11.5.1	Tara .....	118
11.5.2	Rapor .....	126
11.6	EPosta Koruması.....	127
11.6.1	Tara .....	127
11.6.2	Genel.....	132
11.6.3	Rapor .....	133
11.7	Mobil Koruma.....	134
11.8	Genel .....	134
11.8.1	Tehdit kategorileri.....	134
11.8.2	Gelişmiş koruma.....	135

11.8.3	Parola.....	139
11.8.4	Güvenlik .....	141
11.8.5	WMI .....	143
11.8.6	Olaylar.....	143
11.8.7	Raporlar.....	144
11.8.8	Dizinler.....	144
11.8.9	Sesli uyarılar .....	145
11.8.10	Uyarılar .....	145

# 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.
<b>Uyarı</b>	Kritik veri kaybı olabileceği durumlara ilişkin bir uyarının önüne yerleştirilir.

<b>Not</b>	Özellikle önemli bir bilgi bağlantısının veya Avira ürününüzün kullanımını kolaylaştıran bir ipucunun önüne yerleştirilir.
------------	--

Aşağıdaki vurgular kullanılır:

Vurgu	Açıklama
<i>İtalik</i>	Dosya adı veya yol verileri. Görüntülenen yazılım arabirimi öğeleri (örn. pencere bölümü veya hata mesajı).
<b>Kalın</b>	Tıklanılabilir 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 işlemlere 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)
- Hızlı ve kullanışlı arama seçenekleri sağlayan, web tarayıcısında tümleştirilmiş bir arama araç çubuğu olan Avira SearchFree Toolbar. Ayrıca, en yaygın Internet işlevleri için birçok widget içerir.
- HTTP protokolü (80, 8080, 3128 numaralı bağlantı noktalarının izlenmesi) kullanarak Internet'ten aktarılan veri ve dosyaların izlenmesi için Web Koruması
- Avira Free Android Security uygulaması yalnızca hırsızlık önleme tedbirlerine odaklanmaz. Uygulama, kaybettiğinizde veya daha da kötüsü çalındığında mobil aygıtınızı geri almanıza yardımcı olur. Ayrıca, uygulama gelen aramaları veya SMS'leri engelleme sağlar. Avira Free Android Security Android işletim sistemi ile çalışan cep telefonlarını ve akıllı telefonları korur.
- Şüpheli dosyaları yalıtım 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 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)

## 2.2 Sistem gereksinimleri

### 2.2.1 Sistem gereksinimleri Avira Antivirus Suite

Avira Antivirus Suite, 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 Sistem gereksinimleri Avira SearchFree Araç Çubuğu

Avira SearchFree Araç Çubuğu 'nun düzgün kullanımı için aşağıdaki gereksinimlerin karşılanması gerekir:

### 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)

### Web tarayıcısı

- Windows Internet Explorer 6.0 veya sonraki sürümler
- Mozilla Firefox 3.0 veya sonraki sürümler
- Google Chrome 18.0 veya sonraki sürümler

#### Not

Gerekirse, Avira SearchFree Araç Çubuğu 'nu kurmadan önce lütfen önceden kurulu olan arama araç çubuklarını kaldırın. Aksi takdirde, Avira \$araç çubuğu\$ 'nu kuramazsınız.


## 2.2.3 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 Antivirus Suite ürünü, bazı eylemler için yönetici hakları gerektirir. Bu eylemler şu sembollerle 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.

## 2.3 Lisanslama ve Yükseltme

### 2.3.1 Lisanslama

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

Lisans, etkinleştirme kodu şeklinde sağlanır. Etkinleştirme kodu, Avira ürününü satın aldıktan sonra alacağınız harflerden ve numaralardan oluşan bir koddur. Etkinleştirme kodu, lisansınızın tam tarihini; başka bir deyişle, hangi programların hangi süreyle lisanslandığı bilgisini içerir.

Avira ürününüzü İnternet'ten satın aldıysanız veya ürün ambalajında belirtiliyorsa, etkinleştirme kodu size e-postayla gönderilir.

Programınızı lisanslamak için, lütfen etkinleştirme kodunu girerek programı etkinleştirin. Ürün etkinleştirilmesi, kurulum sırasında gerçekleştirilebilir. Ancak, Lisans Yöneticisi'nde kurulumdan sonra **Yardım > Lisans yönetimi** konumunda Avira ürününüzü de etkinleştirebilirsiniz.

### 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. Ancak Avira ürününüzün lisansını **Yardım > Lisans yönetimi** 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.

### 2.3.3 Yükseltme

Lisans Yöneticisi'nde, Avira masaüstü ürün ailesindeki bir ürün için yükseltme başlatma seçeneğiniz vardır. Eski ürünün el ile kaldırılması ve yeni ürünün el ile kurulumu gerekmez. Lisans Yöneticisi'nden yükseltme yaparken, Lisans Yöneticisi giriş kutusuna yükseltmek istediğiniz ürünün etkinleştirme kodunu girersiniz. Yeni ürün otomatik olarak kurulur.

Bilgisayarınızda yüksek güvenilirlik ve güvenlik sağlamak için, Avira size sisteminizi en yeni sürüme yükseltmenizi hatırlatan bir açılır öğe gönderir. Açılır öğenin üzerindeki **Yükselt** bağlantısını tıklatın, ürüne özel yükseltme sitesine yönlendirileceksiniz.

Mevcut ürününüzü yükseltebilir veya daha kapsamlı bir ürün edinebilirsiniz. Ürün genel bakış sayfası şu anda hangi ürün türünü kullanmakta olduğunuzu gösterir ve ürününüzü diğer Avira ürünleriyle karşılaştırma fırsatı verir. Daha fazla bilgi için ürün adının yanındaki **bilgi** simgesini tıklatın. Aynı ürünü kullanmaya devam etmek istiyorsanız **Yükselt**'i tıklatın, yeni sürümün karşıdan yüklemesi başlayacaktır. Daha kapsamlı bir ürün edinmek istiyorsanız, ürün sütununun en altındaki **Satın Al** seçeneğini tıklatın. Otomatik olarak, satın alım işlemlerinizi yapacağınız Avira çevrimiçi mağazaya yönlendirileceksiniz.

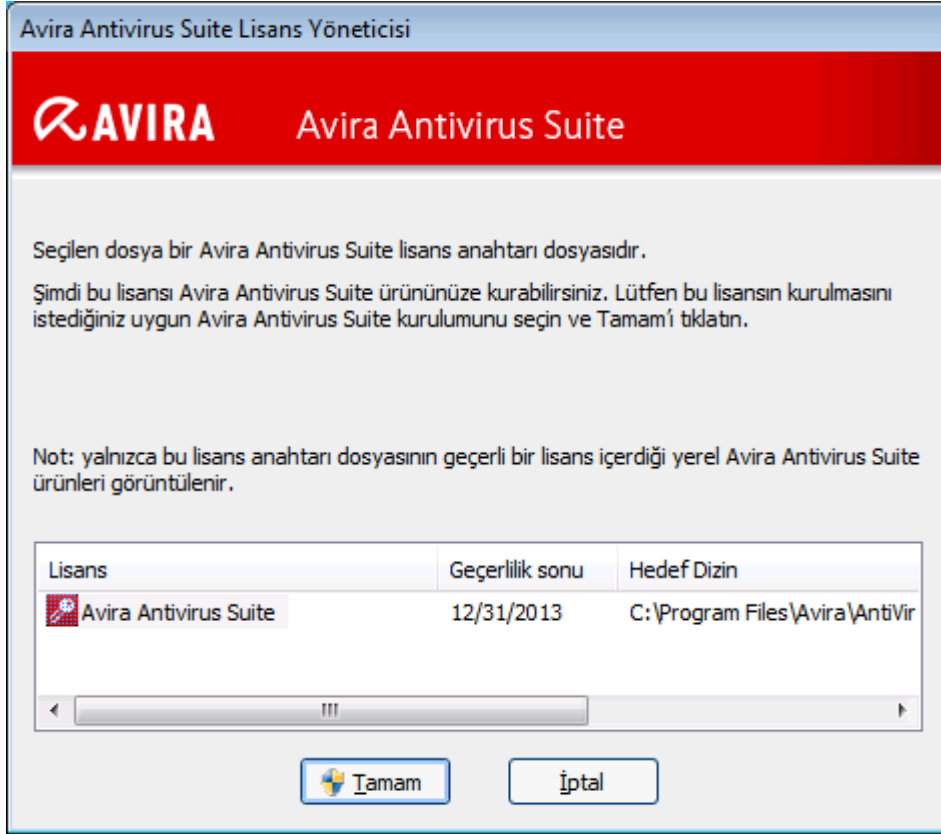
#### Not

Ürününüze ve işletim sisteminize bağlı olarak yükseltme yapmak için yönetici haklarına ihtiyaç duyabilirsiniz. Bir yükseltme yapmadan önce yönetici olarak oturum açın.

### 2.3.4 Lisans yöneticisi

Avira Antivirus Suite Lisans Yöneticisi, Avira Antivirus Suite lisansının çok kolay bir şekilde kurulmasını sağlar.

## Avira Antivirus Suite Lisans Yöneticisi



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

### Not

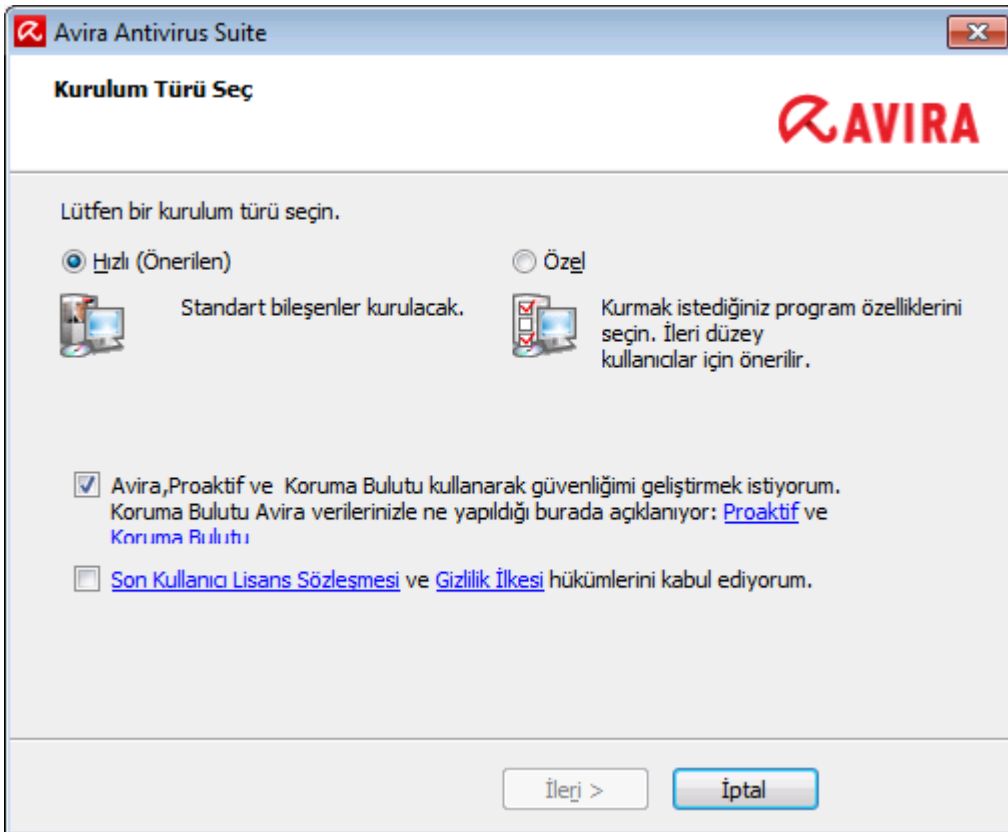
Avira Antivirus Suite Lisans Yöneticisi, karşılık gelen lisansı ilgili ürün klasörüne otomatik olarak kopyalar. Bir lisans zaten varsa, varolan lisans dosyasının değiştirileceğine ilişkin bir not görüntülenir. Bu durumda, yeni lisans dosyası, varsayılan dosyanın üzerine yazılır.

### 3. Kurulum ve kaldırma

Bu bölüm Avira Antivirus Suite ürününün kurulumu ile ilgili bilgi içerir.

- Kurulum için hazırlık
- Çevrimiçiyken CD'den kurulum
- Çevrimdışıyken CD'den kurulum
- Karşıdan yüklenen yazılımın kurulumu
- Uyumsuz yazılımları kaldırma
- [Bir kurulum tipinin seçilmesi](#)
- Avira Antivirus Suite ürününün kurulması
- Kurulumu değiştirme
- Avira Antivirus Suite ürününü kaldırma

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](#)

## 3.1 Ön Kurulum

### Not

Kurulumdan önce, bilgisayarınızın tüm [minimum sistem gereksinimlerini](#) yerine getirip getirmediğini kontrol edin. Bilgisayarınız tüm gereksinimleri yerine getiriyorsa, Avira ürününü kurabilirsiniz.

### Ön Kurulum

- ✓ E-posta programınızı kapatın. Tüm çalışmakta olan uygulamaları sonlandırmanız da önerilir.
- ✓ Başka virüs koruma çözümlerinin kurulmadığından emin olun. Çeşitli güvenlik çözümlerinin otomatik koruma işlevleri birbiriyle etkileşim kurabilir.
  - Avira ürünü bilgisayarınızdaki olası uyumsuz yazılımları arayacaktır.
  - Olası uyumsuz yazılım algılanırsa, Avira 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 programların kaldırılmasını el ile onaylamanız gerekebilir. Programları seçin ve **İleri**'yi tıklatın.
  - Seçilen programlardan en az birinin kaldırma işlemi bilgisayarınızın yeniden başlatılmasını gerektiriyor. Sistem yeniden başlatıldıktan sonra kurulum devam edecek.

### Uyarı

Avira ürününün kurulumu bitene kadar bilgisayarınız korunmaz.

### Kurulum

Kurulum programı, kendinden açıklamalı iletişim modunda çalışır. Her pencere, kurulum işlemini denetlemek için belirli bir düğme grubunu içerir.

En önemli düğmelere şu işlevler atanmıştır:

- **Tamam:** Eylemi onaylayın.
- **Durdur:** Eylemi durdurun.
- **İleri:** Sonraki adıma gidin.
- **Geri:** Önceki adıma gidin.



- ▶ Bir İnternet bağlantısı kurun: Aşağıdaki kurulum adımlarının gerçekleştirilmesi için İnternet bağlantısı gerekir:
- Kurulum programı aracılığıyla geçerli program dosyasını, tarama motorunu ve en son virüs tanımı dosyalarını karşıdan yükleme (internet tabanlı kurulum için)
- Programı etkinleştirme
- Gerekirse, tamamlanan kurulumdan sonra güncelleme gerçekleştirin
- ▶ Programı etkinleştirmek istediğinizde, Avira ürününüzün etkinleştirme kodunu veya lisans dosyasını elinizin altında bulundurun.

**Not****İnternet tabanlı kurulum:**

Programın İnternet tabanlı kurulumu için, Avira web sunucuları tarafından kurulum işleminden önce geçerli program dosyasını yükleyen bir kurulum programı sağlanır. Bu işlem, Avira ürününüzün en son virüs tanımı dosyasıyla kurulmasını sağlar.

**Bir kurulum paketiyle kurulum:**

Kurulum paketi hem kurulum programını hem de tüm gerekli program dosyalarını içerir. Kurulum paketiyle kurulum için Avira ürününüze yönelik bir dil seçimi yoktur. Kurulumdan sonra virüs tanımı dosyasının güncellemesini gerçekleştirmenizi öneririz.

**Not**

Ürün etkinleştirmesi için Avira ürününüz, Avira sunucularıyla iletişim kurmak için HTTP protokolünü, 80 numaralı bağlantı noktasını (web iletişimi), şifreleme protokolü SSL'sini 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 Ekspres bir kurulum yapma

*Ekspres kurulum* önerilen kurulum yordamıdır.

- Avira Antivirus Suite 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 Antivirus Suite 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.

### 3.3 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 Antivirus Suite ürününüz için özel ayarları tanımlayabilirsiniz. Kendinizi rahat hissedeceğiniz güvenlik düzeyini de seçebilirsiniz.
- Kurulumdan sonra, kurulumun ardından otomatik olarak yapılan bir kısa sistem taraması başlatabilirsiniz.

### 3.4 Ürünü sına kurulumu

Avira ürününüzün kurulumu:

İnternet'ten karşıdan yüklediğiniz kurulum dosyasını çift tıklatarak veya program CD'sini takarak kurulum programını başlatın.

#### İnternet tabanlı kurulum

- **Hoş Geldiniz** ekranı görüntülenir.
- ▶ Kurulumu devam etmek için **İleri**'yi tıklatın.
  - **Dil seçimi** iletişim kutusu görüntülenir.
- ▶ Avira ürününüzü kurmak için kullanmak istediğiniz dili seçin ve **İleri**'yi tıklatarak dil seçiminizi onaylayın.
  - **Karşıdan Yükle** iletişim kutusu görüntülenir. Kurulum için gerekli olan tüm dosyalar, Avira web sunucularından karşıdan yüklenir. Karşıdan yükleme sonucundan sonra, **Karşıdan Yükle** penceresi kapatılır.

#### Kurulum paketiyle kurulum

- **Kurulum hazırlanıyor** penceresi görüntülenir.
- Kurulum dosyası ayıklanır. Kurulum yordamı başlatılır.
- **Kurulum türünü seç** iletişim kutusu görüntülenir.

**Not**

Varsayılan olarak, **Ekspres kurulum** önceden ayarlanmıştır. Yapılandırmayabileceğiniz tüm standart bileşenler kurulacak. Bir Özel kurulum başlatmak istiyorsanız, lütfen şu bölüme başvurun: [Kurulum ve kaldırma > Özel kurulum](#).

- ▶ **Avira Proaktif ve Koruma Bulutu'nu kullanarak korumamı iyileştirmek istiyorum** onay kutusu ([Yapılandırma > Genel > Gelişmiş Koruma](#)) varsayılan olarak önceden ayarlanmıştır. Avira Topluluğu'na katılmak istiyorsanız, lütfen bu onay kutusunun işaretini kaldırın.
  - Avira Topluluğu'na katılımınızı onayladığınızda Avira, Avira Zararlı Yazılım Araştırma Merkezi'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 cloud taraması hakkında daha ayrıntılı bilgi almak için **Proaktif ve Koruma Bulutu** bağlantılarını tıklatabilirsiniz.
- ▶ **Son Kullanıcı Lisans Sözleşmesi**'ni kabul ettiğinizi onaylayın. **Son Kullanıcı Lisans Sözleşmesi**'nin ayrıntılı metnini okumak için EULA bağlantısını tıklatın.
- ▶ **İleri**'yi tıklatın.
  - **Lisans Sihirbazı** ürününüzü etkinleştirmenize yardımcı olur.
  - Buradan bir **Proxy sunucusu** yapılandırabilirsiniz.
- ▶ Yapılandırma için **Proxy ayarlarını** tıklatın ve **Tamam** ile ayarlarınızı onaylayın.
- ▶ Lisans Sihirbazında **Ürün sınama** seçeneğini işaretleyin ve **İleri** düğmesini tıklatın.
- ▶ **Kayıt konumunda gerekli alanlara verilerinizi girin**. Lütfen **Avira Bülteni**'ne kayıt olmak isteyip istemediğinize karar verin ve **İleri**'yi tıklatın.
  - Kurulumun ilerleme durumu yeşil bir çubuk ile görüntülenir.
  - **Avira SearchFree Araç Çubuğu'nu kullanan milyonlarca Avira kullanıcısının arasına katılın** iletişim kutusu görüntülenir.
- ▶ Avira SearchFree Araç Çubuğu'nu kurmak istemiyorsanız, lütfen Avira SearchFree Araç Çubuğu'nun, Avira SearchFree Güncelleyici'nin **Son Kullanıcı Lisans Sözleşmesi** ve **Avira SearchFree'yi (search.avira.com)** tarayıcı ana sayfası olarak tanımlayan onay kutularının işaretini kaldırın.

**Not**

Gerekirse, Avira SearchFree Araç Çubuğu'nu kurmadan önce lütfen önceden kurulu olan arama araç çubuklarını kaldırın. Aksi takdirde, Avira SearchFree Araç Çubuğu'nu kuramazsınız.

- ▶ **İleri**'yi tıklatın.
  - Avira SearchFree Araç Çubuğu, yeşil bir çubuk ile görüntülenir.

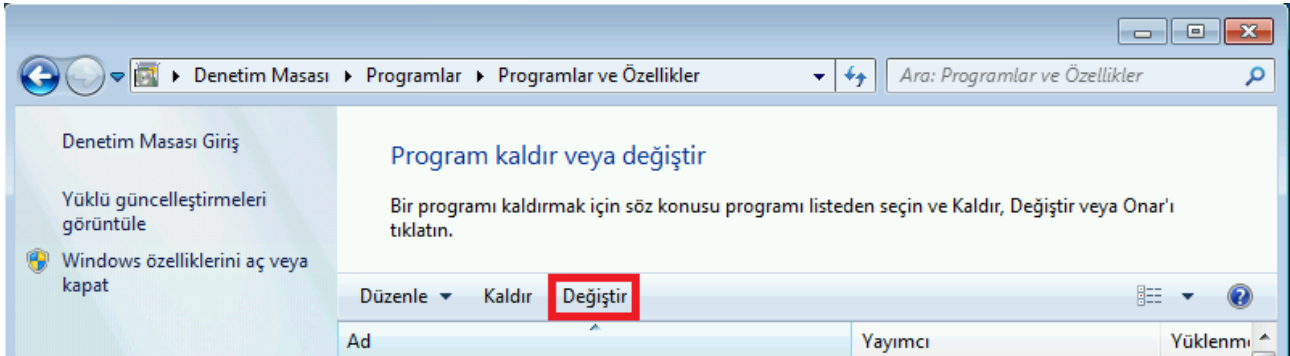
- ▶ Avira ürününüzü etkinleştirmek için sisteminizi yeniden başlatmanız istenir. Bilgisayarınızı hemen yeniden başlatmak için **Evet**'i tıklatın.
  - Avira Tepsi Simgesi görev çubuğunda yer alır.
  - Değerlendirme lisansınız 31 gün etkindir.

### 3.5 Kurulumu yapılandırma

Yapılandırmayı **Parola ata** iletişim kutusunda yetkisiz erişimden parolayla koruyun ve **İleri**'yi tıklatın. Bu, özellikle ebeveyn denetimi etkinleştirilmişse önerilir.

### 3.6 Windows 7'de bir kurulumu değiştirme

Avira Antivirus Suite 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.

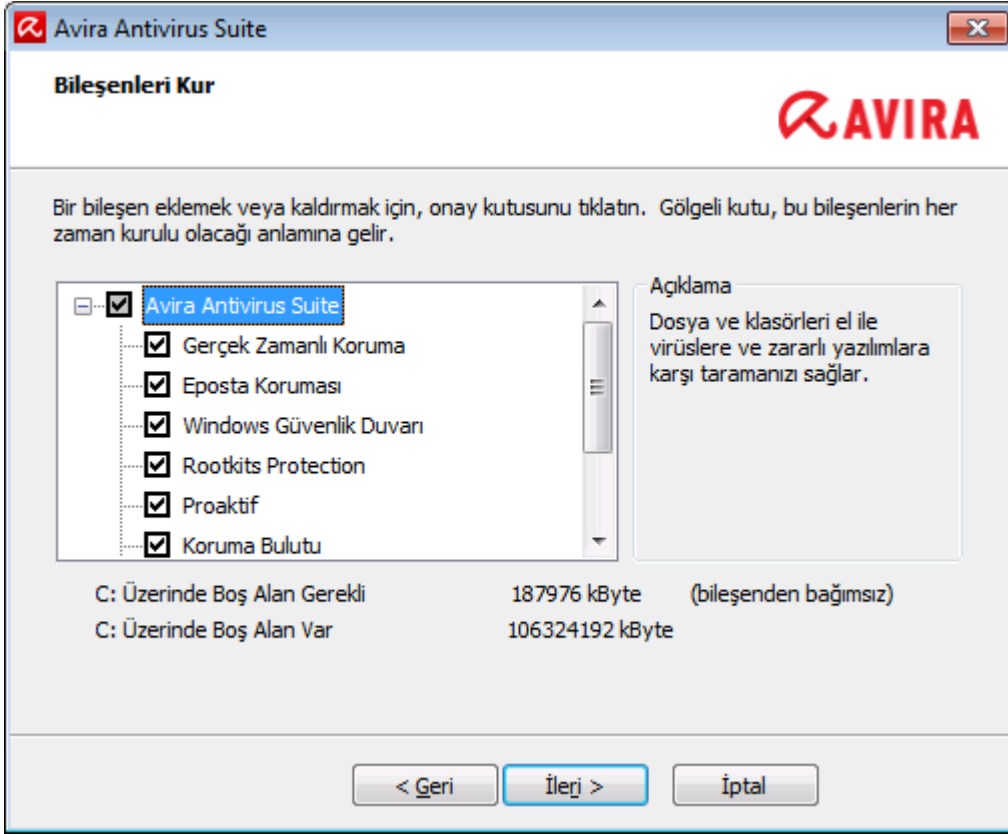
- ▶ Windows'un **Başlat** menüsünden **Denetim Masası**'nı açın.
  - Programlar ve Özellikler** ögesine çift tıklatın.
  - Avira Antivirus Suite ögesini seçin ve **Değiştir**'e tıklatın.
  - Programın **Hoş Geldiniz** iletişim kutusunda **Değiştir** seçeneğini seçin. Kurulum değişiklikleri boyunca size yol gösterilecektir.

İlgili Konular:

[Kurulum bileşenlerinin seçilmesi](#)

### 3.7 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 Antivirus Suite**

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 Antivirus Suite 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.

- **Windows Güvenlik Duvarı** (Windows 7'den itibaren)

Bu bileşen Windows Güvenlik Duvarını Avira Antivirus Suite 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 Gezini'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

## 3.8 Kaldırma

Avira ürününü bilgisayarınızdan kaldırmak istiyorsanız, Windows Denetim Masası'nda programları **Değiştirmek/Kaldırmak** için **Program Ekle veya Kaldır** seçeneğini kullanabilirsiniz.

Avira ürününüzü kaldırmak için (örn. Windows 7'de):

- ▶ Windows'un **Başlat** menüsünden **Denetim Masası**'nı açın.
- ▶ **Programlar ve Özellikler** ögesine çift tıklatın.
- ▶ Listedeki Avira ürününüzü seçin ve **Kaldır**'ı tıklatın.

- Gerçekten programı kaldırmak isteyip istemediğiniz sorulur.
- ▶ Onaylamak için **Evet**'i tıklatın.
  - Tüm program bileşenleri kaldırılır.
- ▶ Kurulumu tamamlamak için **Son**'u tıklatın.
  - Gerekirse, bilgisayarınızın yeniden başlatılmasını öneren bir iletişim kutusu görüntülenir.
- ▶ Onaylamak için **Evet**'i tıklatın.
  - Bilgisayarınız yeniden başlatıldığında Avira ürününüz kaldırılmış ve programın tüm izinleri, dosyaları ve kayıt defteri girdileri silinmiştir.

**Not**

Avira SearchFree Araç Çubuğu, kaldırma programına dahil edilmemiş olup yukarıda ayrıntıları verilen adımlar izlenerek ayrı ayrı kaldırılmalıdır. Firefox'ta bunu yapmak için, Avira SearchFree Araç Çubuğu, Eklenti Yöneticisi aracılığıyla etkinleştirilmelidir. Kaldırma işleminden sonra, arama araç çubuğu artık web tarayıcınızla tümleştirilmez.

## 4. Avira Antivirus Suite ürününe genel bakış

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

- bkz. [Kullanıcı arabirimi ve çalışma](#) Bölümü
- bkz. [Avira SearchFree Araç Çubuğu](#) Bölümü
- bkz. [Nasıl yapılır?](#) Bölümü

### 4.1 Kullanıcı arabirimi ve çalışma

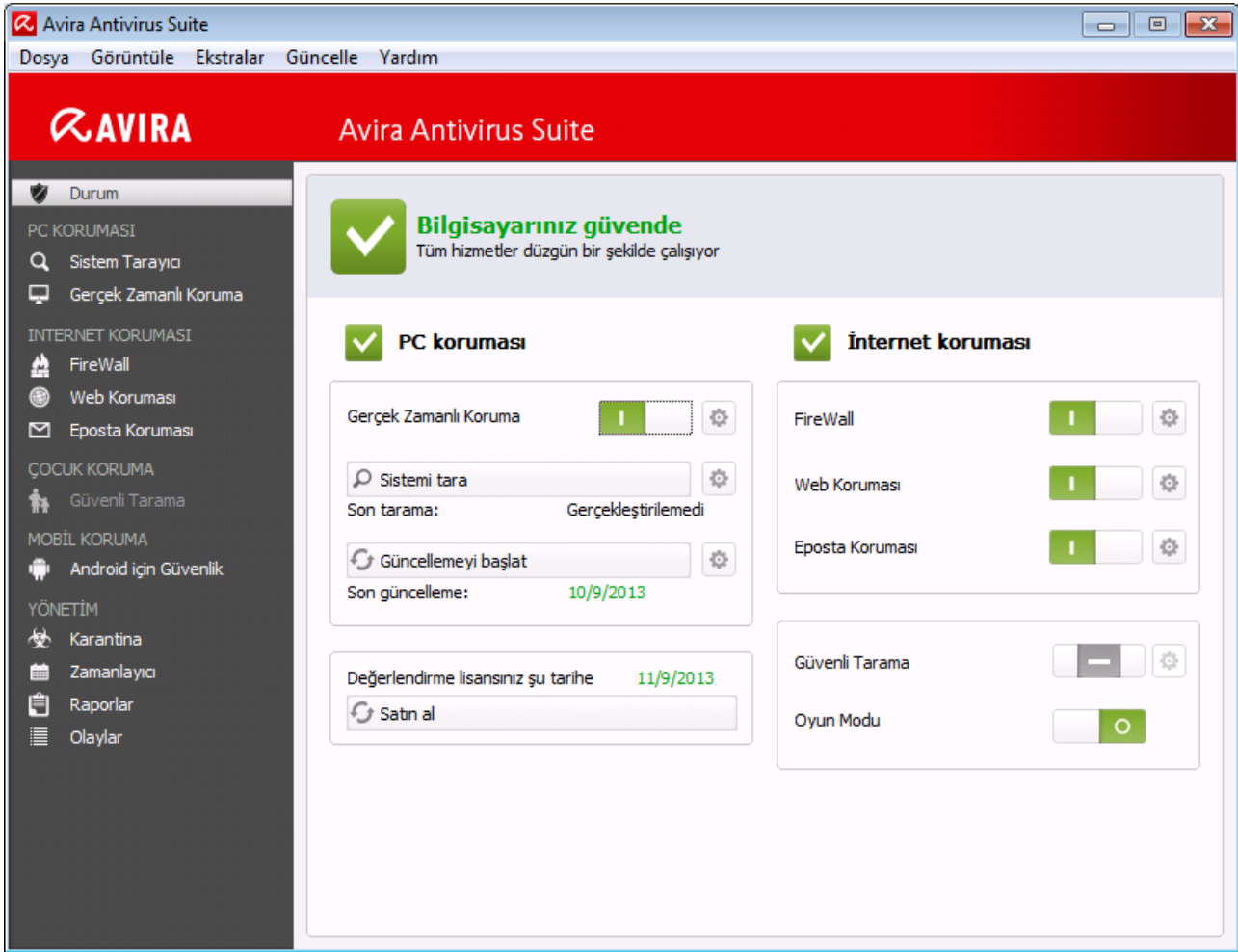
Avira ürününüzü üç program arabirimi ögesi aracılığıyla çalıştırırsınız:

- [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.
  - 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.
- **ÇOCUK KORUMA:** Bu bölümde çocuğunuz için güvenli bir İnternet deneyimi sağlamak amacıyla kullanılan bileşenleri bulabilirsiniz.
- **MOBİL KORUMA:** Bu bölümden Android aygıtlar için çevrimiçi erişime yönlendirilirsiniz.
  - Avira Free Android Security tüm android tabanlı aygıtlarınızı yönetir.
- **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 uyarılmanıza 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 Oyun Modu

Bilgisayar sisteminizde bir uygulama tam ekran modunda yürütüldüğünde, Oyun Modunu etkinleştirerek kendi isteğinizle masaüstü bildirimlerini açılan pencereler ve ürün mesajları olarak askıya alabilirsiniz.

Oyun Modunu etkinleştirebilirsiniz veya **AÇ/KAPAT** düğmesini tıklatarak otomatik moda kalabilirsiniz. Oyun 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 Oyun Moduna geçer.

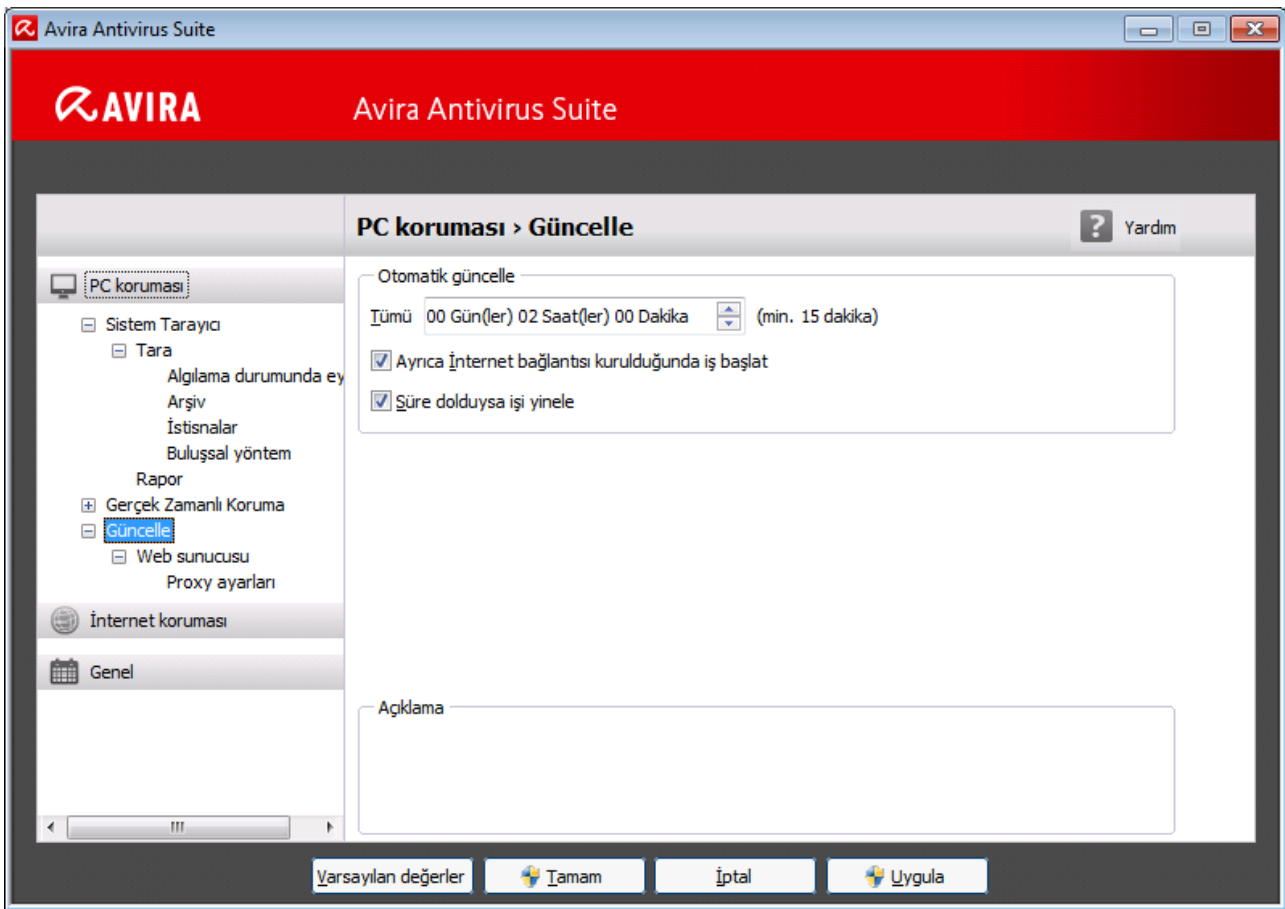
- ▶ Oyun Modunu etkinleştirmek için **KAPALI** düğmesinin sol yanındaki düğmeyi tıklayın.
  - ↳ Oyun Modu etkindir ve sarı renkte gösterilir.

**Not**

Otomatik tam ekran tanınması modu ile varsayılan ayarı geçici olarak **KAPALI** moda değiştirmenizi öneririz, çünkü ağ olayları ve olası tehditler hakkında görünür masaüstü bildirimleri ve uyarıları almayacaksınız.

### 4.1.3 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 tıklararak 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**'i 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 seçeneklerine genel bakış



Aşağıdaki yapılandırma seçenekleri kullanılabilir:

- **Sistem Tarayıcı:** İstek üzerine taramanın yapılandırması
  - Tarama seçenekleri
  - Algılama durumunda 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
  - Proxy ayarları
- **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
- Rapor işlevi ayarı
- **Genel:**
  - 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
  - Zararlı yazılım algılanması durumunda verilen sesli uyarıların yapılandırması

#### 4.1.4 Tepsi simgesi

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

Simge	Açıklama
	Avira Gerçek Zamanlı Koruma etkin
	Avira Gerçek Zamanlı Koruma devre dışı

Tepsi simgesi, Gerçek Zamanlı Koruma 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'nı etkinleştir:** Windows Güvenlik Duvarı'nı etkinleştirir veya devre dışı bırakır (bu özellik Windows 8'den itibaren sunulmaktadır).
- **Avira Antivirus Suite'i başlat:** Kontrol Merkezi'ni açar.
- **Avira Antivirus Suite'i yapılandır:** Yapılandırma'yı açar.
- **İletilerim:** Avira ürününüzle ilgili mevcut bilgiyi içeren bir slide-up açar.
- **İletişim ayarlarım:** Product Message Subscription Center'ı (Ürün Mesajı Abonelik Merkezi) açar
- **Güncellemeyi başlat** Bir güncelleme başlatır.
- **Yardım:** Online Yardım'ı açar.
- **Avira Antivirus Suite hakkında:** Avira ürününüz hakkında bilgiler içeren bir iletişim kutusu açar: Ürün bilgileri, Sürüm bilgileri, Lisans bilgileri.
- **İnternet'te Avira:** İnternet'te Avira web portalını açar. Bunun koşulu, etkin bir İnternet bağlantısının olmasıdır.

## 4.2 Avira SearchFree Araç Çubuğu

Avira SearchFree Araç Çubuğu iki temel bileşen içerir: Avira SearchFree ve Araç Çubuğu.

Avira SearchFree Araç Çubuğu bir eklenti olarak kurulur. Tarayıcıya ilk defa eriştiğinizde (Firefox'ta ve İnternet Explorer'da) araç çubuğunu kurmak için sizden izin isteyen bir ileti görüntülenir. Avira SearchFree Araç Çubuğu'nun kurulumunu başarılı bir şekilde tamamlamak için kabul etmelisiniz.

Avira SearchFree, bir arama motorudur ve Avira web sitesi ile web, görüntü ve video kanallarına bağlantısı olan tıklanabilir bir Avira logosu içerir. Bu, Avira kullanıcılarına daha güvenli İnternet'te gezinme imkanı sunar.

Web tarayıcınıza entegre edilmiş olan araç çubuğu bir arama çubuğundan, Avira web sitesine bağlantılandırılmış bir Avira logosundan, iki durum görüntüsünden, üç widget'tan ve **Options** menüsünden oluşur.

- **Arama araç çubuğu**  
Avira arama motorunu kullanarak İnternet'te hızlı şekilde arama yapmak için ücretsiz olarak arama araç çubuğunu kullanın.
- **Durum görüntüsü**  
Durum görüntüleri, Web Protection durumu ve Avira ürününüzün geçerli güncelleme durumu hakkında bilgi sağlar ve kişisel bilgisayarınızı korumak için uygulamanız gereken eylemleri tanımlamanıza yardımcı olur.
- **Widget'lar**  
Avira, İnternet ile ilgili en önemli işlevler için üç widget sunar. Tek bir tıkla doğrudan Facebook'a veya e-postanıza erişebilir veya güvenli web taraması (yalnızca Firefox ve İnternet Explorer) yapabilirsiniz.
- **Seçenekler**  
Araç çubuğu seçeneklerine erişmek, geçmişi temizlemek, araç çubuğu yardımını ve



bilgilerini bulmak ve Avira SearchFree Araç Çubuğu'nu doğrudan web tarayıcısı aracılığıyla kaldırmak için **Options** menüsünü kullanabilirsiniz (yalnızca Firefox ve Internet Explorer).

#### 4.2.1 Kullanım

##### Avira SearchFree

Internet'te taranacak herhangi bir sayıda terim tanımlamak için Avira SearchFree'yi kullanabilirsiniz.



Arama kutusuna terimi girin ve **Enter** tuşuna basın veya **Search** tıklayın. Daha sonra Avira SearchFree motoru sizin için Internet'te arama yapar ve tarayıcı penceresinde tüm isabetleri görüntüler.



Internet Explorer, Firefox ve Chrome'da Avira SearchFree'nin nasıl özel yapılandırılacağını öğrenmek için [Seçenekler](#) ögesine gidin.

##### Durum görüntüsü

###### Web Protection

Kişisel bilgisayarınızı korumak amacıyla uygulamanız gereken eylemleri tanımlamak için aşağıdaki simgeleri ve iletileri kullanabilirsiniz:

Simge	Durum görüntüsü	Açıklama
	<i>Web Protection</i>	Imleci simgenin üzerine tasırsanız, su ileti görüntülenir: <i>Avira Web Protection is active. Your browsing is protected.</i>  Baska bir eylem gerekmez.
	<i>Web Protection is inactive</i>	Imleci simgenin üzerine tasırsanız, su ileti görüntülenir: <i>Avira Web Protection is off. Click to find out how to turn it on.</i>  → Bilgi Bankasi yazilarimizdan birine yönlendirileceksiniz.

	<i>No Web Protection</i>	<p>İmleci simgenin üzerine tasırsanız, su iletilerden biri görüntülenir:</p> <ul style="list-style-type: none"><li>• <i>You do not have Avira Web Protection installed. Click to find out how to protect your browsing.</i></li></ul> <p>Kurulumu yanlış yaparsanız veya Avira Antivirus'i kaldırırsanız bu ileti görüntülenir.</p> <ul style="list-style-type: none"><li>• <i>Web Protection is included for free with Avira Antivirus. Click to find out how to install it.</i></li></ul> <p>Web Protection'i kurmaz veya kaldırırsanız bu ileti görüntülenir.</p> <p>→ Her iki durumda da, Avira ürününü karsidan yükleyebileceğiniz Avira ana sayfasına yeniden yönlendirilirsiniz.</p>
	<i>Error</i>	<p>İmleci simgenin üzerine tasırsanız, su ileti görüntülenir: <i>Avira reported an error. Click to contact Support for help.</i></p> <ul style="list-style-type: none"><li>▶ Avira Destek sayfasına gitmek için gri simgeyi veya metni tıklatin.</li></ul>

## Widget'lar

Avira SearchFree, günümüzün İnternet web taraması için en önemli işlevleri sunan üç widget içerir: Facebook, E-posta ve Browser Security.

### Facebook

Bu işlev, Facebook'tan tüm iletileri almanızı ve her zaman güncel olmanızı sağlar.

### E-posta

Araç çubuğunda e-posta sembolünü tıkladığınızda, bir açılır liste görüntülenir. En yaygın olarak kullanılan e-posta sağlayıcıları arasından seçim yapabilirsiniz.

### Browser Security

Bu widget, günlük olarak ihtiyacınız olabilecek olan tüm İnternet güvenlik seçeneklerini size tek bir tıkla sunmak üzere tasarlanmıştır. Bu seçenek sadece Firefox ve İnternet Explorer'da kullanılabilir. İşlevlerin adları da tarayıcıdan tarayıcıya farklılık gösterebilir:

- *Açılır Pencere Engelleyici*

Bu seçenek etkinleştirildiğinde, tüm açılır pencereler engellenir.

- *Çerezleri Engelle*

Bu seçeneği etkinleştirdiğinizde, bilgisayarınıza hiçbir çerez kaydedilmez.

- *Private Browsing (Özel Gözetme) (Firefox) / InPrivate Browsing (Özel Gözetme) (Internet Explorer)*

Gezinirken İnternette kişisel bilgilerinizin izlerinin bırakılmasını istemiyorsanız bu seçeneği etkinleştirin. Bu seçenek Internet Explorer 7 ve 8'de kullanılamaz.

- *Clear Recent History (Yakın Geçmişini Temizle) (Firefox) / Delete Browsing History (Gözetme Geçmişini Sil) (Internet Explorer)*






Bu seçenek aracılığıyla İnternet etkinliklerinizin tüm izlerini silebilirsiniz.

### Website Safety Advisor

Website Safety Advisor, gezinme esnasında size bir güvenlik derecelendirmesi sunar. Ziyaret ettiğiniz web sitesinin saygınlık durumuna erişebilir ve güvenliğinizi için düşük mü yoksa yüksek bir risk mi oluşturduğunu kontrol edebilirsiniz.

Bu widget web sitesi ile ilgili başka bilgiler de sağlar, örneğin etki alanı sahibinin kim olduğu veya web sitesinin neden güvenli veya riskli kategorisine atıldığı.

Website Safety Advisor'ın durumu, başka simgeler içeren bir Avira tepsi simgesi olarak Araç Çubuğunda ve arama sonuçlarınızda görüntülenir:

Simge	Durum görüntüsü	Açıklama
	<i>Safe</i>	Güvenli web siteleri için yeşil bir onay isareti.
	<i>Low risk</i>	Düşük bir risk taşıyan web siteleri için sarı bir uyarı isareti.
	<i>High risk</i>	Güvenliğiniz için yüksek bir risk taşıyan web siteleri için kırmızı bir dur isareti.
	<i>Unknown</i>	Durum bilinmediğinde, gri bir soru isareti görüntülenir.
	<i>Verifying</i>	Bir web sitesinin durumu doğrulanırken bu isaret görüntülenir.

### Browser Tracking Blocker

Browser Tracking Blocker ile siz gezinirken izleyicilerin sizin hakkınızda bilgi toplamasını engelleyebilirsiniz.

Bu widget, hangi izleyicilerin engelleneceğini ve hangilerine izin verileceğini belirleyebilirsiniz.

İzleme şirketleri üç kategoriye sınıflandırılmıştır:

- Sosyal Ağlar
- Reklam Ağları
- Diğer şirketler

## 4.2.2 Seçenekler

Avira SearchFree Araç Çubuğu, Internet Explorer, Firefox ve Google Chrome ile uyumludur ve üç web tarayıcısında da yapılandırılabilir:

- [Internet Explorer yapılandırma seçenekleri](#)
- [Firefox yapılandırma seçenekleri](#)
- [Google Chrome yapılandırma seçenekleri](#)

### Internet Explorer

Internet Explorer'da, **Options** menüsünde Avira SearchFree Araç Çubuğu için şu yapılandırma seçenekleri kullanılabilir:

### Toolbar options

#### Search

##### Avira search engine

**Avira search engine** menüsünde, arama için hangi arama motorunun kullanılacağını seçebilirsiniz. Arama motorları; ABD, Brezilya, Almanya, İspanya, Avrupa, Fransa, İtalya, Hollanda, Rusya ve İngiltere için kullanılabilir.

##### Open searches in

**Open searches in** seçenek menüsünde, arama sonucunun nerede görüntüleneceğini (Geçerli pencerede, Yeni bir pencerede veya Yeni bir sekmede) seçebilirsiniz.

##### Display recent searches

**Display recent searches** seçeneği etkinleştirilirse, arama araç çubuğunun metin girdisi kutusunda önceki arama terimlerini görüntüleyebilirsiniz.

##### Auto clear recent search history when I close the browser

Önceki aramaları kaydetmek istemiyorsanız ve web tarayıcısını kapattığınızda geçmişini temizlemek istiyorsanız, **Auto clear recent search history when I close the browser** seçeneğini etkinleştirin.

## More options

### Select toolbar language

**Select toolbar language** konumunda, Avira SearchFree Araç Çubuğu'nun görüntüleneceği dili seçebilirsiniz. Araç çubuğu, İngilizce, Almanca, İspanyolca, Fransızca, İtalyanca, Portekizce ve Hollandaca olarak kullanılabilir.

#### Not

Mümkünse, varsayılan Avira SearchFree Araç Çubuğu dili, programınızinkine karşılık gelir. Araç Çubuğu dilinizde kullanılabilir değilse, varsayılan dil İngilizce'dir.

### Show button text labels

Avira SearchFree Araç Çubuğu simgelerinin yanındaki metni gizlemek istiyorsanız, **Show button text labels** seçeneğini devre dışı bırakın.

## Clear history

Önceki aramaları kaydetmek istemiyorsanız ve hemen geçmişi temizlemek istiyorsanız, **Clear history** seçeneğini etkinleştirin.

## Help

Araç Çubuğu ile ilgili sık sorulan soruları (SSS) içeren web sitesine erişmek için **Help**'i tıklatın.

## Uninstall

Doğrudan Internet Explorer'dan da Avira SearchFree Araç Çubuğu'nu kaldırabilirsiniz: Web tarayıcısı aracılığıyla kaldırma

## About

Avira SearchFree Araç Çubuğu'nun hangi sürümünün kurulduğunu görüntülemek için **About** seçeneğini tıklatın.

## Firefox

Firefox web tarayıcısında, **Options** menüsünde Avira SearchFree Araç Çubuğu için şu yapılandırma seçenekleri kullanılabilir:

## Toolbar options

### Search

#### Select Avira search engine

**Avira search engine** menüsünde, arama için hangi arama motorunun kullanılacağını seçebilirsiniz. Arama motorları; ABD, Brezilya, Almanya, İspanya, Avrupa, Fransa, İtalya, Hollanda, Rusya ve İngiltere için kullanılabilir.

#### Display recent searches

**Display recent searches** seçeneği etkinleştirilirse, arama araç çubuğundaki oku tıklayarak önceki arama terimlerini görüntüleyebilirsiniz. Arama sonucunu yeniden görüntülemek istiyorsanız bir terim seçin.

#### Auto clear recent search history when I close the browser

Önceki aramaları kaydetmek istemiyorsanız ve web tarayıcısını kapattığınızda geçmişini temizlemek istiyorsanız, **Auto clear recent search history when I close the browser** seçeneğini etkinleştirin.

#### Display Avira search results when I type keywords or invalid URLs into the browser address bar

Bu seçenek etkinleştirilirse, web tarayıcısının adres çubuğuna her anahtar sözcük veya geçersiz URL girdiğinizde bir arama başlatılır ve arama sonucu görüntülenir.

### More options

#### Select toolbar language

**Select toolbar language** konumunda, Avira SearchFree Araç Çubuğu'nun görüntüleneceği dili seçebilirsiniz. Araç çubuğu, İngilizce, Almanca, İspanyolca, Fransızca, İtalyanca, Portekizce ve Hollandaca olarak kullanılabilir.

#### Not

Mümkünse, varsayılan Avira SearchFree Araç Çubuğu dili, programınızinkine karşılık gelir. Araç Çubuğu dilinizde kullanılabilir değilse, varsayılan dil İngilizce'dir.

#### Düğme metni etiketlerini göster

Avira SearchFree Araç Çubuğu simgelerinin yanındaki metni gizlemek istiyorsanız, **Düğme metni etiketlerini göster** seçeneğini devre dışı bırakın.

### Clear history

Önceki aramaları kaydetmek istemiyorsanız ve hemen geçmişini temizlemek istiyorsanız, **Clear history** seçeneğini etkinleştirin.

## Help

Araç Çubuğu ile ilgili sık sorulan soruları (SSS) içeren web sitesine erişmek için **Help**'i tıklatın.

## Kaldır

Doğrudan Firefox'tan da Avira SearchFree Araç Çubuğu'nu kaldırabilirsiniz: [Web tarayıcısı aracılığıyla kaldırma](#)

## About

Avira SearchFree Araç Çubuğu'nun hangi sürümünün kurulduğunu görüntülemek için **About** seçeneğini tıklatın.

## Google Chrome

Chrome web tarayıcısında, kırmızı Avira şemsiyesi menüsünde Avira SearchFree Araç Çubuğu için şu yapılandırma seçenekleri kullanılabilir:

## Help

Araç Çubuğu ile ilgili sık sorulan soruları (SSS) içeren web sitesine erişmek için **Help**'i tıklatın.

## Kaldırma yönergeleri

Burada araç çubuğunu kaldırmak için ihtiyacınız olan tüm bilgileri içeren makalelere yönlendirilirsiniz.

## About

Avira SearchFree Araç Çubuğu'nun hangi sürümünün kurulduğunu görüntülemek için **About** seçeneğini tıklatın.

## Avira SearchFree Araç Çubuğu'nu Göster/ Gizle

Avira SearchFree Araç Çubuğu'nu web tarayıcınızda gizlemek veya göstermek için burayı tıklatın.

### 4.2.3 Windows 7'de Avira SearchFree Araç Çubuğu 'nu kaldırma

Avira SearchFree Araç Çubuğu 'nu kaldırmak için:

- Web tarayıcınızı kapatın.

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

**Programlar ve Özellikler** ögesine çift tıklatın.

Listeden Avira SearchFree Araç Çubuğu 'nu ve Web Koruması seçimini yapın ve **Kaldır**'a tıklayın.

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.

## 4.3 Nasıl yapılır...?

"Nasıl yapılır...?" bölümleri lisans ve ürün etkinleştirilmesi 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.

### 4.3.1 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 yönetimi** 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.

### 4.3.2 Ürün etkinleştir

Avira ürününüzü etkinleştirmek için aşağıdaki seçeneklere sahip olursunuz:

#### **Geçerli bir tam lisans ile etkinleştirme**

Programı tam lisans ile etkinleştirmek için, satın aldığınız lisans verilerini barındıran geçerli bir etkinleştirme koduna ihtiyacınız vardır. Bizden e-postayla etkinleştirme kodu almış olursunuz veya etkinleştirme kodu, ürün ambalajında basılı olarak bulunur.

#### **Değerlendirme lisansı ile etkinleştirme**

Avira ürününüz, sınırlı bir süre boyunca tam işlev aralığı ile Avira ürününüzü sınavabileceğiniz, otomatik olarak oluşturulmuş bir değerlendirme lisansı ile etkinleştirilir.

#### **Not**

Ürün etkinleştirme veya sınama lisansı için etkin bir İnternet bağlantısı gerekir. Avira sunucularına bağlantı kuramazsanız, lütfen kullanılan güvenlik duvarının ayarlarını kontrol edin: Ürün etkinleştirme için HTTP protokolü, 80 numaralı bağlantı noktası (web iletişimi) ve şifreleme protokolü SSL ve 443 numaralı bağlantı noktası üzerinden bağlantılar kullanılır. Güvenlik duvarınızın gelen ve giden verileri engellemediğinden emin olun. Öncelikle, web tarayıcınızla web sayfalarına erişip erişemediğinizi kontrol edin.

Aşağıda, Avira ürününüzün nasıl etkinleştirileceği açıklanmaktadır:

Henüz Avira ürününüzü kurmadıysanız:


- ▶ Avira ürününüzü kurun.
  - ↳ Kurulum işlemi boyunca bir etkinleştirme seçeneği belirlemeniz istenir
- **Ürünü etkinleştir:** Geçerli bir tam lisans ile etkinleştirme
- **Ürünü sına:** Değerlendirme lisansı ile etkinleştirme
- ▶ Tam lisans ile etkinleştirme için etkinleştirme kodunu girin.
- ▶ **İleri**'yi tıklatarak etkinleştirme yordamı seçimini onaylayın.
- ▶ Ve gerekirse, kayıt için kişisel verilerinizi girin ve **İleri**'yi tıklatarak onaylayın.
  - ↳ Lisans verileriniz sonraki pencerede görüntülenir. Avira ürününüz etkinleştirildi.
- ▶ Kurulumu devam edin.

Avira ürününüzü kurduysanız:

- ▶ Kontrol Merkezi'ndeki **Yardım > Lisans yönetimi** menü öğesi, lisans sihirbazını açar.
  - ↳ Bir etkinleştirme seçeneği belirleyebileceğiniz *lisans sihirbazı* açılır. Ürün etkinleştirmesinin sonraki adımları, yukarıda açıklanan yordamla aynıdır.

### 4.3.3 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.
- ▶ Listedeki **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: 2 saat.

- ▶ 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

 İş düzenle

 İş sil

 İş başlat

 İş durdur

#### 4.3.4 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: 2 saat.

**Not**

Ayrıca Windows güvenlik merkezi aracılığıyla doğrudan el ile güncelleme yürütebilirsiniz.

### 4.3.5 Virüslere ve zararlı yazılımlara karşı tarama yapmak için bir tarama profili kullanma

Tarama profili, taranacak sürücü ve izin 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 izinler ve dosyalar taranır.



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

- ▶ Kontrol Merkezi'ne gidin ve *PC KORUMASI* > **Sistem Tarayıcı** bölümünü seçin.
  - ↳ Önceden tanımlı tarama profilleri görüntülenir.
- ▶ Önceden tanımlı tarama profillerinden birini seçin.
  - VEYA-
  - Eİ ile seçim** tarama profilini uyarlayın.
  - VEYA-
  - Yeni bir tarama profili oluştur
- ▶ Simgely tıkladın (Windows XP:  veya Windows Vista'dan itibaren: ).
- ▶ **Luke Filewalker** penceresi görüntülenir ve sistem taraması başlatılır.
  - ↳ Tarama tamamlandığında, sonuçlar görüntülenir.

Bir tarama profilini uyarlamak istiyorsanız:

- ▶ Tarama profilinde **Eİ İle Seçim** dosya ağacını genişletin, böylece taramak istediğiniz tüm sürücüler ve izinler açılır.
- + simgesini tıkladın: Sonraki izin düzeyi görüntülenir.
- - simgesini tıkladın: Sonraki izin düzeyi gizlenir.
- ▶ İlgili izin düzeyinin ilgili kutusunu tıklatarak, taramak istediğiniz düğümleri ve izinleri vurgulayın:
  - Aşağıdaki seçenekler, izinleri seçme için kullanılabilir:
  - Alt izinleri de içeren izin (siyah onay işareti)
  - Yalnızca tek bir dizinin alt izinleri (gri onay işareti, alt izinlerin siyah onay işaretleri vardır)
  - Dizin yok (onay işareti yoktur)

Yeni bir tarama profili oluşturmak istiyorsanız:

- ▶  **Yeni profil oluştur** simgesini tıkladın.
  - ↳ **Yeni profil** profili, önceden oluşturulan profillerin aşağısında görüntülenir.
- ▶ Gerekirse,  simgesini tıklatarak tarama profilini yeniden adlandırın.
- ▶ İlgili izin düzeyinin onay kutusunu tıklatarak, kaydedilecek düğümleri ve izinleri vurgulayın.
  - Aşağıdaki seçenekler, izinleri 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)

#### 4.3.6 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.

#### 4.3.7 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.

#### 4.3.8 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

#### 4.3.9 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, izin düzeyinin onay kutusunu tıklatarak, taranacak diğer düğümleri ve izinleri vurgulayın.
- ▶ Simgely tıkkatın (Windows XP:  veya Windows Vista'dan itibaren:  ).
  - ↳ **Luke Filewalker** penceresi görüntülenir ve sistem taraması başlatılır.
  - ↳ Tarama tamamlandığında, sonuçlar görüntülenir.

#### 4.3.10 Algılanan virüslere ve zararlı yazılımlara yanıt verme

**Algılama durumunda eylem** bölümündeki **Yapılandırma'da** Avira ürününüzün tek tek koruma bileşenleri için Avira ürününüzün algılanan bir virüse veya istenmeyen programa nasıl yanıt vereceğini tanımlayabilirsiniz.

Gerçek Zamanlı Koruma'nın Proaktif bileşeni için kullanılabilir durumda bir yapılandırılabilir eylem seçeneği yoktur: Bir algılama olduğuna dair bildirim her zaman **Gerçek Zamanlı Koruma: Süpheli uygulama davranışı** penceresinde gösterilir.



## **Sistem Tarayici için eylem seçenekleri:**

### **Etkilesimli**

Etkilesimli eylem modunda, Sistem Tarayici taramasinin sonuclari bir iletisim kutusunda görüntülenir. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

**Sistem Tarayici taramasi** olması durumunda, tarama tamamlandığında 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 Tarayici'yi iptal edebilirsiniz.

### **Otomatik**

Otomatik eylem modunda bir virüs veya istenmeyen bir program algılandığında, bu alanda seçtiğiniz eylem otomatik olarak uygulanır.

## **Gerçek Zamanlı Koruma için eylem seçenekleri:**

### **Etkilesimli**

Etkilesimli eylem modunda, veri erişimi reddedilir ve bir masaüstü bildirim görüntülenir. Masaüstü bildiriminde, algılanan zararlı yazılımı kaldırabilir veya **Ayrıntılar** düğmesini kullanarak zararlı yazılımı daha fazla virüs yönetimi için Sistem Tarayici bileşenine aktarabilirsiniz. Sistem Tarayici, algılama bildirimini içeren ve etkilenen dosyanın bir bağlam menüsü aracılığıyla yönetilmesine ilişkin çeşitli seçenekleri size sunan bir pencereyi açar (bkz.Algilama > Sistem Tarayici):

### **Otomatik**

Otomatik eylem modunda bir virüs veya istenmeyen bir program algılandığında, bu alanda seçtiğiniz eylem otomatik olarak uygulanır.

## **EPosta Koruması, Web Koruması algılamaları için eylem seçenekleri:**

### **Etkilesimli**

Etkilesimli eylem modunda, bir virüs veya istenmeyen program algılanması durumunda, etkilenen nesnenin ne yapılacağını seçebileceğiniz bir iletişim kutusu görüntülenir. Bu seçenek, varsayılan ayar olarak etkinleştirilir.

### **Otomatik**

Otomatik eylem modunda bir virüs veya istenmeyen bir program algılandığında, bu alanda seçtiğiniz eylem otomatik olarak uygulanır.

Etkilesimli eylem modunda, uyarıdaki etkilenen nesne için bir eylem seçerek ve **Onayla**'yi tıklatıp seçilen eylemi yürüterek, algılanan virüslere ve istenmeyen programlara yanıt verebilirsiniz.

Etkilenen nesnelere ele almaya yönelik aşağıdaki eylemler seçilebilir:

**Not**

Hangi eylemlerin seçilebilir durumda olduğu, işletim sistemine, koruma bileşenlerine (Avira Gerçek Zamanlı Koruma, Avira Sistem Tarayıcı, Avira EPosta Koruması, Avira Web Koruması) algılamanın raporlanmasına ve algılanan zararlı yazılımın türüne bağlıdır.

**Sistem Tarayıcı ve Gerçek Zamanlı Koruma (Proaktif algılamaları değil) eylemleri:****Onar**

Dosya onarılır.

Bu seçenek yalnızca etkilenen dosya onarılabilirse kullanılabilir.

**Yeniden Adlandır**

Dosya, \*.vir uzantisiyle yeniden adlandırılır. Bu nedenle, bu dosyalara doğrudan (örneğin çift tıklatmayla) erişim artık mümkün değildir. Dosyalar daha sonra onarılabilir ve özgün adlarıyla adlandırılabilir.

**Karantina**

Dosya özel bir biçimde (\*.qua) paketlenir ve sabit diskinizdeki *ETKİLENEN* Karantina dizinine taşınır, böylece doğrudan erişim artık mümkün değildir. Bu dizindeki dosyalar daha ileri bir tarihte Karantina'da onarılabilir veya gerekirse Avira şirketine gönderilebilir.

**Sil**

Dosya silinecektir. Bu işlem, **Üzerine yaz ve sil** işleminden daha hızlıdır. Bir önyükleme sektörü virüsü algılandığında bu virüs, önyükleme sektörünü silerek silinebilir. Yeni bir önyükleme sektörü yazılır.

**Yoksay**

Baska bir eylem gerçekleştirilmez. Etkilenen dosya, bilgisayarınızda etkin kalır.

**Üzerine yaz ve sil**

Varsayılan bir şablonla dosyanın üzerine yazılır ve sonra dosya silinir. Geri yüklenemez.

**Uyarı**

Bu, veri kaybı ve işletim sistemi hasarıyla sonuçlanabilir! Yalnızca özel durumlarda **Yoksay** seçeneğini belirleyin.

**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

erisimlere izin verilir ve bilgisayar yeniden baslatılincaya veya virüs tanımı dosyası güncelleninceye kadar baska bir bildirim saglanmaz.

### **Karantinaya kopyala**

Kök kullanıcı takımlarının algılaması için eylem seçeneği: Algılama, karantinaya kopyalanır.

### **Önyükleme sektörünü onar | Onarım aracını karsıdan yükleyin**

Etkilenen önyükleme sektörleri algılandığında eylem seçenekleri: Etkilenen disket sürücülerini onarmak için birkaç seçenek mevcuttur. Avira ürününüz onarım gerçekleştiremiyorsa, önyükleme sektörü virüslerinin algılanması ve kaldırılması için özel bir araç karsıdan yükleyebilirsiniz.

#### **Not**

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

### **Proaktif bileşeni tarafından yapılan algılamalar için Gerçek Zamanlı Koruma eylemleri (bir uygulamanın şüpheli eylemlerine ilişkin bildirim):**

#### **Güvenilen program**

Uygulama çalışmaya devam eder. Program, izin verilen uygulamalar listesine eklenir ve Proaktif bileşenin izlemesi dışında bırakılır. İzin verilen uygulamalar listesine ekleme yapılırken, izleme türü *İçerik* olarak ayarlanır. Baska bir deyişle, uygulama, yalnızca içerik değiştirilmeden kalırsa Proaktif bileşeni izlemesi dışında bırakılır (bkz. [Uygulama filtresi: İzin verilen uygulamalar](#)).

#### **Programı bir defa engelle**

Uygulama engellenir; baska bir deyişle, uygulama sonlandırılır. Uygulama eylemleri, Proaktif bileşeni tarafından izlenmeye devam eder.

#### **Bu programı her zaman engelle**

Uygulama engellenir; baska bir deyişle, uygulama sonlandırılır. Program, engellenen uygulamalar listesine eklenir ve artık çalıştırılmaz (bkz. [Uygulama filtresi: Engellecek uygulamalar](#)).

#### **Yoksay**

Uygulama çalışmaya devam eder. Uygulama eylemleri, Proaktif bileşeni tarafından 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 [varsayılan metin](#) ile degistirilir.

### Postayi sil

Etkilenen e-posta silinir. E-posta metninin gövdesi ve ekler, bir [varsayılan metin](#) ile degistirilir.

### Eki sil

Etkilenen ek, [varsayılan bir metin](#) ile degistirilir. E-posta gövdesi etkilendiyse, silinir ve yerine [varsayılan bir metin](#) gelir. E-posta teslim edilir.

### Eki karantinaya tasi

Etkilenen ek, karantinaya yerlestirilir ve sonra silinir ([varsayılan metin](#) ile degistirilir). E-posta gövdesi teslim edilir. Etkilenen ek daha sonra karantina yöneticisi araciligıyla gönderilebilir.

### Yoksay

Etkilenen e-posta teslim edilir.

#### Uyari

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

## 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 programınızda bir hata iletisi alirsiniz. E-posta hesabınızdan gönderilen diğer tüm e-postalar, zararlı yazılıma karşı taranir.

### Postaların gönderimini engelle (gönderme)

E-posta gönderilmez ve e-posta istemcinizin giden kutusunda kalir. E-posta programınızda bir hata iletisi alirsiniz. E-posta hesabınızdan gönderilen diğer tüm e-postalar, zararlı yazılıma karşı taranir.

### Yoksay

Etkilenen e-posta gönderilir.

**Uyari**

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

**Web Koruması eylemleri:****Erisimi 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.

**Karantinaya tasi**

Web sunucusundan istenen web sitesi ve/veya aktarılan veri ya da dosyalar karantinaya tasınır. 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.

**Uyari**

Bu, virüs ve istenmeyen programların bilgisayar sisteminize erismesine olanak sağlar. Yalnızca özel durumlarda **Yoksay** seçeneğini belirleyin.

**Not**

Onarılamayan şüpheli dosyaları karantinaya tasimanızı öneririz.

**Not**

Ayrıca bulusal yöntemin bildirdiği dosyaları analiz için bize de gönderebilirsiniz. Örneğin bu dosyaları web sitemize yükleyebilirsiniz:

<http://www.avira.com/tr/sample-upload>

*HEUR/* veya *HEURISTIC/* göstergesinden örneğin *HEUR/testfile.\** dosya adına ön ek olarak getirilen bulusal yöntemin bildirdiği dosyaları tanımlayabilirsiniz.


### 4.3.11 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  ögesini 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 pozitiften yeniden tarama ile onaylamanıza ve dosyayı geri yüklemenize olanak sağlar.

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

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

- ▶ Karşıya yüklemek istediğiniz dosyayı vurgulayın.
- ▶  ögesini 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 sıfırlandı 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.

#### Not

Aynı anda yalnızca bir dosya karşıya yükleyebilirsiniz.

Karantinaya alınmış nesnenin özelliklerini bir metin dosyasına dışa aktarmak istiyorsanız:



- ▶ Karantinaya alınmış nesneyi vurgulayın ve  ögesini 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](#)).

### 4.3.12 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 gerekiyorsa, karşılık gelen bir istek görüntülenir.


### Karantinadaki dosyaları geri yüklemek için:

#### Uyarı



Bu, veri kaybı ve bilgisayar işletim sistemi hasarıyla sonuçlanabilir! Yalnızca özel durumlarda **Seçilen nesnelere 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  ögesini 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.

#### 4.3.13 Şüpheli dosyaları karantinaya taşıma

Şüpheli dosyayı el ile karantinaya taşımak için:

- ▶ Kontrol Merkezi'nde, **YÖNETİM > Karantina** bölümünü seçin.
- ▶  ögesini 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](#)).

#### 4.3.14 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 tıkkatın ve giriş kutusuna dosya türünün dosya uzantısını girin.

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

#### 4.3.15 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 tıkkatın.
  - Masaüstü kısayolu oluşturulur.

#### 4.3.16 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:

- 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.

#### 4.3.17 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.

## 5. 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 sürücülerini (örn. yeni dosyaları düzenli olarak depoladığınız çalışma dizininiz veya sürücüler) düzenli olarak taramak istiyorsanız bu yordam önerilir. Her yeni tarama için bu dizinleri ve sürücülerini 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. 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 nesnelere 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 güncellenen daha sonra hatırlatılmasına karar verebilirsiniz. Ürün güncellemeye hemen devam etmek isterseniz, yeniden başlatmanın ne zaman gerçekleşeceğini seçebilirsiniz.

Güncellenen 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: 2 saat.

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 İnternet'ten üreticinin Web sunucusu aracılığıyla edinilebilir. Varolan ağ bağlantısı, Avira karşıdan yükleme sunucuları ile varsayılan bağlantıdır. Bu varsayılan ayarı Yapılandırma'da [Yapılandırma > Güncelle](#) konumunda değiştirebilirsiniz.

## 7. Güvenlik Duvarı

Avira Antivirus Suite bilgisayar ayarlarınıza bağlı olarak gelen ve giden veri trafiğini yönetmenize izin verir:

- Windows Güvenlik Duvarı

Windows 7'den başlayarak, Avira Antivirus Suite Avira Güvenlik Duvarı içermemektedir. Windows Güvenlik Duvarı artık Avira ürünü üzerinden yönetilmektedir.

## 8. 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 \(Windows 7'den itibaren\)](#)

### 8.1 Sorun olması durumunda yardım

Burada, olası sorunların nedenleri ve çözümleriyle ilgili bilgiler bulursunuz.

- [Lisans dosyası açılmıyor](#) hata iletisi görüntülenir.
- Bir güncelleme başlatılmaya çalışılırken [Dosya karışından 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.
- TLS bağlantısı yoluyla gönderilen bir e-posta, EPosta Koruması tarafından engellendi.
- Web sohbeti çalışmıyor: Sohbet iletileri görüntülenmeyecek

#### ***Lisans dosyası açılmıyor* hata iletisi görüntülenir.**

Nedeni: Dosya şifrelidir.

- ▶ Lisansı etkinleştirmek için, dosyayı açmanız gerekmez ancak dosyayı program dizinine kaydedersiniz.

#### ***Bir güncelleme başlatılmaya çalışılırken Dosya karışından yüklenirken bağlantı başarısız oldu...* hata iletisi görüntülenir.**

Nedeni: İnternet bağlantınız etkin değil. Bu nedenle İnternet'te web sunucusuna bağlantı kurulamaz.

- ▶ WWW veya e-posta çalışması gibi diğer İnternet hizmetlerini deneyin. Aksi takdirde, İnternet 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 Yükleme'sini 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. Gerekliyse, 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? Gerekliyorsa, 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.

## TLS bağlantısı yoluyla gönderilen bir e-posta, EPosta Koruması tarafından engellendi.

Nedeni: Taşıma Katmanı Güvenliği (TLS: İnternet 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](#)).

## 8.2 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.

### 8.2.1 İletişim kutularında

Kısayol	Açıklama
<b>Ctrl + Tab</b> <b>Ctrl + Page down</b>	Kontrol Merkezi'nde gezinti Bir sonraki bölüme gidin.
<b>Ctrl + Shift + Tab</b> <b>Ctrl + Page up</b>	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.
<b>Sekme</b>	Sonraki seçeneğe veya seçenekler grubuna geçiş yapın.
<b>Shift + Sekme</b>	Önceki seçeneğe veya seçenekler grubuna geçiş yapın.
<b>Boşluk</b>	Etkin seçenek bir onay kutusuysa, onay kutusunu etkinleştirin veya devre dışı bırakın.

<b>Alt + altı çizili harf</b>	Seçeneği belirleyin veya komutu başlatın.
<b>Alt + ↓</b> <b>F4</b>	Seçili açılan listeyi açın.
<b>Esc</b>	Seçili açılan listeyi kapatın. Komutu iptal edin ve iletişim kutusunu kapatın.
<b>Enter</b>	Etkin seçenek veya düğme için komutu başlatın.

### 8.2.2 Yardımda

Kısayol	Açıklama
<b>Alt + Boşluk</b>	Sistem menüsünü görüntüleyin.
<b>Alt + Sekme</b>	Yardım ve diğer açılan pencereler arasında geçiş yapın.
<b>Alt + F4</b>	Yardıma kapatın.
<b>Shift + F10</b>	Yardıma bağlam menüsünü görüntüleyin.
<b>Ctrl + Tab</b>	Gezinti penceresinde bir sonraki bölüme gidin.
<b>Ctrl + Shift + Sekme</b>	Gezinti penceresinde bir önceki bölüme gidin.
<b>Page up</b>	Dizinde veya arama sonuçları listesinde, içindekilerin yukarısında görüntülenen konuya geçiş yapın.
<b>Page down</b>	Dizinde veya arama sonuçları listesinde, içindekilerdeki geçerli konunun aşağısında görüntülenen konuya geçiş yapın.

<b>Page up</b> <b>Page down</b>	Bir konuya göz atın.
------------------------------------	----------------------

### 8.2.3 Kontrol Merkezi'nde

#### Genel

Kısayol	Açıklama
<b>F1</b>	Yardımlı görüntüle
<b>Alt + F4</b>	Kontrol Merkezi'ni kapat
<b>F5</b>	Yenile
<b>F8</b>	Yapılandırmayı aç
<b>F9</b>	Güncellemeyi başlat

#### Tarama bölümü

Kısayol	Açıklama
<b>F2</b>	Seçilen profili yeniden adlandır
<b>F3</b>	Seçilen profille tarama başlat
<b>F4</b>	Seçilen profil için masaüstü bağlantısı oluştur
<b>Ins</b>	Yeni profil oluştur

<b>Del</b>	Seçilen profili sil
------------	---------------------

### **Karantina bölümü**

Kısayol	Açıklama
<b>F2</b>	Nesneyi yeniden tara
<b>F3</b>	Nesneyi geri yükle
<b>F4</b>	Nesneyi gönder
<b>F6</b>	Nesneyi şuraya geri yükle...
<b>Return</b>	Özellikler
<b>Ins</b>	Dosya ekle
<b>Del</b>	Nesneyi sil

### **Zamanlayıcı bölümü**

Kısayol	Açıklama
<b>F2</b>	İş i düzenle
<b>Return</b>	Özellikler
<b>Ins</b>	Yeni iş i ekle
<b>Del</b>	İş i sil

### Raporlar bölümü

Kısayol	Açıklama
<b>F3</b>	Rapor dosyasını görüntüle
<b>F4</b>	Rapor dosyasını yazdır
<b>Return</b>	Raporu görüntüle
<b>Del</b>	Raporları sil

### Olaylar bölümü

Kısayol	Açıklama
<b>F3</b>	Olay(lar)ı dışarı ver
<b>Return</b>	Olayı göster
<b>Del</b>	Olay(lar)ı sil

## 8.3 Windows Güvenlik Merkezi

- Windows XP Service Pack 2 -

### 8.3.1 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.

### 8.3.2 Windows Güvenlik Merkezi ve Avira ürününüz

#### Virüs koruması yazılımı / Zararlı yazılımlara karşı koruma

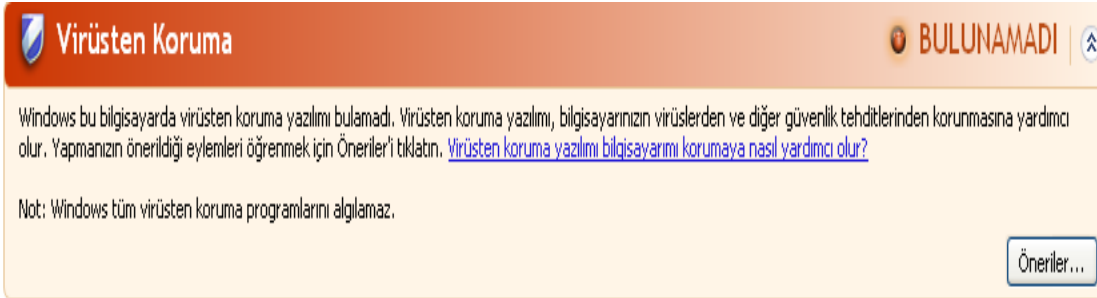
Windows Güvenlik Merkezi'nden virüs korumanızla ilgili aşağıdaki bilgileri alabilirsiniz:



- 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.



**Virüsten Koruma** BULUNAMADI

Windows bu bilgisayarda virüsten koruma yazılımı bulamadı. Virüsten koruma yazılımı, bilgisayarınızın virüslerden ve diğer güvenlik tehditlerinden korunmasına yardımcı olur. Yapmanız önerildiği eylemleri öğrenmek için Öneriler'i tıklayın. [Virüsten koruma yazılımı bilgisayarımı korumaya nasıl yardımcı olur?](#)

Not: Windows tüm virüsten koruma programlarını algılamaz.

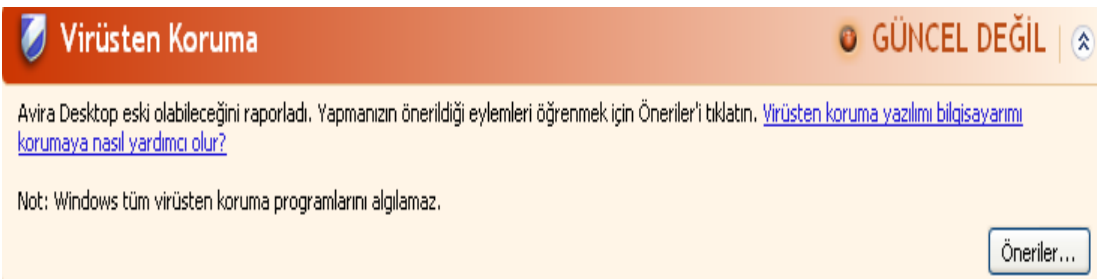
Öneriler...

#### 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:



**Virüsten Koruma** GÜNCEL DEĞİL

Avira Desktop eski olabileceğini raporladı. Yapmanız önerildiği eylemleri öğrenmek için Öneriler'i tıklayın. [Virüsten koruma yazılımı bilgisayarımı korumaya nasıl yardımcı olur?](#)

Not: Windows tüm virüsten koruma programlarını algılamaz.

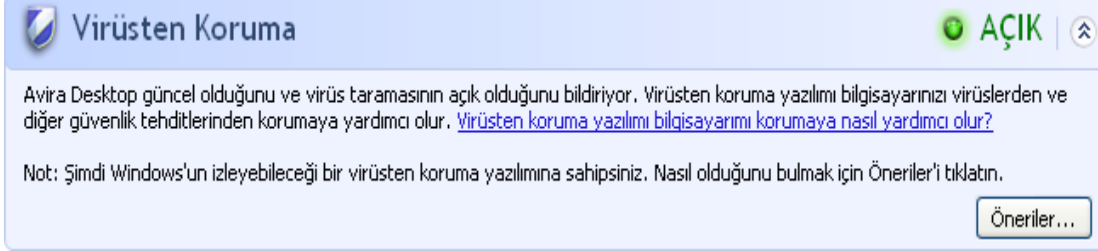
Öneriler...

#### Not

Windows Güvenlik Merkezi'nin, Avira ürününüzü güncel olarak tanıması için, kurulumdan sonra bir güncelleme gerçekleştirilmelidir. Bir güncelleme gerçekleştirerek sisteminizi güncelleyin.

## Virüs koruması AÇIK

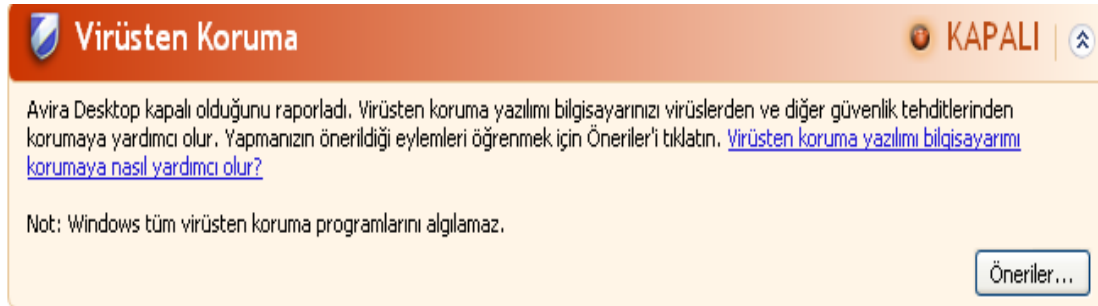
Avira ürününüzü kurduktan ve ardından bir güncelleme gerçekleştirdikten sonra, aşağıdaki iletiyi alırsınız:



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.

 İZLENMİYOR 

Kendi kendinizi izleyeceğiniz bir virüsten koruma yazılımı çalıştırdığınızı belirttiniz. Bilgisayarınızı virüslerden ve diğer güvenlik tehditlerinden korunmasına yardımcı olmak için, virüsten koruma yazılımınızın açık ve güncel olduğundan emin olun. [Virüsten koruma yazılımı bilgisayarımı korumaya nasıl yardımcı olur?](#)

[Öneriler...](#)

**Not**

Windows Güvenlik Merkezi, Avira ürününüz tarafından desteklenir. İsteddiğiniz 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!

## 8.4 Windows Eylem Merkezi

- Windows 7 ve Windows 8 -

### 8.4.1 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. İsteddiğiniz zaman **Windows Eylem Merkezi, Güvenlik** ögesi 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*).

## 8.4.2 Windows Eylem Merkezi ve Avira ürününüz

### • Avira tarafından yönetilen Windows Güvenlik Duvarı

Windows 7'den itibaren, Avira Antivirus Suite 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'yı devre dışı bırakırsanız veya Gerçek Zamanlı Koruma hizmetini durdurursanız, aşağıdaki iletiyi alırsınız.

**Virüsten koruma (Önemli)**

Avira Desktop kapalı olduğunu bildirdi.

[Virüsten koruma ile ilgili iletileri kapat](#)

[Şimdi aç](#)

[Çevrimiçi başka bir virüsten koruma programı edinin](#)

#### 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 iletilerindeki *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:

**Virüsten koruma (Önemli)**

Avira Desktop güncel olmadığını bildirdi.

[Virüsten koruma ile ilgili iletileri kapat](#)

[Şimdi güncelleştir](#)

[Çevrimiçi başka bir virüsten koruma programı edinin](#)

### Not

Windows Eylem Merkezi'nin, Avira ürününüzü güncel olarak tanınması 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.

**Virüsten koruma (Önemli)**

Windows bu bilgisayarda virüsten koruma yazılımı bulamadı.

[Virüsten koruma ile ilgili iletileri kapat](#)

[Çevrimiçi bir program bul](#)

### 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 ürününüzün lisans süresi sona erdiğinde, Windows Eylem Merkezi'nin bilgileri görüntülenir.

**Aboneliği yenile** düğmesine tıkladığınızda, yeni bir lisans alabileceğiniz Avira web sitesine yönlendirilirsiniz.

**Virüsten koruma (Önemli)**

Avira Desktop uygulaması artık kişisel bilgisayarınızı korumuyor.

[Virüsten koruma ile ilgili iletileri kapat](#)

[Yüklü virüsten koruma uygulamalarını görüntüle](#)

[İşlem yap](#)

### 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.

**Casus yazılımlara ve istenmeyen yazılımlara karşı koruma (Önemli)**

Hem Windows Defender hem de Avira Desktop kapalı olduğunu bildirdi.

[Casus yazılım önleme programla...](#)[Casus yazılımlar ve bunlarla ilişkili koruma ile ilgili iletileri kapat](#)**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 iletilerindeki *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:

**Casus yazılımlara ve istenmeyen yazılımlara karşı koruma (Önemli)**

Avira Desktop güncel olmadığını bildirdi.


[Şimdi güncelleştir](#)[Casus yazılımlar ve bunlarla ilişkili koruma ile ilgili iletileri kapat](#)[Çevrimiçinde başka bir casus yazılım önleme program...](#)**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.

**Casus yazılımlara ve istenmeyen yazılımlara karşı koruma (Önemli)**

 Windows Defender güncel değil.


[Şimdi güncelleştir](#)[Casus yazılımlar ve bunlarla ilişkili koruma ile ilgili iletileri kapat](#)[Çevrimiçinde başka bir casus yazılım önleme program...](#)**Not**

Windows Defender Windows tarafından sunulan önceden tanımlı bir casus yazılım ve virüs koruma çözümdür.

**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.

**Casus yazılımlara ve istenmeyen yazılımlara karşı koruma (Önemli)**

 Windows Defender kapalı.

[Şimdi aç](#)[Casus yazılımlar ve bunlarla ilişkili koruma ile ilgili iletileri kapat](#)[Çevrimiçinde başka bir casus yazılım önleme program...](#)



## 9. Virüsler ve daha fazlası

Avira Antivirus Suite 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](#)

### 9.1 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

İnternet'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 İnternet kullanıcısının ISP (İnternet 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 kamuflej 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 alıştırılmaları"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 kaldıracaktır. **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, İnternet hizmeti sağlayıcılarının, bankaların, çevrimiçi bankacılık hizmetlerinin, kayıt yetkililerinin müşterilerini veya olası müşterilerini hedefleyen, akıllıca bir veri hırsızlığı biçimidir.

İnternet üzerinden e-posta adresinizi gönderirken, çevrimiçi formları doldururken, haber gruplarına veya web sitelerine erişirken verileriniz "İnternet'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 algılandığında, 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 algılandığında, 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 algılandığında, karşılık gelen bir uyarı alırsınız.

## **9.2 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

kaldırılmaz 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, İnternet 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 ağ 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 yönlendirme

Websitesini başka siteye yönlendirme, sahtekar web sitelerine sorguları yönlendirmek için web tarayıcılarının barındırma dosyasının bir manipülasyonudur. Bu, klasik kimlik avının daha ileri bir modelidir. Websitesini başka siteye yönlendirme dolandırıcıları, sahte web sitelerinin depolandığı kendi büyük sunucu gruplarını çalıştırır. Websitesini başka siteye yönlendirme 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, İnternet 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 saldırganlara 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 yerleştiği 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 işlem 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.



## 10. Bilgi ve Hizmet

Bu bölüm Avira Bilgi ve Hizmetleri ile ilgili bilgiler içerir.

- [İletişim adresi](#)
- [Teknik destek](#)
- [Şüpheli dosya](#)
- [Yanlış pozitifleri bildirme](#)
- [Daha fazla güvenlik için geribildiriminiz](#)

### 10.1 İletişim adresi

Avira ürün yelpazesıyla ilgili sorularınız veya istekleriniz varsa size yardımcı olmaktan mutluluk duyarız. İletişim adreslerimiz için lütfen **Yardım > Avira Antivirus Suite Hakkında** altında Kontrol Merkezi konumuna bakın.

### 10.2 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/premium-support>

Size hızlı ve güvenilir yardım sağlayabilmemiz için şu bilgileri hazır bulundurmanız gerekir:

- **Lisans bilgileri.** Bu bilgileri **Yardım > Avira Antivirus Suite hakkında > Lisans bilgileri** menü öğesinin altındaki program arabiriminde bulabilirsiniz. Bkz. Lisans bilgileri.
- **Sürüm bilgileri.** Bu bilgileri **Yardım > Avira Antivirus Suite 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.**

### 10.3 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** ögesini seçin.
- Bir e-postanın ekinde gerekli olan dosyayı (WinZIP, PKZip, Arj vb.) şu adrese gönderin: [virus-premium-tr@avira.com](mailto:virus-premium-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>

## 10.4 Yanlış pozitifleri bildirme

Avira Antivirus Suite 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-premium-tr@avira.com](mailto:virus-premium-tr@avira.com)

Bazı e-posta ağ geçitleri anti virüs yazılımı ile birlikte çalıştığından, dosyalara bir parola sağlamanız gerekir (lütfen bize parolayı söylemeyi unutmayın).

## 10.5 Daha fazla güvenlik için geribildiriminiz

Avira 'da müşterilerimizin güvenliği çok önemlidir. Bu nedenle, yalnızca ürün yayınlanmadan önce her Avira çözümünün kalite ve güvenliğini sınanan 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](mailto:vulnerabilities@avira.tr)

## 11. Başvuru: Yapılandırma seçenekleri

Yapılandırma başvurusu tüm kullanılabilir yapılandırma seçeneklerini belgeler.

### 11.1 Sistem Tarayıcı

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

#### 11.1.1 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 görüntülediği 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 önyüklemeye sektörlerini tara**

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

**Ana önyüklemeye sektörlerini tara**

Bu seçenek etkinleştirilirse, Sistem Tarayıcı, sistemde kullanılan sabit disklerin ana önyüklemeye 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.

### 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.

## 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 sürücülerini, 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

**Karantina** eylemi, Sistem Tarayıcı bildiriminde varsayılan olarak önceden seçilidir. Bir bağlam menüsü aracılığıyla daha fazla eylem seçilebilir.

## 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.

### *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.

### **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 girdiyse, 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.

**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.

## 11.1.2 Rapor

Sistem Tarayıcı, kapsamlı bir raporlama işlevine sahiptir. Bu nedenle, istek üzerine tarama sonuçları hakkında kesin bilgiler edebilirsiniz. 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)' son ekini 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.

## 11.2 Gerçek Zamanlı Koruma

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

### 11.2.1 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 görüntülediği 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 sürücülerini **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 nesnelere 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 değer kullanılması önerilir: doğrudan ana arşive yerleştirilen tüm dosyalar taranır.

**Maks. dosya sayısı**

Arşivler taranırken, taramayı arşivdeki maksimum dosya sayısı ile 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 bildirim 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.

*Birincil eylem*

Birincil eylem, Gerçek Zamanlı Koruma bir virüs veya istenmeyen program bulunduğunda 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 nesnelere yapılandırabilirsiniz. İlgili nesnelere, 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 nesnelere 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 izin 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 belirtilmeler 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 sürücülerini gibi bağlı sürücülerde bulunduğu işlemler için tam yol ayrıntıları gerekir. Lütfen [Bağlı ağ sürücülerine 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 görüntülediği "**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 nesnelere

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 nesnelere 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 izin 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 tanır. 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 nesnelere de dışarıda bırakmak için, ilgili kısa dosya adı da listeye girilmelidir.

Joker karakterler içeren bir dosya adı, ters eğik çizgiyle sonlandırılmaz. 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.

## **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.

### **11.2.2 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 yoksayılr. 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 indirmek 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 aşığına ulaşıncaya kadar eski girdiler silinir.

#### **Kısaltmadan önce rapor dosyasını yedekle**

Bu seçenek etkinleştirilirse, kısaltmadan önce rapor dosyası yedeklenir.



## 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.

## 11.3 Güncelle

**Güncelle** bölümünde, güncellemelerin otomatik alınmasını yapılandırabilirsiniz. Çeşitli güncelleme aralıklarını.

### *Otomatik güncelle*

#### **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.

#### **Ayrıca Internet bağlantısı kurulduğunda 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.

### 11.3.1 Web sunucusu

#### **Web sunucusu**

Güncelleme, doğrudan Internet'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.

## **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

## 11.4 Güvenlik Duvarı

### 11.4.1 Güvenlik Duvarını Yapılandırma

Avira Antivirus Suite Avira Güvenlik Duvarını yapılandırmanıza veya Windows Güvenlik Duvarını (Windows 8'den itibaren) yönetmenize izin verir:

- [Windows Güvenlik Duvarı](#)

### 11.4.2 Windows Güvenlik Duvarı

Windows 7'den itibaren **İnternet Koruması > Yapılandırma** altındaki **Güvenlik Duvarı** bölümü, Windows Güvenlik Duvarı'nın yapılandırmasından sorumludur.

## 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.

## 11.5 Web Koruması

**Yapılandırma > İnternet Koruması** altındaki **Web Koruması** bölümü Web Koruması'nın yapılandırmasından sorumludur.

### 11.5.1 Tara

Web Koruması, İnternet'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

## 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 engellenenize 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 bildirim görüntülenir. Bu masaüstü bildirim 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.

Daha fazla bilgi için burayı tıkkatın.

## 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.

### *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 engelleme için 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 yoksayılr.

#### 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 (İnternet adresleri) dosya türlerini temel alarak istisnalar ayarlamana olanak sağlar. Belirtilen MIME türleri ve URL'ler, Web Koruması tarafından yoksayılr; 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](#)) yoksayılar. 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](http://www.avira.com/en/download/index.html), vb.

[www.avira.de](http://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 belirtiler 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.

## 11.5.2 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 yoksayılar. 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 indirmek 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.

## 11.6 EPosta Koruması

Yapılandırma'nın **EPosta Koruması** bölümü, EPosta Koruması yapılandırmasından sorumludur.

### 11.6.1 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.

### Gelen e-postaları tara

Bu seçenek etkinleştirilirse, gelen e-postalar, virüslere, zararlı yazılımlara karşı 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.

**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, İnternet 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.

## 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 bulunduğunda 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 bulunduğunda 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.

## 11.6.2 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 sayısı

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.

## 11.6.3 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 indirmek 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 ulaşıncaya kadar eski girdiler silinir.

### Kısaltmadan önce rapor dosyasını yedekle

Bu seçenek etkinleştirilirse, kısaltmadan önce rapor dosyası yedeklenir.

## 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.

## 11.7 Mobil Koruma

Avira, bilgisayar sisteminizi zararlı yazılımlara ve virüslere karşı korumanın yanı sıra Android işletim sistemi ile çalışan akıllı telefonunuzu kaybolmaya ve hırsızlığa karşı da korur. Avira Free Android Security'ni kullanarak istemediğiniz aramaları veya SMS'leri de engelleyebilirsiniz. Arama günlüğünden, SMS günlüğünden veya kişiler listenizden telefon numaralarını kolayca kara listeye ekleyin veya engellemek istediğiniz bir kişiyi el ile oluşturun.

Web sitemizde daha fazla bilgi bulabilirsiniz:

<http://www.avira.com/android>

## 11.8 Genel

### 11.8.1 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.

## 11.8.2 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 bildirim 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 dosyaların 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 bildiri 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 bileşenin izlemesi dışında bırakılan uygulamaları içerir. Varsayılan kurulum ayarlarında liste, güvenilen üreticilerin imzalanmış uygulamalarını içerir. Yapılandırma aracılığıyla veya Gerçek Zamanlı Koruma bildirimleri aracılığıyla güvenilir olduğuna 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 yapıp yapılmayacağına karar verebilirsiniz: "*İçerik*" türü için, yola ve dosya adına göre belirtilen uygulamalar, Proaktif bileşenin 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 bileşenin izlemesi dışında bırakılır.

## Giriş kutusu

Bu kutuya, Proaktif bileşenin 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.

## 11.8.3 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
<b>Kontrol Merkezi</b>	Bu seçenek etkinleştirilirse, Kontrol Merkezi'ni başlatmak için önceden tanımlı parola gerekir.
<b>Gerçek Zamanlı Koruma'yı etkinleştir / devre dışı bırak</b>	Bu seçenek etkinleştirilirse, Avira Gerçek Zamanlı Koruma'yı etkinleştirmek veya devre dışı bırakmak için önceden tanımlı parola gerekir.
<b>EPosta Koruması'nı etkinleştir/devre dışı bırak</b>	Bu seçenek etkinleştirilirse, EPosta Koruması'nı etkinleştirmek/devre dışı bırakmak için önceden tanımlı parola gerekir.
<b>Web Koruması'nı etkinleştir / devre dışı bırak</b>	Bu seçenek etkinleştirilirse, Web Koruması'nı etkinleştirmek/devre dışı bırakmak için önceden tanımlı parola gerekir.
<b>Karantina</b>	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.
<b>Etkilenen nesnelere geri yükle</b>	Bu seçenek etkinleştirilirse, bir nesneyi geri yüklemek için önceden tanımlı parola gerekir.
<b>Etkilenen nesnelere yeniden tara</b>	Bu seçenek etkinleştirilirse, bir nesneyi yeniden taramak için önceden tanımlı parola gerekir.
<b>Etkilenen nesne özellikleri</b>	Bu seçenek etkinleştirilirse, bir nesnenin özelliklerini görüntülemek için önceden tanımlı parola gerekir.

<b>Etkilenen nesnelere sil</b>	Bu seçenek etkinleştirilirse, bir nesneyi silmek için önceden tanımlı parola gerekir.
<b>Avira'ya e-posta gönder</b>	Bu seçenek etkinleştirilirse, incelenmek üzere Avira Zararlı Yazılım Araştırma Merkezi'ne bir nesne göndermek için önceden tanımlı parola gerekir.
<b>Yapılandırma</b>	Bu seçenek etkinleştirilirse, program yapılandırması yalnızca önceden tanımlı parola girildikten sonra mümkündür.
<b>Kurulum / kaldırma</b>	Bu seçenek etkinleştirilirse, programı kurmak veya kaldırmak için önceden tanımlı parola gerekir.

#### 11.8.4 Güvenlik

##### *Autorun*

##### **Autorun işlevini engelle**

Bu seçenek etkinleştirildiğinde, USB çubuklar, CD ve DVD sürücüler ve ağ sürücüler 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 !

### 11.8.5 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 olayları sağlar. WMI, size programdan işletim verilerini karşıdan yükleme

#### **WMI desteğini etkinleştir**

Bu seçenek etkinleştirildiğinde, WMI aracılığıyla programdan işletim verilerini karşıdan yükleyebilirsiniz.

### 11.8.6 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 aşırsa, 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.

## 11.8.7 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 aşırsa, 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.

## 11.8.8 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.



### 11.8.9 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.

### 11.8.10 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, bildirim doğrudan "slide-up"ta devre dışı bırakma seçeneğiniz vardır. **Uyarılar** yapılandırma penceresinde, bildirim 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 bildirim 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 bildirim alırsınız.

#### **Güncelleme başarısız oldu**

Bu seçenek etkinleştirilirse, bir güncelleme başarısız olduğunda bir masaüstü bildirim 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 bildirim alırsınız.



# Avira

Bu kılavuz çok dikkatli bir şekilde hazırlanmıştır. Buna rağmen tasarım ve içerikte hatalar bulunabilir. Avira Operations GmbH & Co. KG tarafının önceden yazılı olmadan bu yayının tamamen veya kısmen çoğaltılması yasaktır.

Marka ve ürün adları, ilgili sahiplerinin ticari markaları veya tescilli ticari markalarıdır. Korunmalı ticari markalar bu kılavuzda bu şekilde işaretlenmemiştir. Ancak bu, söz konusu markaların serbestçe kullanılabilmesi anlamına gelmez.

Sürüm: 4 çeyrek 2013

© 2013 Avira Operations GmbH & Co. Tüm hakları saklıdır.  
Hatalar ve unutmalar ve teknik değişiklikler bunlara istisnadır.

Avira | Kaplaneiweg 1 | 88069 Tettnang | Almanya | Telefon: +49 7542-500 0  
www.avira.com