



AVG 9.0 File Server

Kullanici Kilavuzu

Belge revizyonu 90.7 (31. 3. 2010)

Telif Hakki AVG Technologies CZ, s.r.o. Tüm haklari saklidir.
Tüm diger ticari markalar ilgili sahiplerine aittir.

Bu ürün, RSA Data Security, Inc. MD5 Message-Digest Algorithm özelligini kullanmaktadır, Telif Hakki (C) 1991-2, RSA Data Security, Inc. Olusturma Tarihi: 1991.

Bu üründe, C-SaCzech kütüphanesi, Telif Hakki (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz) kodlari kullanilmektedir.

Bu ürün sikistirma kitapligi zlib ürününü kullanmaktadır, Telif Hakki (c) 1995-2002 Jean-loup Gailly ve Mark Adler.

Bu ürün sikistirma kitapligi libbzip2 kullanir, Telif Hakki (c) 1996-2002 Julian R. Seward.

İçindekiler

1. Giriş	6
2. Yükleme Gereksinimleri	7
2.1 Desteklenen İşletim Sistemleri	7
2.2 Donanım Gereksinimleri	7
3. AVG Yükleme Seçenekleri	8
4. AVG Yükleme Süreci	9
4.1 Yükleme Baslatma	9
4.2 Lisans Sözleşmesi	10
4.3 Sistem Durumu Kontrolü	11
4.4 Yükleme Türü Seçim	12
4.5 AVG Lisansinizi Etkinleştirin	12
4.6 Özel Yükleme - Hedef Klasör	13
4.7 Özel Yükleme - Bileşen Seçimi	14
4.8 AVG DataCenter	15
4.9 AVG Yükleniyor	16
4.10 Düzenli tarama ve güncellemeleri programlamak	17
4.11 AVG koruması yapılandırması tamamlandı	17
5. Yüklemeden Sonra	19
5.1 Taramayı en iyi hale getirme	19
5.2 Ürün Kaydı	19
5.3 Kullanıcı Arayüzü'ne Eriş	19
5.4 Tam bilgisayar taraması	20
5.5 Eicar Testi	20
5.6 AVG Varsayılan Yapılandırması	21
6. AVG Kullanıcı Arayüzü	22
6.1 Sistem Menüsü	23
6.1.1 Dosya	23
6.1.2 Bileşenler	23
6.1.3 Geçmiş	23
6.1.4 Araçlar	23
6.1.5 Yardım	23

6.2 Güvenlik Durumu Bilgisi	26
6.3 Hizli Baglantilar	27
6.4 Bilesen Genel Görünümü	28
6.5 Sunucu bileşenleri	29
6.6 Istatistikler	30
6.7 Sistem Tepsisi Sembolü	31
7. AVG Bilesenleri	32
7.1 Virüsten Koruma	32
7.1.1 Virüsten Koruma İlkeleri	32
7.1.2 Virüsten Koruma Arayüzü	32
7.2 Casus Yazilimdan Koruma	34
7.2.1 Casus Yazilimdan Koruma Prensipleri	34
7.2.2 Casus Yazilimdan Koruma Arayüzü	34
7.3 Anti-Rootkit	36
7.3.1 Anti-Rootkit Prensipleri	36
7.3.2 Anti-Rootkit Arayüzü	36
7.4 Lisans	38
7.5 Yerlesik Kalkan	39
7.5.1 Yerlesik Kalkan İlkeleri	39
7.5.2 Yerlesik Kalkan Arayüzü	39
7.5.3 Yerlesik Kalkan Tespiti	39
7.6 Güncelleme Yöneticisi	44
7.6.1 Güncelleme Yöneticisi Prensipleri	44
7.6.2 Güncelleme Yöneticisi Arayüzü	44
8. AVG Sunucusu Bilesenleri	47
8.1 MS SharePoint için Belge Tarayici	47
8.1.1 Belge Tarayici Prensipleri	47
8.1.2 Belge Tarayici Arayüzü	47
9. SharePoint Portal Server için AVG	49
9.1 Program Bakimi	49
9.2 SPPS Yapilandirmasi - SharePoint 2007 için AVG	50
9.3 SPPS Yapilandirmasi - SharePoint 2003 için AVG	52
10. AVG Gelismis Ayarlar	55
10.1 Görünüm	55
10.2 Sesler	57

10.3 Hatali Durumlari Yoksay	59
10.4 Virüs Kasasi	60
10.5 PUP Istisnaları	61
10.6 Taramalar	63
10.6.1 Tüm Bilgisayari Tara	63
10.6.2 Kabuk Uzantisi Tarama	63
10.6.3 Belirli Dosyalari veya Klasörleri Tara	63
10.6.4 Çıkarılabilir Aygit Tarama	63
10.7 Programlar	71
10.7.1 Programli Tarama	71
10.7.2 Virüs Veritabani Güncelleme Programi	71
10.7.3 Program Güncelleme Planı	71
10.8 Yerlesik Kalkan	81
10.8.1 Gelismis Ayarlar	81
10.8.2 Hariç Tutulan Dizin	81
10.8.3 Hariç Tutulan Dosyalar	81
10.9 Önbellek Sunucusu	86
10.10 Anti-Rootkit	87
10.11 Güncelle	89
10.11.1 Proxy	89
10.11.2 Çevirmeli	89
10.11.3 URL	89
10.11.4 Yönet	89
10.12 Uzaktan Yönetim	96
10.13 Sunucu bileşenleri	97
10.13.1 MS SharePoint için Belge Tarayıcı	97
11. AVG Tarama	102
11.1 Tarama Arayüzü	102
11.2 Öntanımlı Taramalar	103
11.2.1 Tüm Bilgisayari Tara	103
11.2.2 Belirli Dosyalari veya Klasörleri Tara	103
11.2.3 Anti-Rootkit Tarama	103
11.3 Windows Gezgininde Tarama	113
11.4 Komut Satiri Tarama	114
11.4.1 CMD Tarama Parametreleri	114
11.5 Tarama Planlama	116
11.5.1 Program Ayarlari	116

11.5.2 Tarama Sekli	116
11.5.3 Taranacaklar	116
11.6 Tarama Sonuçları Genel Görünümü	126
11.7 Tarama Sonuçları Ayrıntıları	127
11.7.1 Sonuçlara Genel Bakis Sekmesi	127
11.7.2 Bulasma Sekmesi	127
11.7.3 Casus Yazılım Sekmesi	127
11.7.4 Uyarılar Sekmesi	127
11.7.5 Rootkit'ler Sekmesi	127
11.7.6 Bilgi Sekmesi	127
11.8 Virüs Kasası	136
12. AVG Güncellemeleri	138
12.1 Güncelleme Seviyeleri	138
12.2 Güncelleme Türleri	138
12.3 Güncelleme İşlemi	138
13. Olay Geçmişi	140
14. AVG Ayarları Yöneticisi	142
15. SSS ve Teknik Destek	145



1. Giriş

Bu kullanıcı el kitabı, **AVG 9.0 File Server** için kapsamlı dokümantasyon sağlar.

AVG 9.0 File Server programını satın aldığınız için tebrik ederiz!

AVG 9.0 File Server PC'niz için tam güvenlik ve rahatlık sağlamak üzere tasarlanmış ödüllü AVG ürünlerinden biridir. AVG'nin ünlü ve ödüllü güvenlik korumasını sunmak adına bastan basa tamamen yeniden tasarlanan **AVG 9.0 File Server**, tüm diğer AVG ürünleri gibidir fakat kullanımı daha kolay ve verimlidir.

Yeni **AVG 9.0 File Server** ürününüz daha agresif ve daha hızlı taramayı birleştiren akıcı bir arayüze sahiptir. Güvenliğiniz için daha fazla sayıda güvenlik özelliği otomatik hale getirilmiştir ve yeni 'akıllı' kullanıcı seçenekleri sayesinde gerekli ayarlamaları kendi güvenlik ihtiyaçlarınız doğrultusunda yapabilirsiniz. Artık güvenliğinizden ödün vermek yok!

AVG, bilgisayar ve ağ kurma faaliyetlerinizi korumak için tasarlanmış ve geliştirilmiştir. AVG'nin sağladığı eksiksiz korumanın tadını çıkarın.



2. Yükleme Gereksinimleri

2.1. Desteklenen İşletim Sistemleri

AVG 9.0 File Server aşağıdaki işletim sistemlerine sahip iş istasyonlarını koruma amaçlıdır:

- Windows 2000 Server
- Windows 2003 Server ve Windows 2003 Server x64 Edition
- Windows 2008 Server ve Windows 2008 Server x64 Edition

(ve belirli işletim sistemleri için daha yeni servis paketleri)

2.2. Donanım Gereksinimleri

AVG 9.0 File Server için minimum donanım gereksinimleri:

- Intel Pentium CPU 1,5 GHz
- 470 MB boş sabit disk alanı (yükleme için)
- 512 MB RAM bellek

AVG 9.0 File Server için önerilen donanım gereksinimleri:

- Intel Pentium CPU 1,8 GHz
- 600 MB boş sabit disk alanı (yükleme için)
- 512 MB RAM bellek



3. AVG Yükleme Seçenekleri

AVG, yükleme CD'niz üzerinde bulunan yükleme dosyasından yüklenebilir ya da en güncel yükleme dosyasını AVG'nin web sitesinden (<http://www.avg.com>) indirebilirsiniz.

AVG'yi yüklemeye başlamadan önce yeni yükleme dosyasını kontrol etmek için AVG web sitesini (<http://www.avg.com>) ziyaret etmenizi önemle öneririz. Bu şekilde, en güncel AVG 9.0 File Server sürümünü yüklediğinizden emin olabilirsiniz.

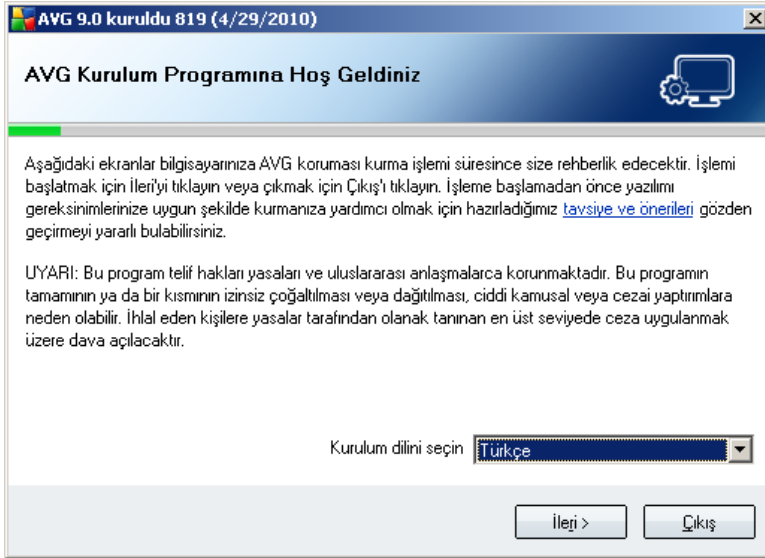
Yükleme işlemi sırasında lisans/satis numaranızı girmeniz istenecektir. Yüklemeye başlamadan önce söz konusu numarayı hazırladığınızdan emin olun. Satis numarası, CD ambalajı üzerinde bulunur. AVG'yi çevrimiçi mağazadan satın aldıysanız lisans numaranız e-posta aracılığıyla gönderilecektir.

4. AVG Yükleme Süreci

Bilgisayarınıza **AVG 9.0 File Server** programini yüklemek için, en güncel yükleme dosyasini edinmeniz gerekir. Kutulu versiyonların içinden çıkan CD'de bulunan yükleme dosyasini da kullanabilirsiniz fakat söz konusu dosya güncel olmayabilir. Bu nedenle en güncel kurulum dosyasini çevrimiçi ortamdan indirmenizi öneriyoruz. Dosyayı AVG web sitesinden (<http://www.avg.com>), **İndirmeler** bölümünden indirebilirsiniz.

Yükleme işlemi, her adımda neler yapmanız gerektiğine dair kısa tanımlamalar içeren bir dizi iletişim kutusu pencerelerinden oluşur. Aşağıda iletişim kutularının her biri için kısa bir açıklama sunuyoruz:

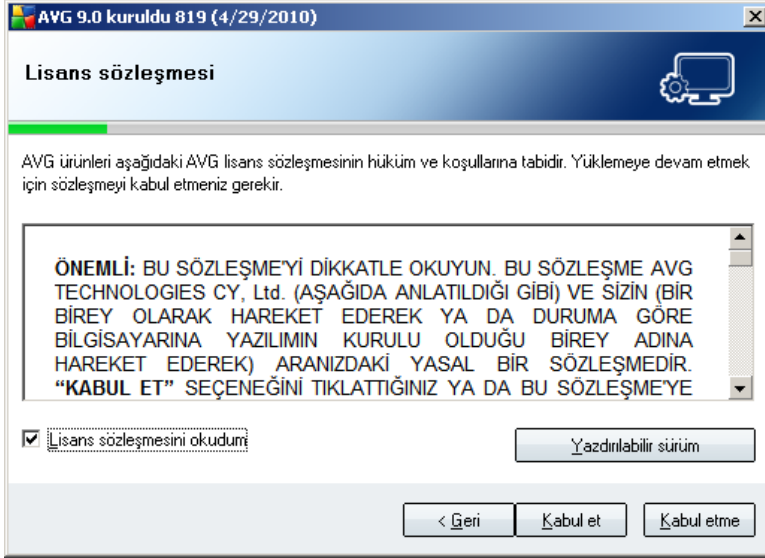
4.1. Yükleme Baslatma



Yükleme işlemi, **AVG Yükleme Programına Hos Geldiniz** penceresi ile başlar. Burada yükleme işlemi için kullanacağınız dili seçebilirsiniz. İletişim kutusu penceresinin alt kısmında **Kurulum dilinizi seçin** ögesini bulun ve açılır menüden istediğiniz dili seçin. Onaylamak ve bir sonraki iletişim kutusuna geçmek için **İleri** düğmesine basın.

Dikkat: Yükleme işleminin basında seçtiğiniz dil AVG uygulamasının dili olarak kullanılır. Ancak, daha sonra [AVG Kullanıcı Arayüzü](#) -> [Araçlar](#) -> [Gelişmiş Ayarlar](#) -> [Görünüm](#) ögesinden değiştirebilirsiniz.

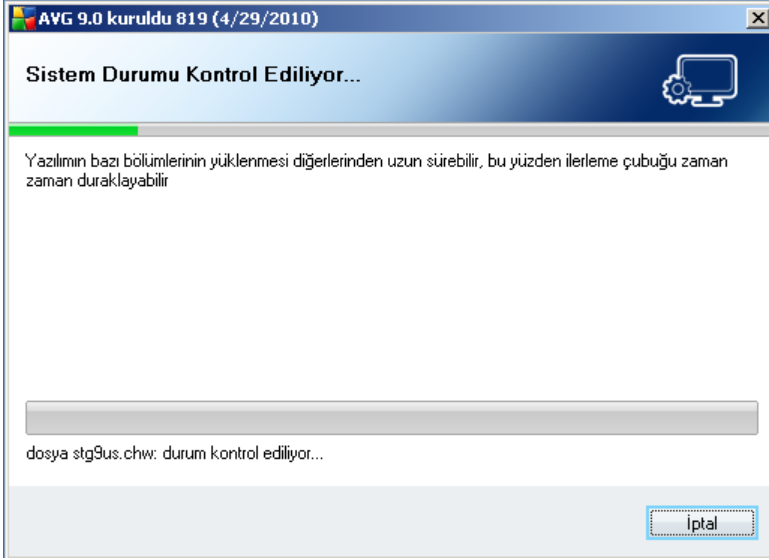
4.2. Lisans Sözleşmesi



Lisans Sözleşmesi iletişim kutusunda AVG lisans sözleşmesinin tamamı bulunmaktadır. Lütfen sözleşmeyi dikkatle okuyun ve **Lisans sözleşmesini okudum** onay kutusunu işaretleyerek ve **Kabul ediyorum** düğmesine basarak okudugunuzu, anladiginizi ve kabul ettiginizi onaylayın.

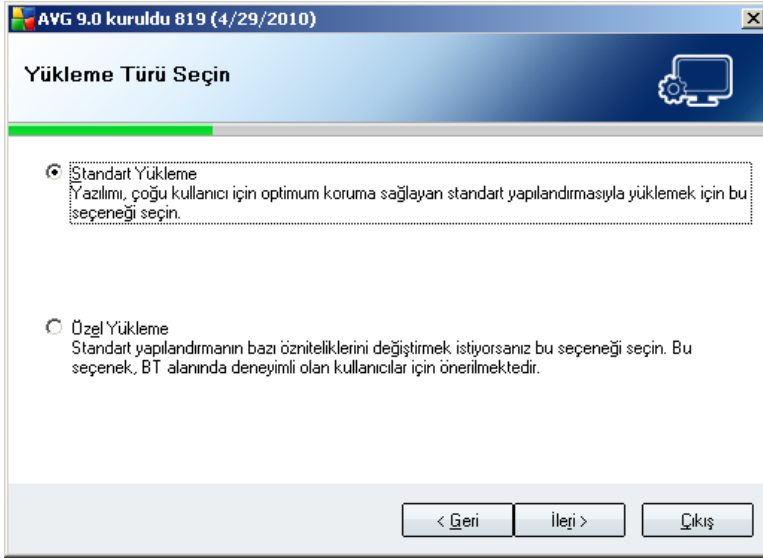
Lisans sözleşmesini kabul etmiyorsanız **Kabul Etmiyorum** düğmesine basın; yükleme işlemi anında iptal edilecektir.

4.3. Sistem Durumu Kontrolü



Lisans sözleşmesini onayladıktan sonra **Sistem Durumu Kontrol Ediliyor** iletişim kutusuna yönlendirileceksiniz. Bu iletişim kutusu herhangi bir müdahale gerektirmez; AVG yüklemesi başlamadan önce sisteminiz kontrol edilir. Lütfen işlem bitene kadar bekleyin ve ardından bir sonraki iletişim kutusuna otomatik olarak geçin.

4.4. Yükleme Türü Seçin



Yükleme Tipini Seç iletişim kutusunda iki farklı yükleme seçeneği sunulur: **standart** ve **özel** kurulum.

Kullanıcıların çoğu için yazılım geliştiricisi tarafından öntanımlı ayarlarla AVG'yi tamamen fonksiyonel şekilde kuran **standart kurulum** önerilmektedir. Bu yapılandırma, minimum kaynak kullanımı ile maksimum güvenliği bir araya getirir. Gelecekte söz konusu yapılandırmayı değiştirme ihtiyacı duyarsanız söz konusu işlemi doğrudan AVG uygulamasından yapabileceksiniz.

Özel yükleme AVG'yi standart olmayan ayarlarla kurmak hususunda geçerli bir nedeni olan deneyimli kullanıcılar tarafından kullanılmalıdır. Örn. belirli sistem gereksinimlerini karşılamak için.

4.5. AVG Lisansinizi Etkinleştirin

AVG Lisansinizi Etkinleştirin iletişim kutusunda kayıt bilgilerinizi girmeniz gerekir. Adınızı (**Kullanıcı Adı** alanına) ve organizasyon adınızı (**Sirket Adı** alanına) girin.

Lisans/satis numaranızı **Lisans Numarası** alanına girin. Satis numarası, **AVG 9.0 File Server** kutusundaki CD paketinde bulunabilir. Lisans numarası **AVG 9.0 File Server** programını çevrimiçi satın aldıktan sonra alacağınız onay e-postasında olacaktır. Sayıları gösterildiği gibi gitmelisiniz. Lisans numarasının dijital formu mevcut ise (*e-postada*) girmek için kopyala ve yapıştır yönteminin kullanılması önerilmektedir.

AVG 9.0 kuruldu 819 (4/29/2010)

AVG Lisansınızı etkinleştirin

Kullanıcı adı:

Şirket adı:

Lisans numarası:

Örnek: 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2ALT-XWMX

Yazılımı çevrimiçi satın aldıysanız, lisans numaranız e-posta ile gönderilecektir. Yazım hatalarını önlemek için numaranızı e-postanızdan kopyalarak bu ekrana yapıştırmanızı öneririz.

Yazılımı bir mağazadan satın aldıysanız, lisans numarasını paketin içindeki ürün kayıt kartı üzerinde bulabilirsiniz. Numarayı doğru şekilde kopyalamaya dikkat edin.

< Geri **İleri** > Çıkış

Yükleme işlemine devam etmek için **İleri** düğmesine basın.

Bir önceki asamada standart yüklemeyi seçtiyseniz doğrudan **AVG'yi yükleme** iletişim kutusuna yönlendirileceksiniz. Özel kurulumu seçtiyseniz **Hedef Klasör** iletişim kutusu ile devam edeceksiniz.

4.6. Özel Yükleme - Hedef Klasör

AVG 9.0 Server Edition kuruldu 819 (4/29/2010)

Hedef Klasör

Varsayılan hedef klasör aşağıda gösterilmektedir. Farklı bir klasör seçmek için Göz at düğmesine tıklayabilirsiniz ancak biz varsayılan ayarları kullanmanızı öneririz.

Hedef klasör:

Göz at

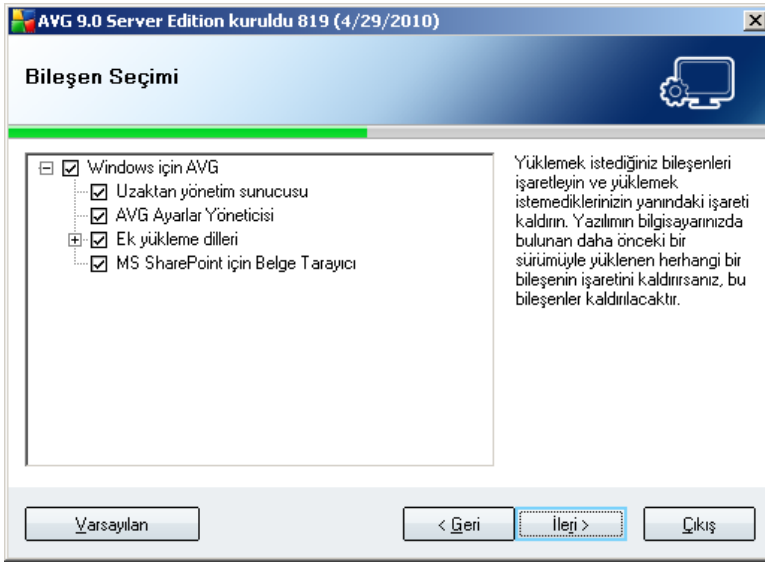
< Geri **İleri** > Çıkış

Hedef Klasör iletişim kutusu, **AVG 9.0 File Server** programının yüklenmesi gereken yeri belirtmenizi sağlar. Varsayılan olarak AVG, C: Sürücüsü üzerinde program dosyaları klasörüne yüklenecektir. Klasör henüz yoksa yeni bir iletişim kutusunda AVG'nin bu klasörü şimdi olusturmasını kabul etmeniz istenecektir.

Bu konumu değiştirmek istiyorsanız, sürücü yapısını görüntülemek ve ilgili klasörü seçmek için **Gözet** düğmesini kullanın.

Onaylamak için **İleri** düğmesini tıklayın.

4.7. Özel Yükleme - Bileşen Seçimi



Bileşen Seçimi iletişim kutusu, yüklenebilir **AVG 9.0 File Server** bileşenlerine genel bir bakış görüntüler. Varsayılan ayarların size uygun olmaması halinde belirli bileşenleri kaldırabilir ya da ekleyebilirsiniz.

• Dil seçimi

Yüklenecek bileşenler listesinde AVG ile birlikte yüklenecek dili (dilleri) seçebilirsiniz. **Ekstra yüklenen diller** öğesini işaretleyin ve sonra ilgili menüden istediğiniz dilleri seçin.

• Uzaktan Yönetim

Bilgisayarınızı AVG Uzaktan Yönetim'e daha sonra bağlamak istiyorsanız, lütfen yüklenecek ilgili öğeyi de işaretleyin.

- **AVG Ayar Yöneticisi**

AVG Ayar Yöneticisi kolayca ve hızlıca yerel AVG yüklemeleri (Uzaktan Yönetim'de çalışmayanları bile) yapılandırmanızı sağlayan küçük bir uygulamadır. Her bilgisayarda AVG uygulaması yüklü olarak AVG Ayar Yöneticisi kullanılarak kolaylıkla oluşturulabilen yapılandırma dosyalarını (.pck biçiminde) kullanır. Sonra bu dosyaları herhangi bir çıkarılabilir cihaza kopyalayabilir ve her bilgisayarda kullanabilirsiniz. Elbette, aynı şey AVG Ayar Yöneticisi'nin kendisi için de geçerlidir. Bu uygulama hakkında daha fazla bilgi için [burayı](#) tıklanın.

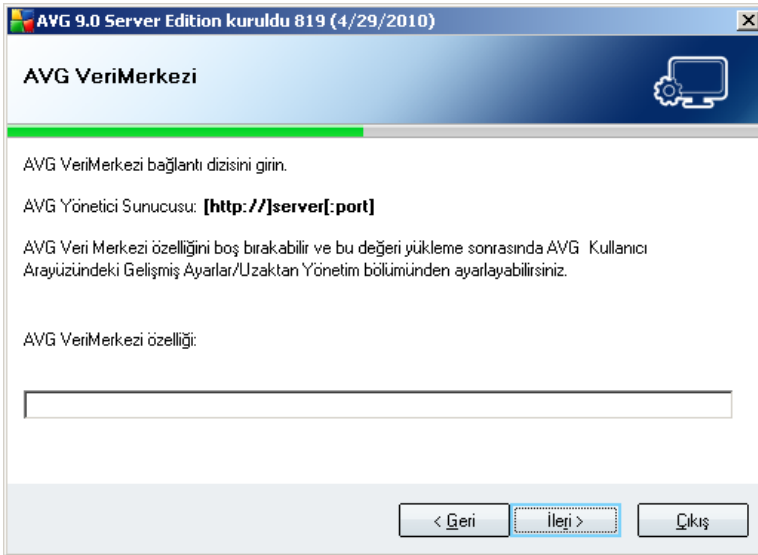
- **MS SharePoint için Belge Tarayıcı**

Bu bileşen MS SharePoint'te saklanan belge dosyalarını tarar ve olası tehlikelere karşı koruma sağlar. Tüm **AVG 9.0 File Server** programlarının önemli bir parçasıdır ve yüklenmesini önemle öneririz.

İleri düğmesine basarak devam edin.

4.8. AVG DataCenter

AVG ag lisansı kullanılıyorsa ve önceki **Özel Yükleme durumunda - Bileşen Seçimi** iletişim kutusunda **Uzaktan yönetim** ögesini yüklenecek olarak işaretlediyseniz, **AVG DataCenter** parametrelerini belirtmeniz gerekir:



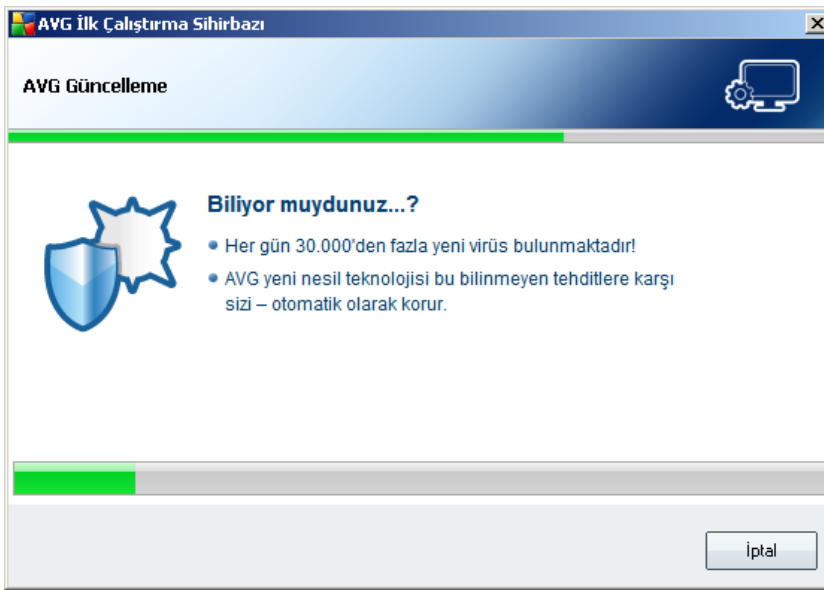
AVG DataCenter belirtimi metin alanına **AVG DataCenter** bağlantı dizisini *sunucu: bağlantı noktası* biçiminde girin. Bu bilgi o anda yoksa, alanı boş bırakın ve

yapılandırmayı [Gelismis Ayarlar / Uzaktan Yönetim](#) iletişim kutusu içinde daha sonra ayarlayabilirsiniz.

Not: AVG Uzaktan yönetim hakkında ayrıntılı bilgiler için, AVG Network Edition kullanıcı kılavuzuna başvurun; AVG web sitesinden (<http://www.avg.com>) indirilebilir.

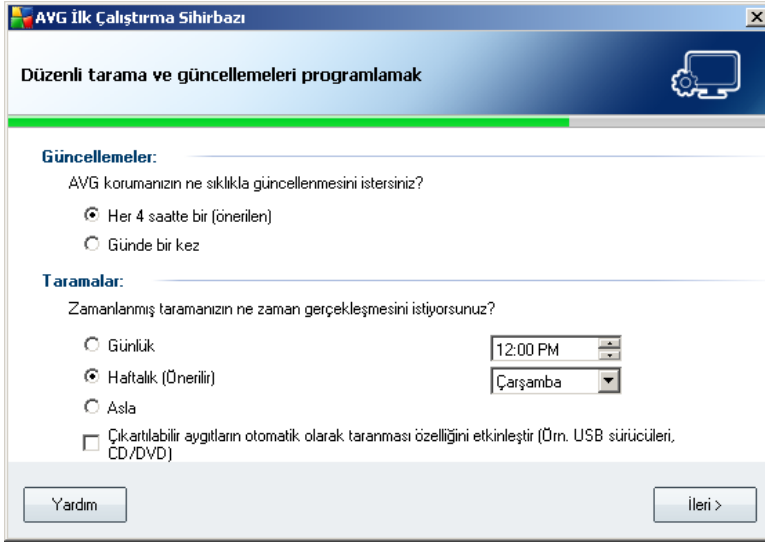
4.9. AVG Yükleniyor

AVG Yükleniyor iletişim kutusunda yükleme işleminin ilerleme durumu görüntülenir ve herhangi bir müdahale gerektirmez:



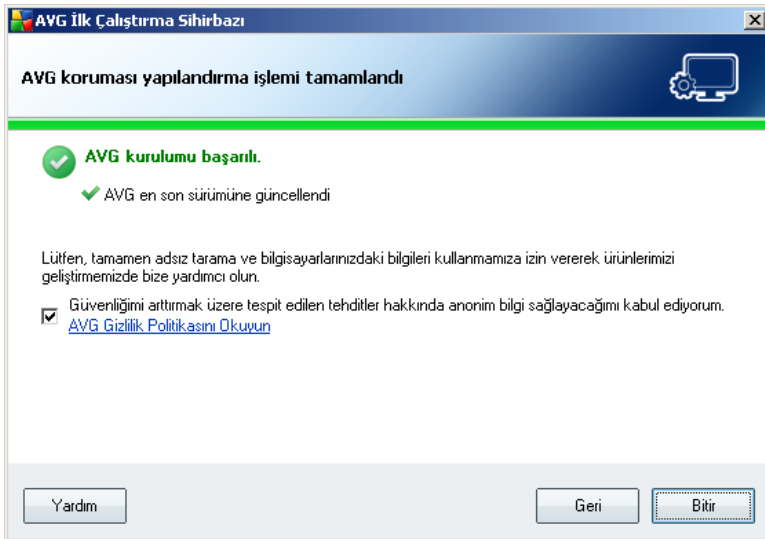
Yükleme işlemi bittiginde, bir sonraki iletişim kutusuna otomatik olarak yönlendirileceksiniz.

4.10. Düzenli tarama ve güncellemeleri programlamak



Düzenli tarama ve güncellemeleri planla iletişim kutusunda yeni güncelleme dosyalarına erişim kontrolleri için zaman aralıkları belirleyebilir ya da [planlanan taramanın](#) saat kaçta baslatılacağını girebilirsiniz. Varsayılan değerleri muhafaza etmeniz önerilir. Devam etmek için **İleri** düğmesini tıklayın.

4.11. AVG koruması yapılandırması tamamlandı





AVG 9.0 File Server ürününüz şimdi yapılandırıldı.

Bu iletişim kutusunda, bilinmeyen açıklardan yararlanma raporunu ve kötü siteleri AVG virüs laboratuvarına bildirme seçeneğini etkinleştirmek isteyip istemediğinize karar verirsiniz. İstiyorsanız, lütfen **Güvenligimi geliştirmek için algılanan tehlikeler hakkında ADSIZ olarak bilgiler sağlamayı kabul ediyorum** seçeneğini işaretleyin.

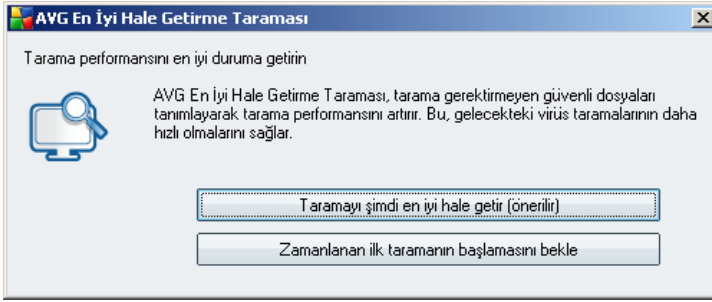
Son olarak, **Son** düğmesine basın.

5. Yüklemeden Sonra

5.1. Taramayı en iyi hale getirme

Taramayı en iyi duruma getirme işlevi, uygun dosyaları algıladığı yerde *Windows* ve *Program dosyaları* klasörlerini arar (*o anda, bunlar *.exe, *.dll ve *.sys dosyalarıdır*) ve bu dosyalardaki bilgileri kaydeder. Bir sonraki erişimde, bu dosyalar bir daha taranmaz ve bu, tarama süresini önemli ölçüde azaltır.

Yükleme işlemi bittiginde taramayı en iyi duruma getirmek için yeni bir iletişim kutusu penceresiyle davet edilirsiniz:



Bu seçeneği kullanmanızı ve ***Taramayı şimdi en iyi duruma getir*** düğmesine basarak taramayı en iyi duruma getirme işlemi çalıştırmanızı öneririz.

5.2. Ürün Kaydı

AVG 9.0 File Server yüklemesini bitirdikten sonra, lütfen ürününüzü AVG web sitesinin (<http://www.avg.com>), **Kayıt** sayfasından kaydedin (*doğrudan sayfada verilen yönergeleri izleyin*). Kayıt işleminin ardından AVG Kullanıcı hesabınıza erişebilecek, AVG Güncelleme bültenini alacak ve sadece kayıtlı kullanıcılara sunulan diğer hizmetlerden yararlanacaksınız.

5.3. Kullanıcı Arayüzü'ne Eris

AVG Kullanıcı Arayüzü'ne çeşitli şekillerde ulaşabilirsiniz:

- sistem tepsisindeki AVG simgesine çift tıklatın
- masaüstünüzdeki AVG simgesine çift tıklatın

- **Baslat/Programlar/AVG 9.0/AVG Kullanici Arayüzü menüsünden**

5.4. Tam bilgisayar taramasi

AVG 9.0 File Server yüklemesinden önce bilgisayarınıza virüs bulasmis olmasi ihtimali bulunmaktadır. Bu nedenle bilgisayarınızda virüs bulunmadigindan emin olmak için **[Tam bilgisayar taramasi](#)** yapmanız gerekmektedir.

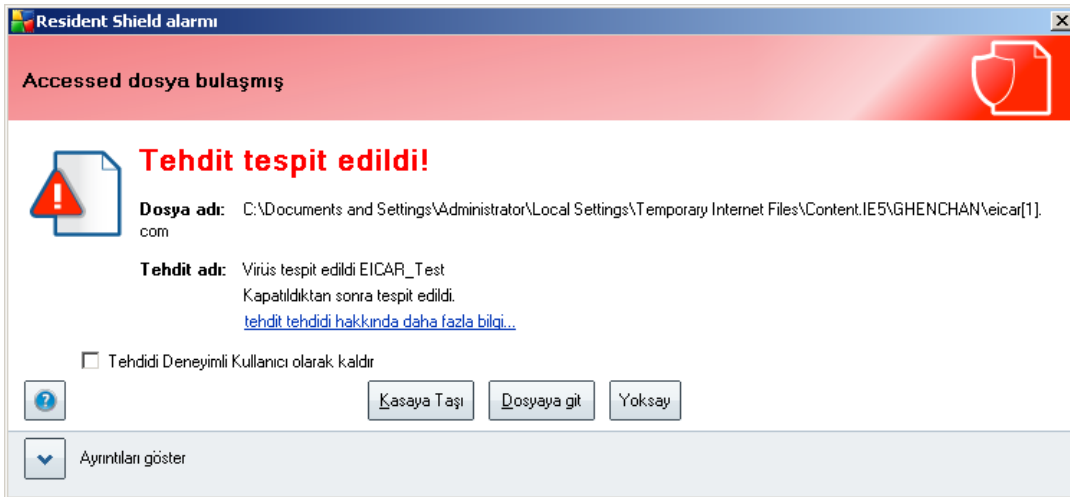
[Tam bilgisayar taramasi](#) konusunda talimatlar için lütfen **[AVG Taramasi](#)** bölümünü inceleyin.

5.5. Eicar Testi

AVG 9.0 File Server programinin düzgün olarak yüklendigini onaylamak için EICAR testini çalıştırabilirsiniz.

EICAR testi, virüsten koruma sistemin çalıştigindan emin olmak üzere kullanılan standart ve kesinlikle güvenli bir yöntemdir. Gerçek bir virüs olmadığı için yayilmasında sakınca yoktur ve herhangi bir virüs kodu içermemektedir. Ürünlerin çoğu sanki bir virüsmüs gibi tepki verir (*ancak "EICAR-AV-Test" adi altında rapor ederler*). EICAR virüsünü www.eicar.com adresinde bulunan EICA'in web sitesinden indirebilir ve bunun yanı sıra EICAR testi hakkında tüm gerekli bilgileri edinebilirsiniz.

eicar.com dosyasini indirmeye çalışın ve sabit diskinize kaydedin. Test dosyasinin indirme islemini onaylar onaylamaz ***Yerlesik Kalkan bir uyarıyla virüse tepki verecektir. Yerlesik Kalkan bildirim, AVG'nin bilgisayarınıza dogru bir sekilde yüklenmiş olduğunu gösterir.***





AVG'nin EICAR test dosyasini virüs olarak algılamaması halinde program yapılandırmasını yeniden kontrol etmeniz gerekir!

5.6. AVG Varsayılan Yapılandırması

AVG 9.0 File Server varsayılan yapılandırması (örn. uygulamanın yüklemesinden sonra doğru şekilde nasıl ayarlanacağı) yazılım satıcısı tarafından ayarlanabilir, böylece optimum performans elde etmek için tüm bileşenler ve işlevler ayarlanabilir.

Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını değiştirmeyin! Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir.

[AVG bileşenlerinde](#) yapılan bazı ufak değişikliklere ilgili bileşenin kullanıcı arayüzünden ulaşabilirsiniz. İhtiyaçlarınızı daha iyi karşılaması açısından AVG yapılandırmasını değiştirme ihtiyacı hissederseniz [AVG Gelişmiş Ayarları](#)'na gidin: sistem menüsü öğesini seçin **Araçlar/Gelişmiş ayarlar** ve AVG yapılandırmasını yeni açılan [AVG Gelişmiş Ayarlar](#) penceresinde düzenleyin.

6. AVG Kullanici Arayüzü

AVG 9.0 File Server, ana pencerede açılır:



Ana pencere çok sayıda bölüme ayrılır:

- **Sistem Menüsü** (penceredeki en üst sistem çubuğu) tüm AVG bileşenlerine, servislerine ve özelliklerine ulaşmanızı sağlayan standart dolanım yöntemidir - [ayrintilar >>](#)
- **Güvenlik Durumu Bilgileri** (pencerenin üst bölümü) AVG programının mevcut durumu hakkında bilgi sunar - [ayrintilar >>](#)
- **Hızlı Bağlantılar** (pencerenin sol bölümü) en önemli ve en sık kullanılan AVG görevlerine hızlı bir şekilde erişebilmenizi sağlar - [ayrintilar >>](#)
- **Bileşenlere Genel Bakış** (pencerenin orta kısmı) yüklü AVG bileşenleri

hakkında genel bilgi verir - [ayrintilar >>](#)

- **Istatistikler** (pencerenin sol alt kısmı) programın çalışmasına ilişkin istatistik verileri görüntüler - [ayrintilar >>](#)
- **Sistem Tepsisi Simgesi** (ekranın sağ alt köşesi, sistem tepsi üzerinde) AVG'nin mevcut durumunu gösterir - [ayrintilar >>](#)

6.1. Sistem Menüsü

Sistem menüsü tüm Windows uygulamalarında kullanılan standart bir dolayım yöntemidir. **AVG 9.0 File Server** ana penceresinin en üstünde yatay olarak konumlandırılmıştır. Belirli AVG bileşenlerine, özelliklerine ve hizmetlerine ulaşmak için sistem menüsünü kullanın.

Sistem menüsü bes ana bölüme ayrılmıştır:

6.1.1. Dosya

- **Çıkış** - **AVG 9.0 File Server**'nin kullanıcı arayüzünü kapatır. Ancak AVG uygulaması arkaplanda çalışmaya devam edecek ve bilgisayarınız korunmaya devam edecektir.

6.1.2. Bileşenler

Sistem menüsünün **Bileşenler** öğesi, yüklenen tüm AVG bileşenlerine ilişkin bağlantılar içerir ve kullanıcı arayüzünde varsayılan iletişim kutularını açar:

- **Sisteme genel bakış** - [Yüklenen bileşenler ve durumlarına ek olarak varsayılan kullanıcı arayüzü iletişim kutusuna geçer](#)
- **Sunucu bileşenleri** - tüm sunucu bileşenlerinin ve durumlarına [genel bakış sunan varsayılan kullanıcı arayüzü iletişim kutusuna geçer](#)
- **Virüsten Koruma** - [Virüsten Koruma](#) bileşeninin varsayılan sayfasını açar
- **Anti-Rootkit**- [Anti-Rootkit](#) bileşeninin varsayılan sayfasını açar
- **Casus Yazılımından Koruma** - [Casus Yazılımından Koruma](#) bileşeninin varsayılan sayfasını açar
- **Uzaktan Yönetim** - **Uzaktan Yönetim** bileşeninin varsayılan sayfasını açar (bu bileşen AVG'nizi AVG Uzaktan Yönetim'e bağlayarak ağ yöneticinizin bazı uygulamaları uzaktan tetiklemesini sağlar). Uzaktan Yönetim bileşeni yalnızca yüklemeyi seçerseniz görünecektir ([Yükleme Süreci](#)'nin [Bileşen Seçimi](#) adımı).

- **SharePoint** - [MS SharePoint için Belge Tarayıcı](#) sunucusu bileseninin varsayılan sayfasını açar
- **Lisans** - [Lisans](#) bileseninin varsayılan sayfasını açar
- **Yerlesik Kalkan** - [Yerlesik Kalkan](#) bileseninin varsayılan sayfasını açar
- **Güncelleme Yöneticisi** - [Güncelleme Yöneticisi](#) bileseninin varsayılan sayfasını açar

6.1.3. Geçmiş

- [Tarama sonuçları](#) - AVG test arayüzüne özellikle [Tarama Sonuçlarına Genel Bakış](#) penceresine gider
- [Yerlesik Kalkan Tespiti](#) - [Yerlesik Kalkan tarafından tespit edilen tehditler hakkında genel bilgi veren bir pencere açar](#)
- [Virüs Kasası](#) - Belirli bir neden doğrultusunda AVG'nin tespit edilmiş temizlenemeyen tüm bulasmaları sildiği karantina alanının arayüzünü açar ([Virüs Kasası](#)) Karantina altında bulunan bulasmis dosyalar, yalıtılmıştır, bilgisayarınızın güvenliği garanti altındadır ve aynı anda bulasmis dosyalar ileride tamir edilebilecekleri göz önünde bulundurularak depolanır.
- [Etkinlik Geçmiş Kayıt Defteri](#) - kaydedilen **AVG 9.0 File Server** eylemlerin tümü hakkında genel bilgi veren bir pencere açar.

6.1.4. Araçlar

- [Bilgisayarı tara](#) - [AVG tarama arayüzüne](#) geçer ve tüm bilgisayar taramasını başlatır
- [Seçilen klasörü tara](#) - [AVG tarama arayüzüne](#) geçer ve bilgisayarınızın dolasımdan ağacından taranmasını istediğiniz dosya ve klasörleri seçmenizi sağlar
- [Dosyayı tara](#) - sabit diskinizin dolasımdan ağacından seçtiğiniz tek bir dosyayı isteye bağlı olarak tarayabilmenizi sağlar
- [Güncelle](#) - otomatik olarak **AVG 9.0 File Server**
- [Dizinden güncelle](#) - sabit diskinizde bulunan belirli bir dosyanın içinde yer alan güncelleme dosyalarını alarak güncelleme işlemini gerçekleştirir. Diğer bir yandan bu seçim sadece acil durumlarda önerilmektedir. Örn. İnternet bağlantısı olmadığı durumlarda (*Örneğin bilgisayarınıza virüs bulasmis ise ve İnternet bağlantınız kesildiyse; bilgisayarınız bir ağa bağlıysa fakat İnternet erişimi yok ise vb.*).

Yeni açılan pencereden, daha önce güncelleme dosyasını depoladığınız klasörü seçin ve güncelleme işlemini başlatın.

- **Gelismis ayarlar** - _yapilandirmasını düzenleyebileceğiniz **AVG 9.0 File ServerAVG gelişmiş ayarlar** iletişim kutusunu açar. Genel olarak uygulamanın yazılım üreticisi tarafından tanımlanan varsayılan ayarlarının muhafaza edilmesi önerilir.

6.1.5. Yardım

- **İçindekiler** - AVG yardım dosyalarını açar
- **Çevrimiçi Yardım Alın** - Müsteri destek merkezi sayfasında AVG web sitesini (<http://www.avg.com>) açar
- **AVG Web** - AVG web sitesini (<http://www.avg.com>) açar
- **Virüsler ve Tehlikeler Hakkında** - tanımlanan virüs hakkında ayrıntılı bilgi edinebildiğiniz çevrimiçi **Virüs Ansiklopedisini** açar
- **AVG Kaynak CD'sini indir** - İnternet tarayıcınızda AVG web sitesi, **Destek merkezi/İndir** sayfasını açar. AVG Rescue CD'nin en son sürümünü indirmek için sağlanan metin alanına lisans numaranızı girin (*AVG tasınabilir sürümü, önemli bir virüs bulması gibi sistemin düzgün şekilde yüklenmemesi gibi bir durumda işletim sistemi kurtarma içindir*).
- **Yeniden Etkinleştir** - **Yükleme işleminin AVG'yi Kisiselleştir** iletişim kutusuna girilen verilerle **AVG'yi Etkinleştir** iletişim kutusunu açar. Bu iletişim kutusunda satış numaranızı (*AVG'yi yüklerken kullandığınız numara*), ya da eski lisans numaranızı (*Örn. yeni bir AVG ürününe geçerken*) değiştirmek için lisans numaranızı girebilirsiniz.
- **Şimdi kaydolun** - AVG web sitesi (<http://www.avg.com>) kayıt sayfasına bağlanır. Lütfen kayıt bilgilerinizi doldurun; sadece AVG ürünlerini kaydettiren müşterilerimiz ücretsiz teknik destek alabilecektir.
- **AVG Hakkında** - **AVG Technologies CZ**'nin iletişim bilgileri, lisans sözleşmesi, sistem bilgileri, program ve virüs veritabanı versiyonu ve program adı hakkında bilgi veren bes sekmeli **Bilgi** iletişim kutusunu açar.

6.2. Güvenlik Durumu Bilgisi

Güvenlik Durumu Bilgisi bölümü, AVG'nin ana penceresinin üst kısmında bulunmaktadır. Bu bölümde **AVG 9.0 File Server** programınızın mevcut güvenlik durumu hakkında her zaman bilgi bulabilirsiniz. Lütfen bu bölümde betimlenmesi muhtemel simgeleri ve anlamlarını inceleyin:



Yesil simge AVG'nizin tamamen fonksiyonel olduğunu gösterir. Bilgisayarınız tamamen korunur, günceldir ve yüklü tüm bileşenler doğru çalışmaktadır.



Turuncu simge, bir ya da daha fazla bileşenin yanlış yapılandırıldığını ve söz konusu bileşenlerin özelliklerine/ayarlarına dikkat etmeniz gerektiğini gösterir. AVG'de herhangi bir kritik sorun yoktur ve muhtemelen bir nedenden dolayı bileşenlerden bazılarını geçici olarak kapatmayı seçmiş olabilirsiniz. Ancak AVG tarafından korunmaya devam edersiniz. Diğer bir yandan lütfen bileşenin ayarlarını inceleyin! Adı **Güvenlik Durumu Bilgisi** kısmında sağlanır.

Bu simge, herhangi bir nedenle [bir bileşenin hata durumunu göz ardı etmeyi seçtiyseniz](#) de görüntülenecektir ("*Bileşen durumunu göz ardı et*" seçeneğine, AVG ana penceresinin bileşenlere genel bakış kısmında bulunan ilgili simgeyi sağ tıklayarak açtığınız bağlam menüsünden ulaşabilirsiniz). Özel durumlar için bu seçeneği kullanmanız gerekebilir ancak en kısa zamanda **Bileşen durumunu gözardı et** seçeneğini devre dışı bırakmanız önerilir.



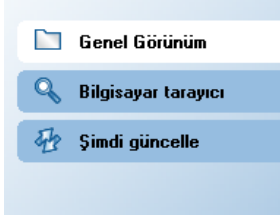
Kırmızı simge, AVG'nin kritik durumda olduğunu gösterir! Bir ya da daha fazla bileşen doğru çalışmıyor ve AVG bilgisayarınızı koruyamıyor anlamına gelir. Lütfen rapor edilen sorunu çözmek için gerekli ilgiyi gösterin. Hatayı kendi basinize çözemezseniz [AVG teknik destek](#) ekibi ile iletişim kurun.

Güvenlik Durumu Bilgisi fonksiyonuna gereken özeni göstermeniz ve herhangi bir sorunun rapor edilmesi halinde anında sorunu çözmeye çalışmanız önerilmektedir. Aksi takdirde bilgisayarınız risk altında olacaktır!

Not: AVG durum bilgilerine [sistem tepsi simgesinden](#) de ulaşabilirsiniz.

6.3. Hizli Baglantilar

Hizli Baglantilar ([AVG Kullanici Arayüzü'nün sol kisminda](#)) en sik kullanılan ve en önemli AVG özelliklerine hemen erisebilmenizi saglar:



- **Genel Bakis** - açık durumdaki herhangi bir AVG arayüzünden yüklü bileşenlerin tümünün görüntülediği varsayılan genel bakis penceresine gitmek için bu bağlantıyı kullanın - bkz. bölüm [Bileşenlere Genel Bakis >>](#)
- **Bilgisayar tarayıcısı** - taramaları doğrudan başlatılabildiğiniz, tarama programlayabildiğiniz ya da parametreleri değiştirebildiğiniz AVG tarama arayüzünü açmak için bu bağlantıyı tıklayın - bkz. bölüm [AVG Taramaları >>](#)
- **Şimdi güncelle** -bu bağlantı güncelleme arayüzünü açacak ve AVG güncelleme işlemini başlatacaktır - bkz. bölüm [AVG Güncellemeleri >>](#)
- **Sunucu bileşenleri** - bu bağlantıyı geçerli olarak açık AVG arayüzünden sunucu bileşenlerinin genel görünümünü içeren varsayılan geçmek için kullanın - [Sunucu bileşenleri >>](#)

Bu bağlantılara kullanıcı arayüzünden istediğiniz zaman ulaşabilirsiniz. Belirli bir işlemi başlatmak üzere hızlı bağlantılardan birini kullandığınızda GUI yeni bir iletişim kutusunda açılacaktır fakat söz konusu pencereden de hızlı bağlantılara ulaşabilirsiniz.

6.4. Bileşen Genel Görünümü

Bileşenlere Genel Bakış bölümü [AVG Kullanıcı Arayüzü](#)'nün orta kısmında yer alır. Bölüm ikiye ayrılır:

- Yanlarında bileşenin simgesinin ve aktif ya da pasif olduğuna dair durum bilgisinin bulunduğu yüklü tüm bileşenlere genel bakış
- Seçilen bileşen hakkında açıklamalar

AVG 9.0 File Server içinde, **Bileşen Genel Görünümü** kısmi aşağıdaki bileşenler hakkında bilgiler içerir:

- **Virüsten Koruma** , bilgisayarınızı bilgisayarınıza girmeye çalışan virüslerden korur - [ayrıntılar >>](#)
- **Casus Yazılımından Koruma** siz çalıştırdıkça uygulamalarınızı arkaplanda tarar - [ayrıntılar >>](#)
- **Uzaktan Yönetim** - AVG'nizi AVG Uzaktan Yönetim'e bağlayarak ağ yöneticinizin bazı uygulama eylemlerini uzaktan tetiklemesine izin verir. Uzaktan Yönetim bileşeni yalnızca yüklemeyi seçerseniz görünecektir ([Yükleme Süreci](#) 'nin [Bileşen Seçimi](#) adımı).
- **Anti-Rootkit** kötü amaçlı yazılımları gizlemeye çalışan program ve teknolojileri tespit eder - [ayrıntılar >>](#)
- **Lisans**, AVG Lisans Sözleşmesinin tümünü sunar - [ayrıntılar >>](#)
- **Yerlesik Kalkan** arkaplanda çalışır ve dosyalar kopyalanır, açılır ve kaydedilirken söz konusu dosyaları tarar - [ayrıntılar >>](#)

- **Güncelleme Yöneticisi** tüm AVG güncellemelerini kontrol eder - [ayrintilar >>](#)

Bilesenlere genel bakis ekraninda bileseni seçmek için üzerine bir defa tiklatin. Aynı anda kullanıcı arayüzünün alt kısmında bilesenin temel fonksiyonları hakkında açıklamalar görüntülenir. Bilesenin kendi arayüzünü açmak ve temel istatistik verileri görüntülemek için simgeye çift tiklatin.

Bir bağlam menüsü açmak için bilesenin simgesi üzerine sağ tiklatin: bilesenin grafik arayüzünü açmanın yanı sıra **Bilesenin durumunu göz ardı et** seçimini de yapabilirsiniz. [Bilesenin hata durumunun](#) bilincinde olduğunuzu göstermek için bu seçeneği seçin, ancak belirli bir neden doğrultusunda AVG'nizin bu şekilde çalışmasını istiyorsanız [sistem tepsisi simgesi](#) değişikliği ile uyarılmayacaksınız.

6.5. Sunucu bileşenleri



AVG File Server Edition
Dosya Bileşenler Geçmiş Araçlar Yardım

AVG Anti-Virus

Koruma altındasınız.
Tüm güvenlik özellikleri düzgün şekilde çalışıyor ve güncel.

Güvenlik bileşenleri ve duruma genel bakış

Sharepoint
Etkin

İstatistikler
Son tarama: 6/20/10, 2:40 PM
Son güncelleme: 6/20/10, 2:35 PM
Virüs veritabanı: 271.1.1/2951
AVG sürümü: 9.0.819
Lisans sona erme tarihi: 12/31/2012

Seçilen bileşenin tanımı
MS SharePoint için Belge Tarayıcı MS Sharepoint'de saklanan belge dosyalarını tarar ve olası tehditlere karşı koruma sağlar.
Bileşen etkin

[Bildirim göster](#)

Sunucu Bileşenleri bölümü [AVG Kullanıcı Arayüzü](#)'nün orta kısmında yer alır. Bölüm ikiye

ayrılır:

- Yanlarında bileşenin simgesinin ve aktif ya da pasif olduğuna dair durum bilgisinin bulunduğu yüklü tüm bileşenlere genel bakış
- Seçilen bileşen hakkında açıklamalar

AVG 9.0 File Server içinde, **Sunucu bileşenleri** kısmı aşağıdaki bileşenler hakkında bilgiler içerir:

- **MS SharePoint için Belge Tarayıcı**, MS SharePoint'te depolanan belge dosyalarını tarar ve olası tehlikelere karşı korur - [ayrıntılar >>](#)

Bileşenlere genel bakış ekranında bileşeni seçmek için üzerine bir defa tıklayın. Aynı anda kullanıcı arayüzünün alt kısmında bileşenin temel fonksiyonları hakkında açıklamalar görüntülenir. Bileşenin kendi arayüzünü açmak ve temel istatistik verileri görüntülemek için simgeye çift tıklayın.

Bir bağlam menüsü açmak için bileşenin simgesi üzerine sağ tıklayın: bileşenin grafik arayüzünü açmanın yanı sıra **Bileşenin durumunu göz ardı et** seçimini de yapabilirsiniz. [Bileşenin hata durumunun](#) bilincinde olduğunuzu göstermek için bu seçeneği seçin, ancak belirli bir neden doğrultusunda AVG'nizin bu şekilde çalışmasını istiyorsanız [sistem tepsisi simgesi](#) değişikliği ile uyarılmayacaksınız.


6.6. İstatistikler


İstatistikler bölümü [AVG Kullanıcı Arayüzü](#)'nün sol alt kısmında yer alır. Programın çalışması hakkında bir dizi bilgi içerir:

- **Son tarama** - son taramanın yapıldığı tarihi gösterir
- **Son güncelleme** - son güncellemenin yapıldığı tarihi gösterir
- **Virüs VT** - mevcut virüs tabanı sürümü hakkında bilgi verir
- **AVG sürümü** - yüklü AVG sürümü hakkında bilgi verir (*numara 9.0.xx formatındadır ve burada 9.0 ürün sürümü iken xx üretim numarasını gösterir*)
- **Lisansin son kullanılma tarihi** - AVG lisansinizin son kullanılma tarihini gösterir

6.7. Sistem Tepsisi Sembolü

Sistem Tepsisi Sembolü (Windows araç çubukunda), **AVG 9.0 File Server** programinizin geçerli durumunu gösterir. AVG ana penceresinin açık ya da kapalı olduğu önemli olmaksızın devamlı olarak sistem tepsiniz üzerinde bulunur.

Tamamen renkli ise  **Sistem Tepsisi Sembolü**, tüm AVG bileşenlerinin aktif ve tamamen fonksiyonel olduğunu gösterir. Buna ek olarak AVG hata durumundayken de AVG sistem tepsi sembolü tamamen renkli görüntülenebilir, ancak bu, durumun tamamen farkındasınız ve bilerek **Bileşen durumunu gözardı et** seçimini yapmışınız demektir.

Ünlem işareti içeren bir simge  bir sorun olduğunu gösterir (*etkin olmayan bileşen, hata durumu vb.*). Ana pencereyi açmak ve bileşeni düzenlemek için **Sistem Tepsisi Sembolünü** çift tıklayın.

Sistem tepsi simgesi, sizi AVG sistem tepsi simgesi üzerinden açılan bir pencere vasıtasıyla AVG eylemleri ve muhtemel durum değişiklikleri hakkında bilgilendirir (*örn. programlanan tarama ya da güncellemenin otomatik olarak baslatılması, bir bileşenin durum değişikliği, hata durumu oluşumu...*):



Sistem Tepsisi Sembolü AVG ana penceresine istediğiniz zaman ulaşabilmeniz için hızlı bir bağlantı olarak da kullanılabilir - sadece simgeyi iki defa tıklayın. **Sistem Tepsisi Sembolü** sağ tıklayarak aşağıdaki seçenekleri sunan kısa bir bağlam menüsü açarsınız:

- **AVG Kullanıcı Arayüzünü Aç** - [AVG Kullanıcı Arayüzünü açmak için tıklayın](#)
- **Taramalar** - [önceden tanımlanan taramalar](#) bağlam menüsünü açmak için tıklayın ([Tüm Bilgisayarı Tara](#), [Belirli Dosyaları veya Klasörleri Tara](#), [Anti-Rootkit tarama](#)) ve gereken taramayı seçin, hemen başlayacaktır
- **Şimdi Güncelle** - anında [güncelleme işlemini başlatır](#)
- **Yardım** - başlangıç sayfasında yardım dosyasını açar



7. AVG Bileşenleri

7.1. Virüsten Koruma

7.1.1. Virüsten Koruma İlkeleri

Virüsten koruma yazılımlarının tarama motorları bilinen tüm virüslere karşı tüm dosya ve dosya eylemlerini (dosyaların açılması/kapatılması vb.) tarar. Tespit edilen virüsler, harekete geçmeden engellenecek ve ardından silinecek ya da karantinaya alınacaktır. Virüsten koruma yazılımlarının çoğu bulgusal taramayı kullanır; diğer bir deyişle, dosyalar virüs imzası olarak adlandırılan tipik virüs özelliklerine karşı taranır. Bu, yeni bir virüs mevcut virüslerin tipik özelliklerinden bazılarında sahipse söz konusu virüsten koruma tarayıcısının yeni ve bilinmeyen bir virüsü tespit edebileceği anlamına gelmektedir.

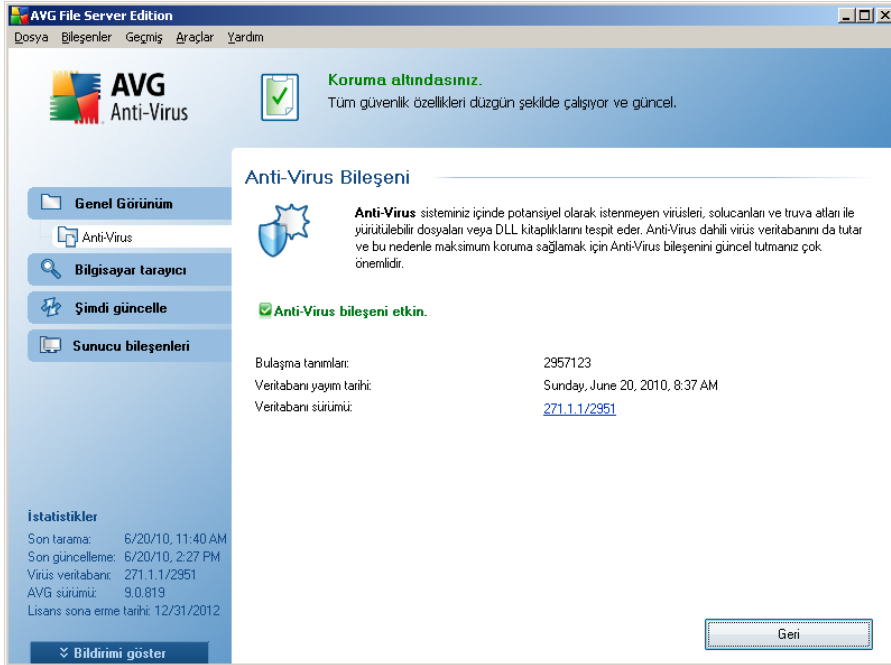
Virüsten koruma korumasının en önemli özelliği, bilgisayarınıza hiçbir virüsün bulasmamasının sağlanmasıdır!

Tek bir teknoloji bir virüsün tespit edilmesinde ya da tanımlanmasında yetersiz kalabileceken ***Virüsten Koruma***, bilgisayarınızın virüslerden korunduğundan emin olmak adına çok sayıda teknolojiyi bir araya getirmektedir:

- Tarama - belirli bir virüsün özelliklerine sahip karakter dizeleri aranır
- Bulgusal analiz - sanal bir bilgisayar ortamında taranan nesnenin 'komutları' dinamik bir şekilde canlandırılır
- Jenerik tespit - belirli bir virüs ya da virüs grubunun komut özelliklerinin tespitidir

AVG bunun yanı sıra sistemde potansiyel anlamda istenmeyen çalıştırılabilir uygulamaları ya da DLL kütüphanelerini de inceleyebilmekte ve tespit edebilmektedir. Söz konusu tehlikeleri Potansiyel Olarak İstenmeyen Programlar (farklı casus yazılım, reklam yazılım türleri vb) olarak adlandırıyoruz. Buna ek olarak AVG, sistem kayıt defterinizi süpheli girdilere, geçici İnternet Dosyalarına ve izleme tanımlama bilgilerine karşı da tarar ve söz konusu potansiyel olarak istenmeyen nesnelere de diğer bulasmalarla aynı şekilde çözebilmenize olanak tanır.

7.1.2. Virüsten Koruma Arayüzü



Anti-Virus bileşeninin arayüzünde bileşenin fonksiyonlarına, bileşenin mevcut durumu hakkında bilgiye (*Anti-Virus bileşeni aktiftir.*) ve **Anti-Virus** istatistikleri hakkında kısa bilgilere ulaşabilirsiniz.

- **Bulasma tanımları** - Sayı, virüs veritabanının güncel sürümünde tanımlanan virüs sayısını gösterir.
- **En son veritabanı güncelleme** - virüs veritabanının en son güncellendiği tarih ve saati gösterir.
- **Veritabanı sürümü**- en son virüs veritabanı sürümünün numarasını tanımlar ve bu numara virüs veritabanı her güncellendiğinde artar

Bu bileşenin arayüzü kapsamında sadece bir adet çalıştırma düğmesi bulunur (**Geri**) - Varsayılan [AVG Kullanıcı Arayüzüne](#) dönmek için bu düğmeye basın (bileşenlere genel bakış).

Lütfen dikkat: Yazılım satıcısı, en iyi performansın sunulabilmesi için tüm AVG bileşenlerini kurmalıdır. Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını değiştirmeyin. Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir. AVG yapılandırmasını değiştirmeniz gerekiyorsa sistem



menüsünden ilgili öğeyi seçin **Araçlar/Gelismis ayarlar** ve yeni açılan [AVG Gelismis Ayarlar](#) iletişim kutusunda AVG yapılandırmasını düzenleyin.

7.2. Casus Yazilimdan Koruma

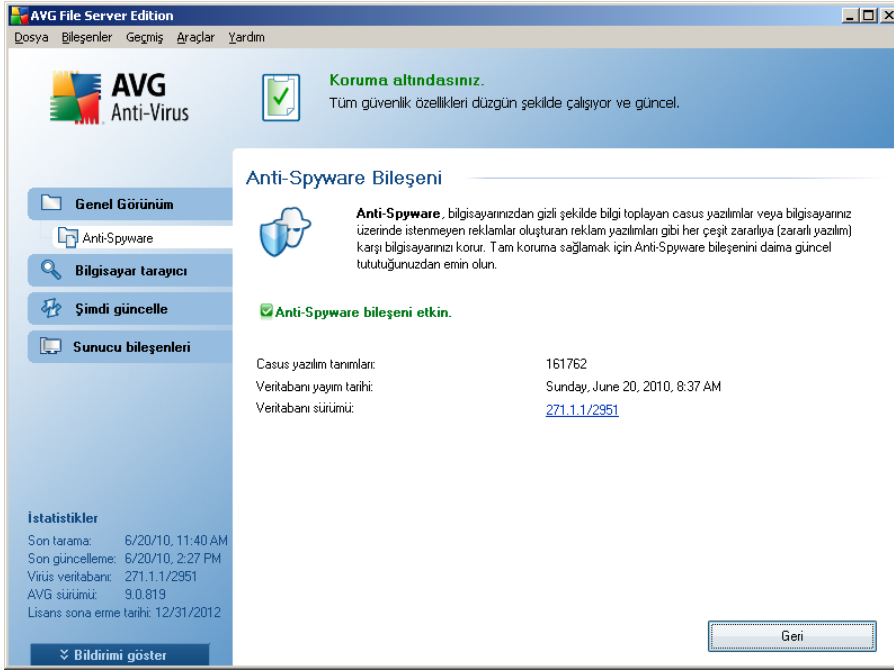
7.2.1. Casus Yazilimdan Koruma Prensipleri

Casus yazılımlar, genellikle kullanıcının bilgisi ya da izni olmaksizin kullanıcının bilgisayarından bilgi toplayan kötü amaçlı bir yazılım türü olarak tanımlanırlar. Bazı casus yazılım uygulamaları genellikle belirli bir amaç doğrultusunda kurulur ve sıklıkla reklam, açılan pencereler veya farklı istenmeyen yazılım türleri içerirler.

Su anda bilinen en yaygın bulaşma kaynağı, potansiyel anlamda tehlikeli öğeler içeren web siteleridir. E-posta ya da solucan ve virüsler yoluyla aktarım gibi diğer bulaşma yöntemleri de oldukça etkilidir. En önemli korunma, yerleşik bir kalkan olarak çalışan ve siz çalıştığınız zaman arka planda uygulamalarını tarayan **Casus Yazilimdan Koruma** gibi devamlı olarak arka planda çalışan bir tarayıcı kullanmaktır.

Kötü amaçlı yazılımın bilgisayarınıza AVG yüklenmesinden önce bulaşmış olması ya da **AVG 9.0 File Server programınızı en güncel veritabanı ve program güncellemeleriyle güncel tutmayı ihmal etmeniz gibi potansiyel riskler de bulunmaktadır.** Bu nedenle AVG, tarama özelliğini kullanarak tüm bilgisayarınızı kötü amaçlı ve casus yazılımlara karşı tarayabilmenize olanak tanır. Ayrıca, uykuda olan ve etkin olmayan kötü amaçlı yazılımları da (örneğin bilgisayara indirilmiş ancak henüz etkinleştirilmemiş) tespit eder.

7.2.2. Casus Yazılımdan Koruma Arayüzü



Anti-Spyware bileşeninin arayüzünde bileşenin fonksiyonlarına, bileşenin mevcut durumu hakkında bilgiye (*Anti-Spyware bileşeni aktiftir.*) ve bazı **Anti-Spyware** istatistiklerine ulaşabilirsiniz:

- **Casus yazılım tanımları** - Sayı, en güncel casus yazılım veri tabanı sürümünde tanımlanan casus yazılım örneği sayısını gösterir.
- **En son veritabanı güncelleme** - casus yazılım veritabanının en son güncellendiği tarih ve saati gösterir.
- **Veritabanı sürümü**- en son casus yazılım veritabanı sürümünün numarasını tanımlar ve bu numara virüs veritabanı her güncellendiğinde artar

Bu bileşenin arayüzü kapsamında sadece bir adet çalıştırma düğmesi bulunur (**Geri**) - Varsayılan [AVG Kullanıcı Arayüzüne](#) dönmek için bu düğmeye basın (bileşenlere genel bakış).

Lütfen dikkat: Yazılım satıcısı, en iyi performansın sunulabilmesi için tüm AVG bileşenlerini kurmuştur. Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını değiştirmeyin. Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir. AVG yapılandırmasını değiştirmeniz gerekiyorsa sistem



menüsünden ilgili öğeyi seçin **Araçlar/Gelismis ayarlar** ve yeni açılan [AVG Gelismis Ayarlar](#) iletişim kutusunda AVG yapilandirmasini düzenleyin.

7.3. Anti-Rootkit

Rootkit, sistem yöneticisinin izni olmaksizin yasal olmayan şekillerde bilgisayar sisteminin kontrolünü ele almak için tasarlanmış bir programdır. Rootkit, donanım üzerinde çalışan işletim sisteminin kontrolünü ele geçirmeyi hedeflediği için donanımsal açıdan erişime gerek duymaz. Genellikle rootkit'ler, standart işletim sistemi güvenlik mekanizmalarını dönüştürerek ya da istila ederek sistem üzerindeki varlıklarını gizlerler. Sıklıkla Truva Ati biçimindedirler, dolayısıyla kullanıcıları sistemleri üzerinden çalışacak kadar güvenli olduklarına inandırır. İzleme programlarının çalışan işlemlerini gizlemek ya da işletim sisteminin sistem bilgilerini ya da dosyalarını saklamak, bunu sağlamak için kullanılan teknikler arasında bulunmaktadır.

7.3.1. Anti-Rootkit Prensipleri

AVG Rootkit Önleme tehlikeli rootkit'ler, diğer bir deyişle bilgisayarınızdaki tehlikeli yazılımları gizleyen program ve teknolojileri etkili bir biçimde tespit edip silen özel bir araçtır. **AVG Rootkit Önleme** öntanımlı kurallar setine göre rootkit'leri algılayabilir. Lütfen tüm rootkit'lerin tespit edildiğini (*sadece bulasanlar değil*) unutmayın. **AVG Rootkit Önleme** bir rootkit bulduğunda, bu rootkit'te mutlaka virüs olduğu anlamına gelmez. Bazen kök dizinleri sürücülerde kullanılır ya da doğru uygulamaların bir parçası olabilir.

7.3.2. Anti-Rootkit Arayüzü



Anti-Rootkit kullanıcı arayüzünde bileşenlerin fonksiyonlarına ait kısa tanımlamalar bulunur, bileşenin mevcut durumu hakkında bilgi verir (*Anti-Rootkit bileşeni aktiftir*) ve bunun yanı sıra **Anti-Rootkit** testinin en son çalıştırıldığı tarih hakkında bilgi görüntüler.

İletişim penceresinin alt kısmında kök kullanıcı taraması sırasında kullanılan fonksiyonlardan bazılarını düzenleyebileceğiniz **Anti-Rootkit ayarlarını** bulabilirsiniz. İlk olarak taranmasını istediğiniz nesnelere belirlemek üzere ilgili kutuları işaretleyin:

- **Uygulamaları tara**
- **DLL kitaplıklarını tara**
- **Sürücülerini tara**

Bunun ardından kök kullanıcı tarama modunu da seçebilirsiniz:

- **Hızlı kök kullanıcı takimi (rootkit) tarama** : yalnızca sistem klasörünü tarar (tipik olarak c:\Windows)
- **Tam kök kullanıcı takimi (rootkit) tarama**: A: ve B: disindeki tüm erişilebilir disk sürücülerini tarar

Mevcut kontrol düğmeleri şunlardır:

- **Kök kullanıcıları tara** - kök kullanıcı tarama işleminin [tüm bilgisayarın taranması](#) prosedürünün baslıca parçalarından biri olmaması nedeniyle kök kullanıcı taramasını doğrudan **Anti-Rootkit** arayüzü üzerinden başlatabilirsiniz.
- **Değişiklikleri kaydet** - bu arayüzde yapılan tüm değişiklikleri kaydetmek ve öntanımlı [AVG kullanıcı arayüzüne](#) dönmek için (bileşenlere genel bakış) bu düğmeye basın.
- **İptal** - yapılan değişiklikleri kaydetmeksizin [AVG kullanıcı arayüzüne](#) (bileşenlere genel bakış) dönmek için bu düğmeye basın.

7.4. Lisans



AVG File Server Edition

Dosya Bileşenler Geçmiş Araçlar Yardım

AVG Anti-Virus

Koruma altındasınız.
Tüm güvenlik özellikleri düzgün şekilde çalışıyor ve güncel.

Lisans Bileşeni

Lisans Bileşeni mevcut lisans durumunuzu yönetir. Lisans numaranız sahip olduğunuz AVG sürümünü belirler. Lütfen lisansınızı doğru şekilde girdiğinizden ve etkinleştirdiğinizden emin olun, aksi halde yazılımınız gerektiği gibi güncellenmeyecektir ve size teknik destek hizmeti sunamayız.

Lisans bileşeni etkin. yüklenen ürün AVG File Server Edition.

Lisans numarası:	9FS-N7AN7-23PAY-S899R-NTVS6-JPU7J
Lisans türü:	Tem
Lisansın sona erdiği tarih:	Monday, December 31, 2012
Konum sayısı:	1

Lisans işlemleri

İstatistikler

Son tarama: 6/20/10, 11:40 AM
Son güncelleme: 6/20/10, 2:27 PM
Virüs veritabanı: 271.1.1/2951
AVG sürümü: 9.0.819
Lisans sona erme tarihi: 12/31/2012

Lisans bileşeninin iletişim kutusunda bileşenlerin fonksiyonlarını, mevcut durumu hakkında bilgiyi (*Istenmeyen Posta Önleme bileşeni aktiftir.*), ve aşağıdaki bilgileri bulabilirsiniz:

- **Lisans numarası** - lisans numaranızın mevcut durumunu gösterir. Lisans numaranızı girerken çok dikkatli olmalı ve gösterildiği gibi girmelisiniz. Bu yüzden, lisans numarasıyla ilgili bir düzeltme için her zaman "kopyala ve yapıştır"

yöntemini kullanmanizi önemle öneririz.

- **Lisans türü** - Yüklene ürün türünü belirtir.
- **Lisans sonu** -bu tarih, lisans numaranizin geçerlilik süresini belirler. Bu tarihten sonra **AVG 9.0 File Server** programini kullanmaya devam etmek istiyorsanız lisansinizi yenilemeniz gerekir. [Lisans yenileme](http://www.avg.com) AVG web sitesinden (<http://www.avg.com>) çevrimiçi gerçekleştirilebilir.
- **Kullanıcı sayısı** - **AVG 9.0 File Server** programinizi yükleme hakkınız olan çalışma istasyonu sayisidir.

Kontrol düğmeleri

- **Kaydol** - AVG web sitesi (<http://www.avg.com>) kayıt sayfasina baglanır. Lütfen kayıt bilgilerinizi doldurun; sadece AVG ürünlerini kaydettiren müsterilerimiz ücretsiz teknik destek alabilecektir.
- **Yeniden Etkinleştir** - **yükleme işleminin** AVG'yi Kisiselleştir [iletisim kutusuna girilen verilerle](#) AVG'yi Etkinleştir [iletisim kutusunu açar](#). Bu iletisim kutusunda satis numaranizi (*AVG'yi yüklerken kullandiginiz numara*), ya da eski lisans numaranizi (*Örn. yeni bir AVG ürününe geçerken*) degistirmek için lisans numaranizi girebilirsiniz.
- **Geri** - Varsayılan [AVG kullanıcı arayüzüne](#) dönmek için bu düğmeye basın (bilesenlere genel bakış).

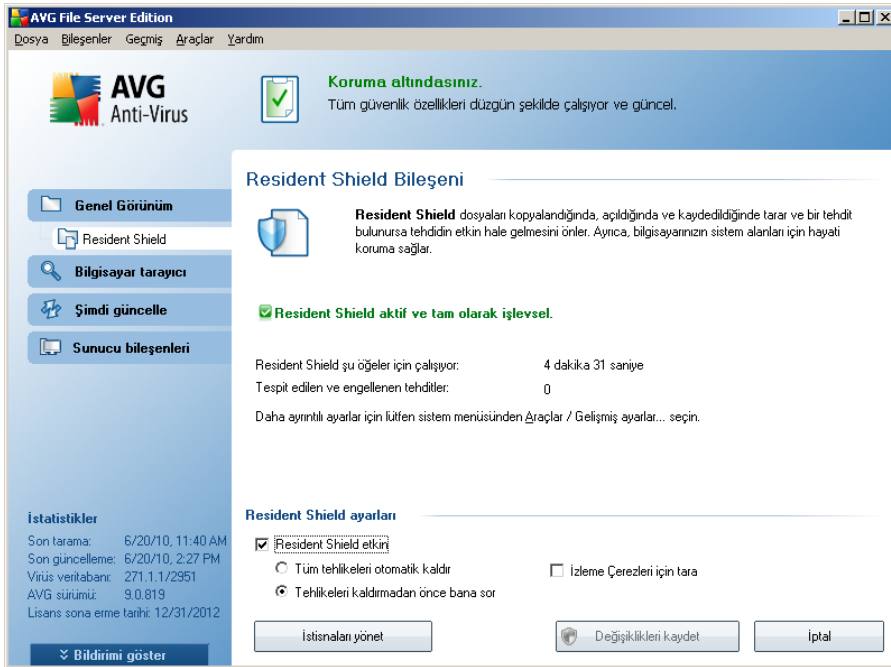
7.5. Yerlesik Kalkan

7.5.1. Yerlesik Kalkan İlkeleri

Yerlesik Kalkan bileşeni, bilgisayarınızın sürekli olarak korunmasını sağlar. Açılan, kaydedilen veya kopyalanan her dosyayı tarar ve bilgisayarın sistem alanlarını korur. **Yerlesik Kalkan** erişilen bir dosyada virüs tespit ederse geçerli işlemi durdurur ve virüsün kendisini etkinleştirmesine izin vermez. Normal olarak, "arka planda" çalıştığından işlemi fark etmezsiniz ve yalnızca tehdit bulunması durumunda bilgilendirilirsiniz; aynı anda, **Yerlesik Kalkan** tehdidin etkinleştirilmesini engeller ve tehdidi kaldırır. **Yerlesik Kalkan** sistemin başlatılması sırasında bilgisayarınızın belleğine yüklenir.

Uyarı: Yerlesik Kalkan, başlatma sırasında bilgisayarınızın belleğine yüklenir ve bu özelliği her zaman açık durumda tutmanız önemlidir!

7.5.2. Yerlesik Kalkan Arayüzü



En önemli istatistik verilerin ve bileşenin mevcut durumu hakkındaki bilgilerin yanı sıra (*Yerlesik Kalkan aktiftir ve tamamen fonksiyoneldir*) **Yerlesik Kalkan** arayüzü, bileşenin ayarlarına dair bazı seçenekler de sunar. İstatistikler aşağıdaki gibidir:

- **Yerlesik Kalkan** 'den beri etkin - bileşenin en son çalıştırıldığı tarihten itibaren geçen zamani gösterir
- **Tespit edilen ve engellenen tehlikeler** - çalıştırılması/açılması engellenen tespit edilen bulasma sayısı (*ihtiyaç duyulursa bu değer sıfırlanabilir; Örn. istatistik amaçlar doğrultusunda - Değeri sıfırla*)

Temel bileşen yapılandırma

İletişim kutusunun alt kısmında **Yerlesik Kalkan ayarları** adı altında bir bölüm göreceksiniz; burada bileşenin fonksiyonlarının temel ayarlarından bazılarını düzenleyebilirsiniz (*diğer bileşenlerde de olduğu gibi ayrıntılı yapılandırma, sistem menüsünün Araçlar/Gelişmiş ayarlar ögesinden yapılabilmektedir*).

Yerlesik Kalkan Etkin seçeneği yerlesik korumayı kolaylıkla açıp kapatabilmenizi sağlar. Varsayılan olarak bu fonksiyon açıktır. Yerlesik koruma açık durumdayken tespit edilen bulasmalar hususunda gerçekleştirilecek eylemi (silmeyi) belirleyebilirsiniz:

- o otomatik olarak (**Tüm tehlikeleri otomatik olarak sil**)
- o ya da sadece kullanıcının onayının ardından (**Tehlikeleri silmeden önce bana sor**)

Bu seçimin güvenlik seviyesi üzerinde herhangi bir etkisi yoktur ve sadece tercihlerinizi yansıtır.

Her iki durumda da **Tanımlama bilgileri otomatik olarak silmek isteyip istemediğinizi seçebilirsiniz**. Belirli durumlarda maksimum güvenlik seviyesine ulaşmak için bu seçeneği kullanabilirsiniz fakat varsayılan olarak kapalıdır. (*tanımlama bilgileri = bir sunucu tarafından web tarayıcısına ve oradan da siteye her ulaşıldığında değiştirilmeksizin tarayıcı tarafından geri gönderilen metin parçalarıdır. HTTP tanımlama bilgileri, site tercihleri veya elektronik alışveriş sepetlerinin içerikleri gibi kullanıcılar hakkındaki belirli bilgilerin kimliklerinin doğrulanması, takibi ve sürdürülmesi için kullanılır.*)

Lütfen dikkat: Yazılım satıcısı, en iyi performansın sunulabilmesi için tüm AVG bileşenlerini kurmuştur. Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını değiştirmeyin. Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir. AVG yapılandırmasını değiştirmeniz gerekiyorsa sistem menüsünden ilgili ögeyi seçin **Araçlar/Gelişmiş ayarlar** ve yeni açılan [AVG Gelişmiş Ayarlar](#) iletişim kutusunda AVG yapılandırmasını düzenleyin.

Kontrol düğmeleri

Yerlesik Kalkan arayüzünde bulunan kontrol düğmeleri şunlardır:

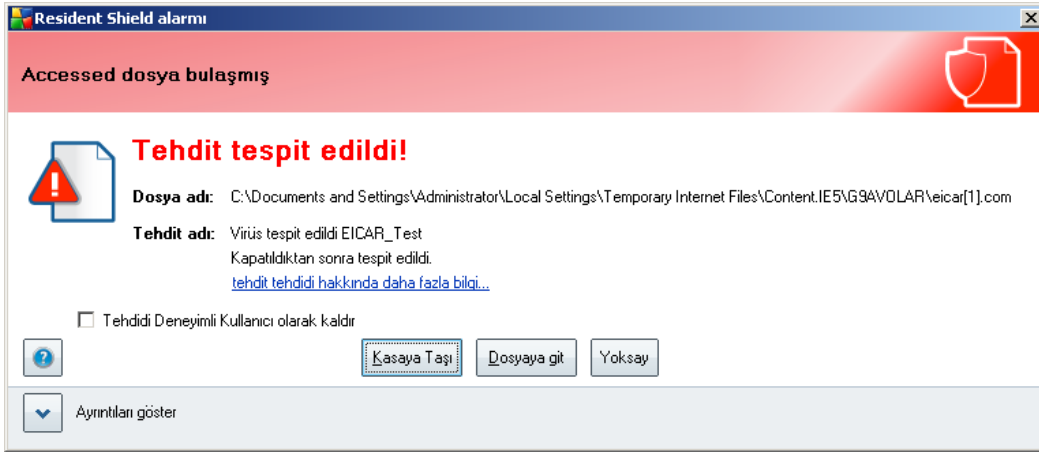
- **İstisnaları yönet** - **Yerlesik Kalkan** taraması dışında tutulması gereken klasörleri/dosyaları tanımlayacağınız yeni bir iletişim kutusu açar (bu iletişim kutusu hakkında bilgi için [Dizin Disi Birakılanlar](#) ve/veya [Hariç Tutulan](#))

[Dosyalar](#) bölümüne bakın).

- **Değişiklikleri kaydet**bu iletişim kutusunda yapılan her tür değişikliği kaydetmek ve uygulamak için bu düğmeye basın
- **İptal** - Varsayılan [AVG kullanıcı arayüzüne](#) dönmek için bu düğmeye basın (bileşenlere genel bakış)

7.5.3. Yerlesik Kalkan Tespiti

Yerlesik Kalkan dosyalar kopyalanırken, açılırken ya da kaydedilirken söz konusu dosyaları tarar. Herhangi bir virüs ya da bir tehlike tespit edildiği zaman aşağıdaki iletişim kutusu ile anında uyarılırsınız:

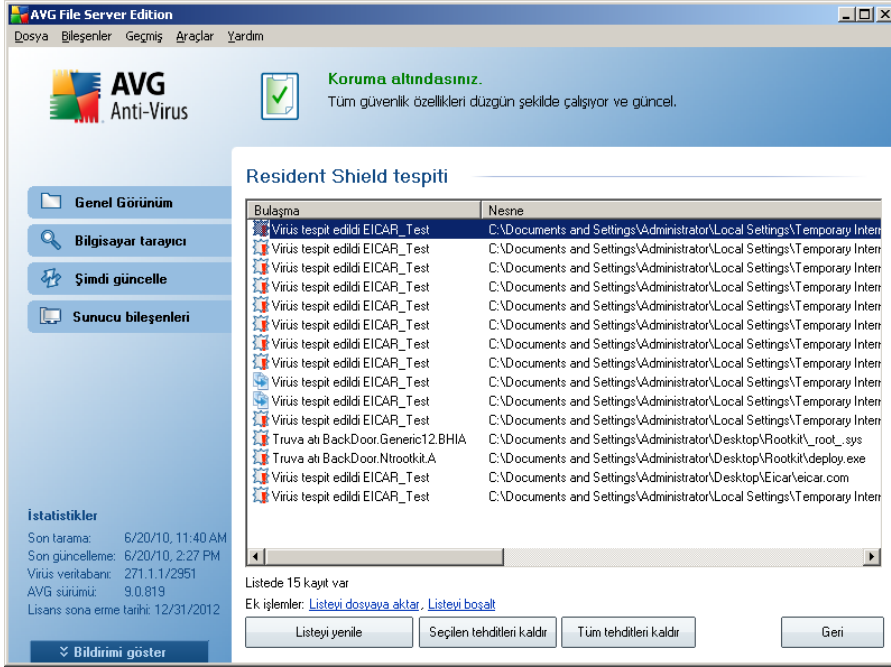


İletişim kutusunda tespit edilen tehlike hakkında bilgi bulunmakta ve sizden hangi eylemin yapılmasını istediğinizi belirtmeniz istenmektedir:

- **Temizle** - Temizleme yöntemi mevcut ise AVG, bulanan nesneyi otomatik olarak temizleyecektir, bu seçenek ilk olarak seçilmesi gereken eylemlerdendir.
- **Kasaya Taşı** - Virüs AVG [Virüs Kasasına tasınacaktır](#)
- **Dosyaya git** - Bu seçenek sizi şüpheli nesnenin tam konumuna yönlendirir (*yeni Windows Gezgini penceresi açar*)
- **Gözardı Et** - çok geçerli bir nedeninizin olmaması halinde KESİNLİKLE bu seçeneği seçmemenizi öneriyoruz!

[Yerlesik Kalkan](#) tarafından algılanan tüm tehlikelerin tamamına genel bakış **Yerlesik Kalkan algılama** iletişim kutusunda bulunabilir, buna [Geçmiş / Yerlesik Kalkan](#)

bulgulari sistem menüsü seçeneğinden erişebilirsiniz:



Yerlesik Kalkan tespiti **Yerlesik Kalkan** tarafından tespit edilip tehlikeli olduğu görülen ve temizlenen ya da **Virüs Kasasına** tasınan nesnelere hakkında genel bilgi vermektedir. Tespit edilen tüm nesnelere için aşağıdaki bilgiler verilir:

- **Bulaşma** - Algılanan nesnenin açıklaması (Muhtemelen adı da)
- **Nesne** - nesnenin konumu
- **Sonuç** - tespit edilen nesne ile gerçekleştirilen eylem
- **Algılama zamanı** - Nesnenin algılandığı tarih ve saat
- **Nesne Türü** - tespit edilen nesnenin türü
- **İslem** - tespit edilmesi amacıyla potansiyel tehlike taşıyan nesneyi uyarıcı işlem nedir

İletişim kutusunun alt kısmında, listenin altında yukarıda listelenen tespit edilen nesnelere toplam sayısı hakkında bilgi bulabilirsiniz. Buna ek olarak tespit edilen nesnelere listesini ayrı bir dosyaya dışarı aktarabilirsiniz (**Listeyi Dosyaya Aktar**) ve tespit edilen nesnelere hakkındaki tüm girişleri silebilirsiniz (**Listeyi Temizle**). **Listeyi Yenile**



düğmesi, **Yerlesik Kalkan** tarafından tespit edilen buluntular listesini günceller. **Seçilen tehlikeleri kaldır** ve **Tüm tehlikeleri kaldır** düğmelerini kullanarak seçili tehlikeleri (veya listelenen tüm tehlikeleri) [Virüs Kasası](#)'na tasiyabilirsiniz. **Geridüğmesi**, sizi varsayılan [AVG kullanıcı arayüzüne](#) götürür (bilesenlere genel bakış).

7.6. Güncelleme Yöneticisi

7.6.1. Güncelleme Yöneticisi Prensipleri

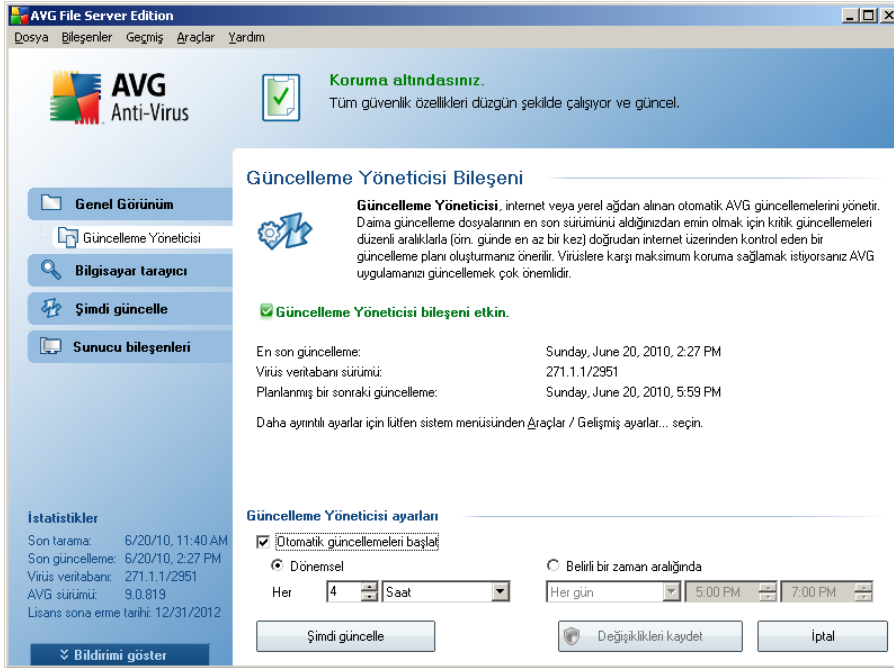
Güvenlik yazılımlarının hiçbiri, rutin olarak güncellenmediği takdirde sizi çeşitli tehlikelere karşı korumayı garanti edemez! Virüs yazarları, yazılım ve işletim sistemlerinde yararlanabilecekleri güvenlik açıkları aramaktadır. Her gün yeni virüsler, yeni kötü amaçlı yazılımlar ve yeni bilgisayar saldırıları gerçekleştirilmektedir. Bu nedenle yazılım geliştiricileri, tespit edilen güvenlik açıklarını kapatmak üzere devamlı olarak güncellemeler ve güvenlik paketleri yayınlamaktadır.

AVG'nizi rutin olarak güncellemeniz çok önemlidir!

Güncelleme Yöneticisi rutin güncelleme işlemi kontrol etmenize yardımcı olur. Bu bileşen kapsamında, güncelleme dosyalarını İnternet'ten ya da yerel ağdan otomatik olarak indirmeyi seçebilirsiniz. Gerekli virüs tanımı güncellemelerinin mümkün ise her gün yapılması gerekmektedir. Daha az önem taşıyan program güncellemeleri haftada bir yapılabilir.

Not: Güncelleme türleri ve seviyeleri hakkında ayrıntılı bilgi edinmek için lütfen [AVG Güncellemeleri](#) bölümünü inceleyin.

7.6.2. Güncelleme Yöneticisi Arayüzü



AVG Anti-Virus

Koruma altındasınız.
Tüm güvenlik özellikleri düzgün şekilde çalışıyor ve güncel.

Güncelleme Yöneticisi Bileşeni

Güncelleme Yöneticisi, internet veya yerel ağdan alınan otomatik AVG güncellemelerini yönetir. Daima güncelleme dosyalarının en son sürümünü aldığınızdan emin olmak için kritik güncellemeleri düzenli aralıklarla (örn. günde en az bir kez) doğrudan internet üzerinden kontrol eden bir güncelleme planı oluşturmanız önerilir. Virüslere karşı maksimum koruma sağlamak istiyorsanız AVG uygulamanızı güncellemek çok önemlidir.

Güncelleme Yöneticisi bileşeni etkin.

En son güncelleme:	Sunday, June 20, 2010, 2:27 PM
Virüs veritabanı sürümü:	271.1.1/2951
Planlanmış bir sonraki güncelleme:	Sunday, June 20, 2010, 5:59 PM

Daha ayrıntılı ayarlar için lütfen sistem menüsünden **Ayarlar / Gelişmiş ayarlar...** seçin.

Güncelleme Yöneticisi ayarları

Otomatik güncellemeleri başlat

Belirli bir zaman aralığında

Dönemsel

Her 4 Saat

Her gün 5:00 PM 7:00 PM

İstatistikler

Son tarama: 6/20/10, 11:40 AM
Son güncelleme: 6/20/10, 2:27 PM
Virüs veritabanı: 271.1.1/2951
AVG sürümü: 9.0.819
Lisans sona erme tarihi: 12/31/2012

Güncelleme Yöneticisi'nin arayüzünde bileşenin fonksiyonları ve mevcut durumu hakkında bilginin yanı sıra (*Güncelleme Yöneticisi etkindir.*) ilgili istatistik bilgileri bulunmaktadır:

- **En son güncelleme** - veritabanının en son güncellendiği tarih ve saati gösterir.
- **Veritabanı sürümü**- en son virüs veritabanı sürümünün numarasını tanımlar ve bu numara virüs veritabanı her güncellendiğinde artar
- **Sonraki programlanan güncelleme** - Veritabanının yeniden güncellenmek için hangi tarih ve saatte programlandığını belirtir

Temel bileşen yapılandırma

İletişim kutusunun alt kısmında güncelleme işlemi kurallarında bazı değişiklikler yapabileceğiniz **Güncelleme Yöneticisi ayarları** bölümünü görebilirsiniz. Güncelleme dosyalarını otomatik olarak (**Güncellemeyi otomatik başlat**) ya da istek üzerine indirmeyi seçebilirsiniz. Varsayılan olarak **Güncellemeyi otomatik başlat** seçeneği etkindir ve bu ayarı değiştirmeden muhafaza etmeniz önerilir! Güvenlik yazılımlarının doğru şekilde çalışması için en güncel güncelleme dosyalarının düzenli aralıklarla

indirilmesi hayati önem tasir!

Bunun yani sira güncellemenin ne zaman baslatilacagini da belirleyebilirsiniz:

- o **Periyodik olarak** - zaman araligini belirleyin
- o **Belirli bir saatte** - kesin gün ve saati belirleyin

Varsayilan olarak her 4 saatte bir güncelleme islemi yapilir. Degistirmek için geçerli bir nedeniniz yoksa bu ayari oldugu sekilde muhafaza etmeniz önerilir!

Lütfen dikkat: Yazilim saticisi, en iyi performansin sunulabilmesi için tüm AVG bileşenlerini kurmustur. Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını degistirmeyin. Ayarlarda yapılacak her tür degisiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir. AVG yapılandırmasını degistirmeniz gerekiyorsa sistem menüsünden ilgili öğeyi seçin **Araçlar/Gelismis ayarlar** ve yeni açılan [AVG Gelismis Ayarlar](#) iletisim kutusunda AVG yapılandırmasını düzenleyin.

Kontrol düğmeleri

Güncelleme Yöneticisi arayüzünde bulunan kontrol düğmeleri sunlardır:

- **Simdi güncelle** - istek üzerine [güncelleme islemini hemen](#) baslatir
- **Degisiklikleri kaydet** bu iletisim kutusunda yapılan her tür degisikligi kaydetmek ve uygulamak için bu düğmeye basin
- **Iptal** - Varsayilan [AVG kullanıcı arayüzüne](#) dönmek için bu düğmeye basin (bileşenlere genel bakis)

8. AVG Sunucusu Bilesenleri

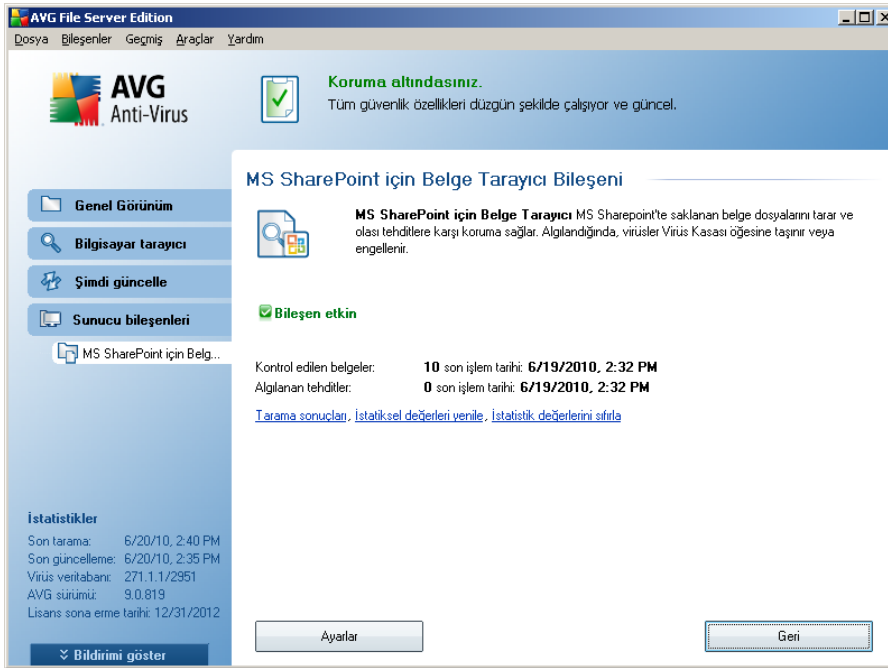
8.1. MS SharePoint için Belge Tarayıcı

8.1.1. Belge Tarayıcı Prensipleri

MS SharePoint için Belge Tarayıcısı sunucu bileseninin amacı, MS SharePoint'te saklanan belgeleri taramaktır. *******Bir virüs algılanırsa, Virüs Kasası'na tasınırlar veya tamamen kaldırılır.

Microsoft SharePoint, gelisen bilesen seçimi, Internet Explorer tabanlı birlikte çalışma işlevleri, süreç yönetimi modülleri, arama modülleri ve bir belge yönetimi platformu içeren ürün ve yazılım öğeleri topluluğudur. SharePoint paylaşılan çalışma alanlarına, bilgi depolarına ve belgelere erişen web sitelerini barındırmada kullanılabilir.

8.1.2. Belge Tarayıcı Arayüzü



The screenshot displays the AVG File Server Edition interface. At the top, there is a status bar with the text "Koruma altındasınız. Tüm güvenlik özellikleri düzgün şekilde çalışıyor ve güncel." Below this, the main content area is titled "MS SharePoint için Belge Tarayıcı Bileşeni". It features a sub-header "MS SharePoint için Belge Tarayıcı" and a description: "MS SharePoint için Belge Tarayıcı MS SharePoint'te saklanan belge dosyalarını tarar ve olası tehditlere karşı koruma sağlar. Algılandığında, virüsler Virüs Kasası ögesine taşınırlar veya engellenir." A green checkmark icon indicates "Bileşen etkin". Below this, there is a table showing scan statistics: "Kontrol edilen belgeler: 10 son işlem tarihi: 6/19/2010, 2:32 PM" and "Algılanan tehditler: 0 son işlem tarihi: 6/19/2010, 2:32 PM". There are links for "Tarama sonuçları", "İstatiksel değerleri venile", and "İstatistik değerlerini sıfırla". On the left side, there is a sidebar with navigation options: "Genel Görünüm", "Bilgisayar tarayıcı", "Şimdi güncelle", "Sunucu bileşenleri", and "MS SharePoint için Belg...". At the bottom left, there is a section for "İstatistikler" with details: "Son tarama: 6/20/10, 2:40 PM", "Son güncelleme: 6/20/10, 2:35 PM", "Virüs veritabanı: 271.1.1/2951", "AVG sürümü: 9.0.819", and "Lisans sona erme tarihi: 12/31/2012". At the bottom right, there are buttons for "Ayarlar" and "Geri".

Bilesenin geçerli durumunda en önemli istatistik verilere ve bilgilere genel bakışın yanı sıra (*Bilesen aktif*), **MS SharePoint için Belge Tarayıcısı** arayüzü bileşenlerin istatistiklerine kısa bir bakış sunar:

- **Kontrol edilen belgeler** - belirli bir tarihten itibaren kontrol edilen belge sayısı
- **Algılanan tehlikeler** - belirli bir tarihten itibaren algılanan bulasmaların sayısıdır

Bu istatistikleri istediğiniz zaman ***Istatistiksel degerleri yenile*** bağlantısını tıklayarak güncelleyebilirsiniz. Yeni veri hemen görünecektir. Tüm istatistiksel degerleri sıfır olarak ayarlamak istiyorsanız, ***Istatistiksel degerleri sıfırla*** bağlantısını tıklayın. Son olarak, ***Tarama sonuçları*** bağlantısını tıklamak, tarama sonuçları listesi içeren yeni bir iletişim kutusu açacaktır. Radyo düğmelerini ve/veya sekmeleri kullanarak listedeki verileri sıralayın.

Kontrol düğmeleri

MS SharePoint için Belge Tarayıcısı arayüzündeki kontrol düğmeleri şunlardır:

- **Ayarlar** - ***MS SharePoint için Belge Tarayıcısı*** belge virüs tarama performansı ile ilgili birçok parametresi ayarlayabileceğiniz yeni bir iletişim kutusu açar (bu iletişim kutusu hakkında daha fazla bilgi için [MS SharePoint için Belge Tarayıcısı için Gelismis Ayarlar](#) ve/veya [Algılama eylemleri](#) bölümlerini okuyun).
- **Geri** - varsayılan [Sunucu bileşenleri arayüzüne](#) geri dönmek için bu düğmeye basın.

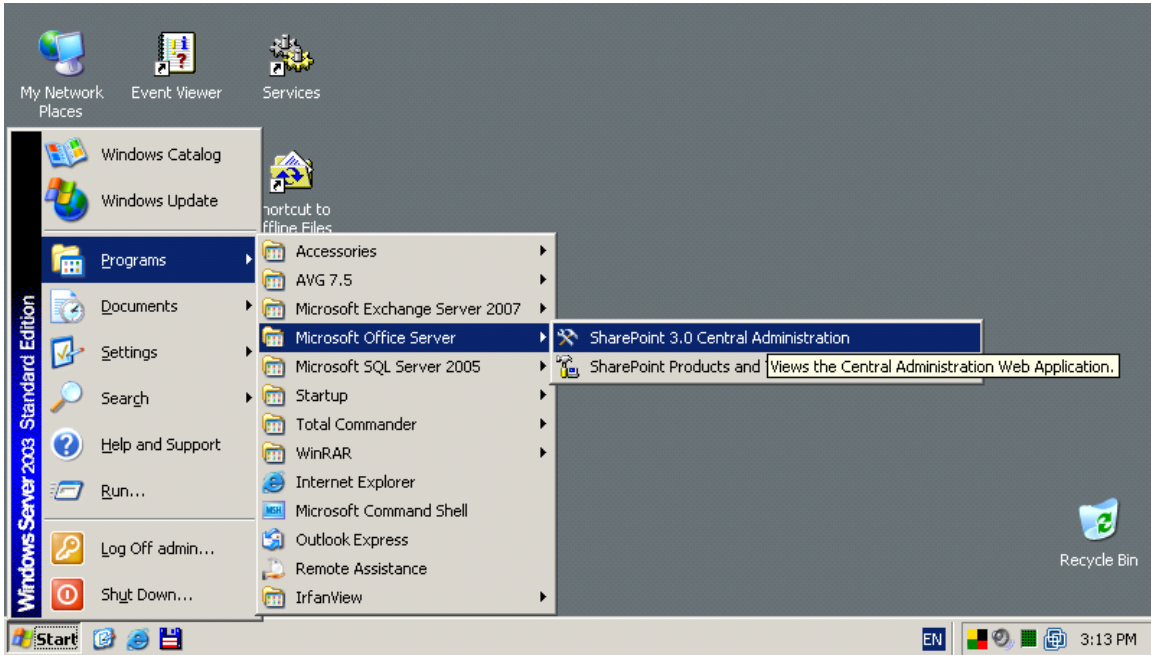
9. SharePoint Portal Server için AVG

Bu bölüm, özel bir dosya sunucusu türü olarak ele alınabilen **MS SharePoint Portal Server**'da AVG bakımını içerir.

9.1. Program Bakimi

SharePoint Portal Server için AVG, sunucunuzun olası virüs bulasmalarına karşı korunması için Microsoft SP VSAPI 1.4 virüs tarama arayüzünü kullanır. Sunucudaki nesnelere, kullanıcılar tarafından sunucuya/sunucudan indirildiklerinde ve/veya karşıya yüklendiklerinde kötü amaçlı yazılıma karşı test edilir. Virüsten koruma yapılandırması SharePoint Portal Sunucunuzun **Merkezi Yönetim** arayüzü kullanılarak ayarlanır. **Merkezi Yönetim** içinden **SharePoint Portal Server için AVG** günlük dosyasını da görüntüleyebilir ve yönetebilirsiniz.

Sunucunuzun çalıştığı bilgisayarda oturum açtığınızda **SharePoint Portal Server Central Administration**'i başlatabilirsiniz. Yönetim arayüzü web tabanlıdır (*SharePoint Portal Server* kullanıcı arayüzünde olduğu gibi) ve **SharePoint (3.0) Merkezi Yönetim** seçeneğini kullanarak **Programlar/Microsoft Office Server** klasöründe (*veya SharePoint Portal Server*), Windows **Baslat** menüsünden açabilirsiniz:



Ayrıca, **SharePoint Portal Server Merkezi Yönetim** web sayfasına uygun erişim hakları ve URL ile uzaktan girebilirsiniz.

9.2. SPPS Yapilandirmasi - SharePoint 2007 için AVG

SharePoint 3.0 Central Administration arayüzünde, kolayca **SharePoint Portal Server için AVG** tarayicisi performans parametrelerini ve eylemleri yapilandirabilirsiniz. **Merkezi Yönetim** kisminda **Islemler** seçenegini seçin. Yeni bir iletisim kutusu görünecektir. **Güvenlik Yapilandirmasi** bölümünde **Virüsten koruma** ögesini seçin.

Security Configuration

- Service accounts
- Information Rights Management
- Antivirus
- Blocked file types
- Update farm administrator's group
- Information management policy configuration
- Manage settings for single sign-on

Asagidaki pencere görüntülenecektir:

Antivirus

Use this page to configure settings for virus scanning. You must install virus scanning software on all Web servers that are hosting documents before these settings can take effect. [Learn about configuring antivirus settings.](#)

Antivirus Settings

Specify when you want documents stored in document libraries and lists to be virus scanned, and whether you want your virus scanner to attempt to clean infected documents.

- Scan documents on upload
- Scan documents on download
- Allow users to download infected documents
- Attempt to clean infected documents

Antivirus Time Out

You can specify how long the virus scanner should run before timing out. If server response time is slow while scanning, you may want to decrease the number of seconds.

Time out duration (in seconds):

Antivirus Threads

You can specify the number of execution threads on the server that the virus scanner may use. If server response time is slow while scanning, you may want to decrease the number of threads allowed for virus scanning.

Number of threads:

OK

Cancel

Çeşitli **SharePoint Portal Server için AVG** virüsten koruma tarama eylemlerini ve performans özelliklerini burada yapılandırabilirsiniz:

- **Yüklemede belgeleri tara** – belgelerin yüklenirken taranmasını etkinleştirin/devre dışı bırakın
- **İndirmede belgeleri tara** – belgelerin indirilirken taranmasını etkinleştirin/devre dışı bırakın
- **Kullanıcıların virüslü belgeleri indirmesine izin ver** – kullanıcıların virüslü belgeleri indirmesine izin verin/yasaklayın
- **Virüslü belgeleri temizlemeye çalış** – virüslü belgelerin otomatik silinmesini etkinleştirin/devre dışı bırakın
- **Zaman asımı süresi (saniye cinsinden)** – tek bir baslatmadan sonra virüs tarama işleminin çalışacağı maksimum saniye sayısı (belgeler taranırken sunucunun yanıtı yavaş görünüyorsa değeri azaltın)

- **Is parçacığı sayısı** – aynı anda çalıştırılabilen virüs tarama is parçacığı sayısını belirtebilirsiniz; sayıyı artırmak daha yüksek paralelizm düzeyi nedeniyle taramayı hızlandırabilir, ancak öte yandan sunucunun yanıt süresini artırabilir

9.3. SPPS Yapılandırması - SharePoint 2003 için AVG

SharePoint Portal Server Central Administration arayüzünde, kolayca **SharePoint Portal Server için AVG** tarayıcısı performans parametrelerini ve eylemleri yapılandırabilirsiniz. **Güvenlik Yapılandırması** kısmındaki **Virüsten Koruma Eylemleri Yapılandırması** seçeneğini seçin:

Component Configuration



Use these links to manage search settings, configure single sign-on, manage shared services, configure usage analysis, HTML viewer settings and configure diagnostic settings. If you have installed the optional document library component, you can configure document libraries (Web Storage System-based) from here.

- ▣ [Manage the Search Service](#)
- ▣ [Manage settings for single sign-on](#)
- ▣ [Manage shared services for the server farm](#)
- ▣ [Configure usage analysis processing](#)
- ▣ [Configure HTML viewer](#)
- ▣ [Configure diagnostic settings](#)

Aşağıdaki pencere görüntülenecektir:

Configure Antivirus Settings

Use this page to configure settings for virus scanning. You must install virus scanning software on all Web servers that are hosting documents before these settings can take effect. [Show me more information.](#)

Antivirus Settings

Specify when you want documents stored in document libraries and lists to be virus scanned, and whether you want your virus scanner to attempt to clean infected documents. You can also specify how long the virus scanner should run before timing out, and the number of execution threads on the server that it may use. If server response time is slow while scanning, you may want to decrease the number of seconds and threads allowed for virus scanning.

- Scan documents on upload
- Scan documents on download
- Allow users to download infected documents
- Attempt to clean infected documents
- Time out scanning after seconds
- Allow scanner to use up to threads

OK

Cancel

Çesitli **SharePoint Portal Server için AVG** virüsten koruma tarama eylemlerini ve performans özelliklerini burada yapılandırabilirsiniz:

- **Yüklemede belgeleri tara** – belgelerin yüklenirken taranmasını etkinleştirin/devre dışı bırakın
- **İndirmede belgeleri tara** – belgelerin indirilirken taranmasını etkinleştirin/devre dışı bırakın
- **Kullanıcıların virüslü belgeleri indirmesine izin ver** – kullanıcıların virüslü belgeleri indirmesine izin verin/yasaklayın
- **Virüslü belgeleri temizlemeye çalış** – virüslü belgelerin otomatik silinmesini etkinleştirin/devre dışı bırakın
- **Taramada zaman sınırı** – tek bir baslatmadan sonra virüs tarama işleminin çalışacağı maksimum saniye sayısı (*belgeler taranırken sunucunun yanıtı yavaş görünüyorsa değeri azaltın*)
- **Belgeleri tararken maks. X alt işlem kullan** – X, aynı anda çalıştırılabilen virüs tarama iş parçacığını belirtir; sayıyı artırmak daha yüksek paralelizm düzeyi nedeniyle taramayı hızlandırabilir, ancak öte yandan sunucunun yanıt süresini



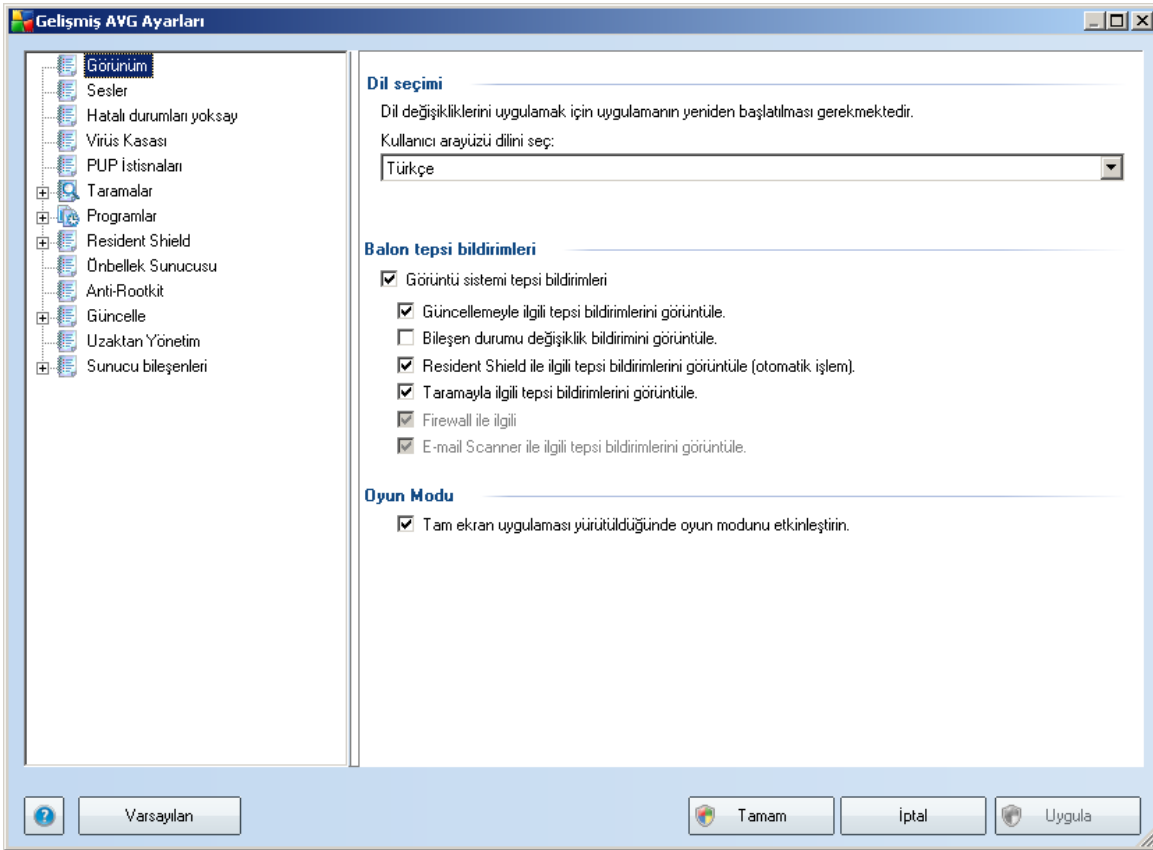
artirabilir

10. AVG Gelismis Ayarlar

AVG 9.0 File Server Gelismis yapilandirma iletisim kutusu **Gelismis AVG Ayarlari** adli yeni bir pencerede açilir. Pencere iki bölüme ayrilir: sol tarafta program yapilandirma seçeneklerini gösteren ağaç tipli menü bulunmaktadır. İletisim penceresini pencerenin sag kısmında görüntülemek için *'nin ya da belirli bir bileşenin* () yapilandirmasını degistirmek istediğiniz bileşeni seçin.

10.1. Görünüm

Dolasim agacinin ilk ögesi olan **Görünüm**, [AVG kullanıcı arayüzünün](#) genel ayarlarına ve uygulamanın bazı temel seçeneklerine iliskindir:

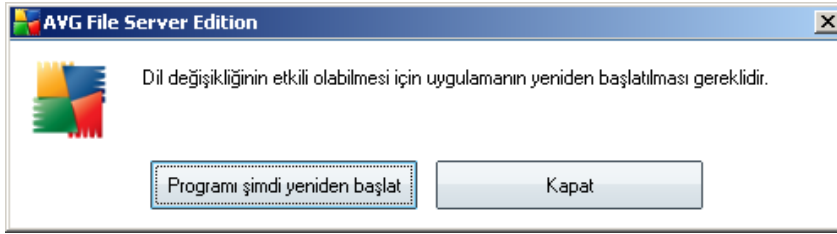


Dil seçimi

Dil seçimi bölümünde açılır menüden istediğiniz dili seçebilirsiniz; bunun ardından

seçtiğiniz dil tüm [AVG Kullanıcı Arayüzünde](#) kullanılacaktır. Açılır menü, sadece [Yükleme işlemi](#) sırasında yüklenmesini onayladığınız dilleri gösterir ([Özel Yükleme - Bileşen Seçimi](#) bölümünü inceleyiniz). Diğer bir yandan uygulamayı başka bir dile çevirme işlemi bitirmek için kullanıcı arayüzünü yeniden başlatmanız gerekir; aşağıdaki işlemleri takip edin:

- Uygulamada kullanılmasını istediğiniz dili seçin ve **Uygula** düğmesine (sağ alt köşede) basarak seçiminizi onaylayın.
- **Tamam** onay düğmesine basın
- AVG kullanıcı arayüzündeki dil değişiminin uygulamayı yeniden başlatmayı gerektirdiğini bildiren yeni iletişim kutusu penceresi açılır:



Balon tepsi bildirimleri

Bu bölümde uygulama durumu hakkında sistem tepsi üzerinde beliren balon bildirimlerini kaldırabilirsiniz. Balon bildirimlerinin varsayılan olarak görüntülenmesine izin verilir ve söz konusu yapılandırmanın değiştirilmemesi önerilir! Balon bildirimleri, genellikle AVG bileşenlerinin durum değişiklikleri hakkında bilgi verir ve bunlara dikkat etmeniz gerekir!

Diğer bir yandan, belirli bir neden dolayısıyla söz konusu bildirimlerin görüntülenmesini istemiyorsanız ya da sadece belirli bildirimlerin görüntülenmesini istiyorsanız (belirli AVG bileşenlerine ilişkin) tercihlerinizi aşağıdaki seçenekleri işaretleyerek ya da işaretlemeyerek tanımlayabilir ya da belirleyebilirsiniz:

- **Sistem tepsi bildirimlerini görüntüle** - Bu öge varsayılan olarak işaretlidir (açıktır), ve bildirimler görüntülenir. Tüm balon bildirimleri kapatmak için bu öğenin işaretini kaldırın. Açıldığı zaman hangi bildirimlerin görüntüleneceğini seçebilirsiniz:
 - **Güncelleme** hakkında bildirimleri görüntüle- AVG güncellemesi işleminin başlaması, ilerleyişi ve bitisi hakkında bilgilerin görüntülenmesini isteyip istemediğinize karar verin;

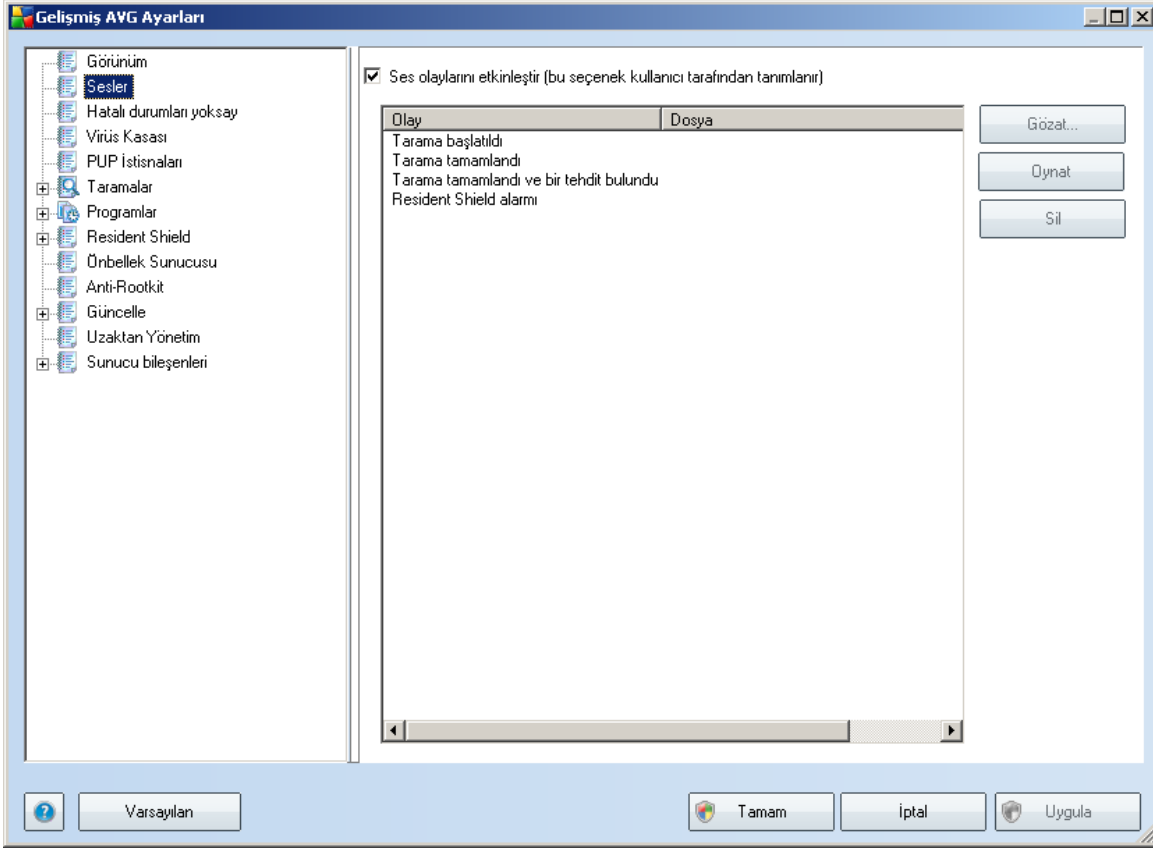
- **Bilesen durum degisimi hakkında bildirimleri görüntüle** - Bilesenlerin aktif ya da pasif durumlarına ilişkin ya da muhtemel sorunları ile ilgili bildirimlerin görüntülenmesini isteyip istemediğinize karar verin. Bir bilesenin hata durumu rapor edilirken bu seçenek, [sistem tepsi simgesinin](#) (renk degistirme) herhangi bir AVG bileseninde meydana gelen sorunu rapor ederken kullandığı bilgilendirici fonksiyonuna esdegerdir (*bu seçenek varsayılan olarak devre dışı olan tek seçenektir*);
- **Yerlesik Kalkan ile ilgili tepsi bildirimlerini görüntüle** - Dosya kaydetme, kopyalama ve açma işlemlerine ilişkin bildirimlerin görüntülenip görüntülenmeyeceğine karar verin;
- **Tarama** hakkında bildirimleri görüntüle- Programlı taramaların otomatik olarak başlaması, ilerleyişi ve sonuçları hakkında bilgilerin görüntülenmesini isteyip istemediğinize karar verin.

Oyun Modu

Bu AVG işlevi, olası AVG bilgi balonlarının (*örn. zamanlanmış bir tarama başlatıldığında gösterilir*) rahatsız edici olabileceği yerlerde (*uygulamayı küçültebilir veya grafiklerini bozabilir*) tam ekran uygulamalar için tasarlanmıştır. Bu durumdan kaçınmak için, **Tam ekran uygulama çalıştırılırken oyun modunu etkinleştir** seçeneği işaretli bırakın (*varsayılan ayar*).

10.2. Sesler

Sesler iletişim kutusu içinde, belirli AVG eylemleri hakkında bir ses bildirimiyle bilgilendirilmek isteyip istemediğinizi belirtebilirsiniz. İstiyorsanız, AVG eylemleri listesini etkinleştirmek için **Ses olaylarını etkinleştir** seçeneğini (*varsayılan olarak kapalıdır*) işaretleyin:

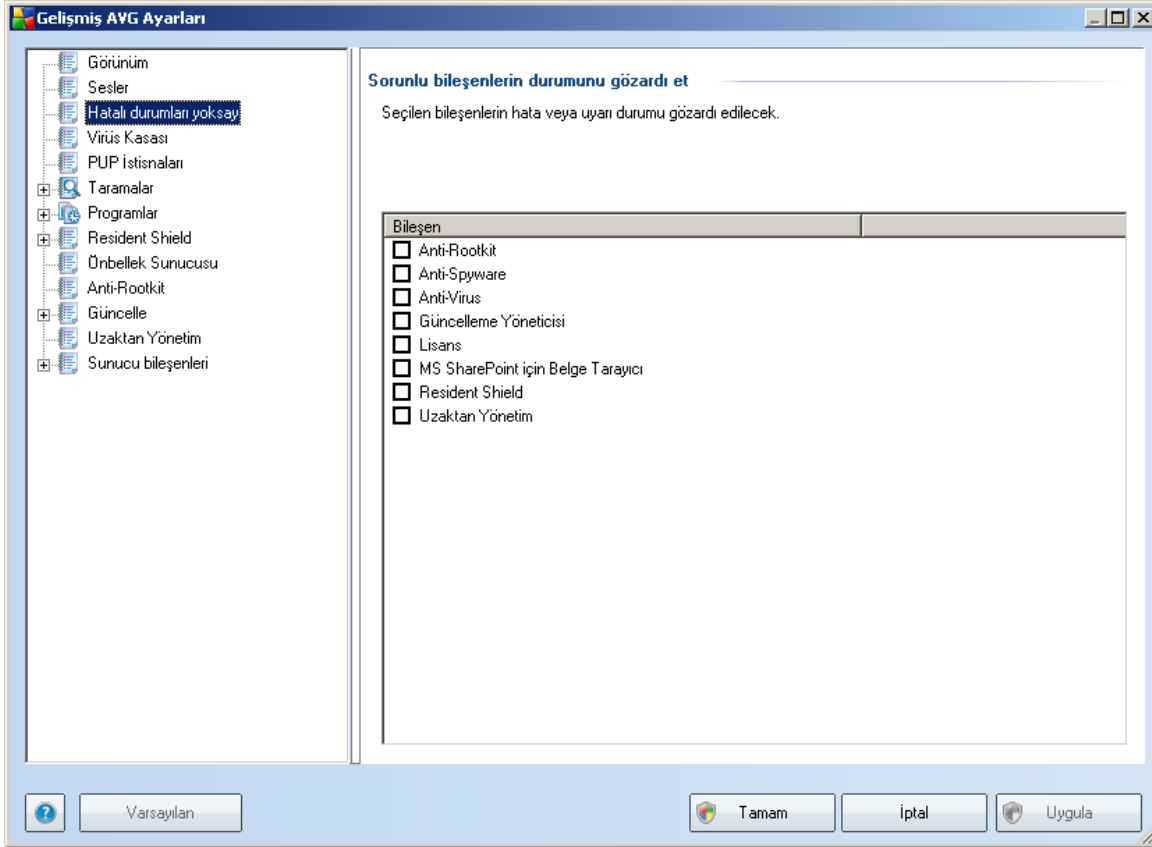


Sonra, ilgili olayı listeden seçin ve bu olaya atamak istediğiniz uygun ses için diskinize gözetin (**Gözet**). Seçili sesi dinlemek için, listede olayı vurgulayın ve **Çal** düğmesine basın. Belirli olaya atanan sesi kaldırmak için **Sil** düğmesini kullanın.

Not: Yalnızca *.wav sesleri desteklenir!

10.3. Hatali Durumlari Yoksay

Hatali bileşenleri göz ardı etme koşulları iletişim kutusunda, bilgilendirilmek istemediğiniz bileşenleri seçebilirsiniz:



Varsayılan olarak listede herhangi bir bileşen seçilmemiştir. Bileşenlerden herhangi biri hatalı duruma düşerse aşağıdaki yöntemlerden biri vasıtasıyla uyarılacaksınız demektir:

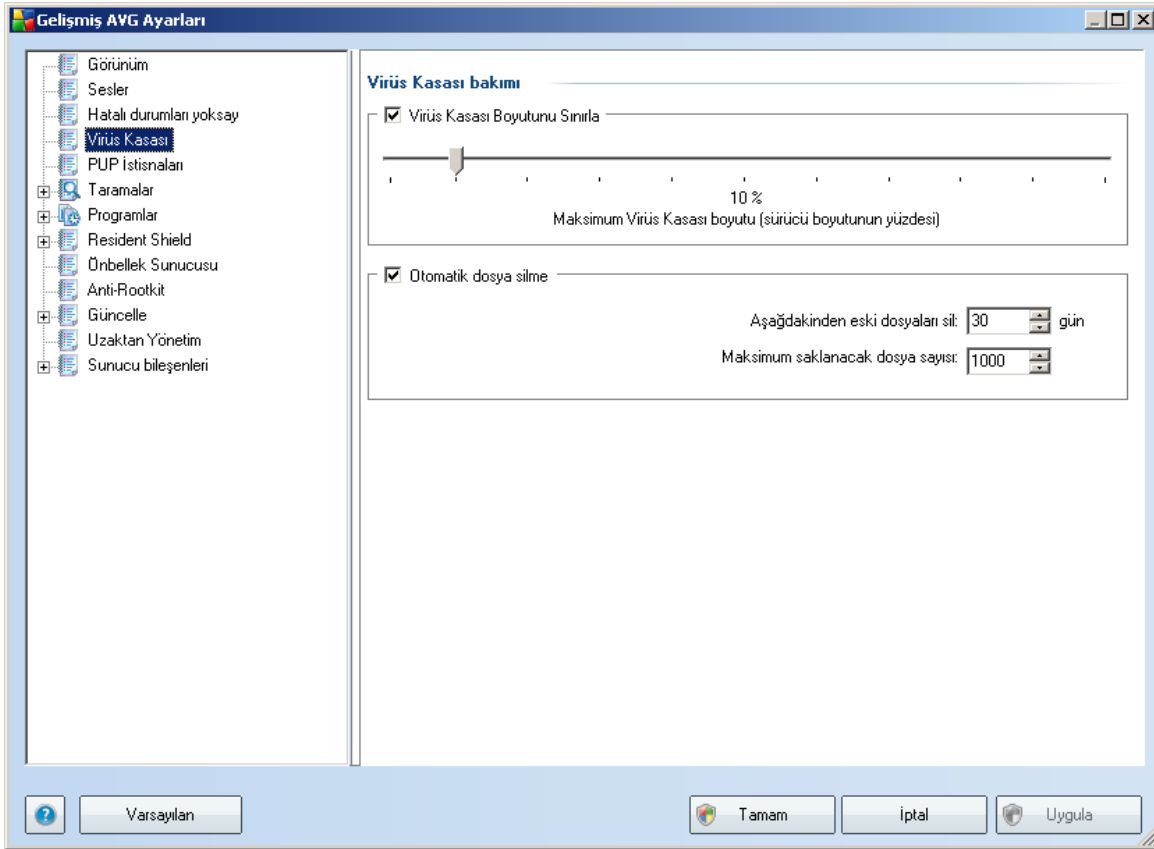
- **[sistem tepsisi simgesi](#)** - AVG'nin tüm bileşenleri doğru şekilde çalışırken simge olduğu gibi görünecektir, ancak herhangi bir aksaklık olursa simgenin yanında sarı bir ünlem işareti görülür,
- AVG ana penceresinin **[Güvenlik Durumu Hakkında Bilgi](#)** bölümünde mevcut sorun açıklanır

Bileşenlerden birini geçici bir süre ile kapatmanız gereken bir durum ile karşılaşabilirsiniz(*bileşenlerin geçici süre ile kapatılması önerilmemektedir, tüm bileşenleri daima açık*)

durumda ve varsayılan yapılandırmayı muhafaza etmeniz gerekir ancak aksi durumlarla karşılaşabilirsiniz). Bu durumda sistem tepsisi simgesi, otomatik olarak bileşenin hata durumunda olduğunu bildirir. Ancak bu durumda gerçek bir hatadan söz edemeyiz çünkü hatayı siz baslatmışsınızdır ve potansiyel riskin farkında olmalısınız. Aynı zamanda, simge ünlem isaretiyle görüntüledikten sonra daha sonra vuku bulacak hataları rapor etmeyecektir.

Bu durumda yukarıdaki iletişim kutusunda hata durumunda olan (ya da kapatılmış) bileşenleri seçebilirsiniz ve söz konusu durum hakkında bilgilendirilmek istemeyebilirsiniz. **Bileşen durumunun gözardı edilmesi** işlemi doğrudan [AVG ana penceresinin bileşenlere genel bakış](#) penceresinden de gerçekleştirilebilir.

10.4. Virüs Kasası



Virüs Kasası bakımı iletişim kutusu, [Virüs Kasası](#)'nda depolanan nesnelerin yönetimi hususunda çeşitli parametreleri tanımlayabilmenizi sağlar:

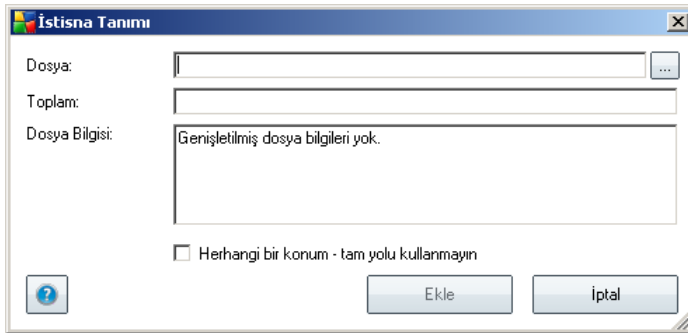


- **Virüs Kasasi boyutunu sinirla** - [Virüs Kasasi](#)'nin maksimum boyutu için kaydiriciyi kullanin. Söz konusu boyut, sabit diskinizin boyutu ile dogru orantili olacaktır.
- **Otomatik dosya silme** - bu bölümde nesnelere [Virüs Kasasinda](#) depolanacaklari maksimum süreyi (... **Günden eski dosyalari sil**), [Virüs Kasasinda](#) depolanacak maksimum dosya sayisini(**Depolanacak maksimum dosya sayisi**) belirleyebilirsiniz.

10.5. PUP Istisnaları

AVG 9.0 File Server, bunun yanı sıra sistemde potansiyel anlamda istenmeyen çalıştırılabilir uygulamaları ya da DLL kütüphanelerini de inceleyebilmekte ve tespit edebilmektedir. Bazı durumlarda kullanıcı belirli istenmeyen programların (*bilerek yüklenen programlar*) bilgisayarında bulunmasını tercih edebilir. Bunlardan bazıları reklam yazılımları ve özellikle ücretsiz yazılımlardır. Söz konusu reklam yazılımları AVG tarafından tespit edilip **potansiyel olarak istenmeyen program** statüsü ile rapor edilebilir. Söz konusu programın bilgisayarınızda bulunmasını istiyorsanız ilgili programı, potansiyel olarak istenmeyen program istisnası şeklinde atayabilirsiniz:

- **Düzenle** - önceden tanımlanmış olan bir istisnanın parametrelerini düzenleyebileceğiniz bir düzenleme iletişim kutusu açar (*yeni istisna tanımlama iletişim kutusuyla aynı, aşağıya bakın*)
- **Sil** - seçilen öğeyi istisnalar listesinden siler
- **İstisna Ekle** - oluşturulacak yeni istisnanın parametrelerini tanımlayabileceğiniz yeni bir düzenleme iletişim kutusunu açar:



- **Dosya** - istisna olarak belirlemek istediğiniz dosyanın tam yolunu girin
- **İmzayı Kontrol Et** - seçilen dosyanın "özel imzasını" görüntüler. Bu sağlama, AVG'nin seçilen dosyayı diğer dosyalardan ayırmasını sağlamak üzere otomatik oluşturulan karakter dizelerinden meydana gelmektedir. Sağlama, dosyanın başarıyla eklenmesinin ardından oluşturulur ve görüntülenir.
- **Dosya Bilgisi** - dosya hakkında (*lisans/sürüm bilgileri vb*) mevcut tüm bilgileri görüntüler
- **Herhangi bir yerde - tam yolu kullanma** - söz konusu dosyayı sadece belirli bir konumda istisna olarak atamak istiyorsanız bu kutucuğu işaretlemeyin

10.6. Taramalar

Gelişmiş tarama ayarları, yazılım geliştiricisi tarafından tanımlanan belirli tarama türlerine ilişkin dört kategoriye bölünmüştür:

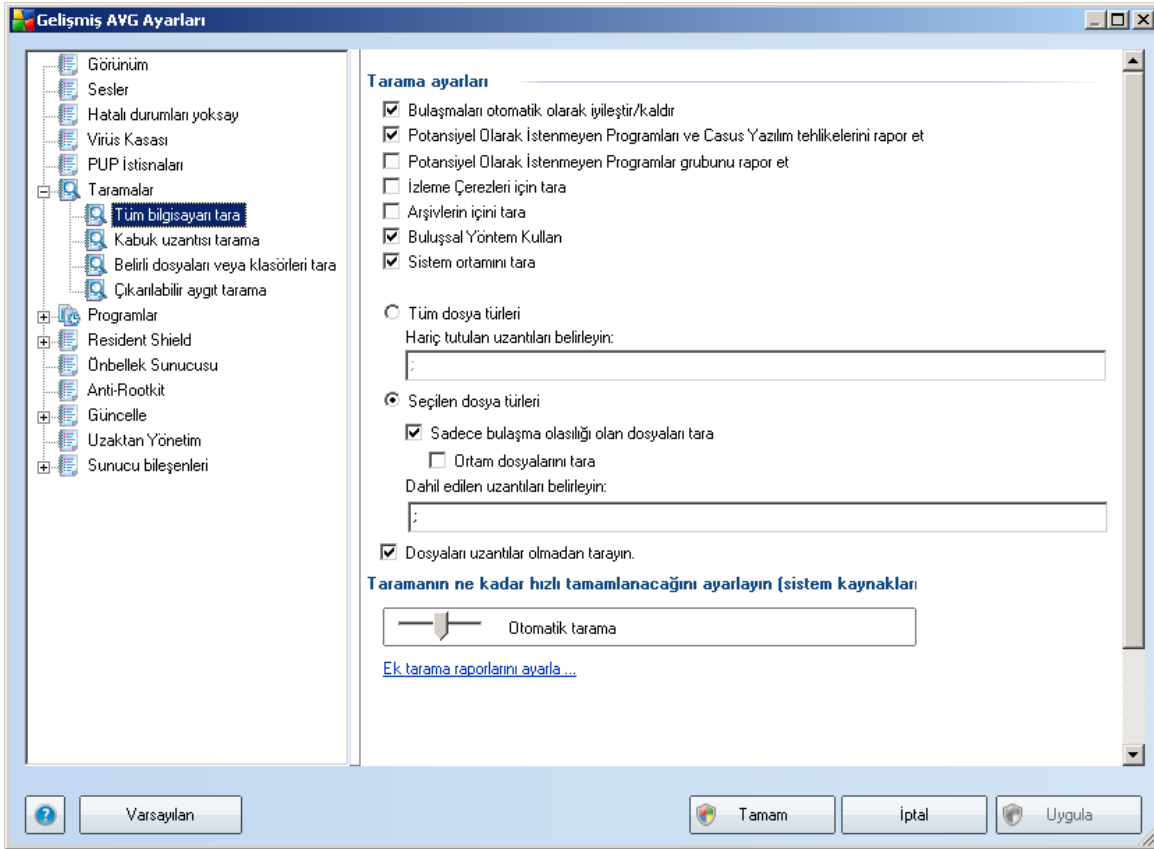
- **Tam Bilgisayar Taraması** - bilgisayarın tamamen tarandığı standart öntanımlı taramadır
- **Kabuk Uzanti Taraması** - seçilen nesnenin doğrudan Windows Gezginini

ortamında taraması işlemidir

- **Belirli Dosya ya da Klasörlerin Taranması** - bilgisayarınızın seçilen alanlarının tarandığı standart öntanımlı taramadır
- **Çıkarılabilir Aygıt Taraması** - bilgisayarınıza bağlanan çıkarılabilir aygıtların taraması işlemidir

10.6.1. Tüm Bilgisayarı Tara

Bilgisayarın tümünü tara seçeneği, yazılım satıcısı tarafından belirlenmiş öntanımlı tarama yöntemlerinden birinin parametrelerini düzenleyebilmenize olanak tanır, **Bilgisayarın tümünün taranması**:



Tarama ayarları

Tarama ayarları bölümünde isteğe bağlı olarak açılıp kapatılabilecek tarama parametreleri listelenmiştir:

- **Bulasmayı otomatik temizle/sil** - tarama işlemi sırasında bir virüs tanımlanırsa ve temizlenmesi mümkün ise otomatik olarak temizlenir. Etkilenen dosya otomatik olarak silinmiyorsa ya da bu seçeneği kapatmayı seçerseniz bir virüs tespit edildiğinde bilgilendirileceksiniz ve tespit edilen bulasma hakkında ne yapılacağına karar vermek zorunda kalacaksınız. Önerilen işlem, bulasmis dosyayı [Virüs Kasasına](#) kaldırmaktır.
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım Tehlikelerini Rapor Et** - Bu parametre, [potansiyel olarak istenmeyen programların tespit edilmesini](#) (casus yazılım ya da reklam yazılımı gibi işleyen çalıştırılabilir dosyalar) sağlayan *Virüsten Koruma* fonksiyonunu kontrol eder.
- **Gelişmiş Potansiyel Olarak İstenmeyen Programlar setini bildir** - bu parametre kutusunun genişletilmiş [casus yazılım](#): programlarını algılamasını sağlar; bunlar doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılan programlardır. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır;
- **Tanımlama Bilgilerini Tara** - [Casus Yazılımdan Koruma](#) bileşeninin bu parametresi, tarama sırasında tespit edilmesi istenen tanımlama bilgilerini tanımlar (*HTTP tanımlama bilgileri site tercihleri ya da elektronik alışveriş sepeti içeriği gibi kullanıcı hakkında belirli bilgilerin toplanması, temin edilmesi ve izlenmesi için kullanılır*)
- **Arsivleri tara** - bu parametre, ZIP, RAR vb. arşiv dosyalarının içinde sıkıştırılmış dosyaların bile taranmasını sağlar.
- **Bulgusal Analiz Kullan** - bulgusal analiz (*taranan nesnenin sanal bir bilgisayar ortamında dinamik olarak canlandırılması'na ilişkin talimatlar*) tarama sırasında kullanılacak virüs tespiti yöntemlerinden birisidir;
- **Sistem ortamını tara** - tarama işlemi, bilgisayarınızın sistem alanlarını da kontrol edecektir.

Ayrıca, taramak isteyip istemediğinize karar vermelisiniz

- **Tüm dosya türleri** taranmaması gereken virgülle ayrılmış dosya uzantılarının listesini sağlayarak taramada istisnaları tanımlama seçeneğiyle;
- **Seçili dosya türleri** - Yalnızca virüs bulasabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulasamayan dosyalar taranmayacaktır*,

örneğin, bazı düz metin dosyaları veya bazı diğer çalıştırılmayan dosyalar); ortam dosyaları (video, ses dosyaları - bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulaşma olasılıkları çok az olduğundan tarama süresini daha da azaltır). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.

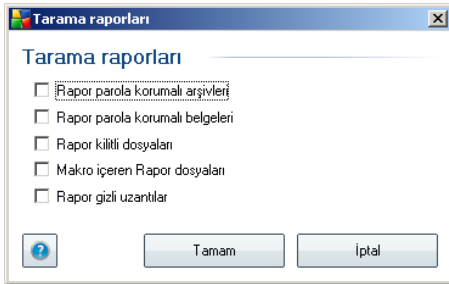
- İsteğe bağlı olarak, **Uzantıları olmayan dosyaları taramaya** da karar verebilirsiniz - bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmeniz önerilir. Uzantısı olmayan dosyalar süpheli olabilir ve her zaman taranmalıdır.

Tarama işlemi önceliği

Tarama işlemi önceliği bölümünde, sistem kaynakları kullanımına bağlı olarak istediğiniz tarama hızını seçebilirsiniz. Varsayılan olarak bu seçenek değeri, otomatik kaynak kullanımının ortalama düzeyine ayarlıdır. Tarama işleminin daha hızlı ilerlemesini istiyorsanız tarama işlemi daha kısa sürecektir fakat tarama işlemi sırasında sistem kaynakları oldukça yüklü bir şekilde kullanılacak ve bilgisayar üzerindeki diğer işlemleri yavaşlatacaktır (bu seçenek bilgisayarınız açıkken kullanılmadığı sırada seçilebilir). Öte yandan tarama süresini uzatarak da sistem kaynaklarının kullanımını azaltabilirsiniz.

Ek tarama raporlarını ayarla...

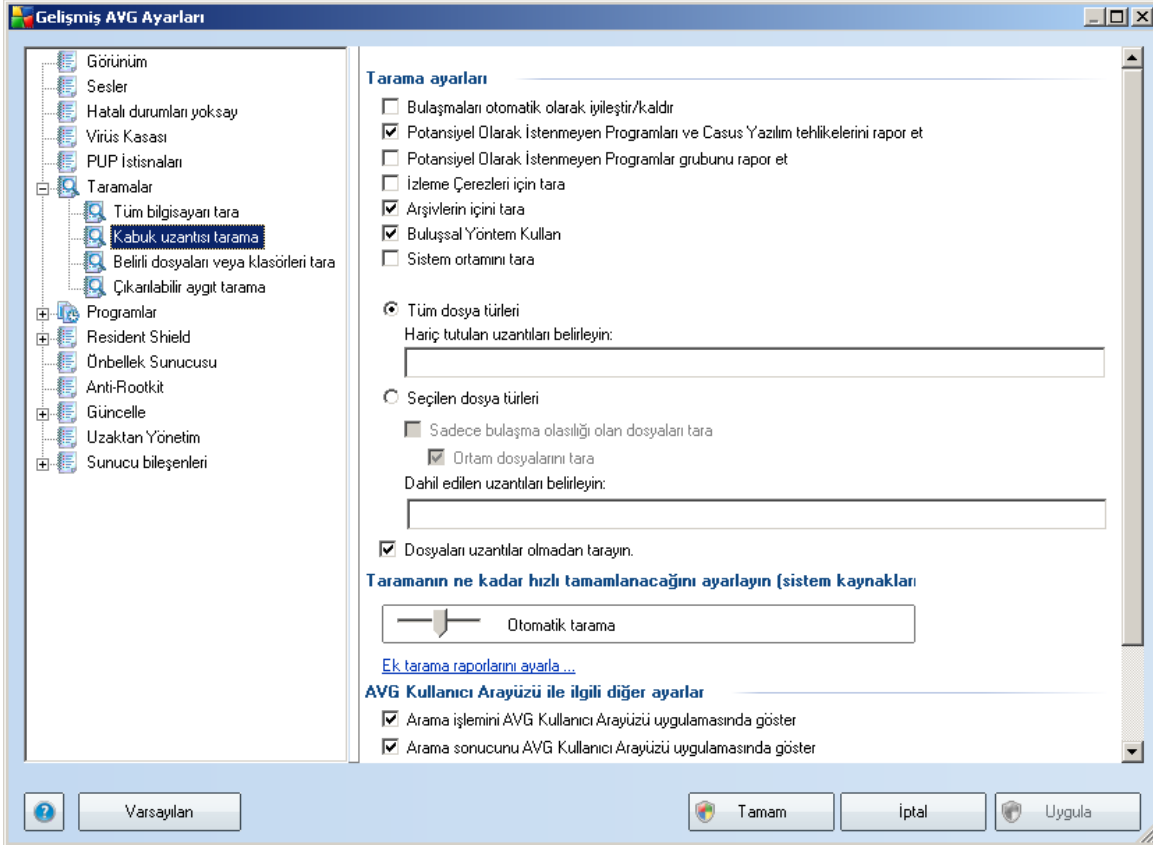
Diğer tarama raporlarını belirle... bağlantısına tıklayarak hangi tarama bulgularının rapor edileceğine ilişkin seçimleri yapabileceğiniz **Tarama raporları** iletişim kutusu penceresini açabilirsiniz:



10.6.2. Kabuk Uzantisi Tarama

Daha önce bahsettiğimiz **Tam bilgisayar taraması** ögesine benzer olan bu öge, **Kabuk uzantisi taraması** olarak adlandırılır ve yazılım satıcısı tarafından varsayılan olarak belirlenmiş tarama parametrelerine ek olarak çok daha fazla sayıda seçenek

sunar. Bu sefer, yapılandırma [doğrudan Windows Gezgini üzerinden baslatılan belirli nesnelerin taranması](#) esasına dayanmaktadır (*kabuk uzantisi*), **[Windows Gezgini'nde Tarama](#)** bölümüne bakın:



Parametre listesi, **[Tüm Bilgisayarı Tarama](#)** öğesinin parametre listesi ile aynıdır. Diğer bir yandan varsayılan ayarlar farklılık göstermektedir: **[Tüm Bilgisayar Taramasında](#)** parametrelerin çoğu seçilmiştir ancak **[Kabuk Uzantisi Taramasında \(Windows Gezgini Taraması\)](#)** sadece ilgili parametreler etkinleştirilmiştir.

Not: Belirli parametrelerin tanımlar hususunda bilgi almak için **[AVG Gelişmiş Ayarlar / Taramalar / Tüm Bilgisayar Taraması](#)** bölümünü inceleyin.

Ancak, yalnızca Kabuk Uzantisi Tarama'da görünen bazı parametreler de vardır. Bu parametreleri **AVG Kullanıcı Arayüzü ile İlgili Diğer Ayarlar** bölümünde bulabilirsiniz:

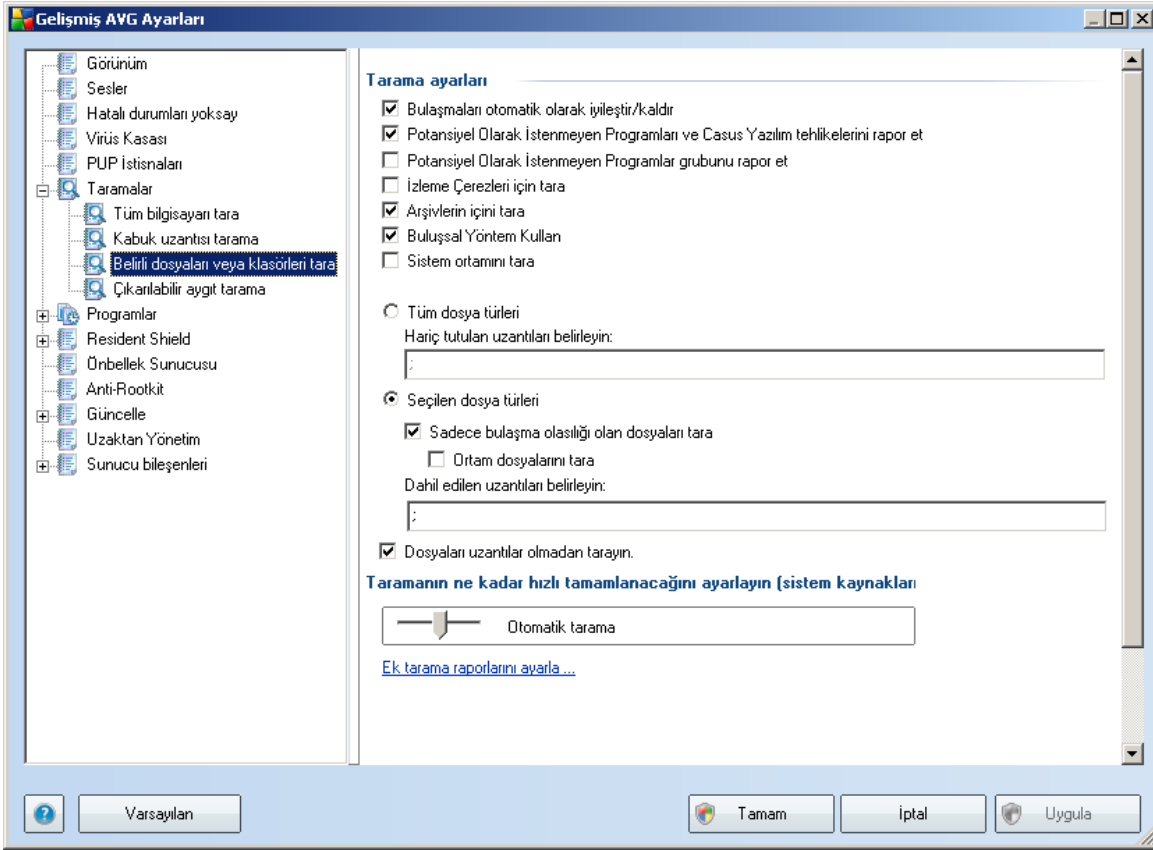
- **AVG Kullanıcı Arayüzü'nde tarama işlemini göster** - bu onay kutusu işaretlenirse, Kabuk Uzantisi Tarama her başladığında/bittiginde size bildirilir

(küçük bir bilgi baloncugu ekranin sag altinda görünecektir).

- **AVG Kullanici Arayüzü'nde tarama sonucunu göster** - bu kutu isaretlenirse, Kabuk Uzantisi Tarama her bittiginde, AVG Kullanici Arayüzü açilir ve standart [Tarama Sonuçlari Ayrıntilari](#) iletisim kutusu görünür (sekme sayisi gerçek tarama sonucuna baglidir).
 - **Yalnizca tarama sonucu bir tehlike içerirse** - bu kutu yalnizca önceki isaretliyse etkinlesir. Isaretlerseniz, [Tarama Sonuçlari Ayrıntilari](#) iletisim kutusu yalnizca Kabuk Uzantisi Tarama sirasinda bir tehlike bulunursa görünecektir.

10.6.3. Belirli Dosyalari veya Klasörleri Tara

Belirli dosya ya da klasörleri tara fonksiyonunun düzenleme arayüzü [Tüm Bilgisayar Taramasi](#) fonksiyonunun düzenleme penceresi ile aynidir. Tüm konfigürasyon seçenekleri aynidir; diger bir yandan [Tüm bilgisayar taramasi](#) için varsayilan ayarlar daha kesindir:

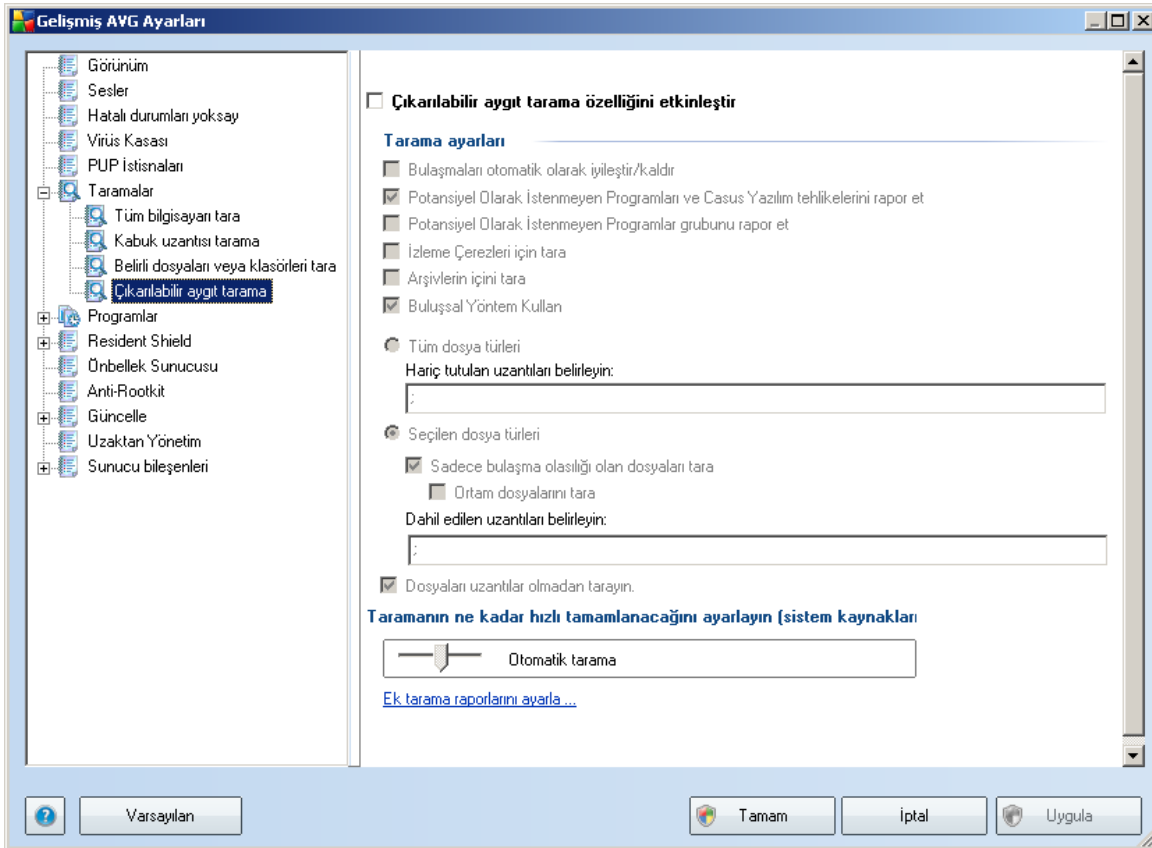


Bu yapılandırma iletişim kutusunda ayarlanan tüm parametreleri **[Belirli dosya ya da klasörleri tara](#)** ile tarama sırasında seçilen alanlar için geçerlidir!

Not: Belirli parametrelerin tanımlar hususunda bilgi almak için **[AVG Gelişmiş Ayarlar / Taramalar / Tüm Bilgisayar Taraması](#)** bölümünü inceleyin.

10.6.4. Çıkarılabilir Aygıt Tarama

Çıkarılabilir sürücü taraması'nin düzenleme arayüzü [Tüm Bilgisayar Taraması](#) düzenleme penceresine oldukça benzerdir:



Çıkarılabilir sürücü taraması bilgisayarınıza çıkarılabilir bir aygıt taktığınız anda otomatik olarak baslar. Öntanımlı olarak söz konusu tarama işlemi kapalıdır. Diğer bir yandan baslıca bulaşma kaynaklarından biri oldukları için söz konusu çıkarılabilir sürücülerin potansiyel tehditlere karşı taranması hayati önem taşımaktadır. Bu tarama özelliğinin istendiği zaman otomatik olarak baslatılacak şekilde hazır bulundurulması için **Çıkarılabilir aygıt taramasını etkinleştir** seçeneğini işaretleyin.

Not: Belirli parametrelerin tanımlar hususunda bilgi almak için [AVG Gelişmiş Ayarlar / Taramalar / Tüm Bilgisayar Taraması](#) bölümünü inceleyin.

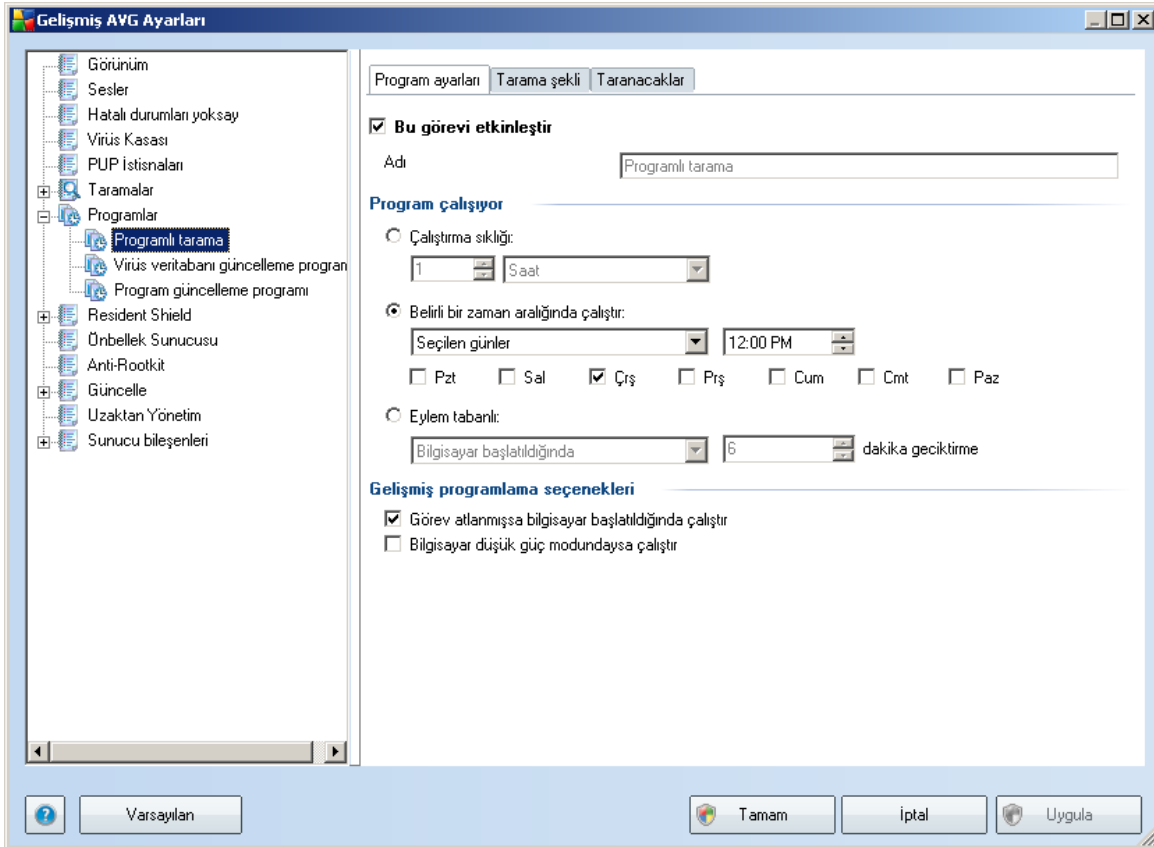
10.7. Programlar

Programlar bölümünde aşağıdaki bileşenlerin öntanımlı ayarlarını düzenleyebilirsiniz:

- [Tüm bilgisayar taraması programı](#)
- [Virüs veritabanı güncelleme programı](#)
- [Program güncelleme programı](#)

10.7.1. Programlı Tarama

Planlanan tarama parametreleri üç sekmeden düzenlenebilir: (*ya da yeni tarama planla*)



Planlama ayarlari sekmesinde **Bu görevi etkinlestir** ögesini isaretleyerek ya da isareti kaldırarak planlanan taramayı geçici olarak devre dışı bırakabilir ve ihtiyaç duyduğunuzda yeniden açabilirsiniz.

Daha sonra, **Ad** adındaki metin alanında (*tüm varsayılan programlamalar için devre dışı bırakılmış*) bu programlamaya program satıcı tarafından atanan ad bulunur. Yeni eklenen zamanlamalar için (*sol gezinti ağacındayken **Taramayı programla** ögesi üzerinde sağ tıklatarak* yeni bir zamanlama ekleyebilirsiniz) kendi adınızı belirtebilirsiniz ve bu durumda metin alanı düzenleme için açılacaktır. Programladığınız taramaları diğerlerinden kolaylıkla ayırmak için her zaman taramalarınıza kısa, açıklayıcı adlar vermeye çalışın.

Örnek: *Taramayı "Yeni Tarama" veya "Taramam" adıyla adlandırmanız uygun değildir çünkü bu adlar, taramanın fiilen neyi kontrol ettiğini açıklamaz. Diğer bir yandan "Sistem alanları taraması" oldukça açıklayıcı bir isim olacaktır. Ayrıca, taramanın adında söz konusu taramanın tam bilgisayar taraması ya da sadece seçilen dosya ya da klasörlerin taraması olup olmadığını belirtmenize gerek yoktur - taramalarınız [seçilen dosya ya da klasörleri tara](#) işlevinin farklı şekillerinden ibaret olacaktır.*

Bu iletişim kutusunda taramanın aşağıdaki parametrelerini de tanımlayabilirsiniz:

Program çalışıyor

Burada, yeni programlanan tarama başlatması için zaman aralıkları belirtebilirsiniz. Zamanlama belirli bir sürenin ardından tekrarlanan tarama başlatması ile (**Her ...'de bir**) ya da kesin bir tarih ve saat tanımlayarak (**Belirli bir zaman aralığında çalıştır ...**) veya tarama başlangıcıyla ilgili bir olay tanımlanarak (**Bilgisayarın başlatılmasıyla ilişkili eylem**) tanımlanabilir.

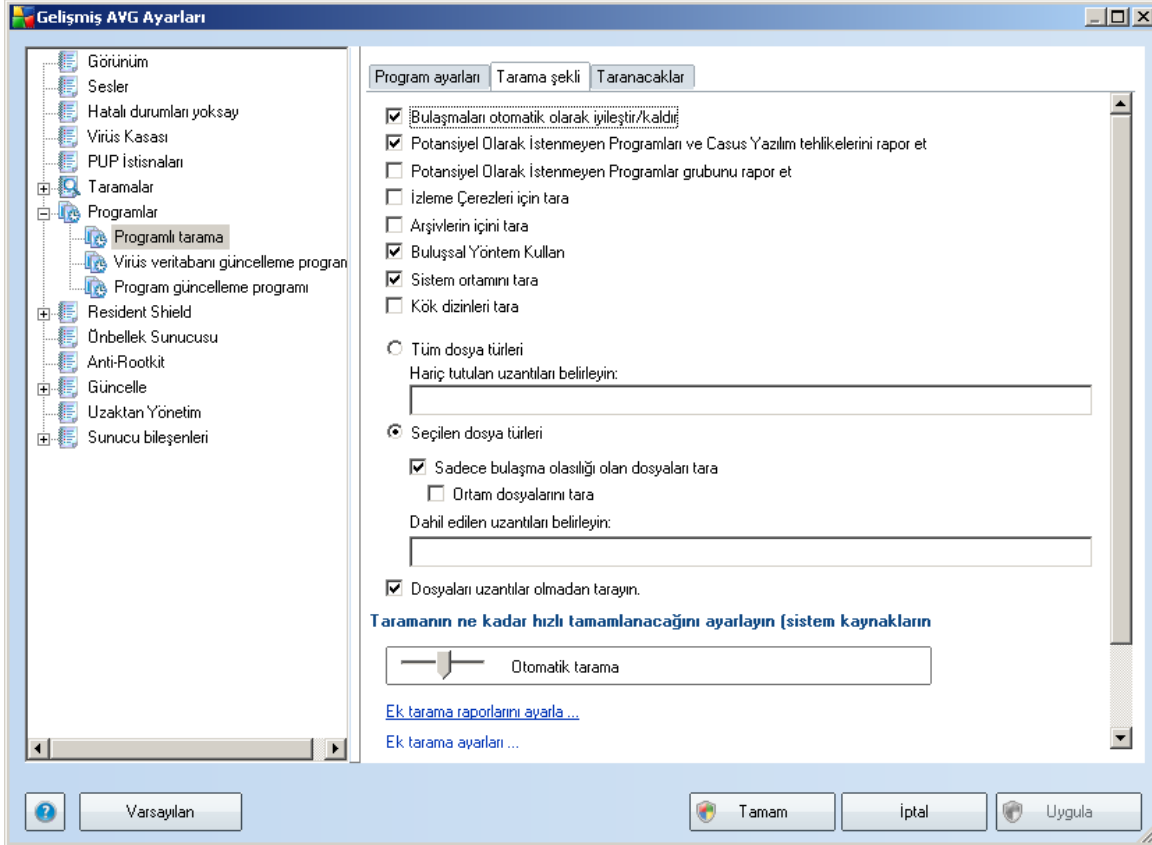
Gelişmiş programlama seçenekleri

Bu bölümde, bilgisayar düşük güç modundaydı ya da tamamen kapatılmışsa hangi koşullar altında taramanın başlatılması/baslatılmaması gerektiğini tanımlamanızı sağlar.

Programlanan tarama belirttiğiniz saatte başlatıldığında, [AVG sistem tepsi simgesi](#) üzerinde açılan bir açılır pencere ile bu konuda bilgilendirileceksiniz:



Bunun ardından [AVG sistem tepsisi simgesi](#) görüntülenir (üzerinde beyaz bir ok bulunur ve tamamen renklidir - yukarıdaki resme bakın)ve programlanan taramanın başladığını bildirir.



Tarama Sekli sekmesinde, isteğe bağlı olarak açılıp/kapatılabilen tarama parametrelerine ilişkin bir liste bulabilirsiniz. Varsayılan olarak birçok parametre devreye sokulur ve işlevsellik de tarama sırasında uygulanacaktır. Söz konusu ayarları değiştirmek açısından geçerli bir nedeniniz yoksa öntanımlı konfigürasyonu olduğu gibi muhafaza etmeniz önerilir:

- **Bulasmayı otomatik temizle/sil** - (varsayılan olarak açıktır): tarama işlemi sırasında bir virüs tanımlanırsa ve temizlenmesi mümkün ise otomatik olarak temizlenir. Etkilenen dosya otomatik olarak silinmiyorsa ya da bu seçeneği kapatmayı seçerseniz bir virüs tespit edildiğinde bilgilendirileceksiniz ve tespit edilen bulaşma hakkında ne yapılacağına karar vermek zorunda kalacaksınız. Önerilen işlem, bulaşmış dosyayı [Virüs Kasasına](#) kaldırmaktır.

- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım Tehlikelerini Rapor Et** - (varsayılan olarak açıktır): Bu parametre [potansiyel olarak istenmeyen programların algılanmasını](#) (casus yazılım veya reklam yazılımı olarak çalıştırılabilen çalıştırılabilir dosyalar) sağlayan ve bunları engelleyebilen veya kaldırılabilen *Virüsten Koruma* işlevselliğini kontrol eder;
- **Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et** - (varsayılan olarak kapalıdır): bu parametre [casus yazılım](#): doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılan programların genişletilmiş paketini algılamaya izin verir. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir - bu yüzden varsayılan olarak kapalıdır;
- **Tanımlama Bilgilerini Tara** - (varsayılan olarak kapalıdır): [Casus Yazılımdan Koruma](#) bileşeninin bu parametresi, tarama sırasında tespit edilmesi istenen tanımlama bilgilerini tanımlar (*HTTP tanımlama bilgileri site tercihleri ya da elektronik alışveriş sepeti içeriği gibi kullanıcı hakkında belirli bilgilerin toplanması, temin edilmesi ve izlenmesi için kullanılır*)
- **Arsivleri Tara** - (varsayılan olarak kapalıdır): Bu parametreler, tarama işleminin ZIP, RAR gibi belirli bir arşiv türü ile sıkıştırılmış olsa bile tüm dosyaları taramasını öngörür.
- **Bulgusal Analiz Kullan** - (varsayılan olarak açıktır): bulgusal analiz (*taranan nesnenin sanal bir bilgisayar ortamında dinamik olarak canlandırılması'na ilişkin talimatlar*) tarama sırasında kullanılacak virüs tespiti yöntemlerinden birisidir;
- **Sistem ortamını tara** - (varsayılan olarak açıktır): tarama işlemi, bilgisayarınızın sistem alanlarını da kontrol edecektir;
- **Rootkit'leri tara** - Tam bilgisayar taraması yaparken rootkit tespitini de yapabilmek için bu öğeyi işaretleyin. Rootkit tespiti işlemi [Anti-Rootkit](#) bileşeninden de yapabilirsiniz;

Ayrıca, taramak isteyip istemediğinize karar vermelisiniz

- **Tüm dosya türleri** taranmaması gereken virgülle ayrılmış dosya uzantılarının listesini sağlayarak taramada istisnaları tanımlama seçeneğiyle;
- **Seçili dosya türleri** - Yalnızca virüs bulaşabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulaşmayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya bazı diğer çalıştırılmayan dosyalar*); ortam dosyaları (*video, ses dosyaları - bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulaşma olasılıkları çok az olduğundan tarama süresini daha da azaltır*). Tekrar, her zaman taranması

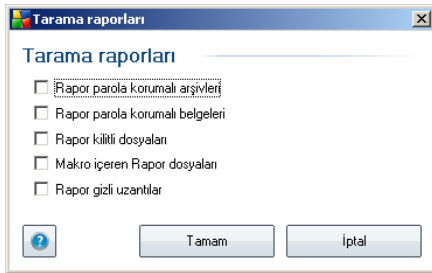
gereken dosyaları uzantılarına göre belirtebilirsiniz.

- İsteğe bağlı olarak, **Uzantıları olmayan dosyaları taramaya** da karar verebilirsiniz - bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmeniz önerilir. Uzantısı olmayan dosyalar süpheli olabilir ve her zaman taranmalıdır.

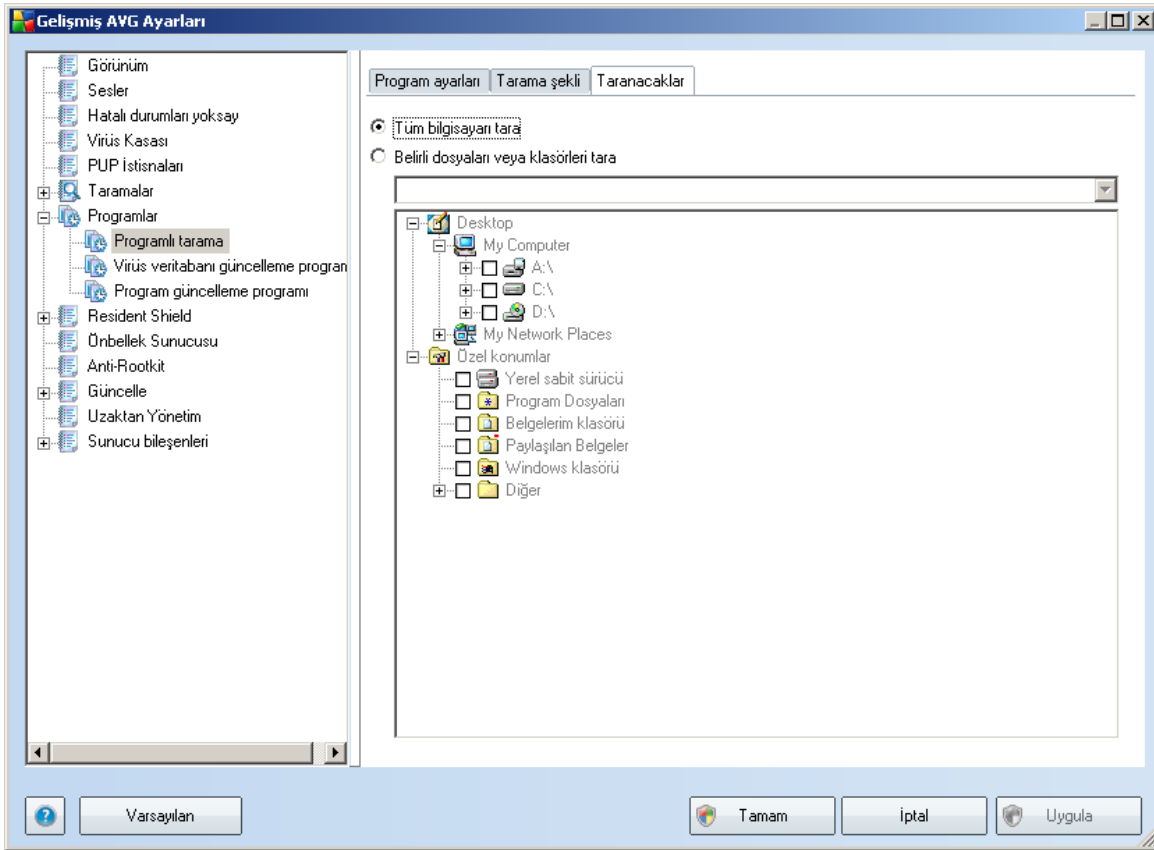
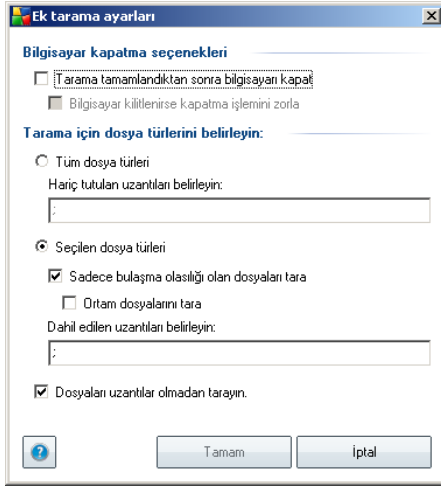
Tarama işlemi önceliği

Tarama işlemi önceliği bölümünde, sistem kaynakları kullanımına bağlı olarak istediğiniz tarama hızını seçebilirsiniz. Varsayılan olarak bu seçenek, otomatik kaynak kullanımının ortalama düzeyine ayarlıdır. Tarama işleminin daha hızlı ilerlemesini istiyorsanız tarama işlemi daha kısa sürecektir fakat tarama işlemi sırasında sistem kaynakları oldukça yüklü bir şekilde kullanılacak ve bilgisayar üzerindeki diğer işlemleri yavaşlatacaktır (*bu seçenek bilgisayarınız açıkken kullanılmadığı sırada seçilebilir*). Öte yandan tarama süresini uzatarak da sistem kaynaklarının kullanımını azaltabilirsiniz.

Diger tarama raporlarını belirle... bağlantısına tıklayarak hangi tarama bulgularının rapor edileceğine ilişkin seçimleri yapabileceğiniz **Tarama raporları** iletişim kutusu penceresini açabilirsiniz:

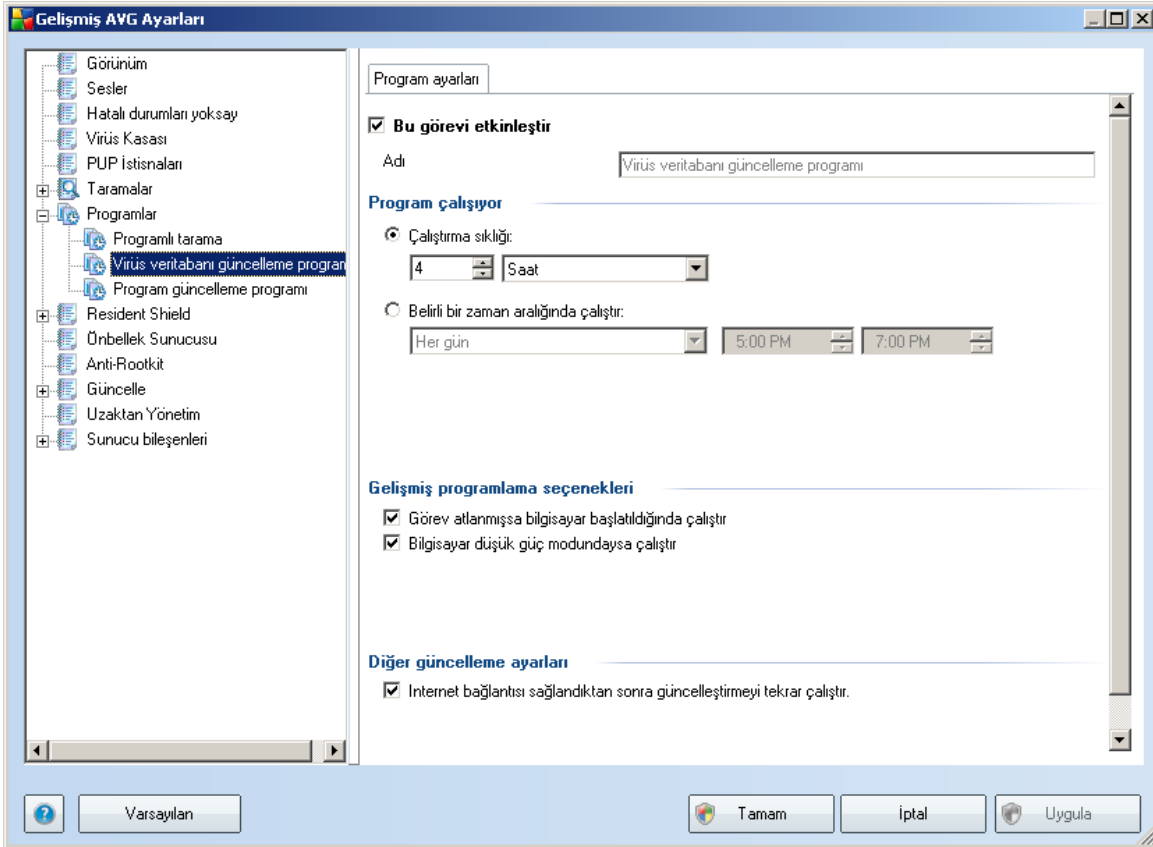


Ekstra tarama ayarları'na tıklamak yeni bir **Bilgisayar Kapatma seçenekleri** iletişim kutusunu açar. Burada tarama işlemi bittikten sonra bilgisayarın otomatik olarak kapanmasını ayarlayabilirsiniz. Bu seçeneği seçerseniz (**Tarama bittikten sonra bilgisayarı kapat**) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (**Bilgisayar kilitliyse bilgisayarı kapanmaya zorla**).



Taranacaklar sekmesinde, [tüm bilgisayarı tarama](#) veya [belirli dosya veya klasörleri taramayı](#) programlamak isteyip istemediğinizi belirleyebilirsiniz. Belirli dosya ve klasörleri taramayı seçerseniz, bu iletişim penceresinin alt kısmında görüntülenen ağaç yapısı etkinleşir ve taranacak klasörleri seçebilirsiniz.

10.7.2. Virüs Veritabanı Güncelleme Programı



Program ayarları sekmesinde **Bu görevi etkinleştir** ögesini işaretleyerek ya da işareti kaldırarak programlı virüs veritabanı güncellemesini geçici olarak devre dışı bırakabilir ve ihtiyaç duyduğunuzda yeniden açabilirsiniz.

Temel virüs veritabanı güncelleme programlama işlemi **Güncelleme Yöneticisi** bileşeni kapsamında açıklanmıştır. Bu iletişim kutusunda virüs veritabanı güncelleme planı parametrelerinden bazılarını ayrıntılarıyla yapılandırabilirsiniz:

Ad adındaki metin alanında (*tüm varsayılan programlamalar için devre dışı bırakılmış*) bu programlamaya program satıcısı tarafından atanan ad bulunur. Yeni eklenen

zamanlamalar için (*sol gezinti ağacındayken **Virüs veritabanı güncelleme zamanlaması** ögesi üzerinde sağ tıklatarak yeni bir zamanlama ekleyebilirsiniz*) kendi adınızı belirtebilirsiniz ve bu durumda metin alanı düzenleme için açılacaktır. Daha sonra kolaylıkla hatırlayabilmek için her zaman kısa, açıklayıcı ve zamanlamalarınıza uygun adlar kullanmaya çalışın.

Program çalışıyor

Bu bölümde, yeni programlanan virüs veritabanı güncellemesini başlatmak için zaman aralıkları belirtin. Zamanlama belirli bir sürenin ardından tekrarlanan güncelleme ile (**Her ...'de bir**) ya da kesin bir tarih ve saat tanımlayarak (**Belirli bir saatte çalıştır...**), ya da (**Bilgisayar başlangıcında**) ilgili bir programın güncellemesiyle tanımlanabilir.

Gelişmiş programlama seçenekleri

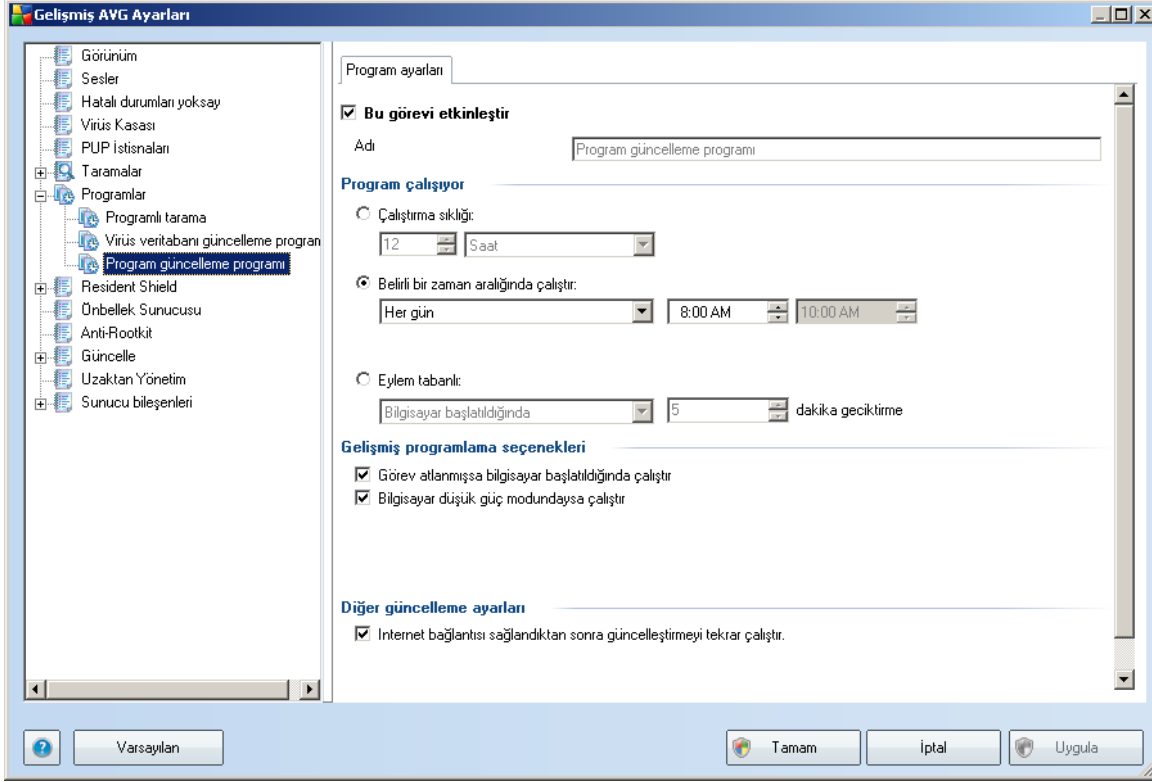
Bu bölümde, bilgisayar düşük güç modundaydı veya tamamen kapatılmışsa hangi koşullar altında virüs veritabanı güncellemesinin başlatılması/baslatılmaması gerektiğini belirleyebilirsiniz.

Diğer güncelleme ayarları

Son olarak, **İnternet bağlantısı kurulduktan sonra güncellemeyi yeniden çalıştır** seçeneğini işaretleyerek İnternet bağlantısı bozulduğunda ve güncelleme işlemi başarısız olduğunda, İnternet bağlantısı yeniden sağlanır sağlanmaz yeniden başlatıldığından emin olun.

Programlı güncelleme işlemi sizin belirlediğiniz tarih ve saatte başladıktan sonra [AVG sistem tepsisi simgesi](#) üzerinde açılan bir açılır pencere vasıtasıyla bilgilendirileceksiniz (**Gelişmiş Ayarlar/Görünüm** iletişim kutusunun varsayılan yapılandırmasını *değiştirmemiş olmanız kaydıyla*).

10.7.3. Program Güncelleme Planı



Planlama ayarları sekmesinde **Bu görevi etkinleştir** ögesini işaretleyerek ya da işareti kaldırarak programlı güncellemesini geçici olarak devre dışı bırakabilir ve ihtiyaç duyduğunuzda yeniden açabilirsiniz.

Ad adındaki metin alanında (tüm varsayılan programlamalar için devre dışı bırakılmış) bu programlamaya program satıcısı tarafından atanan ad bulunur. Yeni eklenen zamanlamalar için (sol gezinti ağacındayken **Program güncelleme zamanlaması** ögesi üzerinde sağ tıklayarak yeni bir zamanlama ekleyebilirsiniz) kendi adınızı belirtebilirsiniz ve bu durumda metin alanı düzenleme için açılacaktır. Daha sonra kolaylıkla hatırlayabilmek için her zaman kısa, açıklayıcı ve zamanlamalarınıza uygun adlar kullanmaya çalışın.

Program çalışıyor

Burada, yeni programlanan program güncellemesinin başlaması için zaman aralıklarını girin. Zamanlama belirli bir sürenin ardından tekrarlanan güncelleme ile (**Her ...'de bir**)

ya da kesin bir tarih ve saat tanımlayarak (**Belirli bir saatte çalıştır...**) ya da (**Bilgisayar başlangıcında**) ilgili bir programın güncellemesiyle tanımlanabilir.

Gelismis programlama seçenekleri

Bu bölümde, bilgisayar düşük güç modundaydı veya tamamen kapatılmışsa hangi koşullar altında program güncellemesinin başlatılması/baslatılmaması gerektiğini belirleyebilirsiniz.

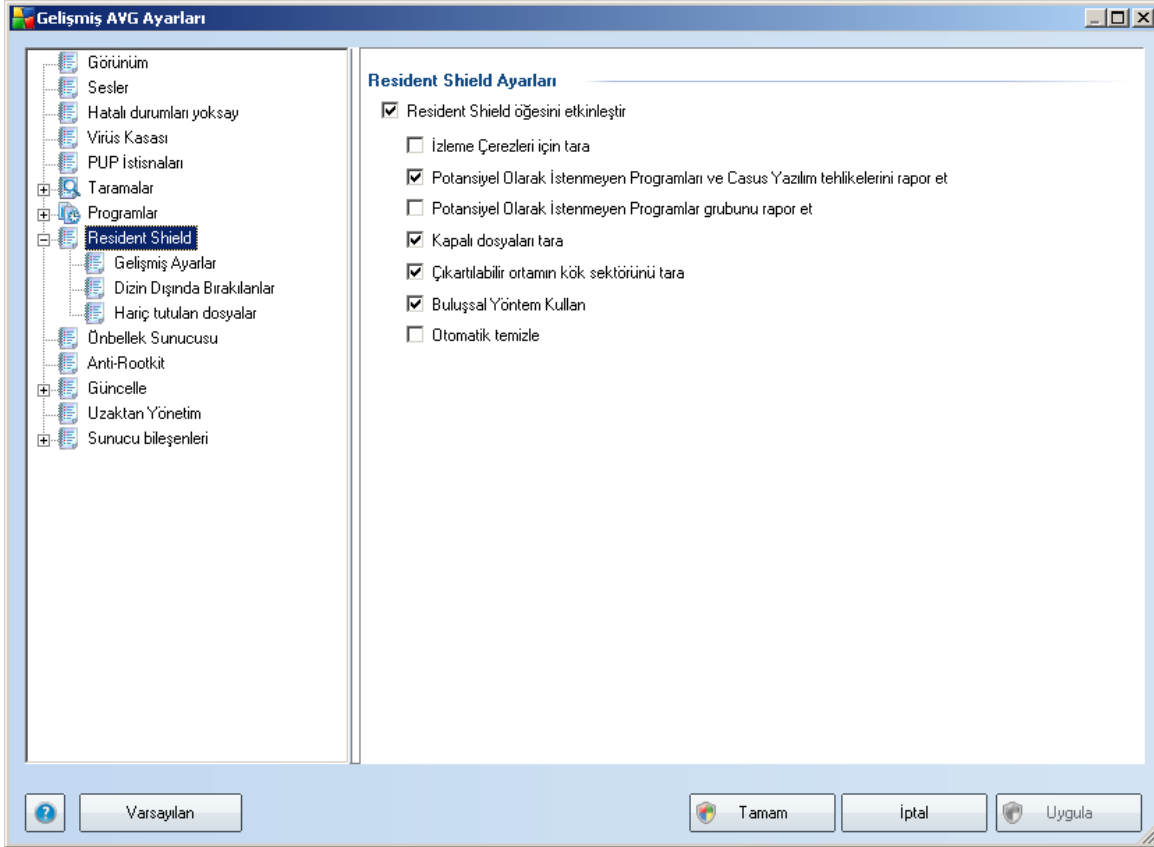
Diğer güncelleme ayarları

İnternet bağlantısı kurulduktan sonra güncellemeyi yeniden çalıştır seçeneğini işaretleyerek İnternet bağlantısı bozulduğunda ve güncelleme işlemi başarısız olduğunda, İnternet bağlantısı yeniden sağlanır sağlanmaz yeniden başlatıldığından emin olun.

Programlı güncelleme işlemi sizin belirlediğiniz tarih ve saatte başladıktan sonra [AVG sistem tepsi simgesi](#) üzerinde açılan bir açılır pencere vasıtasıyla bilgilendirileceksiniz (**[Gelismis Ayarlar/Görünüm](#)** iletişim kutusunun varsayılan yapılandırmasını değiştirmemiş olmanız kaydıyla).

10.8. Yerlesik Kalkan

Yerlesik Kalkan bileşeni, dosya ve klasörlerinizi çevrimiçi ortamda virüslere, casus yazılımlar ve diğer kötü amaçlı yazılımlara karşı korur.



Yerlesik Kalkan Ayarları iletişim kutusunda **Yerlesik Kalkan** korumasını **Yerlesik Kalkanı Etkinleştir** ögesini işaretleyerek ya da işaretini kaldırarak etkinleştirebilir ya da devre dışı bırakabilirsiniz (*bu seçenek varsayılan olarak açıktır*). Buna ek olarak **Yerlesik Kalkan** hangi özelliklerinin etkinleştirileceğini de seçebilirsiniz:

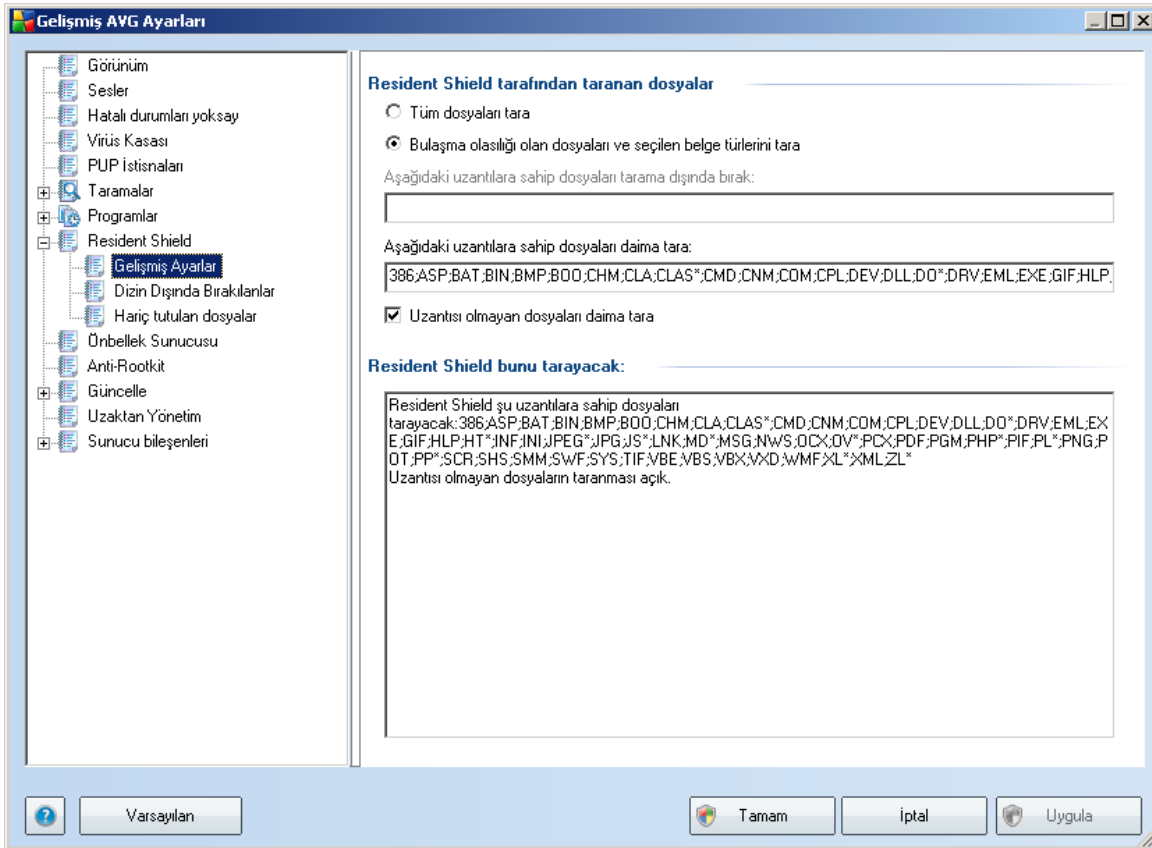
- **Tanımlama bilgilerini izlemek için tara** - bu parametre, tanımlama bilgilerinin tarama işlemi sırasında tespit edilmesi gerektiğini belirtir. (*HTTP tanımlama bilgileri, site tercihleri veya elektronik alışveriş sepetlerinin içerikleri gibi kullanıcılar hakkındaki belirli bilgilerin kimliklerinin doğrulanması, takibi ve sürdürülmesi için kullanılır.*)
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım Tehlikelerini**

Rapor Et- (varsayilan olarak aıktir) [Potansiyel olarak istenmeyen programlari](#) (casus yazilim ya da reklam yazilimi gibi davranan alistirilabilir uygulamalar) tarar

- **Potansiyel Olarak Istenmeyen Programlar gelismis grubunu rapor et** - (varsayilan olarak kapalidir) dogrudan üreticiden alınan tamamen zararsiz olan, ancak daha sonra kötüye kullanılan programlar olan genişletilmiş [casus yazilim](#) paketini algılar. Bu, bilgisayar güvenliğini daha da artıran ek bir önlemdir, ancak yasal programlari da engelleyebilir - bu yüzden varsayilan olarak kapalidir;
- **Islem sonunda tara** - islem sonunda tarama, AVG'nin etkin nesneleri hem açılırlarken hem de kapatılırlarken taradığından emin olmanizi sağlar. Bunun yanı sıra bu özellik, bilgisayarınızı karmaşık virüslere karşı korumaniza da yardımcı olur
- **ıkarılabilir ortamlarin önyükleme kesimini tara** - (varsayilan olarak aıktir)
- **Bulgusal Analiz Kullan** - (varsayilan olarak aıktir) [bulgusal analiz](#), tespit etme islemi sırasında kullanılır(*taranan nesne'nin komutlarının sanal bilgisayar ortamında dinamik olarak canlandırılması*)
- **Otomatik Temizle** - tespit edilen bulasmalar, temizleme yöntemi mevcut ise otomatik olarak temizlenir.

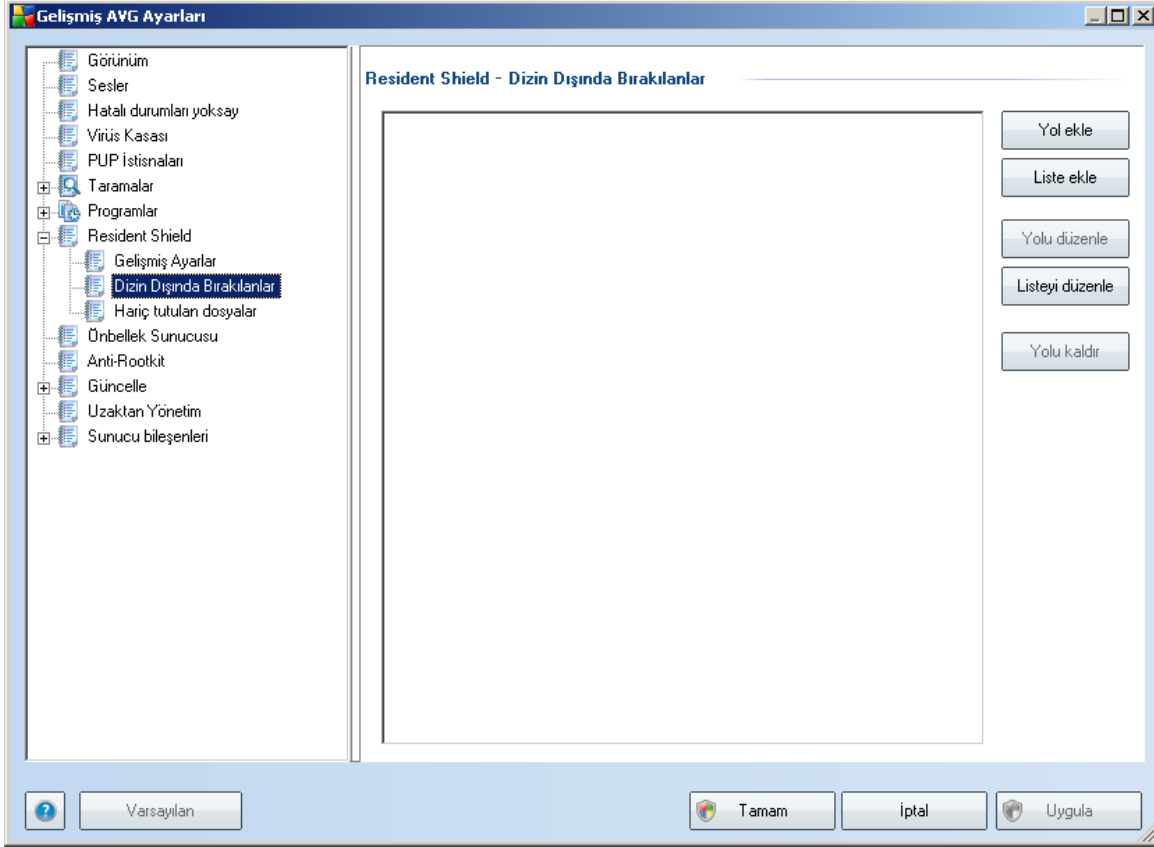
10.8.1. Gelişmiş Ayarlar

Yerlesik Kalkan tarafından taranan dosyalar penceresinde taranan dosyaların yapılandırılması mümkündür (*belirli dosya uzantılarına göre*):



Tüm dosyaların mı yoksa sadece bulaşmış dosyaların mı taranacağına karar verin - Bunun ardından tarama işlemi sırasında hariç tutulacak dosyaları tanımlayan dosya uzantısı listesini de seçebilirsiniz, bunun yanı sıra her ne şart altında olursa olsun taranmasını istediğiniz dosyaları tanımlayan dosya uzantılarını gösteren bir liste de oluşturabilirsiniz.

10.8.2. Hariç Tutulan Dizin



Yerlesik Kalkan - İstisnalar Dizini iletişim kutusu [Yerlesik Kalkan](#) taraması sırasında hariç tutulacak klasörleri seçebilmenizi sağlar.

Gerekli değildir dolayısıyla dizinlerin tarama işleminden çıkartılmasını kesinlikle önermiyoruz!

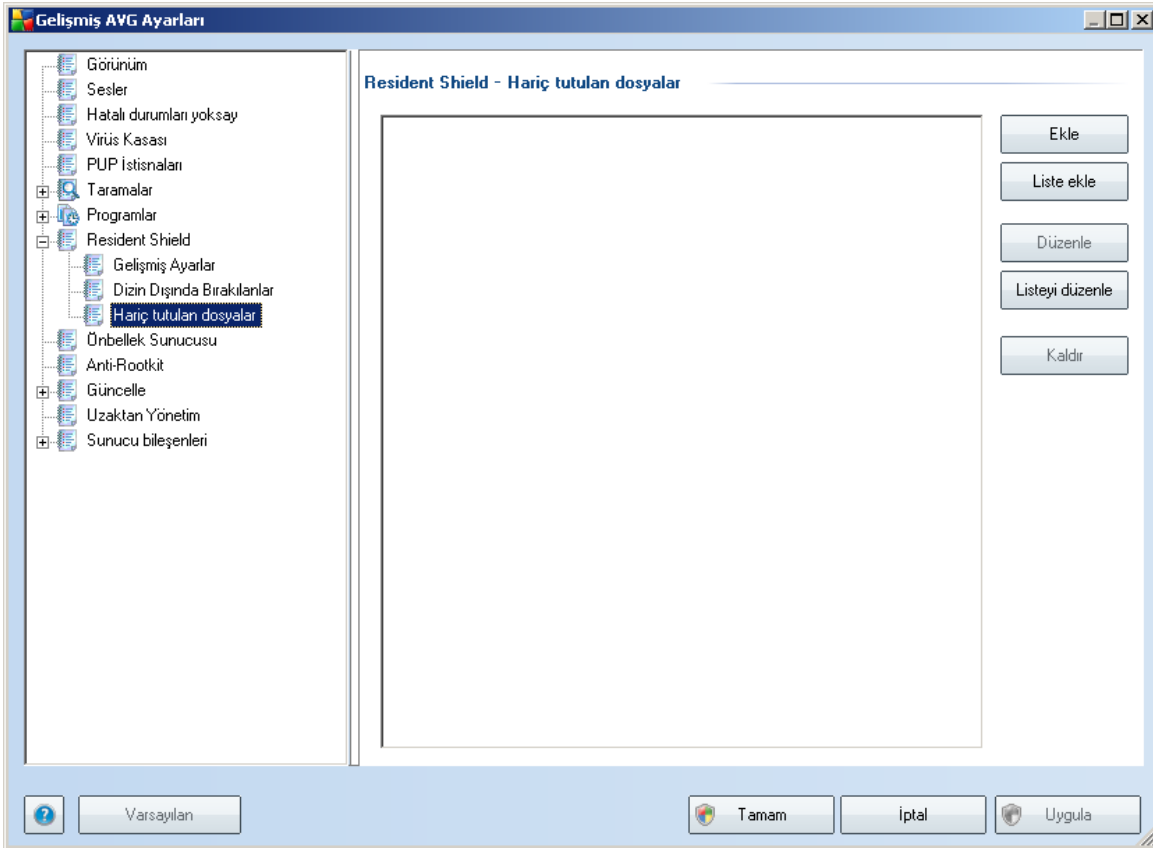
İletişim kutusunda aşağıdaki kontrol düğmeleri bulunur:

- **Veriyolu ekle**– yerel diskin dolayım ağacından teker teker seçmek suretiyle tarama işleminden hariç tutulacak dizinleri belirleyin.
- **Liste ekle**– [Yerlesik Kalkan](#) taramasından hariç tutulacak dizinlere ilişkin tam bir liste hazırlayabilmenizi sağlar
- **Veriyolunu düzenle**– seçilen klasöre giden veriyolunu düzenleyebilmenizi

saglar.

- **Listeyi düzenle**– klasör listesini düzenleyebilmenizi saglar.
- **Veriyolunu sil**– listeden seçilen klasöre giden yolu silebilmenizi saglar.

10.8.3. Hariç Tutulan Dosyalar



Yerlesik Kalkan - Hariç tutulan dosyalar iletisim kutusu önceden tanımlanan [Yerlesik Kalkan - Hariç Tutulan Dizin](#) olarak davranir, ancak klasörler yerine şimdi [Yerlesik Kalkan](#) taramasından hariç tutulacak belirli dosyaları tanımlayabilirsiniz.

Gerekmiyorsa, dosyaların hariç tutulmasını kesinlikle önermiyoruz!

İletisim kutusunda aşağıdaki kontrol düğmeleri bulunur:

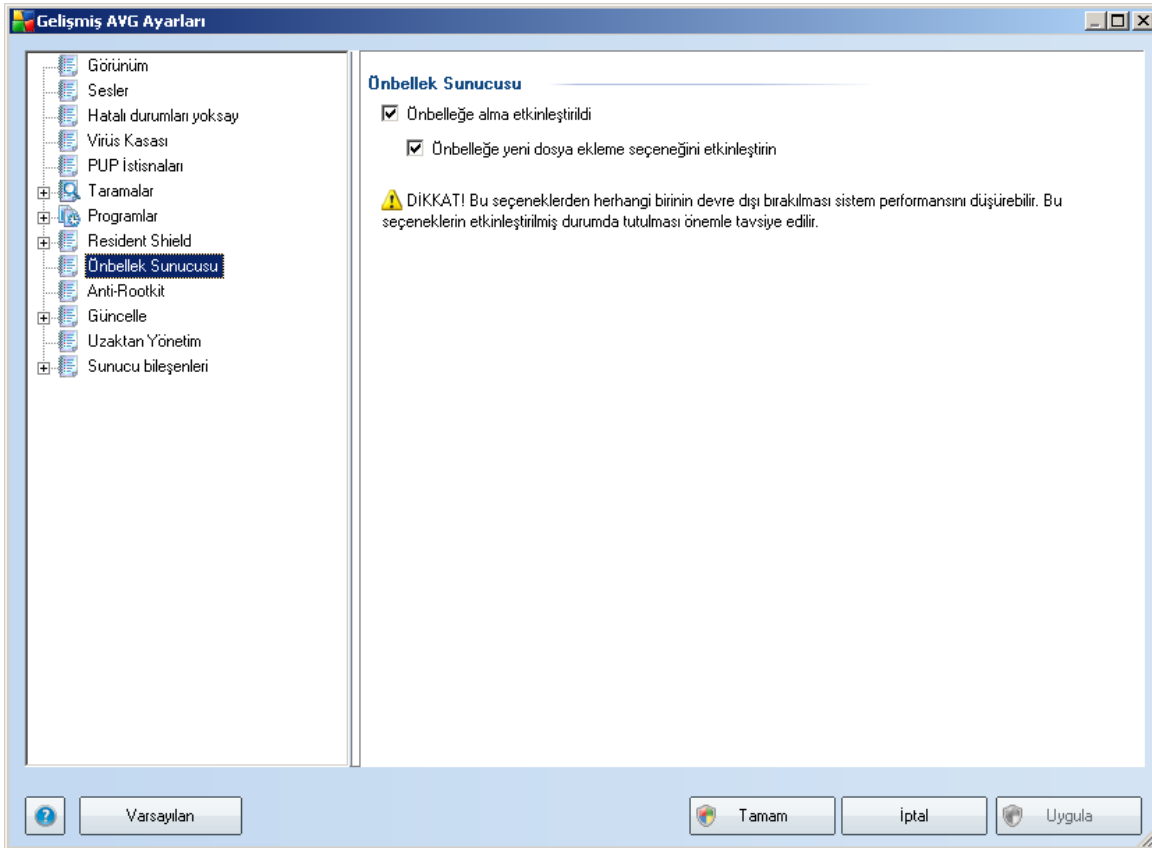
- **Ekle** – yerel diskin dolayım ağacından teker teker seçmek suretiyle tarama

isleminden hariç tutulacak dosyaları belirleyin.

- **Liste ekle**– [Yerlesik Kalkan](#) taramasından hariç tutulacak dosyalara ilişkin tam bir liste hazırlayabilmenizi sağlar
- **Düzenle** – seçilen dosyaya giden yolu düzenleyebilmenizi sağlar
- **Listeyi düzenle** – dosya listesini düzenlemenizi sağlar
- **Sil**– listeden seçilen dosyaya giden yolu silmenizi sağlar

10.9. Önbellek Sunucusu

Önbellek Sunucusu, herhangi bir taramayı hızlandırmak için tasarlanmış bir işlemidir (*istek üzerine tarama, programlanmış tüm bilgisayarı tarama, [Yerlesik Kalkan](#) taraması*). Güvenilir dosyaların bilgilerini toplar ve saklar (*dijital imzalı sistem dosyaları vb.*): Bu dosyalar, daha sonra güvenli olarak ele alınırlar ve tarama sırasında atlanırlar.

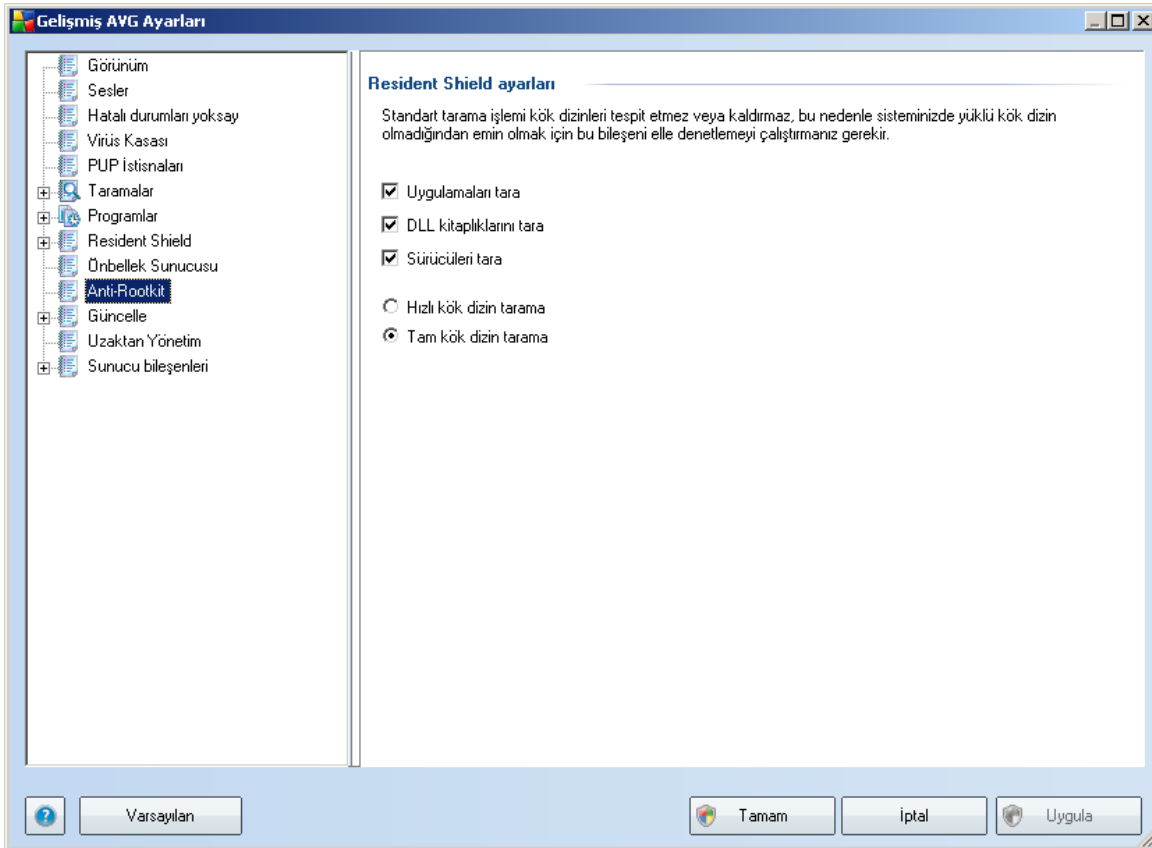


Ayarlar iletişim kutusu iki seçenek sunar:

- **Önbelleğe alma etkin** (varsayılan olarak açıktır) - **Önbellek Sunucusu**'nu kapatmak için kutunun isareti kaldırın ve önbellek belleğini boşaltın. Lütfen, kullanımdaki her bir dosya virüs ve casus yazılım için ilk kez taranacağından taramanın yavaş olabileceğini ve bilgisayarınızın genel performansının azalacağını unutmayın.
- **Önbelleğe yeni dosyaların eklenmesini etkinleştir** (varsayılan olarak açıktır) - önbelleğe daha fazla dosya eklenmesini durdurmak için kutunun isaretini kaldırın. Önceden önbelleğe alınmış her dosya korunacak ve önbelleğe alma tamamen kapatılıncaya kadar veya virüs veritabanının bir sonraki güncellenmesine kadar kullanılacaktır.

10.10. Anti-Rootkit

Bu iletişim kutusunda **Anti-Rootkit** bileşenlerinin yapılandırmasını düzenleyebilirsiniz:





İletişim kutusu içinde sağlanan [Anti-Rootkit](#) bileşenin tüm işlevlerinin düzenlenmesine [Anti-Rootkit bileşenin arayüzünden](#) de ulaşabilirsiniz.

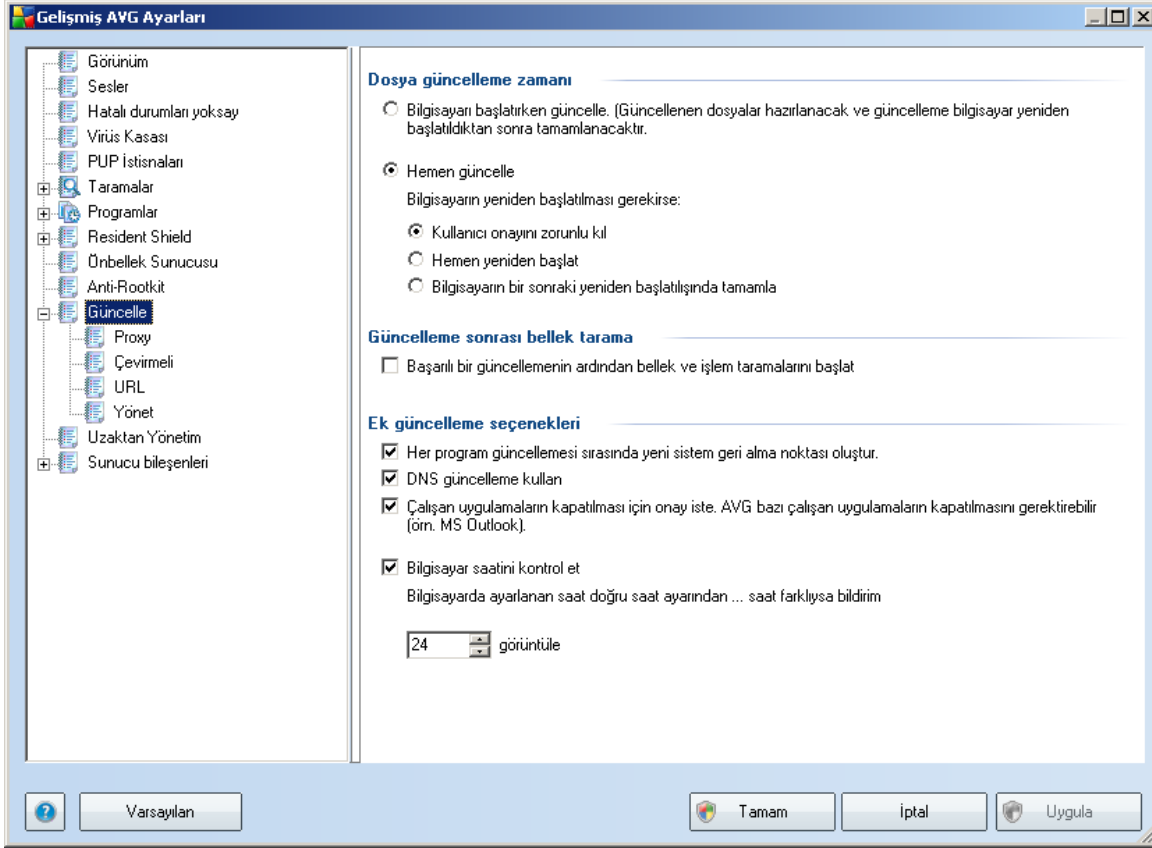
Taranmasını istediğiniz nesnelere belirlemek üzere ilgili kutuları işaretleyin:

- **Uygulamaları tara**
- **DLL kitaplıklarını tara**
- **Sürücülerini tara**

Bunun ardından kök kullanıcı tarama modunu da seçebilirsiniz:

- **Hızlı kök kullanıcı takımı (rootkit) tarama** : yalnızca sistem klasörünü tarar (tipik olarak c:\Windows)
- **Tam kök kullanıcı takımı (rootkit) tarama**: A: ve B: disindeki tüm erişilebilir disk sürücülerini tarar

10.11. Güncelle



Güncelle navigasyonu ögesi, [AVG güncellemesine](#) ilişkin genel parametreleri belirleyebileceğiniz yeni bir iletişim kutusu açar:

Dosya güncelleme zamanı

Bu bölümde iki seçenek arasında seçim yapabilirsiniz: [güncelleme](#) bir sonraki bilgisayar açılışında yapılabilir ya da [güncellemeyi](#) hemen başlatabilirsiniz. Varsayılan olarak hemen güncelleme seçeneği seçilmiştir çünkü AVG bu şekilde maksimum güvenlik seviyesini temin edebilir. Güncellemenin bir sonraki bilgisayar açılışında gerçekleştirilmesi, ancak bilgisayarınızın günde en az bir kere açıldığından emin olduğunuz durumlarda önerilir.

Tüm varsayılan konfigürasyonu muhafaza etmek ve güncelleme işlemini hemen başlatmak istiyorsanız gerekli yeniden başlatma işleminin hangi şartlar altında gerçekleştirileceğini belirleyebilirsiniz:

- **Kullanıcının onayını iste-** [işlemini tamamlamak üzere bilgisayarın yeniden başlatılacağını onaylamanız istenir](#)
- **Hemen yeniden başlat** - [güncelleme](#) işlemi tamamlanır tamamlanmaz onayınız istenmeden bilgisayarınız yeniden başlatılacaktır.
- **Bir sonraki bilgisayar başlangıcında tamamla** - [güncelleme işleminin](#) sonlandırılması bir sonraki bilgisayar açılışına ertelenecektir - aynı şekilde bu işlem, bilgisayarınızın günde en az bir kere açıldığından emin olduğunuz durumlarda önerilir.

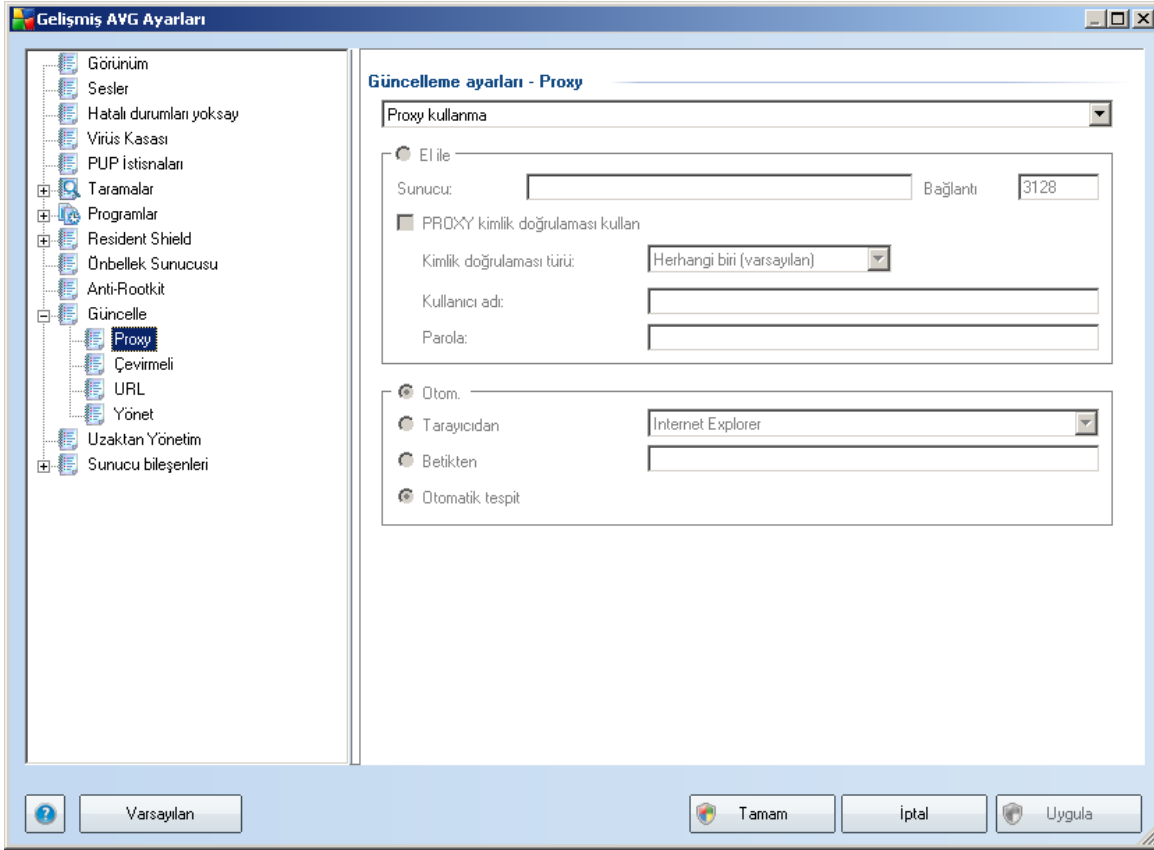
Güncelleme sonrası bellek tarama

Basarıyla tamamlanan her güncelleme sonrasında yeni bir bellek taraması başlatmak istediğinizi tanımlamak için bu onay kutusunu işaretleyin. En son indirilen güncelleme yeni virüs tanımlarını içerebilir ve bunlar taramaya hemen uygulanır.

Ek güncelleme seçenekleri

- **Her program güncellemesinden sonra sistem geri yükleme noktası olustur** - AVG programının güncelleme işlemi başlamadan önce geri yükleme noktası oluşturulur. Güncelleme işleminin başarısız olması ve işletim sisteminizin çökmesi halinde işletme sisteminizi bu noktaya geri döndürebilirsiniz. Bu seçeneğe Baslat/Tüm Programlar bilgisayarınızın günde en az bir kere açıldığından emin olduğunuz durumlarda önerilir/Donatılar /Sistem Araçları / Sistem Geri Yükleme menüsünden erişebilirsiniz fakat değişikliklerin sadece uzman kullanıcılar tarafından yapılması önerilmektedir! Bu fonksiyonu kullanmak istiyorsanız bu kutucuğu işaretleyin.
- **DNS güncellemesini kullan** - güncelleme sunucusu ile AVG istemcisi arasında aktarılan veri miktarını minimize eden güncelleme dosyalarını tespit etme yöntemini kullanmak istediğinizi onaylamak için bu kutucuğu işaretleyin;
- **Çalışan uygulamaları kapatmak için onay iste** (varsayılan olarak açıktır) güncelleme işleminin tamamlanması için gerekirse izniniz olmaksızın geçerli olarak çalışan uygulamaların kapatılmamasını sağlayacaktır;
- **Bilgisayar saatini kontrol et** - bilgisayar saati ile doğru saat arasındaki fark belirlenen süreden uzun olduğunda bilgilendirilmek isterseniz bu seçeneği işaretleyin.

10.11.1. Proxy



Proxy sunucusu, İnternet'e daha güvenli bir şekilde bağlanmanızı sağlayan bağımsız bir sunucu ya da bilgisayarınızda çalışan bir hizmet programıdır. Belirlenen ağ kuralları doğrultusunda, İnternet'e doğrudan ya da bir proxy sunucusu üzerinden ulaşabilirsiniz; aynı anda her iki işleme de izin verilir. Bunun ardından **Güncelleme ayarları- Proxy** iletişim kutusunun ilk ögesinden aşağıdaki seçimleri yapmanız gerekmektedir:

- **Proxy kullan**
- **Proxy sunucusu kullanma** - varsayılan ayarlar
- **Proxy kullanarak bağlanmayı dene; başarısız olursa doğrudan bağlan**

Proxy sunucusunu kullanan herhangi bir seçeneği seçerseniz daha ayrıntılı bilgi girmeniz istenecektir. Sunucu ayarları manuel ya da otomatik olarak yapılandırılabilir.

Manüel yapılandırma

Manüel yapılandırmayı seçerseniz (ilgili iletişim kutusu bölümünü etkinleştirmek için **Manüel** seçeneğini işaretleyin) aşağıdaki bilgileri girmeniz gerekir:

- **Sunucu**– sunucunun IP adresini ya da sunucunun adını girin
- **Baglantı Noktası**– İnternet erişimine açık bağlantı noktasının numarasını girin (varsayılan olarak bu değer 3128 olarak atanmıştır fakat istediğiniz doğrultusunda değiştirebilirsiniz – emin değilseniz lütfen ağ yöneticiniz ile irtibat kurun)

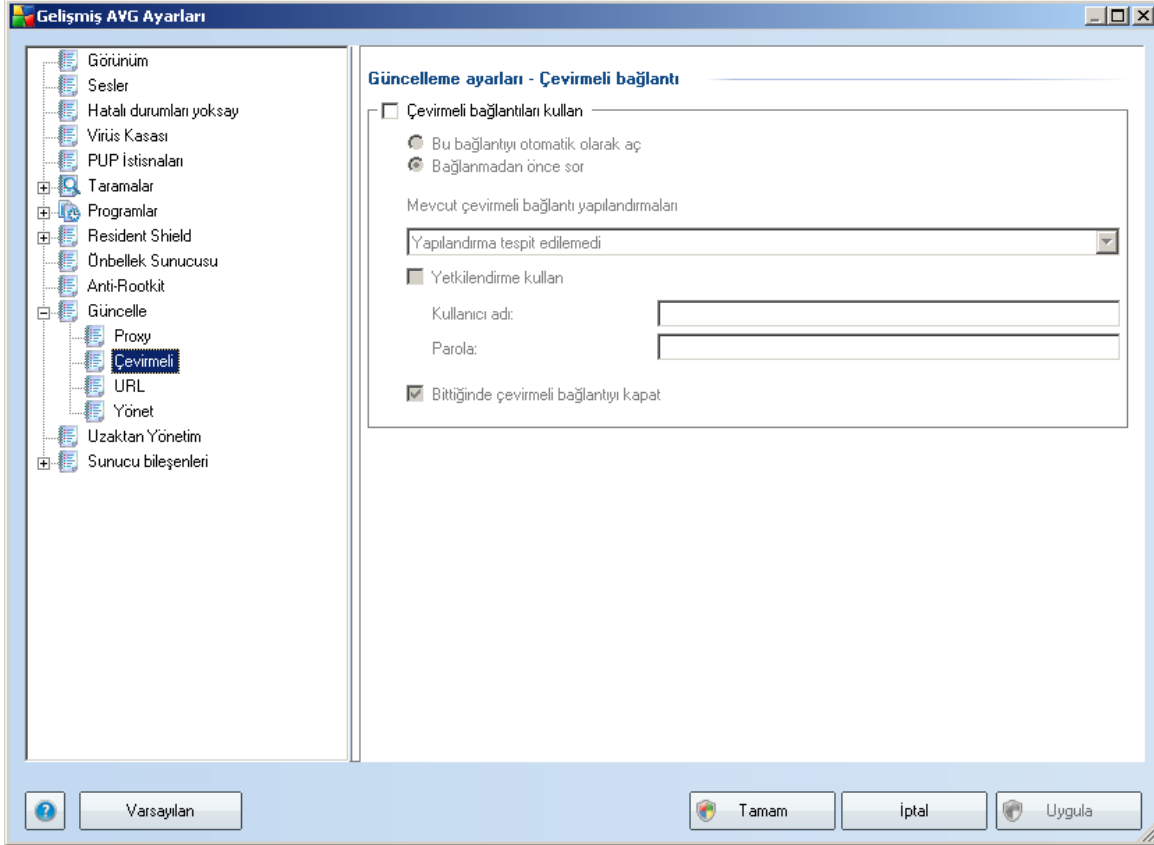
Proxy sunucusunda her kullanıcı için farklı kurallar yapılandırılabilir. Proxy sunucunuz bu şekilde yapılandırılmış ise proxy sunucusu üzerinden yapılan İnternet bağlantınıza ilişkin kullanıcı adı ve parolanızı onaylamak için **PROXY kimlik doğrulamasını kullan** seçeneğini işaretleyin.

Otomatik yapılandırma

Otomatik yapılandırmayı seçerseniz (ilgili iletişim kutusunu etkinleştirmek için **Oto** seçeneğini işaretleyin) ardından proxy yapılandırmasının nereden alınacağını belirleyin:

- **Tarayıcıdan** - Yapılandırma varsayılan İnternet tarayıcınızdan okunacaktır
- **Komut satırından** - yapılandırma, proxy adresine dönme fonksiyonu olan indirilmiş bir komut satırından okunacaktır
- **Otomatik Tespit Et** - yapılandırma otomatik olarak doğrudan proxy sunucusundan tespit edilecektir

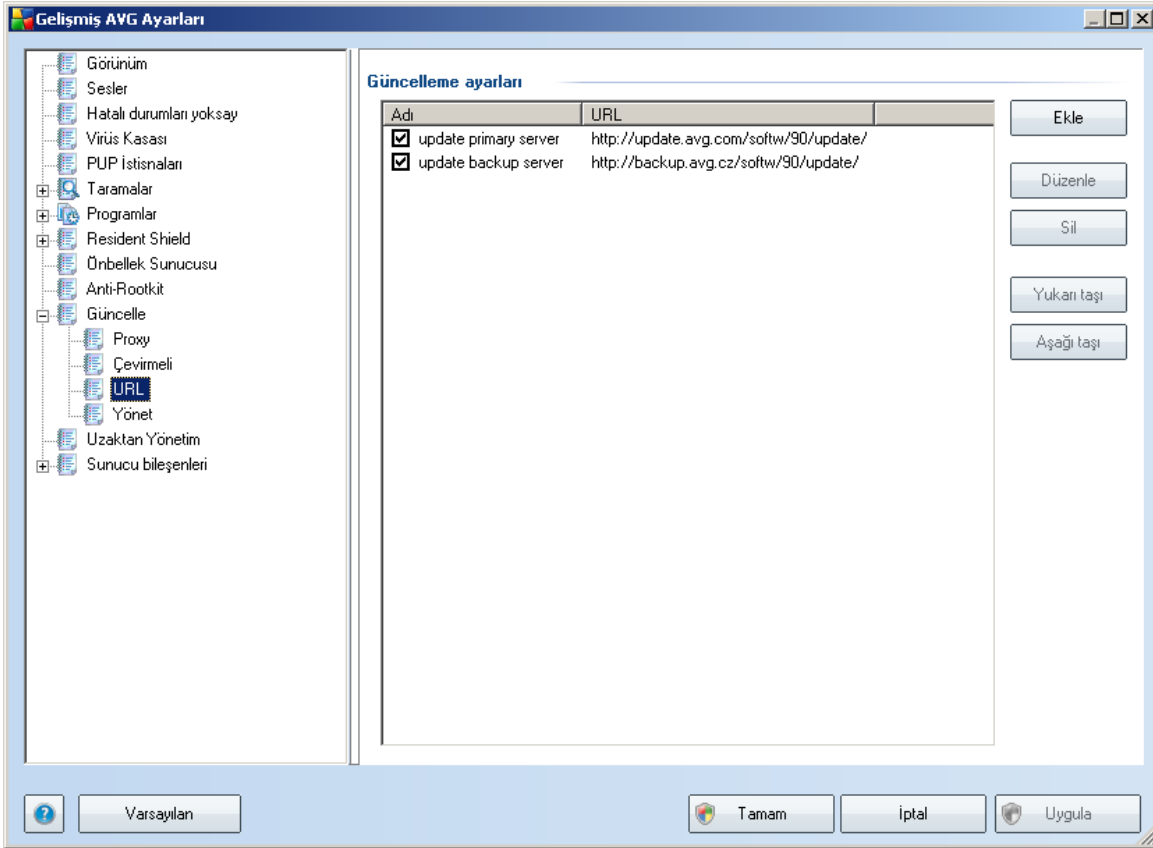
10.11.2. Çevirmeli



İsteğe bağlı olarak **Güncelleme ayarlarında tanımlanan tüm parametreler - Çevirmeli Bağlantı** iletişim kutusu İnternet'e çevirmeli bağlantı ile bağlanılmasına iliskindir. **Çevirmeli bağlantı kullan** seçeneği seçilip alanlar etkinleştirilene kadar iletişim kutusunun alanları pasif olacaktır.

İnternet'e otomatik olarak bağlanmak isteyip istemediğinizi (**Bu bağlantıyı otomatik olarak aç**) ya da bağlantıyı her seferinde manüel olarak kurmak isteyip istemediğinizi (**Bağlanmadan önce sor**) seçin. Otomatik bağlantılarda güncellemenin tamamlanmasının ardından bağlantının kesilmesini isteyip istemediğinizi de seçin (**Tamamlandığı zaman çevirmeli bağlantıyı kes**).

10.11.3. URL



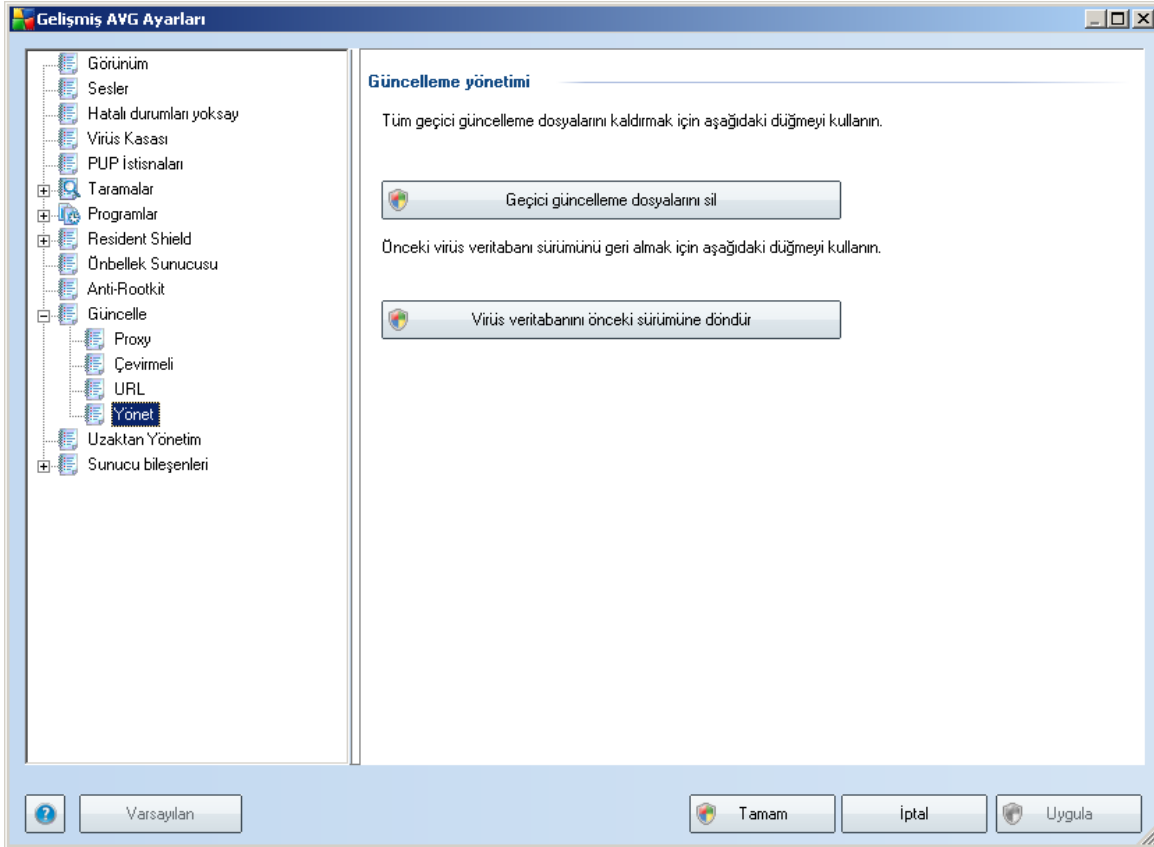
URL iletişim kutusunda güncelleme dosyalarının indirilebileceği bir dizi Internet adresi bulunur. Liste ve liste öğeleri aşağıdaki kontrol düğmeleri kullanılarak düzenlenebilir:

- **Ekle**– Listenize yeni bir URL eklemek için kullanacağınız iletişim kutusunu açar
- **Düzenle** - seçilen URL parametrelerini düzenleyebileceğiniz iletişim kutusunu açar
- **Sil**– seçilen URL'yi listeden seçer
- **Yukarı Tasi/Asağı Tasi** – bu iki düğme oldukça önemlidir. Listedeki ilk sunucu her zaman, her güncelleme girişimi sırasında ilk kullanılandır. Bu yüzden sunucuları listede yukarı ve aşağı taşıyarak aslında önceliklerini belirlersiniz. **Yukarı tasi** düğmesi seçili URL'yi listede bir konum yukarı tasir, **Asağı Tasi** ise seçili URL'yi listede bir konum aşağı tasir

Bir sunucu adinin yanındaki kutunun isareti kaldırıldığında geçici olarak bu sunucuyu devre dışı bırakır (liste girişinden silmeye gerek kalmadan).

10.11.4. Yönet

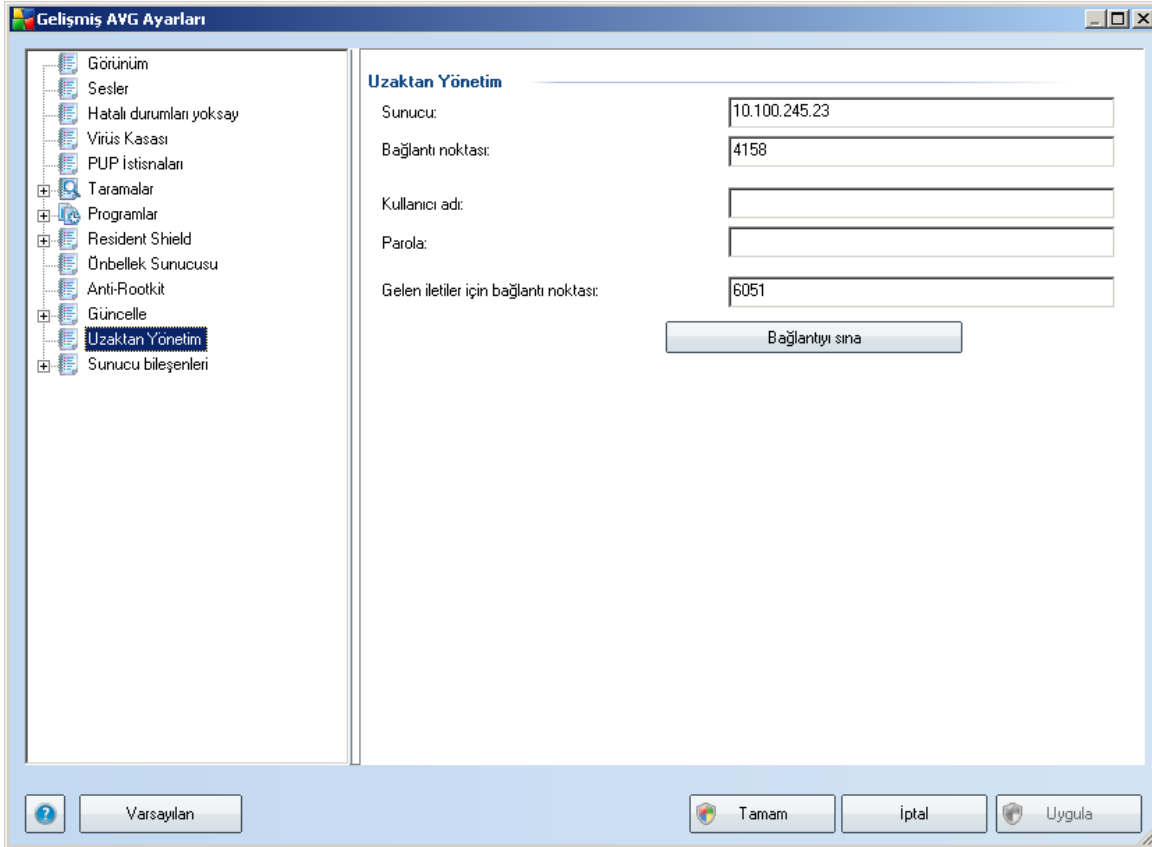
Yönet iletişim penceresi, iki adet düğme ile ulaşılabilen iki seçenek sunmaktadır:



- **Geçici güncelleme dosyalarını sil** - tüm gereksiz güncelleme dosyalarını sabit diskinizden silmek için bu düğmeye basın (*öntanımlı olarak söz konusu dosyalar 30 gün boyunca saklanır*)
- **Virüs veritabanını bir önceki sürümüne döndür** - En güncel virüs veritabanını sabit diskinizden silmek ve daha önce kaydedilmiş sürümüne dönmek için bu düğmeye basın (*yeni virüs tabanı sürümü, bir sonraki güncellemenin bir parçası olacaktır*)

10.12. Uzaktan Yönetim

Uzaktan Yönetim ögesi yalnızca önceden **Uzaktan Yönetim** yüklendiyse (yani [yükleme sırasında](#)), bu seçeneği **Bilesen Seçimi** iletişim kutusunda işaretlediyseniz **Gelişmiş Ayarlar** genel görünümünde görüntülenir:



Uzaktan Yönetim ayarları, AVG istemci istasyonunu uzak yönetici sisteme bağlamaya iliskindir. İlgili istasyonu uzaktan yönetime bağlamak istiyorsanız lütfen aşağıdaki parametreleri girin:

- **Sunucu** - AVG Admin Sunucusunun yüklü olduğu sunucu adı (ya da sunucunun IP adresi)
- **Bağlantı Noktası** - AVG istemcisinin AVG Admin Sunucusu ile iletişim kurduğu bağlantı noktası numarasıdır (*varsayılan olarak 4158 numaralı bağlantı noktası kullanılmaktadır - bu bağlantı noktası numarasını kullanırsanız herhangi bir işlem yapmanıza gerek kalmaz*)



- **Oturum Açma Bilgileri** - iAVG istemcisi ile AVG Admin Sunucusu arasındaki ilişki güvenli bir bağlantı ise kullanıcı adınızı girin...
- **Parola** - ... parolanızı girin
- **Gelen mesajlar için bağlantı noktası** - AVG istemcisinin AVG Admin Sunucusu'ndan gelen mesajları kabul ettiği bağlantı noktası numarasıdır

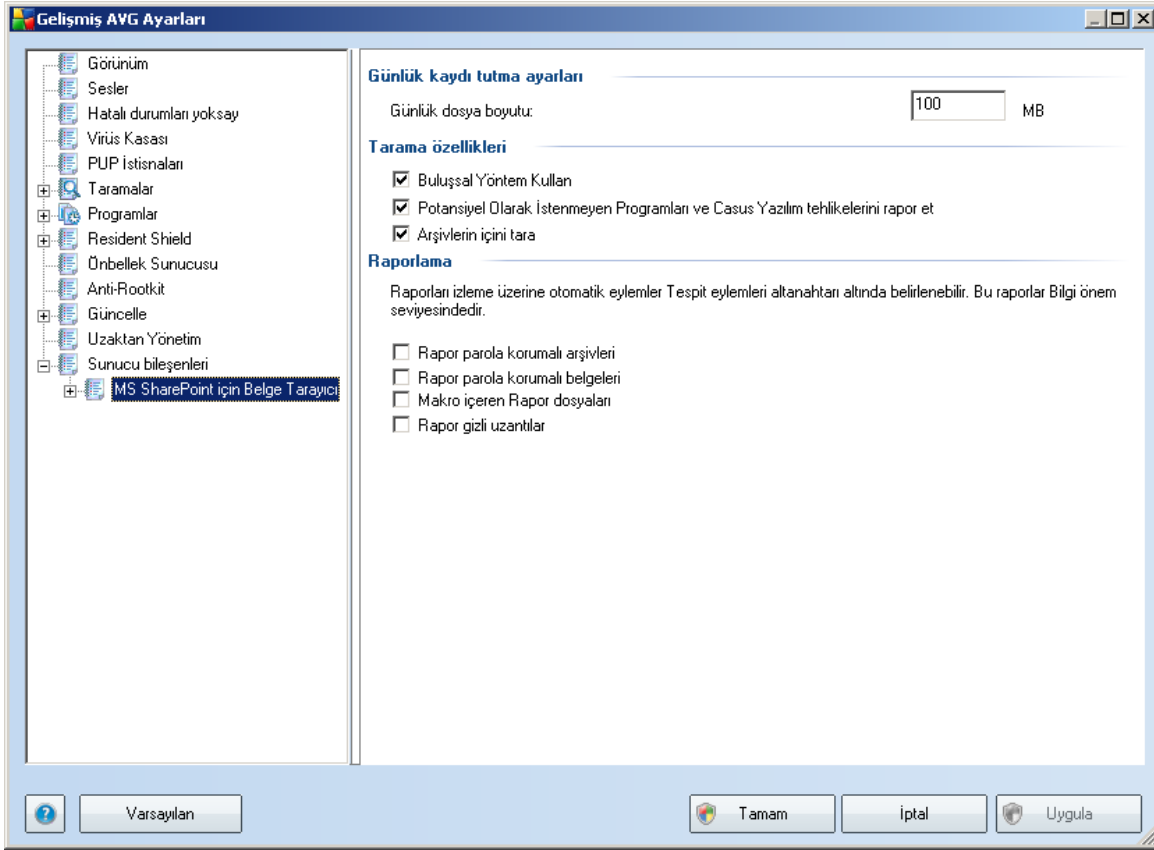
Baglantıyı sına düğmesi, yukarıda belirtilen verilerin tümünün geçerliliğini onaylamanıza yardımcı olur ve DataCenter'a başarıyla bağlanmak için kullanılabilir.

Not: *Uzaktan yönetim konusunda ayrıntılı bilgi için lütfen AVG Business Edition dokümantasyonunu inceleyin.*

10.13. Sunucu bileşenleri

10.13.1. MS SharePoint için Belge Tarayıcı

Bu iletişim kutusunda, [MS SharePoint için Belge Tarayıcı](#) belge virüs tarama performansı ile ilgili birçok önceden tanımlı seçenek bulacaksınız. Bu iletişim kutusu çok sayıda bölüme ayrılır:



Günlük kaydi tutma ayarları

Günlük dosyasi boyutu alanı – Günlük dosyasi, program kitapliklari yükleme notlari, virüs bulunma olaylari, sorun giderme uyarilari vb. gibi MS SharePoint için Belge Tarayici ile ilgili çeşitli olaylarin kaydini içerir. Bu dosyanin maksimum boyutunu ayarlamak için metin alanini kullanin.

Tarama özellikleri

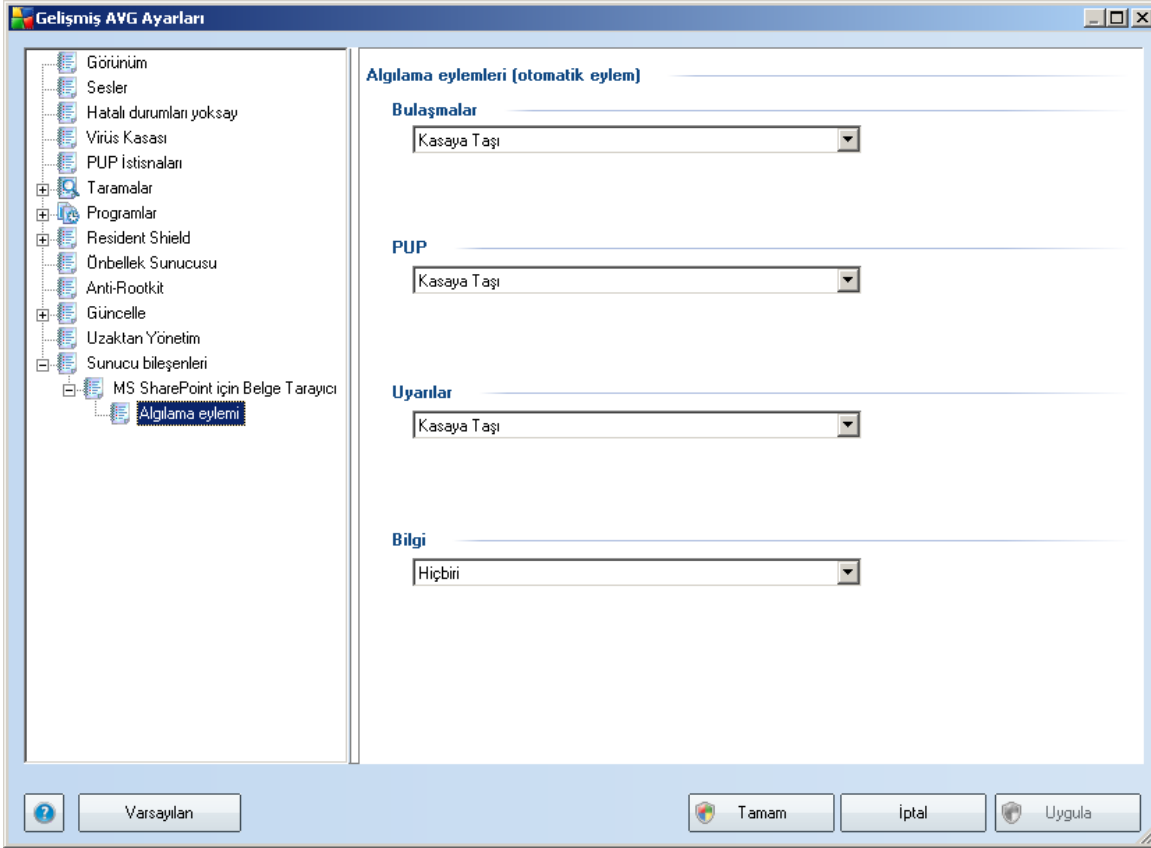
- **Bulussal Yöntem Kullan** - Belgeleri tararken Bulussal tani yöntemi kullanmak için işaretleyin. Bu seçenek açık olduğunda, belgeleri uzantiya göre filtrelemenin yanında belgenin gerçek içeriği de göz önünde bulundurulur.
- **Potansiyel İstenmeyen Programlari ve Casus Yazilim tehlikelerini bildir** - Örneğin, belgeleri tararken şüpheli ve potansiyel olarak istenmeyen programlari

tespit etmesi ve bildirmesi için Casus Yazılımları Önleme motorunu kullanmak üzere işaretleyin.

- **Arsivlerin içini tara** - Arsivlerin içeriklerini taramak için işaretleyin.

Raporlama

- **Parola korumalı arşivleri bildir** - Parolayla korunan arşivlerin (ZIP, RAR vb.) virüs için taranması mümkün değildir; bunların potansiyel olarak tehlikeli olduklarını rapor etmek için kutuyu işaretleyin.
- **Parola korumalı belgeleri bildir** - Parolayla korunan belgelerin virüs için taranması mümkün değildir; bunların potansiyel olarak tehlikeli olduklarını rapor etmek için kutuyu işaretleyin.
- **Makro içeren dosyaları bildir** - Makro, bazı görevlerin kullanıcı için daha kolay hale getirilmesini amaçlayan önceden tanımlanmış adımlar dizisidir (MS Word makroları yaygın olarak tanınır). Makro, potansiyel olarak tehlikeli talimatlar içerebilir ve makro içeren dosyaların şüpheli olarak rapor edilmesini sağlamak için kutuyu işaretleyebilirsiniz.
- **Gizlenen uzantıları bildir** - Gizli uzantılar şüpheli bir çalıştırılabilir dosyayı (örn. "birsey.txt.exe") zararsız bir düz metin dosyası gibi (örn. "birsey.txt") gösterebilir; bunları potansiyel olarak tehlikeli olarak rapor etmek için kutuyu işaretleyin.



Bu iletişim kutusunda, **MS SharePoint için Belge Tarayıcı** bileşeninin bir tehlike algıladığında nasıl davranması gerektiğini yapılandırabilirsiniz. Tehlikeler birçok kategoriye bölünmüştür:

- **Bulaşmalar** – Kendilerini kopyalayan ve yayan zararlı kodlar zarar verene kadar genellikle anlaşılmaz.
- **PUP (Potansiyel Olarak İstenmeyen Programlar)** – Bu tür programlar genellikle gizliliğinizi tehdit eden ciddi tehlikelerden yalnızca potansiyel tehlikelere kadar değişebilir.
- **Uyarılar** – Algılanan nesnelere taranamadı.
- **Bilgi** – Yukarıdaki kategorilerden hiç biri içinde yer almayan algılanan olası tüm tehlikeleri içerir.



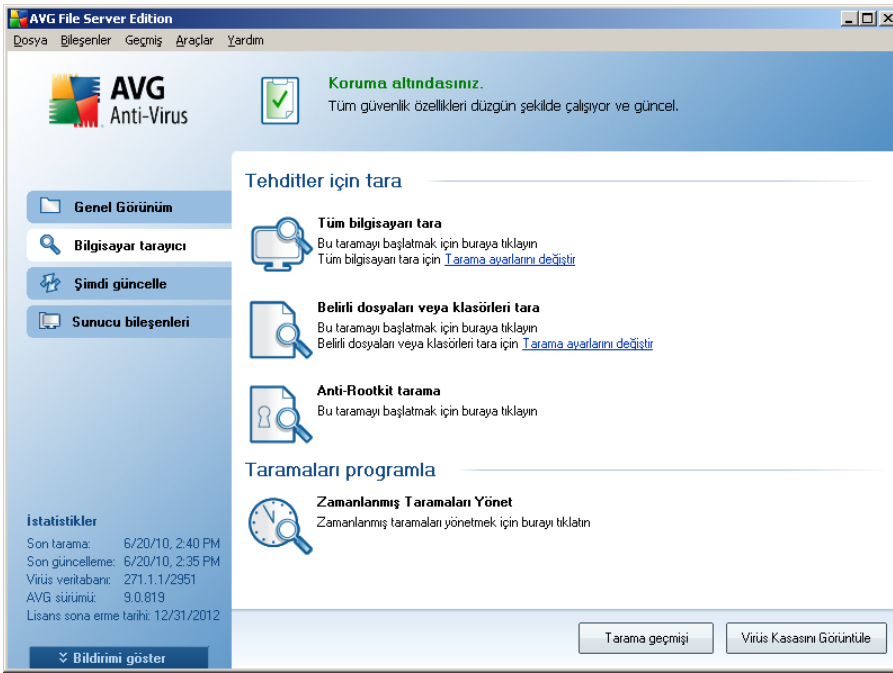
Her biri için otomatik bir eylem seçmek için aşağı açılır menüleri kullanın:

- **Hiçbiri** – Bu tür bir tehlikeyi içeren bir belge yalnız bırakılacaktır.
- **Virüs Kasasına Tasi***** – Virüs bulanan her belge Virüs Kasası karantina ortamına taşınacaktır.
- **Kaldır** – Bir virüsün algılandığı her belge silinecektir.

11. AVG Tarama

Tarama, **AVG 9.0 File Server** islevinin önemli bir parçasıdır. Talebe uygun taramalar yapabilir ya da istediğiniz zamanlarda [periyodik taramalar planlayabilirsiniz](#).

11.1. Tarama Arayüzü



AVG tarama arayüzüne, [Bilgisayar tarayıcısı hızlı bağlantısından](#) ulaşabilirsiniz. **Tehditleri tara** iletişim kutusuna geçmek için bu bağlantıyı tıklatın. Bu iletişim kutusunda aşağıdakiler bulunmaktadır:

- [öntanimli taramalara](#) genel bakış - yazılım satıcısı tarafından tanımlanan üç tarama türü isteğe bağlı olarak hemen veya programlı olarak kullanılmaya hazırdır:
 - [Tüm bilgisayarı tara](#)
 - [Belirli dosyaları veya klasörleri tara](#)
 - [Rootkit Önleme tarama](#)
- [tarama programlama](#) bölümü - İhtiyacınız doğrultusunda yeni programlar

olusturabilir ya da yeni taramalar tanımlayabilirsiniz.

Kontrol düğmeleri

Tarama arayüzünde bulunan genel kontrol düğmeleri şunlardır:

- **Tarama geçmişi** - tüm tarama geçmişi ile birlikte [Tarama sonuçlarına genel bakış](#) iletişim kutusunu açar
- **Virüs Kasasını Görüntüle** - tespit edilen bulasmaların karantina altına alındığı [Virüs Kasasını](#) yeni bir pencerede açar.

11.2. Öntanımlı Taramalar

AVG 9.0 File Server programının ana özelliklerinden biri istek üzerine taramadır. İsteğe bağlı taramalar, muhtemel bir virüs hakkında şüpheye düştüğünüz an bilgisayarınızın istediğiniz zamanda istediğiniz zaman yapabileceğiniz taramalardır. Kısacası, bilgisayarınızda virüs olduğunu düşünmeseniz bile söz konusu taramaların düzenli aralıklarla yapılması önerilmektedir.

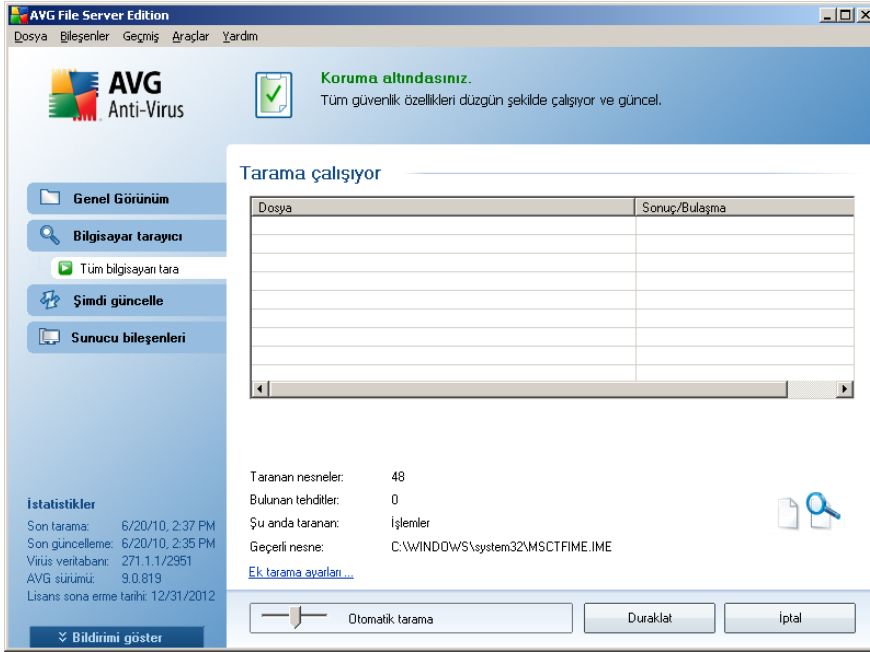
AVG 9.0 File Server içinde, yazılım satıcısının önceden tanımladığı aşağıdaki tarama türlerini bulacaksınız:

11.2.1. Tüm Bilgisayarı Tara

Tüm bilgisayarı tara - tüm bilgisayarı muhtemel bulasmalara ve/veya potansiyel olarak istenmeyen programlara karşı tarar. Bu tarama, bilgisayarınızın tüm sabit disklerini tarayacak, virüsleri tespit edecek ve temizleyecek ya da tespit edilen bulasmayı [Virüs Kasasına](#) taşıyacaktır. Bilgisayarın tümü haftada en az bir defa taranmalıdır.

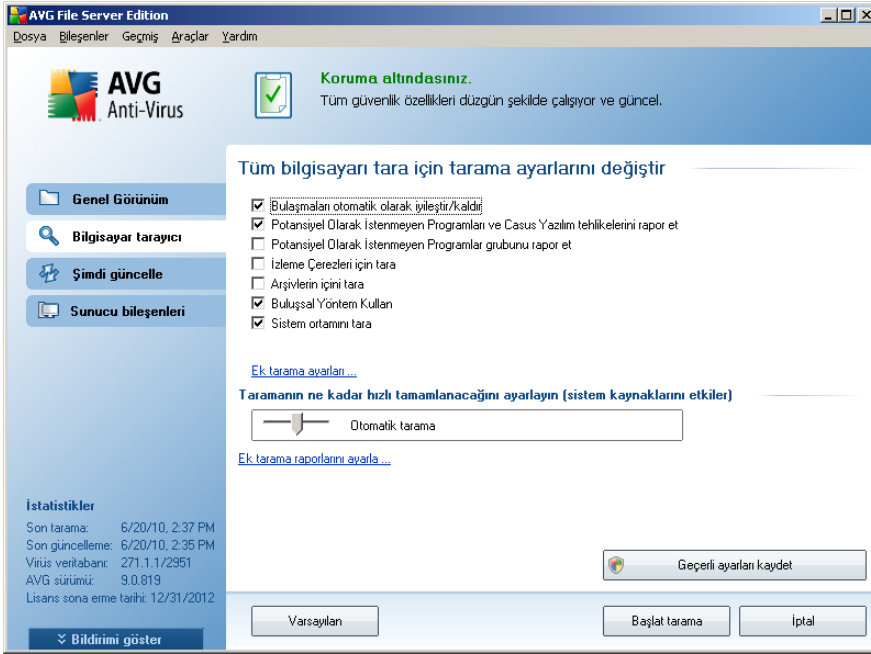
Tarama başlatma

Tüm bilgisayarı tara fonksiyonu tarama simgesine tıklamak suretiyle doğrudan [tarama arayüzünden](#) başlatılabilir. Bu tarama türü için başka belirli ayarlamaların yapılmasına gerek yoktur, tarama **Tarama yapılıyor** iletişim kutusunda anında başlayacaktır (*bkz. ekran görüntüsü*). Tarama işlemi gerekirse geçici olarak kesilebilir (**Duraklat**) ya da iptal edilebilir (**Durdur**).

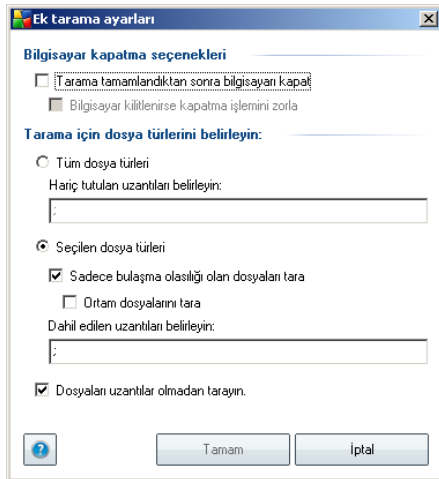


Tarama yapılandırması düzenleme

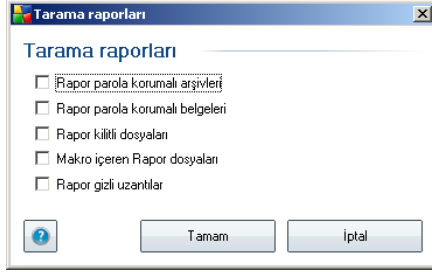
Tam bilgisayar taraması fonksiyonunun öntanımlı varsayılan ayarlarını düzenleme opsiyonunuz da bulunmaktadır. **Tarama ayarlarını değiştir** bağlantısına tıklayarak **Tüm bilgisayar taramasına ilişkin tarama ayarlarını değiştir** iletişim kutusuna gidin. **Varsayılan ayarları değiştirmeniz için geçerli bir nedeniniz olmadığı müddetçe bu ayarları korumanız önerilir!**



- **Tarama parametreleri** - tarama parametreleri listesindeki belirli parametreleri istediğiniz doğrultusunda açıp kapatabilirsiniz. Varsayılan olarak parametrelerin çoğu açıktır ve tarama sırasında otomatik olarak kullanılacaktır.
- **Ek tarama ayarları** - Bağlantı, şu parametreleri belirtebileceğiniz yeni bir **Ek tarama ayarları** iletişim kutusu açar:



- **Bilgisayar kapatma seçenekleri** - Çalışan tarama işlemi bittiginde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verir. Bu seçeneği seçerseniz (**Tarama bittikten sonra bilgisayarı kapat**) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (**Bilgisayar kilitliyse bilgisayarı kapanmaya zorla**).
- **Tarama için dosya türlerini tanımla** - Nelerin taranmasını istediğine de karar vermelisiniz:
 - **Tüm dosya türleri** taranmaması gereken virgülle ayrılmış dosya uzantılarının listesini sağlayarak taramada istisnaları tanımlama seçeneğiyle;
 - **Seçili dosya türleri** - Yalnızca virüs bulaşabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulasamayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya bazı diğer çalıştırılmayan dosyalar*); ortam dosyaları (*video, ses dosyaları - bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulaşma olasılıkları çok az olduğundan tarama süresini daha da azaltır*). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.
 - İsteğe bağlı olarak, **Uzantıları olmayan dosyaları taramaya** da karar verebilirsiniz - bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmemeniz önerilir. Uzantısı olmayan dosyalar süpheli olabilir ve her zaman taranmalıdır.
- **Tarama işlemi önceliği** - tarama işlemi önceliğini değiştirmek için kaydırma çubuğunu kullanabilirsiniz. Varsayılan olarak öncelik, sistem kaynaklarının kullanımını ve tarama işleminin hızını optimize eden orta seviyeye ayarlanmıştır (*Otomatik tarama*). Buna alternatif olarak, sistem kaynakları kullanımını minimize etmek için tarama işlemini daha yavaş (*bilgisayarda çalışmanız gerektiği ve taramanın ne kadar sürdüğünü önemsemediğiniz durumlar için uygundur*), ya da sistem kaynaklarını oldukça yoğun kullanmak suretiyle daha hızlı (*Örn. bilgisayar geçici olarak kimse kullanmayacak ise*) gerçekleştirebilirsiniz.
- **Tarama raporu oluşturma** - bağlantı üzerinden **Tarama Raporları** isimli bir iletişim kutusu açılır ve buradan ne tip buluntuların rapor edileceğini seçebilirsiniz:



Uyari: Bu tarama parametreleri, yeni tanımlanan taramanın parametreleri ile aynıdır - [AVG Taraması / Tarama Planlama / Tarama Tipi](#) bölümünde açıklandığı doğrultuda. **Tüm bilgisayarı tara** fonksiyonunun varsayılan yapılandırmasını değiştirmeye karar vererseniz yeni ayarlarınızı, belirli dosya ya da klasörlerin taraması için kullanılacak varsayılan yapılandırma olarak atayabilirsiniz.

11.2.2. Belirli Dosyaları veya Klasörleri Tara

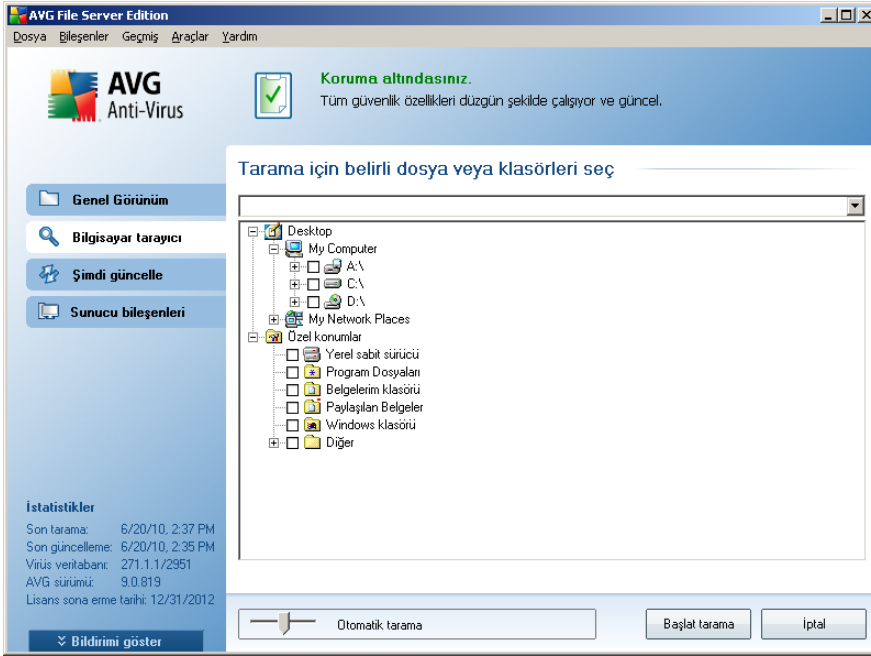
Belirli dosya ve klasörleri tara - bilgisayarınızın sadece taraması için seçtiğiniz alanlarını tarar (seçilen klasörler, sabit diskler, disket sürücüler, CD'ler vb.). Virüs tespiti ve temizlenmesi sırasında tarama işlemi, tüm bilgisayar taraması ile aynıdır: bulunan virüsler temizlenir ya da [Virüs Kasasına](#) tasınır. Belirli dosya ve klasörlerin taraması, ihtiyaçlarınız doğrultusunda programladığınız taramalarda kullanılabilir.

Tarama başlatma

Belirli dosya ve klasörleri tara fonksiyonu tarama simgesine tıklamak suretiyle doğrudan [tarama arayüzünden](#) başlatılabilir. Yeni bir **Taramak için belirli dosya ve klasörleri seçin** iletişim kutusu açılır. Bilgisayarınızın ağaç görünümünden taramasını istediğiniz klasörleri seçin. Seçilen klasörlerin her birine giden yol, otomatik olarak oluşturulacak ve iletişim kutusunun üst kısmındaki metin alanında görüntülenecektir.

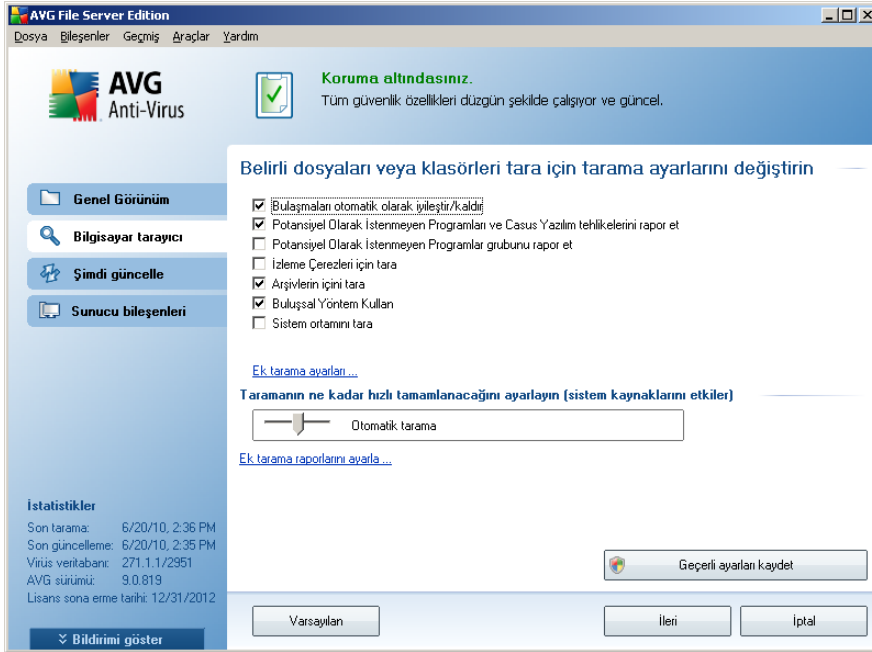
Belirli bir klasör taranırken içinde bulunan klasörlerin taranmaması gibi bir ihtimal de vardır; bunu yapabilmek için otomatik olarak oluşturulan yolun başına "-" isareti koyun. Klasörün tümünü tarama dışında tutmak için "!" parametresini kullanın.

Son olarak taramayı başlatabilmek için **Taramayı başlat** düğmesine basın; tarama işleminin kendisi temel olarak [tam bilgisayar taraması](#) ile aynıdır.

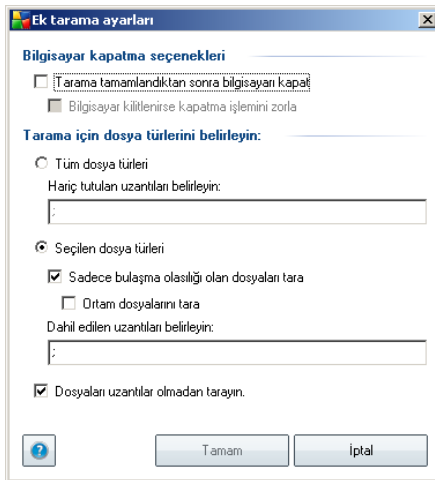


Tarama yapılandırması düzenleme

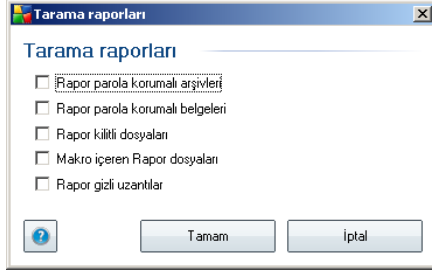
Belirli dosya ve klasörleri tara fonksiyonunun varsayılan ayarlarını düzenleme opsiyonunuz da bulunmaktadır. **Tarama ayarlarını değiştir** bağlantısına tıklayarak **Belirli dosya ve klasörlerin taranmasına ilişkin tarama ayarlarını değiştir** iletişim kutusuna gidin. **Varsayılan ayarları değiştirmeniz için geçerli bir nedeniniz olmadığı müddetçe bu ayarları korumanız önerilir!**



- **Tarama parametreleri** - tarama parametreleri listesindeki belirli parametreleri gerektiğinde açabilir ya da kapatabilirsiniz (*bu ayarlar hakkında ayrıntılı bilgi için lütfen [AVG Gelismis Ayarlar / Taramalar / Belirli Dosya veya Klasörleri Tara](#) bölümünü inceleyin*).
- **Ek tarama ayarları** - Bağlantı, su parametreleri belirtebileceğiniz yeni bir Ek tarama ayarları iletişim kutusu açar:



- **Bilgisayar kapatma seçenekleri** - Çalışan tarama işlemi bittiginde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verir. Bu seçeneği seçerseniz (**Tarama bittikten sonra bilgisayarı kapat**) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (**Bilgisayar kilitliyse bilgisayarı kapanmaya zorla**).
- **Tarama için dosya türlerini tanımla** - Nelerin taranmasını istediğinize de karar vermelisiniz:
 - **Tüm dosya türleri** taranmaması gereken virgülle ayrılmış dosya uzantılarının listesini sağlayarak taramada istisnaları tanımlama seçeneğiyle;
 - **Seçili dosya türleri** - Yalnızca virüs bulaşabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulasamayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya bazı diğer çalıştırılmayan dosyalar*); ortam dosyaları (*video, ses dosyaları - bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulaşma olasılıkları çok az olduğundan tarama süresini daha da azaltır*). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.
 - İsteğe bağlı olarak, **Uzantıları olmayan dosyaları taramaya** da karar verebilirsiniz - bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmemeniz önerilir. Uzantısı olmayan dosyalar süpheli olabilir ve her zaman taranmalıdır.
- **Tarama işlemi önceliği** - tarama işlemi önceliğini değiştirmek için kaydırma çubuğunu kullanabilirsiniz. Varsayılan olarak öncelik, sistem kaynaklarının kullanımını ve tarama işleminin hızını optimize eden orta seviyeye ayarlanmıştır (*Otomatik tarama*). Buna alternatif olarak, sistem kaynakları kullanımını minimize etmek için tarama işlemini daha yavaş (*bilgisayarda çalışmanız gerektiği ve taramanın ne kadar sürdüğünü önemsemediğiniz durumlar için uygundur*), ya da sistem kaynaklarını oldukça yoğun kullanmak suretiyle daha hızlı (*Örn. bilgisayar geçici olarak kimse kullanmayacak ise*) gerçekleştirebilirsiniz.
- **Tarama raporu oluşturma** - bağlantı üzerinden **Tarama Raporları** isimli bir iletişim kutusu açılır ve buradan ne tip buluntuların rapor edileceğini seçebilirsiniz:



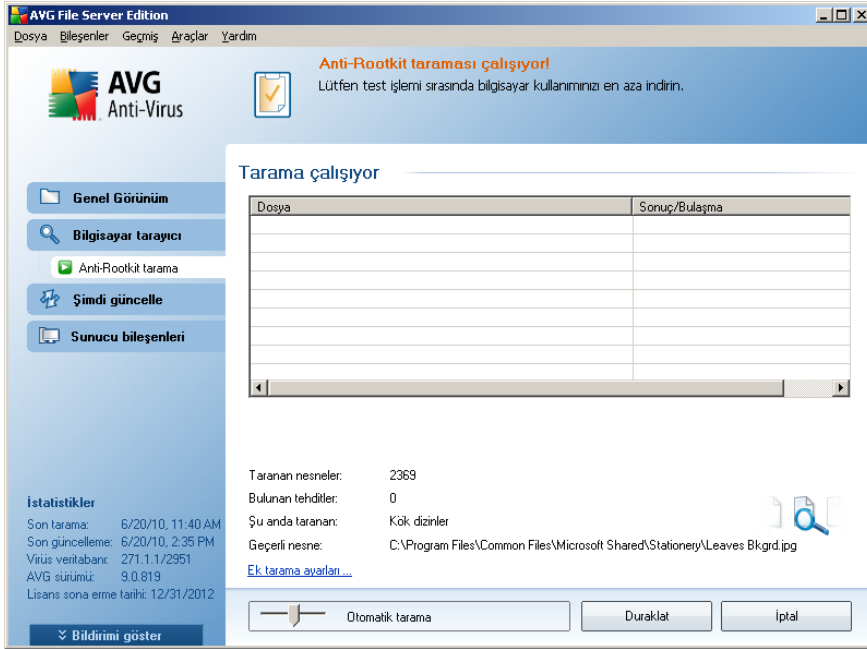
Uyari: Bu tarama parametreleri, yeni tanımlanan taramanın parametreleri ile aynıdır - [AVG Taraması / Tarama Planlama / Tarama Tipi](#) bölümünde açıklandığı doğrultuda. **Belirli dosya veya klasörleri tara** fonksiyonunun varsayılan yapılandırmasını değiştirmeye karar vererseniz yeni ayarlarınızı, belirli dosya ya da klasörlerin taranması için kullanılacak varsayılan yapılandırma olarak atayabilirsiniz. Buna ek olarak söz konusu yapılandırma tüm yeni programlanmış taramalarınız için sablon görevi görecektir ([tüm özelleştirilmiş taramalar, Seçilen dosya ya da klasörleri tara fonksiyonunun mevcut yapılandırmasına dayanmaktadır](#)).

11.2.3. Anti-Rootkit Tarama

Anti-Rootkit tarama olası rootkit'e karşı bilgisayarınızı (*bilgisayarınızdaki kötü amaçlı yazılım etkinliği içerebilecek programlar ve teknolojiler*) açısından tarar. Bir rootkit algılanırsa, bu, bilgisayarınızda mutlaka virüs olduğu anlamına gelmez. Bazı durumlarda, belirli sürücüler veya normal uygulamaların bölümleri rootkit olarak yanlış algılanabilir.

Tarama başlatma

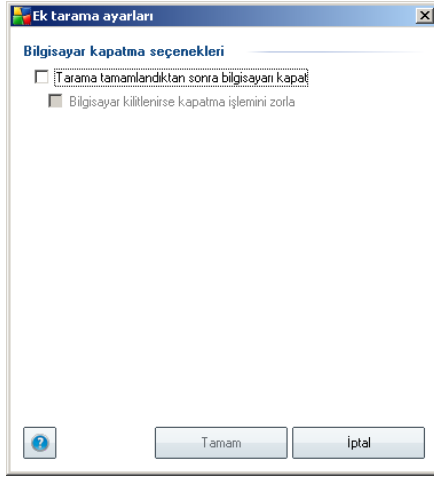
Anti-Rootkit tarama fonksiyonu tarama simgesi tıklanarak suretiyle doğrudan [tarama arayüzünden](#) başlatılabilir. Bu tarama türü için belirli ayarlamaların yapılmasına gerek yoktur, tarama **Tarama yapılıyor** iletişim kutusunda anında başlayacaktır (*bkz. ekran görüntüsü*). Tarama işlemi gerekirse geçici olarak kesilebilir (**Duraklat**) ya da iptal edilebilir (**Durdur**).



Tarama yapılandırması düzenleme

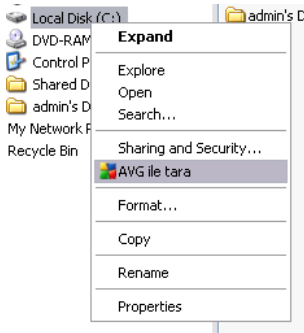
Anti-Rootkit tarama varsayılan ayarlarda her zaman baslatılır ve tarama parametrelerinin düzenlenmesine yalnızca [AVG Gelismis Ayarları / Anti-Rootkit](#) iletişim kutusundan erişilebilir. [Tarama arayüzünde](#), yalnızca aşağıdaki yapılandırma kullanılabilir:

- **Otomatik tarama** - Tarama işlemi önceliğini değiştirmek için kaydırma çubuğunu kullanabilirsiniz. Varsayılan olarak öncelik, sistem kaynaklarının kullanımını ve tarama işleminin hızını optimize eden orta seviyeye ayarlanmıştır (*Otomatik tarama*). Buna alternatif olarak, sistem kaynakları kullanımını minimize etmek için tarama işlemini daha yavaş (*bilgisayarda çalışmanız gerektiği ve taramanın ne kadar sürdüğünü önemsemediğiniz durumlar için uygundur*), ya da sistem kaynaklarını oldukça yoğun kullanmak suretiyle daha hızlı (*Örn. bilgisayarı geçici olarak kimse kullanmayacak ise*) gerçekleştirebilirsiniz.
- **Ek tarama ayarları** - Bu bağlantı, **Anti-Rootkit tarama** ile ilgili olası bilgisayar kapatma koşulları tanımlayabileceğiniz yeni bir **Ek tarama ayarları** iletişim kutusu açar (**Tarama tamamlandığında bilgisayarı kapat**, büyük olasılıkla **Bilgisayar kilitliyse kapatmaya zorla**):



11.3. Windows Gezgini'nde Tarama

Bilgisayarın tümünde ya da seçilen bölümlerinde gerçekleştirilen öntanımlı taramaların yani sıra **AVG 9.0 File Server**, doğrudan Windows Gezgini ortamında bulunan belirli nesnelere hızlı bir şekilde taramasını da sağlamaktadır. Bilinmeyen bir dosyayı açmak istiyorsanız içeriğinden emin olamıyorsanız isteğe bağlı olarak tarayabilirsiniz. Bu adımları takip edin:



- Windows Gezgini'nde taramak istediğiniz dosyayı (ya da klasörü) seçin
- Bağlam menüsünü açmak için nesneye fare ile sağ tıklayın
- **AVG ile Tara** seçeneğini seçerek dosyanın AVG tarafından taramasını sağlayın

11.4. Komut Satiri Tarama

AVG 9.0 File Server içinde, taramayı komut satirinden çalıştırma seçeneği vardır. Söz konusu seçeneği, sunucularda ya da bilgisayar yeniden başlatıldıktan sonra otomatik olarak çalıştırılacak komut satirlarının oluşturulması sırasında kullanabilirsiniz. Komut satirinde AVG'nin grafik kullanıcı arayüzünde sunulan parametrelerden daha fazlasını kullanarak tarama işlemini gerçekleştirebilirsiniz.

AVG taramasını komut satirinden çalıştırmak için AVG'nin yüklendiği klasörde aşağıdaki komutu çalıştırın:

- **32 bit OS için avgscanx**
- **64 bit OS için avgscana**

Komut sözdizimi

Komut söz dizimi aşağıdaki gibidir:

- **Tam bilgisayar taraması yapılırken avgscanx /parametre ...** Örn. **avgscanx /comp**
- **avgscanx /parametre /parametre ..** Birden fazla parametre kullanıldığı zaman bunlar bir sıra halinde dizilmeli ve bir boşluğun yani sıra bir de bölme işareti ile ayrılmalıdır
- Parametrelerden biri için belirli bir değer verilmesi gerekiyorsa (**/scan** parametresi taranmak üzere seçilen bilgisayar konumları hakkında bilgi talep eder ve siz de seçilen bölüme ilişkin veri yolunu tam olarak verirseniz) söz konusu değerler virgül ile birbirinden ayrılır, Örn: **avgscanx /scan=C:\,D:**

Tarama parametreleri

Mevcut parametrelerin tam görünümünü görüntülemek için **/?** ya da **/HELP** (e.g. **avgscanx /?**). Zorunlu olan tek parametre, bilgisayarın hangi alanlarının taranması gerektiğini belirlemek için kullanılan **/SCAN** parametresidir. Seçenekler hakkında daha ayrıntılı açıklama almak için [komut satiri parametrelerine genel bakış](#) bölümüne bakın.

Tarama işlemini başlatmak için **Enter** düğmesine basın. Tarama sırasında işlemi **Ctrl+C** veya **Ctrl+Pause** tuşlarına basarak durdurabilirsiniz.

Grafik arayüzünden çalıştırılan CMD taraması

Bilgisayarınızı Windows Güvenli Modda çalıştırdığınız zaman komut satırı taramasını grafik kullanıcı arayüzünden başlatma ihtimaliniz de bulunmaktadır. Taramanın kendisi komut satırından başlatılacaktır, **Komut Satırı Oluşturucu** iletişim kutusu, en yaygın tarama parametrelerini konforlu grafik arayüzü vasıtasıyla görüntüler.

Söz konusu iletişim kutusuna sadece Windows Güvenli Moddan ulaşılabilirdi için iletişim kutusu hakkında ayrıntılı bilgi almak için doğrudan iletişim kutusundan açılan yardım dosyasını inceleyin.

11.4.1. CMD Tarama Parametreleri

Komut satırı taramasında kullanılan parametrelerin listesi aşağıda verilmiştir:

- **/SCAN** [Belirli dosya ya da klasörleri tara](#) /SCAN=yol;yol (örn. /SCAN=C:\;D:\)
- **/COMP** [Bilgisayarı tamamen tara](#)
- **/HEUR** [Bulgusal analizi kullan](#)
- **/EXCLUDE** Tarama işleminden izin yolu veya dosyaları hariç tutun
- **/@** Komut dosyası /dosya adı/
- **/EXT** Bu uzantıları tarayın / örneğin EXT=EXE,DLL/
- **/NOEXT** u uzantıları tarama /örneğin NOEXT=JPG/
- **/ARC** Arşivleri tara
- **/CLEAN** Otomatik olarak temizle
- **/TRASH** Bulunan dosyaları [Virüs Kasasına taşı](#)
- **/QT** Hızlı test
- **/MACROW** Makroları rapor et
- **/PWDW** Parola ile korunan dosyaları rapor et
- **/IGNLOCKED** Kilitli dosyaları göz ardı et

- **/REPORT** /dosya adi/ dosyasina rapor et
- **/REPAPPEND** Rapor dosyasina ekle
- **/REPOK** Bulasmamis dosyalari Tamam olarak raporla
- **/NOBREAK** CTRL-BREAK ile islemin kesilmesine izin verme
- **/BOOT** MBR/BOOT kontrolünü etkinlestir
- **/PROC** Aktif islemleri tara
- **/PUP** [""Potansiyel olarak istenmeyen programlari"](#) rapor et
- **/REG** Kayit defterini tara
- **/COO** Tanimlama bilgilerini tara
- **/?** Bu konuyla ilgili yardimi görüntüle
- **/HELP** Bu konuyla ilgili yardimi görüntüle
- **/PRIORITY** Tarama önceligini belirle /Düşük, Oto, Yüksek/ (Bkz [Gelismis ayarlar / Taramalar](#))
- **/SHUTDOWN** Tarama tamamlandıktan sonra bilgisayari kapat
- **/FORCESHUTDOWN** Tarama tamamlandıktan sonra bilgisayari kapatmayı zorla
- **/ADS** Alternatif Veri Akislarini Tara (sadece NTFS)
- **/ARCBOMBSW** "Arsiv bombalarini" raporla (tekrar tekrar sikistirilan arshivler)

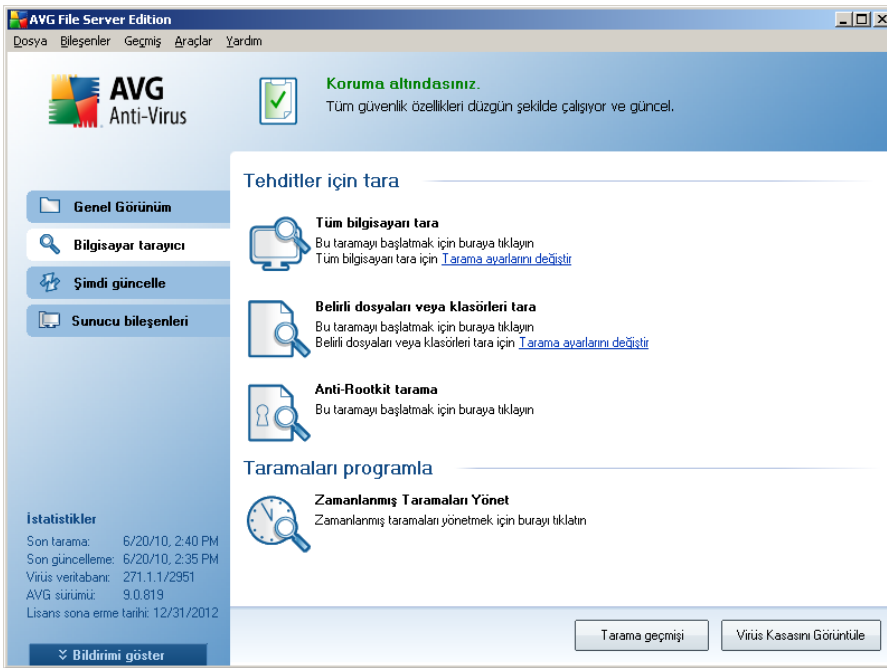
11.5. Tarama Planlama

AVG 9.0 File Server ile isteginiz dogrultusunda tarama yapmanin (örneğin bilgisayarınıza virüs bulastigidan süphelenirseniz) yani sıra programlanan bir plan dogrultusunda da tarama yapabilirsiniz. Taramaların bir program dogrultusunda yapılması önerilmektedir: bu şekilde, bilgisayarınızın virüs bulasma ihtimaline karsi korundugundan emin olursunuz ve ne zaman tarama yapmanız gerektiği konusunda endiselenmenize gerek kalmaz.

Tüm bilgisayar taramasini düzenli araliklarla ve en azından haftada bir kere yapmanız

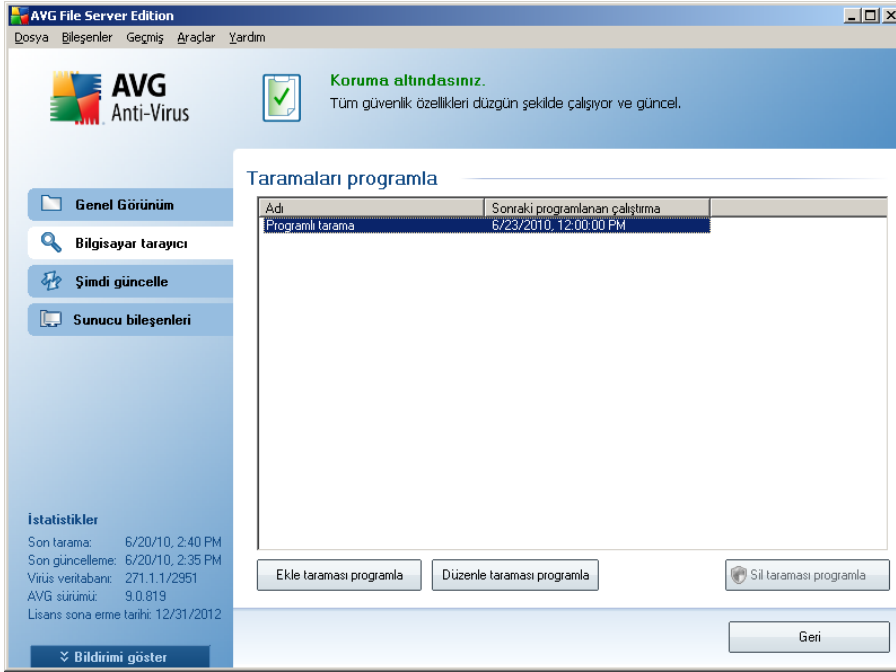
gerekir. Diğer bir yandan, mümkün olması halinde programlı tarama varsayılan yapılandırmasında ayarlandığı gibi tüm bilgisayar taramasını günlük olarak gerçekleştirin. Bilgisayarınız "daima açık" ise taramayı çalışma saatlerinden sonra gerçekleştirilecek şekilde programlayabilirsiniz. Bilgisayarınızı arada sırada kapatıyorsanız taramayı, taramaları [görev yerine getirilemediginde bilgisayarın başlaması ile baslat](#) şeklinde programlayın.

Yeni tarama programları oluşturmak için [AVG tarama arayüzünü](#) inceleyin ve **Tarama programla** adı altındaki bölümü bulun:



Taramaları programla

Geçerli olarak zamanlanmış taramaların bir listesini bulabileceğiniz yeni bir **Taramaları programla** iletişim kutusunu açmak için **Taramaları programla** bölümündeki grafik simgeyi tıklayın:

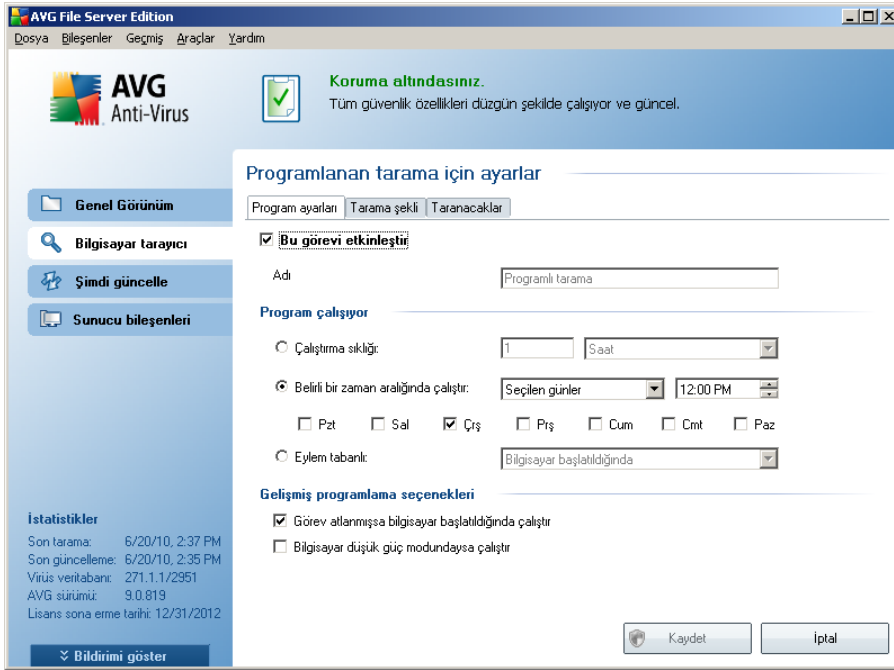


Su kontrol düğmelerini kullanarak taramalari düzenleyebilir/ekleyebilirsiniz:

- **Tarama programi ekle** - düğme, **Programlanan tarama ayarlari** iletişim kutusunu ve **Programlama Ayarlari** sekmesini açar. Bu iletişim kutusunda yeni tanımladığınız taramanın parametrelerini belirleyebilirsiniz.
- **Tarama programini düzenle** - bu düğme, programlanan taramalar listesinden mevcut bir taramayı seçtiyseniz kullanılabilir. Bu durumda düğme etkinlesir ve **Programlanan tarama ayarlari** iletişim kutusuna ve **Programlama ayarlari** sekmesine geçmek için düğmeyi kullanabilirsiniz. Seçilen tarama parametreleri, zaten belirlenmiştir ve düzenlenebilir.
- **Tarama programini sil** - bu düğme, programlanan taramalar listesinden mevcut bir taramayı seçmeniz halinde etkinlesir. Bu tarama, ilgili kontrol düğmesine basılarak listeden silinebilir. Diğer bir yandan sadece kendi taramalarınızı silebilirsiniz; varsayılan ayarlar içinde **Tüm bilgisayar taramasi programi** öntanımlıdır ve kesinlikle silinemez.
- **Geri** - [AVG tarama arayüzüne geri döner](#)

11.5.1. Program Ayarları

Yeni bir test programlamayı ve düzenli olarak başlamasını istiyorsanız, **Programlanan testin ayarları** iletişim kutusuna girin, (**Taramaları programla iletişim kutusundaki Tarama programı ekle** düğmesini tıklayın). Bu iletişim kutusu üç sekmeye ayrılmıştır: **Programlama ayarları** - aşağıdaki resme bakın (doğrudan yönlendirileceğiniz varsayılan sekmedir), **Tarama türü** ve **Taranacaklar**.



Planlama ayarları sekmesinde **Bu görevi etkinleştir** ögesini işaretleyerek ya da işareti kaldırarak planlanan taramayı geçici olarak devre dışı bırakabilir ve ihtiyaç duyduğunuzda yeniden açabilirsiniz.

Sonra oluşturmak ve programlamak üzere olduğunuz taramanın adını verir. **İsim** ögesini kullanarak metin alanına bir isim girin. Programladığınız taramaları diğerlerinden kolaylıkla ayırmak için taramalarınıza kısa, açıklayıcı isimler vermeyi deneyin.

Örnek: Taramayı "Yeni Tarama" veya "Taramam" adıyla adlandırmanız uygun değildir çünkü bu adlar, taramanın fiilen neyi kontrol ettiğini açıklamaz. Diğer bir yandan "Sistem alanları taraması" oldukça açıklayıcı bir isim olacaktır. Ayrıca, taramanın adında söz konusu taramanın tam bilgisayar taraması ya da sadece seçilen dosya ya da klasörlerin taraması olup olmadığını belirtmenize gerek yoktur - taramalarınız **seçilen dosya ya da klasörleri tara** işlevinin farklı şekillerinden ibaret olacaktır.

Bu iletisim kutusunda taramanın asagidaki parametrelerini de tanimlayabilirsiniz:

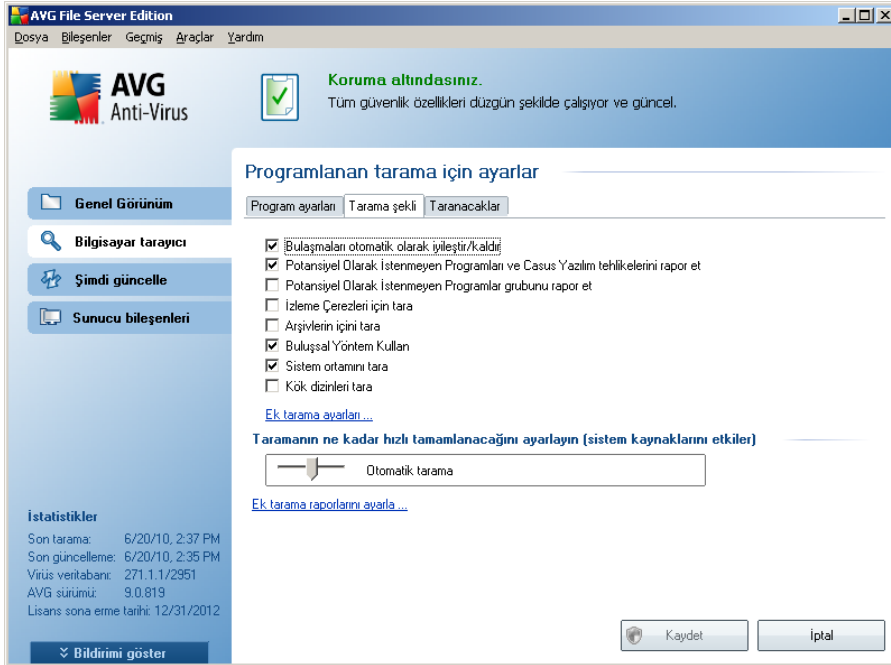
- **Planlama çaliliyor** - yeni planlanan taramanın baslamasi için zaman araligi girin. Zamanlama belirli bir sürenin ardindan tekrarlanan tarama ile (**Her ...'de bir**) ya da kesin bir tarih ve saat tanimlayarak (**Belirli bir saatte çalistir ...**), ya da (**Bilgisayar baslangicinda**) ilgili bir programin taranmasiyla tanimlanabilir.
- **Gelismis planlama seçenekleri** - bu bölümde, bilgisayar düşük güç modundaysa veya tamamen kapatilmis hangii kosullar altinda taramanın baslatilmasi/baslatilmamasii gerektigini belirleyebilirsiniz.

Programli tarama iletisim kutusuna dair ayarlarin kontrol düğmeleri

Programli tarama ayarlari iletisim kutusunun üç sekmesinde (**Programlama ayarlari**, **Tarama sekli** ve **Taranacaklar**) iki kontrol düğmesi bulunmaktadir ve hangii sekmede oldugunuz önemli olmaksizin asagidaki düğmelerin fonksiyonlari aynidir:

- **Kaydet** - bu sekmede veya bu iletisim kutusunun baska herhangi bir sekmesinde gerçeklestirdiginiz tüm deęisiklikleri kaydeder ve [AVG tarama arayüzü varsayilan penceresine](#) geri döner. Bu nedenle tüm sekmelerdeki test parametrelerini yapilandirmak istiyorsanız gereksinimlerinizin tamamini belirledikten sonra bunlari kaydetmek için düğmeye basin.
- **Iptal**- bu iletisim kutusunun bu sekmesinde veya baska bir sekmesinde yaptiginiz deęisiklikleri iptal eder ve [AVG tarama arayüzü varsayilan iletisim kutusuna geri döner](#).

11.5.2. Tarama Sekli



Tarama Sekli sekmesinde, isteğe bağlı olarak açılıp/kapatılabilen tarama parametrelerine ilişkin bir liste bulabilirsiniz. Varsayılan olarak birçok parametre devreye sokulur ve işlevsellik de tarama sırasında uygulanacaktır. Söz konusu ayarları değiştirmek açısından geçerli bir nedeniniz yoksa varsayılan yapılandırmayı olduğu gibi muhafaza etmeniz önerilir:

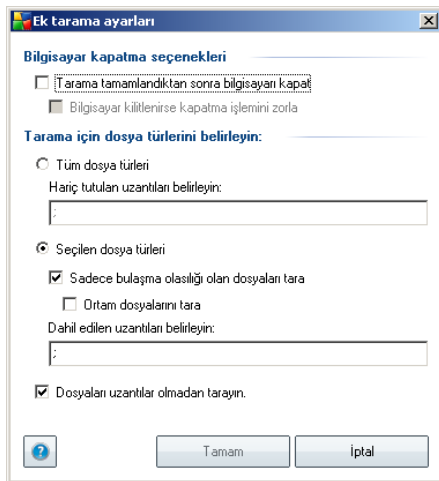
- **Bulaşmayı otomatik temizle/sil** - tarama işlemi sırasında bir virüs tanımlanırsa ve temizlenmesi mümkün ise otomatik olarak temizlenir. Etkilenen dosyanın otomatik olarak silinmiyor olması halinde ya da bu seçeneği kapatmayı seçerseniz bir virüs tespit edildiğinde bilgilendirileceksiniz ve tespit edilen bulaşma hakkında ne yapılacağına karar vermek zorunda kalacaksınız. Önerilen işlem, bulaşmış dosyayı [Virüs Kasasına](#) kaldırmaktır.
- **Potansiyel Olarak İstenmeyen Programları ve Casus yazılım Tehlikelerini Rapor Et** - Bu parametre, [potansiyel olarak istenmeyen programların tespit edilmesini](#) (casus yazılım ya da reklam yazılımı gibi işleyen çalıştırılabilir dosyalar) sağlayan [Virüsten Koruma](#) fonksiyonunu kontrol eder.
- **Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et** - Doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılan programlar olan genişletilmiş casus yazılım paketini algılar. ******* Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları

da engelleyebilir - bu yüzden varsayılan olarak kapalıdır;

- **Τανήμιλαμα Βιγιλιερνι Ταρα - Casus Yazılımından Koruma***** bileşeninin bu parametresi, tarama sırasında tespit edilmesi istenen tanımlama bilgilerini tanımlar (
- **Arsivleri Tara** - Bu parametreler, tarama işleminin ZIP, RAR gibi belirli bir arşiv türü ile sıkıştırılmış olsa bile tüm dosyaları taramasını öngörür.
- **Bulgusal Analiz Kullan** - bulgusal analiz (*taranan nesnenin sanal bir bilgisayar ortamında dinamik olarak canlandırılması'na ilişkin talimatlar*) tarama sırasında kullanılacak virüs tespiti yöntemlerinden birisidir;
- **Sistem ortamını tara** - tarama işlemi, bilgisayarınızın sistem alanlarını da kontrol edecektir;
- **Rootkit'leri tara** - Tam bilgisayar taraması yaparken rootkit tespitini de yapabilmek için bu öğeyi işaretleyin. Rootkit tespiti işlemi **Anti-Rootkit** bileşeninden de yapabilirsiniz;

Sonra, tarama yapılandırmasını şu şekilde değiştirebilirsiniz:

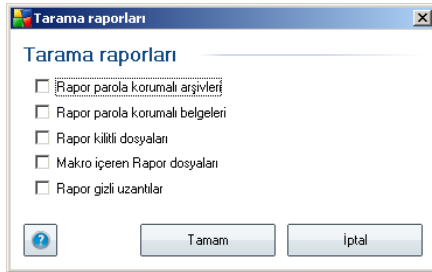
- **Ek tarama ayarları** - Bağlantı, şu parametreleri belirtebileceğiniz yeni bir **Ek tarama ayarları** iletişim kutusu açar:



- **Bilgisayar kapatma seçenekleri** - Çalışan tarama işlemi bittiginde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verir. Bu seçeneği seçerseniz (**Tarama bittikten sonra bilgisayarı kapat**) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını

saglayan bir seçenegin bulunduđu bir pencere açılacaktır (**Bilgisayar kilitliyse bilgisayari kapanmaya zorla**).

- o **Tarama için dosya türlerini tanımla** - Nelerin taranmasını istediğine de karar vermelisiniz:
 - **Tüm dosya türleri** taranmaması gereken virgülle ayrılmış dosya uzantılarının listesini sağlayarak taramada istisnaları tanımlama seçeneğiyle;
 - **Seçili dosya türleri** - Yalnızca virüs bulasabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulamayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya bazı diğer çalıştırılmayan dosyalar*); ortam dosyaları (*video, ses dosyaları - bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulama olasılıkları çok az olduğundan tarama süresini daha da azaltır*). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.
 - İsteğe bağlı olarak, **Uzantıları olmayan dosyaları taramaya** da karar verebilirsiniz - bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmemeniz önerilir. Uzantısı olmayan dosyalar süpheli olabilir ve her zaman taranmalıdır.
- **Tarama işlemi önceligi** - tarama işlemi öncelğini değiştirmek için kaydırma çubuğunu kullanabilirsiniz. Varsayılan olarak öncelik, sistem kaynaklarının kullanımını ve tarama işleminin hızını optimize eden orta seviyeye ayarlanmıştır (*Otomatik tarama*). Buna alternatif olarak, sistem kaynakları kullanımını minimize etmek için tarama işlemini daha yavaş (*bilgisayarda çalışmanız gerektiği ve taramanın ne kadar sürdüğünü önemsemediğiniz durumlar için uygundur*), ya da sistem kaynaklarını oldukça yoğun kullanmak suretiyle daha hızlı (*Örn. bilgisayarı geçici olarak kimse kullanmayacak ise*) gerçekleştirebilirsiniz.
- **Tarama raporu oluşturun** - bağlantı üzerinden **Tarama Raporları** isimli bir iletişim kutusu açılır ve buradan ne tip buluntuların rapor edileceğini seçebilirsiniz:



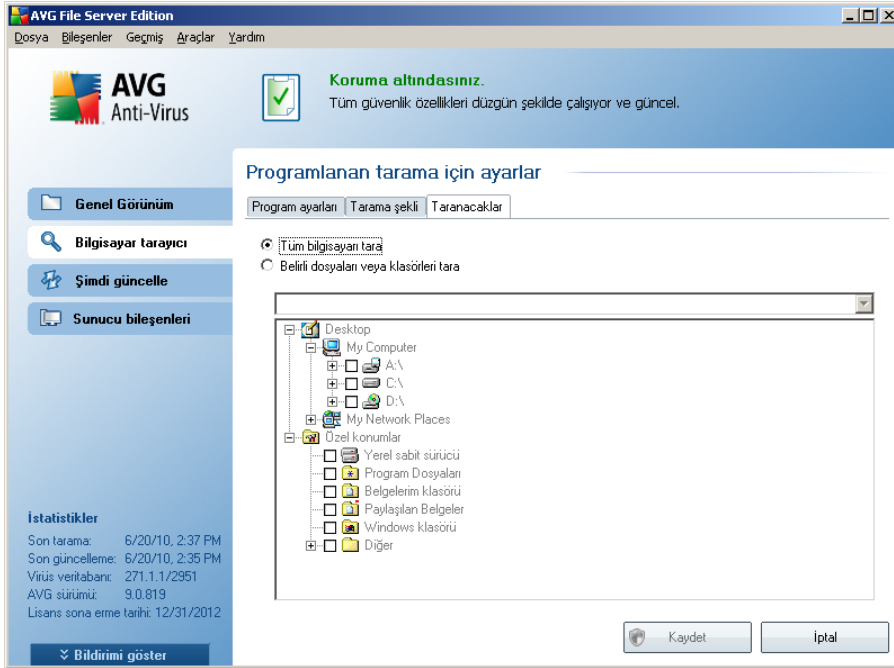
Not: Tarama yapılandırması varsayılan olarak optimum performansta gerçekleşecek şekilde ayarlanmıştır. Tarama ayarlarını değiştirmek için geçerli bir nedeniniz yoksa mevcut yapılandırmayı muhafaza etmeniz önerilmektedir. Yapılandırma, sadece deneyimli kullanıcılar tarafından değiştirilmelidir. Tarama yapılandırma hakkında daha fazla seçenek görmek için **Dosya / Gelismis ayarlar** sistem menüsünden ulaşabileceğiniz [Gelismis ayarlar](#) iletişim kutusunu açın.

Kontrol düğmeleri

Programlı tarama ayarları iletişim kutusunun her üç sekmesinde (**Programlama ayarları**, **Tarama şekli** ve **Taranacaklar**) iki kontrol düğmesi bulunmaktadır ve hangi sekmede olduğunuz önemli olmaksızın bunların fonksiyonları aynıdır:

- **Kaydet** - bu sekmede veya bu iletişim kutusunun başka herhangi bir sekmesinde gerçekleştirdiğiniz tüm değişiklikleri kaydeder ve [AVG tarama arayüzü varsayılan penceresine](#) geri döner. Bu nedenle tüm sekmelerdeki test parametrelerini yapılandırmak istiyorsanız gereksinimlerinizin tamamını belirledikten sonra bunları kaydetmek için düğmeye basın.
- **İptal**- bu iletişim kutusunun bu sekmesinde veya başka bir sekmesinde yaptığınız değişiklikleri iptal eder ve [AVG tarama arayüzü varsayılan iletişim kutusuna geri döner](#).

11.5.3. Taranacaklar



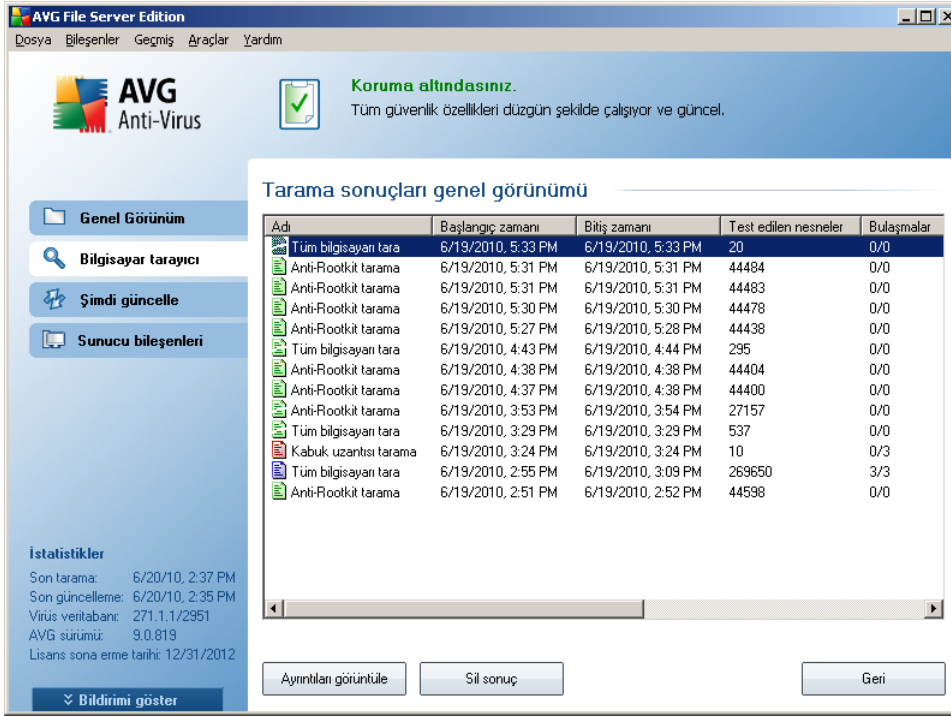
Taranacaklar sekmesinde, [tüm bilgisayarı tarama](#) veya [belirli dosya veya klasörleri taramayı](#) programlamak isteyip istemediğinizi belirleyebilirsiniz. Belirli dosya ve klasörleri taramayı seçerseniz, bu iletişim penceresinin alt kısmında görüntülenen ağaç yapısı etkinleşir ve taranacak klasörleri seçebilirsiniz.

Programlı tarama iletişim kutusuna dair ayarların kontrol düğmeleri

Programlı tarama ayarları iletişim kutusunun üç sekmesinde (**Programlama ayarları**, **Tarama şekli** ve **Taranacaklar**) iki kontrol düğmesi bulunmaktadır ve hangi sekmede olduğunuz önemli olmaksızın aşağıdaki düğmelerin fonksiyonları aynıdır:

- **Kaydet** - bu sekmede veya bu iletişim kutusunun başka herhangi bir sekmesinde gerçekleştirdiğiniz tüm değişiklikleri kaydeder ve [AVG tarama arayüzü varsayılan penceresine](#) geri döner. Bu nedenle tüm sekmelerdeki test parametrelerini yapılandırmak istiyorsanız gereksinimlerinizi tamamını belirledikten sonra bunları kaydetmek için düğmeye basın.
- **İptal** - bu iletişim kutusunun bu sekmesinde veya başka bir sekmesinde yaptığınız değişiklikleri iptal eder ve [AVG tarama arayüzü varsayılan iletişim kutusuna geri döner](#).


11.6. Tarama Sonuçları Genel Görünümü





Adı	Başlangıç zamanı	Bitiş zamanı	Test edilen nesnelere	Bulaşmalar
Tüm bilgisayarı tara	6/19/2010, 5:33 PM	6/19/2010, 5:33 PM	20	0/0
Anti-Rootkit tarama	6/19/2010, 5:31 PM	6/19/2010, 5:31 PM	44484	0/0
Anti-Rootkit tarama	6/19/2010, 5:31 PM	6/19/2010, 5:31 PM	44483	0/0
Anti-Rootkit tarama	6/19/2010, 5:30 PM	6/19/2010, 5:30 PM	44478	0/0
Anti-Rootkit tarama	6/19/2010, 5:27 PM	6/19/2010, 5:28 PM	44438	0/0
Tüm bilgisayarı tara	6/19/2010, 4:43 PM	6/19/2010, 4:44 PM	295	0/0
Anti-Rootkit tarama	6/19/2010, 4:38 PM	6/19/2010, 4:38 PM	44404	0/0
Anti-Rootkit tarama	6/19/2010, 4:37 PM	6/19/2010, 4:38 PM	44400	0/0
Anti-Rootkit tarama	6/19/2010, 3:53 PM	6/19/2010, 3:54 PM	27157	0/0
Tüm bilgisayarı tara	6/19/2010, 3:29 PM	6/19/2010, 3:29 PM	537	0/0
Kabuk uzantısı tarama	6/19/2010, 3:24 PM	6/19/2010, 3:24 PM	10	0/3
Tüm bilgisayarı tara	6/19/2010, 2:55 PM	6/19/2010, 3:09 PM	269650	3/3
Anti-Rootkit tarama	6/19/2010, 2:51 PM	6/19/2010, 2:52 PM	44598	0/0

Tarama sonuçlarına genel bakış penceresine, [AVG tarama arayüzünde Tarama geçmişi](#) düğmesine basarak ulaşabilirsiniz. İletişim kutusunda, daha önce baslatılan tüm taramalar ve sonuçları hakkında bilgi bulunmaktadır.

- **Adı** - taramanın amacı; [öntanimli taramalardan](#) birinin adı ya da [programladığınız taramaya](#) verdığınız adlardan biri olabilir. Her ismin yanında tarama sonucunu belirten bir simge bulunmaktadır:

 - yeşil simge tarama sırasında herhangi bir bulaşmanın tespit edilemediğini gösterir

 - mavi simge tarama sırasında bir bulaşmanın tespit edildiğini ancak bulaşmış nesnenin otomatik olarak silindiğini gösterir

 - kırmızı simge tarama sırasında bir bulaşmanın tespit edildiğini, ancak bulaşmış nesnenin silinemediğini gösterir!

Simgeler bütün halinde ya da yarısı kesilmiş olabilir - bütün halindeki simge, tarama işleminin doğru şekilde tamamlandığını ve bitirildiğini

gösterirken yarisi kesilmiş simge, taramanın iptal edildiğini ya da kesildiğini gösterir.

Not: Taramaların her biri hakkında ayrıntılı bilgi almak için lütfen **Ayrıntıları Görüntüle** düğmesine (bu pencerenin alt kısmındadır) basarak ulaşabileceğiniz **Tarama Sonuçları** penceresini inceleyin.

- **Baslangıç zamanı** - taramanın başlatıldığı tarih ve saati gösterir.
- **Bitiş zamanı** - taramanın bittiği tarih ve saati gösterir.
- **Taranan nesnelere** - tarama sırasında kontrol edilen nesne sayısıdır
- **Bulasmalar** - tespit edilen / silinen [virüs bulasmaları](#) sayısı
- **Casus yazılım** - tespit edilen / silinen [casus yazılım](#) sayısı
- **Tarama kaydı bilgileri** - tarama işlemine ve sonucuna ilişkin bilgiler (genellikle işlemin tamamlanmasının ya da kesilmesinin hemen ardından görüntülenir)

Kontrol düğmeleri

Tarama sonuçlarına genel bakış penceresindeki kontrol düğmeleri şunlardır:

- **Ayrıntıları görüntüle** - bu düğme, yukarıdaki genel bakış ekranından belirli bir tarama seçildiyse etkin hale gelir; seçilen tarama hakkında ayrıntılı bilgi görüntülemek için **Tarama sonuçları** düğmesine basın
- **Sonuçları sil** - bu düğme, yukarıdaki genel bakış ekranından belirli bir tarama seçildiyse etkin hale gelir; seçilen öğeyi tarama sonuçlarına genel bakış penceresinden silmek için düğmeye basın
- **Geri** - [AVG tarama arayüzünün öntanımlı iletişim penceresine geri döner](#)

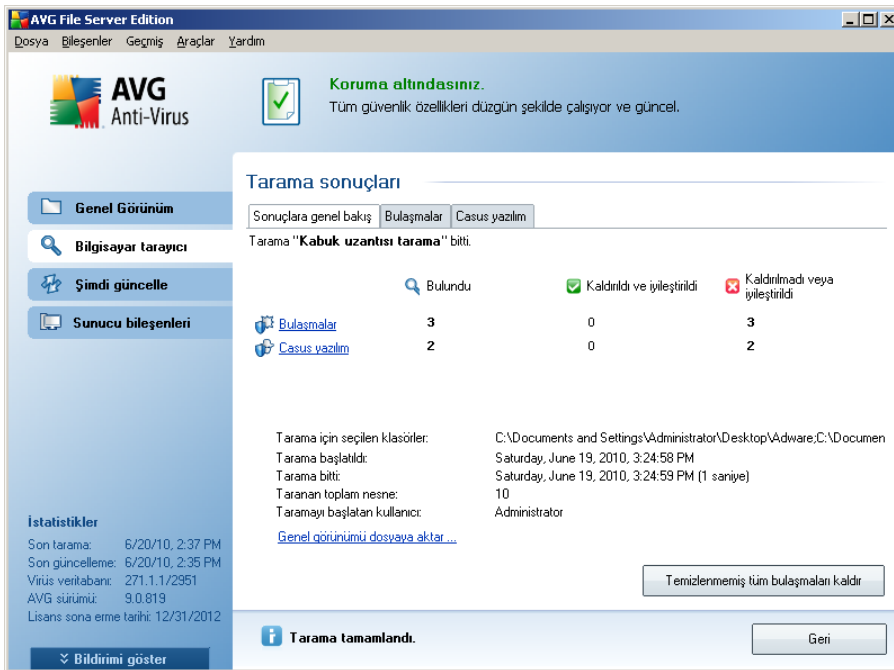
11.7. Tarama Sonuçları Ayrıntıları

Tarama Sonuçlarına Genel Bakış penceresinde belirli bir tarama türü seçildiyse tarama ve seçilen taramanın sonuçları hakkında ayrıntılı bilgi veren **Tarama Sonuçları** penceresini açmak için **Ayrıntıları görüntüle** düğmesine tıklayabilirsiniz.

İletişim penceresi çok sayıda sekme ayrılır:

- **[Sonuçlara Genel Bakis](#)** - bu sekme daima görüntülenir ve tarama işlemini tanımayan istatistik verileri sunar.
- **[Bulaşmalar](#)** - bu sekme tarama sırasında [virüs bulaşması](#) tespit edilirse görüntülenir
- **[Casus yazılım](#)** - bu sekme tarama sırasında [casus yazılım](#) tespit edilirse görüntülenir
- **[Uyarılar](#)** - bu sekme, tarama sırasında taranamayan nesnelere tespit edildiğinde görüntülenir
- **[Kök kullanıcı](#)** - bu sekme tarama sırasında [kök kullanıcı](#) tespit edilirse görüntülenir
- **[Bilgi](#)** - bu sekme, yukarıdaki kategorilerde sınıflandırılmayan potansiyel tespit edildiğinde görüntülenir; ardından söz konusu sekmede buluntu hakkında bir uyarı mesajı görüntülenir

11.7.1. Sonuçlara Genel Bakis Sekmesi



The screenshot shows the AVG File Server Edition interface. The main window displays the AVG Anti-Virus logo and a status message: "Koruma altındasınız. Tüm güvenlik özellikleri düzgün şekilde çalışıyor ve güncel." Below this, the "Tarama sonuçları" section is active, showing results for a search named "Kabuk uzantısı tarama". The search is completed. The results table shows:

	Bulundu	Kaldırıldı ve iyileştirildi	Kaldırılmadı veya iyileştirildi
Bulaşmalar	3	0	3
Casus yazılım	2	0	2

Below the table, the search details are listed:

- Tarama için seçilen klasörler: C:\Documents and Settings\Administrator\Desktop\Adware;C:\Documen
- Tarama başlatıldı: Saturday, June 19, 2010, 3:24:58 PM
- Tarama bitti: Saturday, June 19, 2010, 3:24:59 PM (1 saniye)
- Taranan toplam nesne: 10
- Taramayı başlatan kullanıcı: Administrator

There is a button "Genel görünümü dosyaya aktar ..." and a button "Temizlenmemiş tüm bulaşmaları kaldır". At the bottom, a status bar indicates "Tarama tamamlandı." and a "Geri" button.

Tarama sonuçları sekmesinde aşağıdaki hususlar hakkında ayrıntılı istatistikler ve bilgi

bulabilirsiniz:

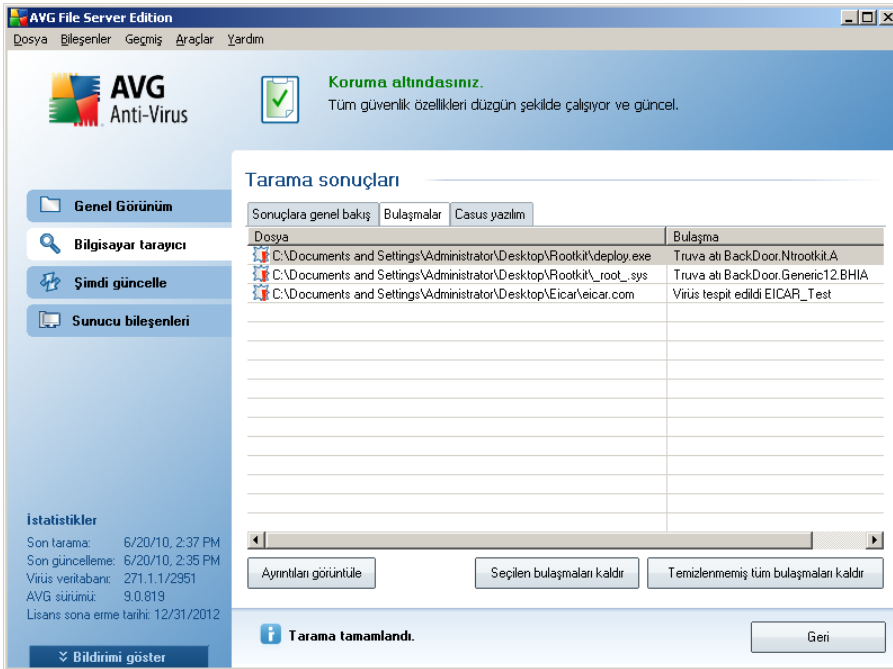
- tespit edilen [virüs bulasmaları](#) / [casus yazılım](#) / [uyarılar](#) / [rootkit'ler](#) / [bilgi](#)
- kaldırıldı [virüs bulasmaları](#) / [casus yazılım](#) / [uyarılar](#) / [rootkit'ler](#)
- virüs bulasmaları [sayısı](#) / [casus yazılım](#) / [uyarılar](#) / [rootkit'ler](#) kaldırılamayan veya temizlenemeyen

Buna ek olarak, tarama başlangıcı hakkında tam tarih ve zaman verileri, toplam taranan nesne sayısı, tarama süresi ve tarama sırasında ortaya çıkan hataların sayısı ve taramayı başlatan kullanıcı hakkında da bilgi bulabilirsiniz.

Kontrol düğmeleri

Bu iletişim kutusunda yalnızca iki kontrol düğmesi bulunur. **Sonuçları kapat** düğmesi **Tarama sonuçlarına genel bakış** iletişim kutusuna dönmeyi sağlar. **Temizlenmemiş tüm bulasmaları kaldır** düğmesi yalnızca tarama otomatik olarak kaldıramayacağı tehlikeler algılandığında görünür. Tıklatıldığında bu tür tehlikeler **Virüs Kasası**'na tasınırlanır.

11.7.2. Bulasma Sekmesi



AVG File Server Edition

Dosya Bileşenler Geçmiş Araçlar Yardım

AVG
Anti-Virus

Koruma altındasınız.
Tüm güvenlik özellikleri düzgün şekilde çalışıyor ve güncel.

Tarama sonuçları

Sonuçlara genel bakış Bulasmalar Casus yazılım

Dosya	Bulasma
C:\Documents and Settings\Administrator\Desktop\Rootkit\deploy.exe	Truva atı BackDoor.Ntrootkit.A
C:\Documents and Settings\Administrator\Desktop\Rootkit\root.sys	Truva atı BackDoor.Generic12.BHIA
C:\Documents and Settings\Administrator\Desktop\Eicar\veicar.com	Virüs tespit edildi EICAR_Test

Ayrıntıları görüntüle Seçilen bulasmaları kaldır Temizlenmemiş tüm bulasmaları kaldır

Tarama tamamlandı. Geri

İstatistikler
Son tarama: 6/20/10, 2:37 PM
Son güncelleme: 6/20/10, 2:35 PM
Virüs veritabanı: 271.1.1/2951
AVG sürümü: 9.0.819
Lisans sona erme tarihi: 12/31/2012

Bildirimi göster

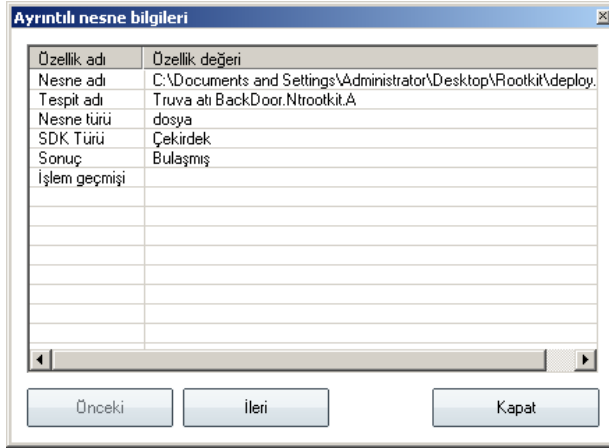
Tarama sırasında bir [virüs bulasmasi](#) tespit edilirse ilgili **Bulasmalar** sekmesi sadece **Tarama Sonuçları** iletişim kutusunda görüntülenir. Sekme, su bilgileri sağlayan üç bölüme ayrılmıştır:

- **Dosya** - bulasmis nesnenin orijinal konumunun tam dizin yolu
- **Bulasmalar** - tespit edilen [virüs](#)ün adı (*belirli virüs türleri hakkında ayrıntılı bilgi almak için lütfen çevrimiçi [Virüs Ansiklopedisine](#) danisin*)
- **Sonuç** - tarama sırasında tespit edilen bulasmis nesnenin mevcut durumunu tanımlar:
 - **Bulasanlar** - bulasan nesne tespit edildi ve orijinal konumunda bırakıldı (*örneğin _ belirli bir tarama işlemi sırasında otomatik temizleme seçeneğini devre dışı bıraktıysanız*)
 - **Temizlenenler** - bulasmis nesne otomatik olarak temizlenmiştir ve orijinal konumunda bırakılmıştır
 - **Virüs Kasasına Tasınanlar** - bulasmis nesne [Virüs Kasası](#) karantinasına taşınmıştır
 - **Silinenler**- bulasmis nesne silinmiştir
 - **PUP istisnalarına eklenenler** -bulgu bir istisna olarak değerlendirilmiş ve PUP istisnaları listesine eklenmiştir (*gelismis ayarların [PUP Istisnaları](#) iletişim kutusundan yapılandırılır*)
 - **Kilitli dosya - taranamayanlar** - ilgili nesne kilitlidir ve bu nedenle AVG tarafından taranamamaktadır
 - **Potansiyel olarak tehlikeli nesne** - nesnenin potansiyel anlamda tehlikeli olduğu tespit edilmiş fakat nesneye herhangi bir virüs bulasmamıştır (*örneğin makro içeriyor olabilir*); bilgi sadece uyarı amaçlıdır
 - **Eylemi tamamlamak için bilgisayarınızın yeniden başlatılması gerekmektedir** - bulasmis nesne silinememektedir ya da nesneyi tamamen silmek için bilgisayarınızın yeniden başlatılması gerekmektedir

Kontrol düğmeleri

Bu iletişim kutusunda kullanılabilir üç kontrol düğmesi var:

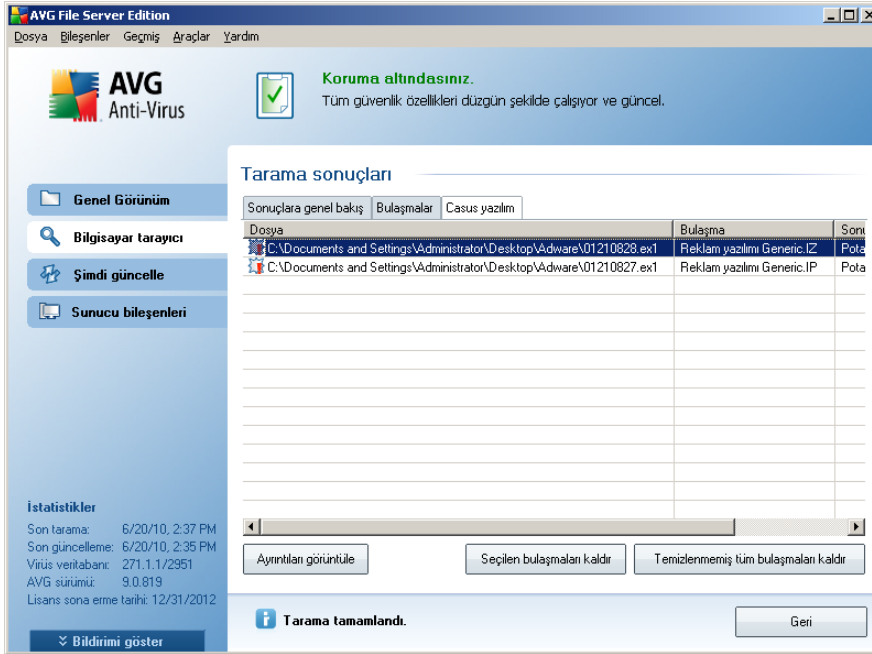
- **Ayrıntıları görüntüle** - düğme Ayrıntılı nesne bilgileri adlı yeni bir iletişim kutusu penceresi açar:



Bu iletişim kutusunda tespit edilen bulasıcı nesnenin konumuna dair bilgileri bulabilirsiniz(**Nesne adı**). **Geri /İleri** düğmelerini kullanarak belirli bulgular hakkında ayrıntılı bilgi görüntüleyebilirsiniz. İletişim kutusunu kapatmak için **Kapat** düğmesine tıklayın.

- **Seçilen bulasmaları kaldır** - düğmeyi seçili bulguları iyilestirmek veya **Virüs Kasası**'na tasımak için kullanın (iyileştirilemezse)
- **Temizlenmemiş tüm bulasmaları kaldır** - düğmeyi listedeki tüm bulguları iyilestirmek veya **Virüs Kasası**'na tasımak için kullanın (iyileştirilemezse)
- **Sonuçları kapat** - ayrıntılı bilgi penceresini kapatır ve **Tarama sonuçlarına genel bakış** iletişim kutusuna döner

11.7.3. Casus Yazılım Sekmesi



The screenshot shows the AVG File Server Edition interface. The main window displays a status message: "Koruma altındasınız. Tüm güvenlik özellikleri düzgün şekilde çalışıyor ve güncel." Below this, the "Tarama sonuçları" (Search Results) section is active, showing a table with two rows of detected spyware. The table has columns for "Dosya" (File), "Bulaşma" (Infection), and "Sonuç" (Result). The first row shows a file named "C:\Documents and Settings\Administrator\Desktop\Adware\01210828.exe1" with the infection type "Reklam yazılımı Generic.IZ" and the result "Pota". The second row shows a file named "C:\Documents and Settings\Administrator\Desktop\Adware\01210827.exe1" with the infection type "Reklam yazılımı Generic.IP" and the result "Pota". The interface also includes a sidebar with navigation options like "Genel Görünüm", "Bilgisayar taramacı", "Şimdi güncelle", and "Sunucu bileşenleri". At the bottom left, there are statistics for the last scan and update. At the bottom right, there are buttons for "Ayrıntılı görüntüle", "Seçilen bulaşmaları kaldır", "Temizlenmemiş tüm bulaşmaları kaldır", and "Geri".

Dosya	Bulaşma	Sonuç
C:\Documents and Settings\Administrator\Desktop\Adware\01210828.exe1	Reklam yazılımı Generic.IZ	Pota
C:\Documents and Settings\Administrator\Desktop\Adware\01210827.exe1	Reklam yazılımı Generic.IP	Pota

Tarama sırasında bir [casus yazılım](#) tespit edilirse ilgili **Casus Yazılım** sekmesi sadece **Tarama Sonuçları** iletişim kutusunda görüntülenir. Sekme, şu bilgileri sağlayan üç bölüme ayrılmıştır:

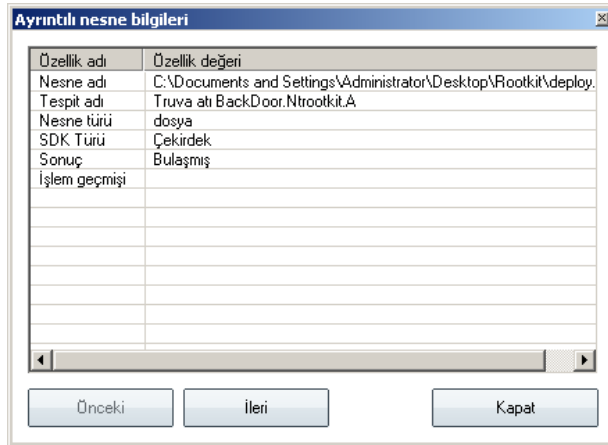
- **Dosya** - bulasmis nesnenin orijinal konumunun tam dizin yolu
- **Bulaşmalar** - tespit edilen [casus yazılım](#)ın adı (*belirli virüs türleri hakkında ayrıntılı bilgi almak için lütfen çevrimiçi [Virüs Ansiklopedisine](#) danisin*)
- **Sonuç** - tarama sırasında tespit edilen nesnenin mevcut durumunu tanımlar:
 - **Bulasanlar** - bulasan nesne tespit edildi ve orijinal konumunda bırakıldı (örneğin _ belirli bir tarama işlemi sırasında otomatik temizleme seçeneğini devre dışı bıraktıysanız)
 - **Temizlenenler** - bulasmis nesne otomatik olarak temizlenmiştir ve orijinal konumunda bırakılmıştır
 - **Virüs Kasasına Tasinanlar** - bulasmis nesne [Virüs Kasası karantinasına tasınmıştır](#)

- **Silinenler**- bulasmis nesne silinmistir
- **PUP istisnalarina eklenenler** -bulgu bir istisna olarak degerlendirilmis ve PUP istisnolari listesine eklenmistir (*gelismis ayarlarin [PUP Istisnolari](#) iletisim kutusundan yapilandirilir*)
- **Kilitli dosya - taranmayanlar** - ilgili nesne kilitlidir ve bu nedenle AVG tarafından taranamamaktadır
- **Potansiyel olarak tehlikeli nesne** - nesnenin potansiyel anlamda tehlikeli oldugu tespit edilmiş fakat nesneye herhangi bir virüs bulasmamıştır (örneğin makro içeriyor olabilir); bilgi sadece uyarı amaçlıdır
- **Eylemi tamamlamak için bilgisayarınızın yeniden baslatılması gerekmektedir** - bulasmis nesne silinememektedir ya da nesneyi tamamen silmek için bilgisayarınızın yeniden baslatılması gerekmektedir

Kontrol düğmeleri

Bu iletisim kutusunda kullanilabilir üç kontrol düğmesi var:

- **Ayrıntıları görüntüle** - düğme, **Tarama sonuçları hakkında ayrıntılı bilgi** isimli yeni bir iletisim kutusu penceresi açar:



Bu iletisim kutusunda tespit edilen bulasici nesnenin konumuna dair bilgileri bulabilirsiniz(**Nesne adı**). **Geri /İleri** düğmelerini kullanarak belirli bulgular hakkında ayrıntılı bilgi görüntüleyebilirsiniz. İletisim kutusunu kapatmak için **Kapat** düğmesine tıklayın.

- **Seçilen bulasmaları kaldır** - düğmeyi seçili bulguları iyilestirmek veya [Virüs Kasası](#)'na tasimak için kullanin (iyileştirilemezse)
- **Temizlenmemiş tüm bulasmaları kaldır** - düğmeyi listedeki tüm bulguları iyilestirmek veya [Virüs Kasası](#)'na tasimak için kullanin (iyileştirilemezlerse)
- **Sonuçları kapat** - ayrıntılı bilgi penceresini kapatir ve [Tarama sonuçlarına genel bakış](#) iletişim kutusuna döner

11.7.4. Uyarılar Sekmesi

Uyarılar sekmesinde, tarama sırasında tespit edilip "şüpheli duyulan" nesnelere (*tipik olarak dosyalar*) hakkında çeşitli bilgiler görüntülenir. [Yerleşik Kalkan](#) tarafından tespit edildiği zaman tespit edilen dosyalara erişim engellenir. Bu şekilde tespit edilen buluntulardan bazıları gizli dosyalar, tanımlama bilgileri, şüpheli kayıt anahtarları, parola korumalı belgeler ya da arşivlerdir. Bu dosyalar bilgisayarınıza ya da güvenliğinize karşı doğrudan tehlike teşkil etmez. Bu dosyalar hakkında verilen bilgiler, bilgisayarınızda reklam yazılımı ya da casus yazılım tespit edildiği durumlarda oldukça yararlıdır. AVG testi tarafından sadece Uyarılar tespit edildiği takdirde herhangi bir işlem yapmanıza gerek kalmaz.

Aşağıda bu tür nesnelere ilişkin en yaygın örnekler kısaca açıklanmıştır:

- **Gizli dosyalar** - Gizli dosyalar, Windows'da varsayılan olarak görünmez durumdadır ve bazı virüsler ya da diğer tehditler dosyalarını söz konusu gizli dosyalara kaydederek algılanma ihtimallerini ortadan kaldırmaya çalışır. AVG'niz, zararlı olabileceğinden şüphelendiğiniz gizli bir dosya rapor ederse, [AVG Virüs Kasası](#)'na tasiyabilirsiniz.
- **Tanımlama Bilgileri** - Tanımlama bilgileri, kullanıcılara ilişkin bilgileri kaydetmek ve daha sonra söz konusu bilgileri web site şablonlarını yükleme ve kullanıcı adını girmek üzere web siteleri tarafından kullanılan düz metin dosyalarıdır.
- **Şüpheli kayıt anahtarları** - Bazı kötü amaçlı yazılımlar, sistem başlatıldığında yüklendiğinden emin olmak ya da işletim sistemi üzerindeki etkisini artırmak üzere bilgilerini Windows kayıt defterine kaydeder.

11.7.5. Rootkit'ler Sekmesi

Rootkit'ler sekmesi [Anti-Rootkit tarama](#)'yi baslattiyysanız tarama sirasinda algilanan rootkit'ler hakkında bilgi görüntüler.

Rootkit, sistem yöneticisinin izni olmaksizin yasal olmayan şekillerde bilgisayar sisteminin kontrolünü ele almak için tasarlanmış bir programdır. Rootkit, donanim üzerinde çalışan işletim sisteminin kontrolünü ele geçirmeyi hedeflediği için donanimsal açıdan erişime gerek duymaz. Genellikle rootkit'ler, standart işletim sistemi güvenlik mekanizmalarını dönüştürerek ya da istila ederek sistem üzerindeki varlıklarını gizlerler. Sıklıkla Truva Ati biçimindedirler, dolayısıyla kullanıcıları sistemleri üzerinden çalışacak kadar güvenli olduklarına inandırır. İzleme programlarının çalışan işlemlerini gizlemek ya da işletim sisteminin sistem bilgilerini ya da dosyalarını saklamak, bunu sağlamak için kullanılan teknikler arasında bulunmaktadır.

Bu sekmenin yapısı temel olarak [Bulasmalar sekmesi](#) ya da [Casus Yazılım sekmesi](#) ile aynıdır.

11.7.6. Bilgi Sekmesi

Bilgi sekmesinde, bulasma ya da casus yazılım şeklinde sınıflandırılmayan "buluntular" hakkında bilgi bulunmaktadır. Bunlar tehlikeli şekilde etiketlenebilir ancak söz konusu öğeler hususunda dikkatli olmalısınız. AVG taraması, bulasmayan fakat şüpheli olan dosyaları tespit edebilir. Bu dosyalar [Uyari](#) veya **Bilgi** olarak rapor edilir.

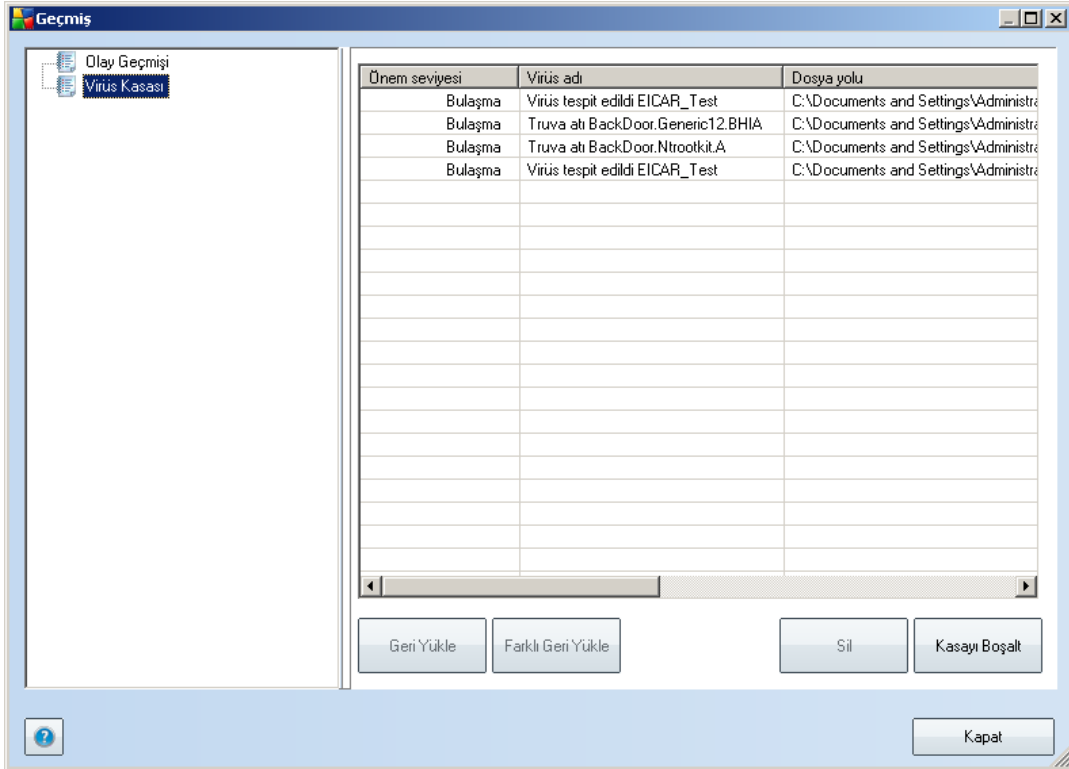
Önem derecesi **Bilgiler** aşağıdaki nedenlerden birine bağlı olarak rapor edilebilir:

- **Çalışma zamanı paketli** - Dosya, dosyanın taranmasını önleme çabası olarak değerlendirilebilecek yaygın olmayan paketleyicilerinden biri kullanılarak paketlenmiştir. Diğer bir yandan bu tür dosyalar her rapor edildiğinde virüs teşkil etmezler.
- **Çalışma zamanı paketi yinelemeli** - Yukarıdakine benzerdir, ancak yaygın yazılımlar arasında nispeten daha az sıklıkta kullanılır. Söz konusu dosyalar şüphelidir ve kaldırılmaları ya da incelenmeleri için bize gönderilmeleri göz önünde bulundurulmalıdır.
- **Parola ile korunan arşiv ya da belge** - Parola ile korunan dosyalar, AVG (ya da genellikle diğer kötü amaçlı yazılımlara karşı koruma programları) tarafından taranamaz.
- **Makro içeren belge** - Rapor edilen belge, zararlı olabilecek makrolar içermektedir.
- **Gizli uzantı** - Gizli uzantılı dosyalar resimler gibi görünebilir, ancak aslında

çalistirilabilir dosyalar olabilir (örn *resim.jpg.exe*). İkinci uzanti, varsayilan olarak Windows'da görünür degildir ve AVG yanlislikla açilmalarini engellemek için bu tür dosyalari rapor eder.

- **Uygun olmayan dosya yolu** - Önemli bir sistem dosyasi varsayilan yoldan baska bir yerden çalisiyorsa (örn. *winlogon.exe* Windows klasöründen baska bir yerde çalisiyorsa) AVG bu durumu rapor eder. Bazi durumlarda virüsler, sistemde fark edilmemek için standart sistem islemlerinin adini alır.
- **Kilitli dosya** - Rapor edilen dosya kilitli, bu yüzden AVG tarafından taranamıyor. Bu, genellikle bir dosyanin sistem tarafından kullanilmakta oldugu anlamina gelir (örn. *takas dosyası*).

11.8. Virüs Kasasi



Virüs Kasasi AVG taramalari sirasinda tespit edilen süpheli/bulasmis nesnelere yönetilmesi için güvenli bir ortamdır. Tarama sirasinda bulasmis bir nesne tespit edildikten sonra AVG, söz konusu bulasmayi otomatik olarak temizleyemiyorsa süpheli nesne hakkında ne yapmak istediginiz sorulur. Önerilen çözüm, nesneyi daha sonra

ilgilenmek üzere **Virüs Kasasına** tasimaktır.

Virüs Kasası arayüzü, yeni bir pencerede açılır ve karantina altındaki bulasmis nesnelere hakkında genel bilgi içerir:

- **Önem seviyesi** - ilgili bulgunun önem seviyesi ve türünün kimliğini sağlar
- **Bulasma türü** - bulguları bulasma seviyelerine göre sınıflandırır (*listelenen tüm nesnelere bulasmis ya da bulasmis olması muhtemel nesnelere*)
- **Virüs Adı** - [Virüs ansiklopedisi](#)'ne (çevrimiçi) göre tespit edilen bulasmanın adını görüntüler
- **Dosya yolu**- Bulasmis dosyanın orijinal konumuna giden tam yol
- **Orijinal nesne adı** - Tabloda listelenmekte olan tespit edilmiş nesnelere, tarama işlemi sırasında AVG tarafından verilen standart isim ile etiketlenmiştir. Nesnenin bilinmeyen farklı bir adı olması halinde (*Örn. bir e-posta ekinin adının ekin mevcut içeriğine yanıt vermemesi halinde*), söz konusu isim bu sütunda gösterilecektir.
- **Saklama tarihi** - Süpheli dosyanın tespit edildiği ve Virüs Kasası'na kaldırıldığı tarih ve saat

Kontrol düğmeleri

Virüs Kasası arayüzünden ulaşabileceğiniz kontrol düğmeleri şunlardır:

- **Geri Yükle** - bulasmis dosyayı sabit diskinizdeki orijinal konumuna geri yükler
- **Farklı Geri Yükle** - tespit edilen süpheli nesneyi **Virüs Kasasından** seçilen bir klasöre geri yüklemek için bu düğmeyi kullanın. Süpheli ve tespit edilen nesne orijinal adıyla kaydedilecektir. Orijinal adı bilinmiyorsa standart adı kullanılacaktır.
- **Sil** - bulasmis dosyayı **Virüs Kasasından** tamamen siler
- **Kasayı Bosalt** - **Virüs Kasası** içeriğini tamamen temizler

12. AVG Güncellemeleri

Yeni bulunan tüm virüslerin mümkün olduğunca çabuk algılanabilmesi için AVG'nizi güncel tutmak çok önemlidir. AVG güncellemeleri sabit tarihlerde değil, yeni tehlikelerin miktarına ve önemine göre yayınlandığından, günde en az bir kez yeni güncellemeleri kontrol etmeniz önerilir. Her 4 saatte bir kontrol etmek, AVG Virüs tabanınızın gün boyunca da güncel kalmasını sağlar.

12.1. Güncelleme Seviyeleri

AVG, arasından seçim yapabileceğiniz iki güncelleme seviyesi sunmaktadır:

- **Tanım güncellemeleri** güvenilir virüsten koruma için gerekli değişiklikleri içerir. Tipik olarak kodu değiştirmemekte, değişiklikler sadece veritabanını kapsamaktadır. Bu güncelleme sunulur sunulmaz yüklenmelidir.
- **Program güncellemeleri** çeşitli program değişikliklerini, onarımlarını ve gelişimlerini içerir.

[Bir güncelleme programlanırken](#) indirme ve uygulanma açısından öncelik sırasını seçmek mümkündür.

12.2. Güncelleme Türleri

İki güncelleme türü arasında seçim yapabilirsiniz:

- **İsteğe Bağlı Güncelleme** ihtiyacınız olduğu durumlarda hemen gerçekleştirilebilecek AVG güncellemesidir.
- **Programlanan güncelleme** - AVG menüsünden [bir güncelleme planı programlayabilirsiniz](#). Programlı güncelleme, yapılandırma ayarlarınıza bağlı olarak periyodik olarak gerçekleştirilir. Belirli bir konumda yeni güncelleme dosyaları bulunur bulunmaz doğrudan İnternet'te ya da ağ dizininden indirilirler. Yeni güncelleme dosyası yoksa herhangi bir işlem yapılmaz.

12.3. Güncelleme İşlemi

Güncelleme işlemi **Şimdi Güncelle** [hızlı bağlantısına](#) tıklanarak istenilen anda başlatılabilir. Bu bağlantıya bütün [AVG Kullanıcı Arayüzü](#) pencerelerinden ulaşabilirsiniz. Diğer bir yandan [Güncelleme yöneticisi](#) bileşeninden düzenlenebilen güncelleme programlarında planlanan güncellemelerin düzenli olarak yapılması önerilmektedir.

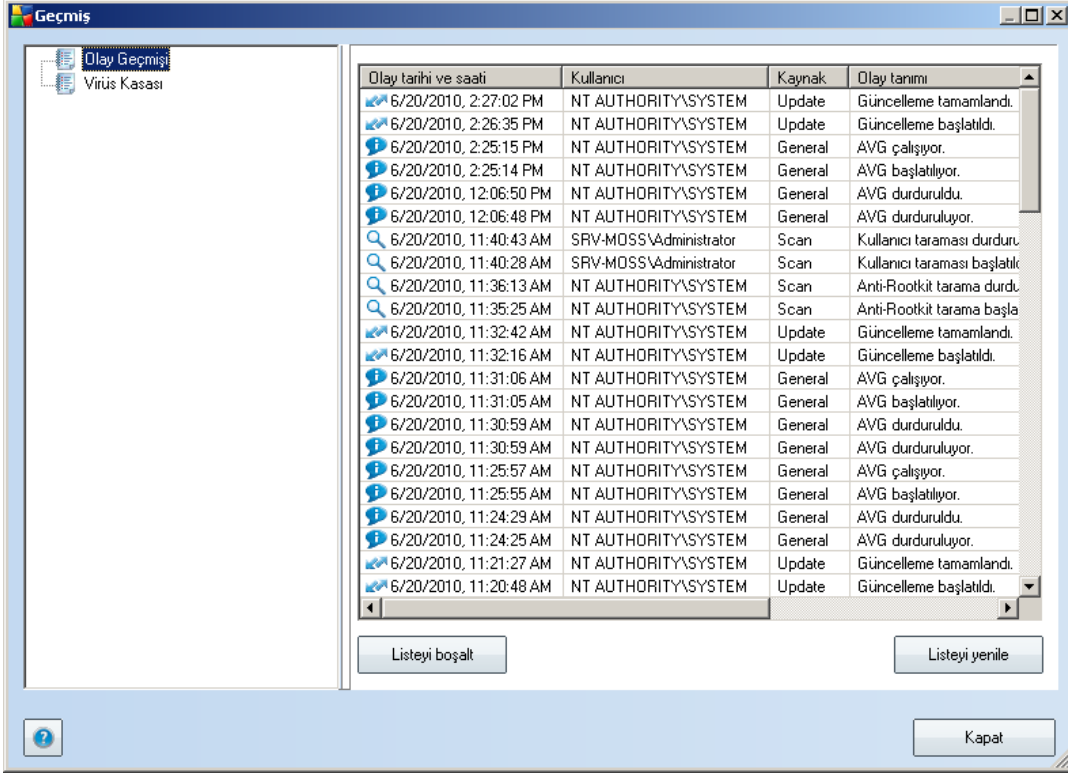
Güncellemeye başladıktan sonra AVG, yeni güncelleme dosyasının olup olmadığını aramaya başlayacaktır. Varsa AVG indirme işlemine başlat ve güncelleme işlemi otomatik olarak başlatır. Güncelleme işlemi sırasında güncelleme işleminin ilerleyişinin



yani sira ilgili istatistiki parametreleri de görüntüleyebileceginiz **Güncelleme** arayüzüne yeniden yönlendirileceksiniz (*güncelleme dosyasinin boyutu, alinan veriler, indirme hizi, kalan süre...*).

Not: AVG program güncellemesi baslatilmadan önce sistem geri yükleme noktası oluşturulur. Güncelleme isleminin basarisiz olmasi ve isletim sisteminizin çökmesi halinde isletme sisteminizi bu noktaya geri döndürebilirsiniz. Bu seçenege Baslat/Tüm Programlar bilgisayarinizin günde an az bir kere açildigindan emin oldugunuz durumlarda önerilir/Donatılar /Sistem Araçlari /Sistem Geri Yükleme menüsünden erisebilirsiniz fakat degisikliklerin sadece uzman kullanıcılar tarafından yapılması önerilmektedir.

13. Olay Geçmisi



Olay tarihi ve saati	Kullanıcı	Kaynak	Olay tanımı
6/20/2010, 2:27:02 PM	NT AUTHORITY\SYSTEM	Update	Güncelleme tamamlandı.
6/20/2010, 2:26:35 PM	NT AUTHORITY\SYSTEM	Update	Güncelleme başlatıldı.
6/20/2010, 2:25:15 PM	NT AUTHORITY\SYSTEM	General	AVG çalışıyor.
6/20/2010, 2:25:14 PM	NT AUTHORITY\SYSTEM	General	AVG başlatılıyor.
6/20/2010, 12:06:50 PM	NT AUTHORITY\SYSTEM	General	AVG durduruldu.
6/20/2010, 12:06:48 PM	NT AUTHORITY\SYSTEM	General	AVG durduruluyor.
6/20/2010, 11:40:43 AM	SRV-MOSS\Administrator	Scan	Kullanıcı taraması durdu.
6/20/2010, 11:40:28 AM	SRV-MOSS\Administrator	Scan	Kullanıcı taraması başlatıldı.
6/20/2010, 11:36:13 AM	NT AUTHORITY\SYSTEM	Scan	Anti-Rootkit tarama durdu.
6/20/2010, 11:35:25 AM	NT AUTHORITY\SYSTEM	Scan	Anti-Rootkit tarama başla
6/20/2010, 11:32:42 AM	NT AUTHORITY\SYSTEM	Update	Güncelleme tamamlandı.
6/20/2010, 11:32:16 AM	NT AUTHORITY\SYSTEM	Update	Güncelleme başlatıldı.
6/20/2010, 11:31:06 AM	NT AUTHORITY\SYSTEM	General	AVG çalışıyor.
6/20/2010, 11:31:05 AM	NT AUTHORITY\SYSTEM	General	AVG başlatılıyor.
6/20/2010, 11:30:59 AM	NT AUTHORITY\SYSTEM	General	AVG durduruldu.
6/20/2010, 11:30:59 AM	NT AUTHORITY\SYSTEM	General	AVG durduruluyor.
6/20/2010, 11:25:57 AM	NT AUTHORITY\SYSTEM	General	AVG çalışıyor.
6/20/2010, 11:25:55 AM	NT AUTHORITY\SYSTEM	General	AVG başlatılıyor.
6/20/2010, 11:24:29 AM	NT AUTHORITY\SYSTEM	General	AVG durduruldu.
6/20/2010, 11:24:25 AM	NT AUTHORITY\SYSTEM	General	AVG durduruluyor.
6/20/2010, 11:21:27 AM	NT AUTHORITY\SYSTEM	Update	Güncelleme tamamlandı.
6/20/2010, 11:20:48 AM	NT AUTHORITY\SYSTEM	Update	Güncelleme başlatıldı.

Etkinlik Geçmisi iletişim kutusuna [sistem menüsü](#) üzerinden **Geçmiş/Etkinlik Geçmisi Kayıt Defteri** öğesi vasıtasıyla ulaşabilirsiniz. Bu iletişim kutusu içinde, **AVG 9.0 File Server** işlemi sırasında oluşan önemli olayların bir özetini bulabilirsiniz. **Etkinlik Geçmisi** aşağıdaki etkinlik türlerini kaydeder:

- AVG uygulamasının güncellemeleri hakkında bilgi
- Tarama başlangıcı, sonu veya taramanın durdurulması (otomatik olarak gerçekleştirilen taramalar dahil olmak üzere)
- Virüs tespitine ilişkin etkinlikler ve virüsün konumu ([Yerlesik Kalkan](#) ya da [tarama](#) tarafından)
- Diğer önemli etkinlikler

Kontrol düğmeleri



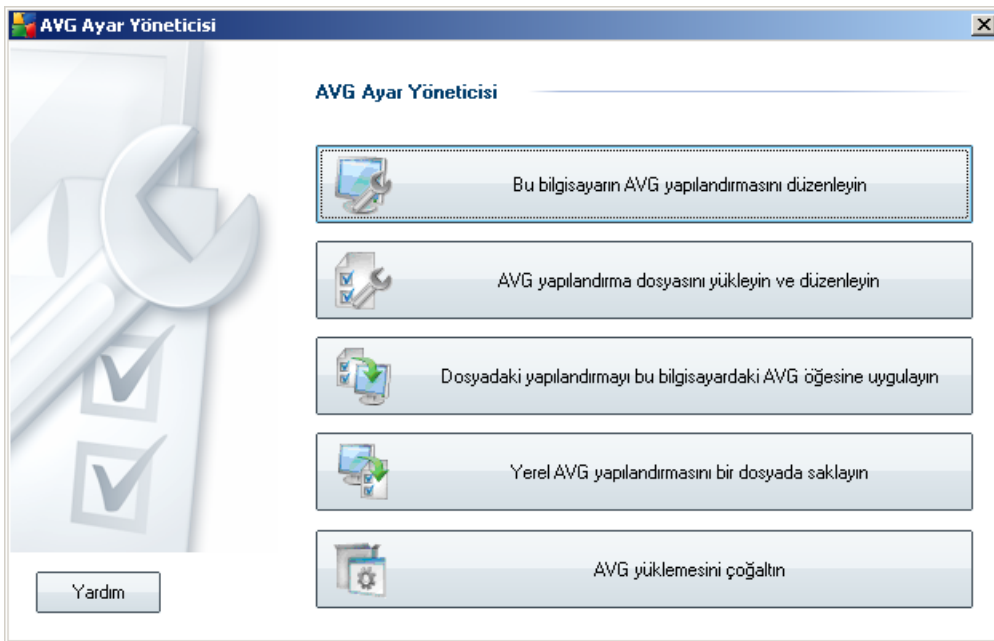
- **Listeyi temizle** - etkinlik listesindeki tüm girisleri siler
- **Listeyi yenile** - etkinlik listesindeki tüm girisleri günceller

14. AVG Ayarları Yöneticisi

AVG Ayar Yöneticisi, temel olarak AVG yapılandırmasını kopyalayabildiğiniz, düzenleyebildiğiniz ve dağıtabildiğiniz daha küçük ağlar için uygun bir araçtır. Yapılandırma taşınabilir bir cihaza kaydedilebilir (USB flash sürücü vb.) ve sonra istasyonları seçmek için manuel olarak uygulanır.

Araç AVG yüklemesinde bulunur ve Windows Başlat menüsünden kullanılabilir:

Tüm Programlar/AVG 9.0/AVG Ayar Yöneticisi



- ***Bu bilgisayarın AVG yapılandırmasını düzenle***

Bu düğmeyi iletişim kutusunu yerel AVG'nizin gelişmiş ayarlarıyla açmak için kullanın. Burada yapılan tüm ayarlar yerel AVG yüklemesine de yansitilir.

- ***AVG yapılandırma dosyasını yükle ve düzenle***

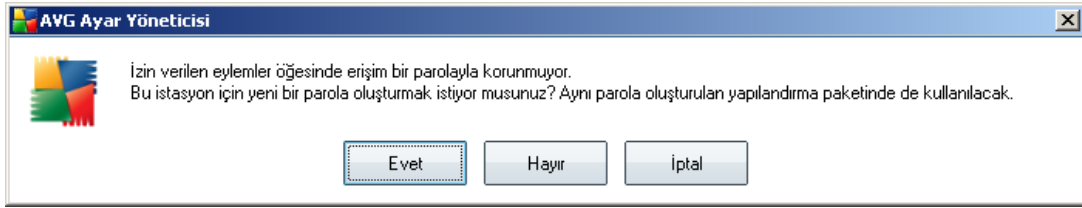
Zaten bir AVG yapılandırma dosyanız (.pck) varsa, düzenlemek için bu düğmeyi kullanın. **Tamam** veya **Uygula** düğmesiyle değişiklikleri onayladığınızda, dosya yeni ayarlarla değiştirilir!

- ***Bu bilgisayarda yapılandırmayı dosyadan AVG'ye uygula***

Bu düğmeyi bir AVG yapılandırma dosyası (.pck) açmak ve AVG'nin yerel yüklemesine uygulamak için kullanın.

- **Yerel AVG yapılandırmasını bir dosyaya kaydet**

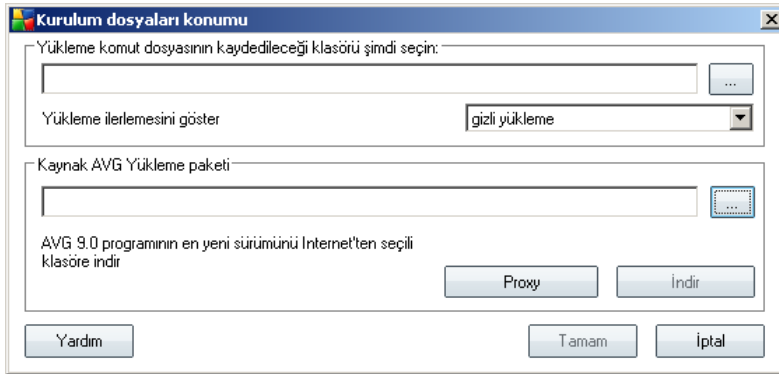
Bu düğmeyi yerel AVG yüklemesinin AVG yapılandırma dosyasını (.pck) kaydetmek için kullanın. İzin verilen eylemler için bir parola ayarlamadıysanız, aşağıdaki iletişim kutusuyla karşılaşacaksınız:



İzin verilen öğelere şimdi erişmek için parola ayarlamak istiyorsanız **Evet** öğesini seçin ve sonra gerekli bilgileri doldurun ve seçiminizi onaylayın. Parola oluşturmayı atlamak ve yerel AVG yapılandırmasını bir dosyaya kaydetmek istiyorsanız **Hayır** öğesini seçin.

- **AVG yüklemesini çoğalt**

Bu seçenek, özel seçeneklerle yükleme paketi oluşturarak yerel AVG yüklemesinin tam bir kopyasını yapmanızı sağlar. İlerlemek için, önce yükleme komut dosyasının kaydedileceği klasörü seçin.



Sonra, açılır menüden aşağıdakilerden birini seçin:

- **Gizli yükleme** - kurulum işlemi sırasında hiç bilgi görüntülenmez.
- **Yalnızca yükleme ilerlemesini göster** - yükleme kullanıcının dikkat



etmesini gerektirmez, ancak ilerleme tam olarak görülebilir.

- o **Yükleme sihirbazını göster** - yükleme görünür olacaktır ve kullanıcının tüm adımları manuel olarak onaylaması gerekir.

En son kullanılabilir AVG yükleme paketini doğrudan AVG web sitesinden seçili klasöre indirmek için **İndir** düğmesini kullanın veya manuel olarak AVG yükleme paketini o klasöre koyun.

Ağınız başarılı bir bağlantı için gerektiriyorsa **Proxy** düğmesini proxy sunucusu ayarlarını tanımlamak için kullanabilirsiniz.

Tamam düğmesini tıklattığınızda klonlama işlemi başlar ve kısa bir sürede bitmelidir. Ayrıca izin verilen öğeler için parola ayarlama hakkında size soru soran bir iletişim kutusu da görürsünüz (yukarıya bakın). Bittiginde, seçili klasörde diğer dosyalarla birlikte **AvgSetup.bat** dosyası bulunmalıdır. **AvgSetup.bat** dosyasını çalıştırırsanız, AVG'yi yukarıda seçilen parametrelere göre yükler.



15. SSS ve Teknik Destek

Isletmenizde ya da teknik aıdan AVG ile herhangi bir sorun yatarsanız ltfen, AVG web sitesinin (<http://www.avg.com>) **SSS** blmne bakın.

Bu sekilde yardım alamazsanız teknik destek blmne e-posta ile basvurun. Ltfen **Yardım/evrimii yardım al** sistem mensnden ulaşabileceğiniz iletişim formunu kullanın.