



AVG Email Server Edition 2012

Kullanıcı Kılavuzu

Belge revizyonu 2012.06 (2/28/2012)

Telif Hakkı AVG Technologies CZ, s.r.o. Tüm hakları saklıdır.
Tüm diğer ticari markalar ilgili sahiplerine aittir.

Bu ürün, RSA Data Security, Inc. MD5 Message-Digest Algorithm özelliğini kullanmaktadır, Telif Hakkı (C) 1991-2, RSA Data Security, Inc. Oluşturma Tarihi: 1991.

Bu üründe, C-SaCzech kütüphanesi, Telif Hakkı (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz) kodları kullanılmaktadır.

Bu ürün sıkıştırma kitaplığı zlib ürününü kullanmaktadır, Telif Hakkı (c) 1995-2002 Jean-loup Gailly ve Mark Adler.



İçindekiler

1. Giriş	4
2. AVG Yükleme Gereksinimleri	5
2.1 Desteklenen İşletim Sistemleri	5
2.2 E-posta Sunucuları Desteklendi	5
2.3 Donanım Gereksinimleri	5
2.4 Önceki Sürümleri Kaldır	5
2.5 MS Exchange Hizmet Paketleri	6
3. AVG Yükleme Süreci	7
3.1 Yükleme Başlatma	7
3.2 Lisansınızı Etkinleştirin	8
3.3 Yükleme Türünü Seçin	9
3.4 Özel Yükleme - Özel Seçenekler	10
3.5 Yüklemeyi Tamamlama	12
4. MS Exchange Server 2007/2010 için E-posta Tarayıcısı	13
4.1 Genel Görünüm	13
4.2 MS Exchange için E-posta Tarayıcısı (Aktarım Ajanını yönlendirme)	16
4.3 MS Exchange için E-posta Tarayıcısı (SMTP TA)	17
4.4 MS Exchange için E-posta Tarayıcısı (VSAPI)	18
4.5 Algılama Eylemleri	21
4.6 Posta Filtreleme	22
5. MS Exchange Server 2003 için E-posta Tarayıcı	23
5.1 Genel Görünüm	23
5.2 MS Exchange için E-posta Tarayıcısı (VSAPI)	26
5.3 Algılama Eylemleri	29
5.4 Posta Filtreleme	30
6. Kerio MailServer için AVG	31
6.1 Yapılandırma	31
6.1.1 Virüsten koruma	31
6.1.2 Ek Filtresi	31
7. Anti-Spam Yapılandırması	35
7.1 İstenmeyen Posta Önleme Arayüzü	35



7.2 İstenmeyen Posta Önleme Prensipleri	37
7.3 Anti-Spam Ayarları	37
7.3.1 İstenmeyen Posta Önleme Eğitim Sihirbazı	37
7.3.2 Mesajların Olduğu Klasörü Seç	37
7.3.3 Mesaj filtreleme seçenekleri	37
7.4 Performans	42
7.5 RBL	43
7.6 Beyaz Liste	44
7.7 Kara Liste	45
7.8 Uzman Ayarları	46
8. AVG Ayarları Yöneticisi	47
9. SSS ve Teknik Destek	50



1. Giriş

Bu kullanıcı el kitabı, **AVG Email Server Edition 2012** için kapsamlı dokümantasyon sağlar.

AVG Email Server Edition 2012 programını satın aldığınız için tebrik ederiz!

AVG Email Server Edition 2012 sunucunuz için tam güvenlik ve rahatlık sağlamak üzere tasarlanmış ödüllü AVG ürünlerinden biridir. AVG'nin ünlü ve ödüllü güvenlik korumasını sunmak adına baştan başa tamamen yeniden tasarlanan **AVG Email Server Edition 2012**, tüm diğer AVG ürünleri gibidir fakat kullanımı daha kolay ve verimlidir.

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

Not: Bu dokümantasyon özel E-posta Sunucusu Sürümü özelliklerinin açıklamasını içerir. Diğer AVG özellikleriyle ilgili bilgi gerekiyorsa, lütfen gerekli tüm ayrıntıları içeren Internet Security sürümünün kullanıcı kılavuzuna başvurun. Kılavuzu <http://www.avg.com> adresinden indirebilirsiniz.



2. AVG Yükleme Gereksinimleri

2.1. Desteklenen İşletim Sistemleri

AVG Email Server Edition 2012 şu işletim sistemleri altında çalışan e-posta sunucularını korumak için tasarlanmıştır:

- Windows 2008 Server Edition (x86 ve x64)
- Windows 2003 Server (x86, x64) SP1

2.2. E-posta Sunucuları Desteklendi

Aşağıdaki e-posta sunucuları desteklenir:

- MS Exchange 2003 Server sürümü
- MS Exchange 2007 Server sürümü
- MS Exchange 2010 Server sürümü
- Kerio MailServer - sürüm 6.7.2 ve üstü

2.3. Donanım Gereksinimleri

AVG Email Server Edition 2012 için minimum donanım gereksinimleri:

- Intel Pentium CPU 1.5 GHz
- 500 MB boş sabit disk alanı (yükleme için)
- 512 MB RAM bellek

AVG Email Server Edition 2012 için önerilen donanım gereksinimleri:

- Intel Pentium CPU 1.8 GHz
- 600 MB boş sabit disk alanı (yükleme için)
- 512 MB RAM bellek

2.4. Önceki Sürümleri Kaldır

AVG E-posta Sunucusu'nun eski bir sürümü yüklüyse, **AVG Email Server Edition 2012** programını yüklemeye başlamadan önce onun yüklemesini kaldırmanız gerekir. Standart Windows işlevselliğini kullanarak önceki sürümün kaldırılmasını manuel olarak gerçekleştirmeniz gerekir.

- Başlat menüsünden **Başlat/Ayarlar/Denetim Masası/Program Ekle veya Kaldır** ve yüklü



yazılımlar listesinden doğru programı seçin (veya aynı işlemi **Başlat/Tüm Programlar/AVG/AVG Ürünü Kaldır** yoluyla daha kolay yapabilirsiniz).

- Daha önce AVG 8.x veya daha eski sürüm kullandıysanız, tek tek sunucu eklentilerini de kaldırmayı unutmayın.

Not: Depolama hizmetini kaldırma işlemi sırasında yeniden başlatmanız gerekecektir.

Exchange Eklentisi - eklentinin yüklendiği klasörden /uninstall parametresiyle setupes.exe dosyasını çalıştırın.

örn. C:\AVG4ES2K\setupes.exe /uninstall

Lotus Domino/Notes eklentisi - eklentinin yüklendiği klasörden /uninstall parametresiyle setupln.exe dosyasını çalıştırın:

örn. C:\AVG4LM\setupln.exe /uninstall

2.5. MS Exchange Hizmet Paketleri

MS Exchange 2003 Server için hizmet paketi gerekmez. Ancak, maksimum güvenlik elde etmek için sisteminizi en son hizmet paketleriyle ve düzeltmelerle mümkün olduğunca güncel tutmanız önerilir.

MS Exchange 2003 Server için Service Pack (isteğe bağlı):

<http://www.microsoft.com/exchange/evaluation/sp2/overview.msp>

Kurulumun başında, tüm sistem kitaplıklarının sürümleri incelenecektir. Daha yeni kitaplıklar yüklemek gerekirse, yükleyici eskilerini .delete uzantısıyla yeniden adlandırır. Bunlar, sistem yeniden başlatıldıktan sonra silinirler.

MS Exchange 2007 Server için Service Pack (isteğe bağlı):

<http://www.microsoft.com/downloads/details.aspx?FamilyID=44c66ad6-f185-4a1d-a9ab-473c1188954c&displaylang=en>



3. AVG Yükleme Süreci

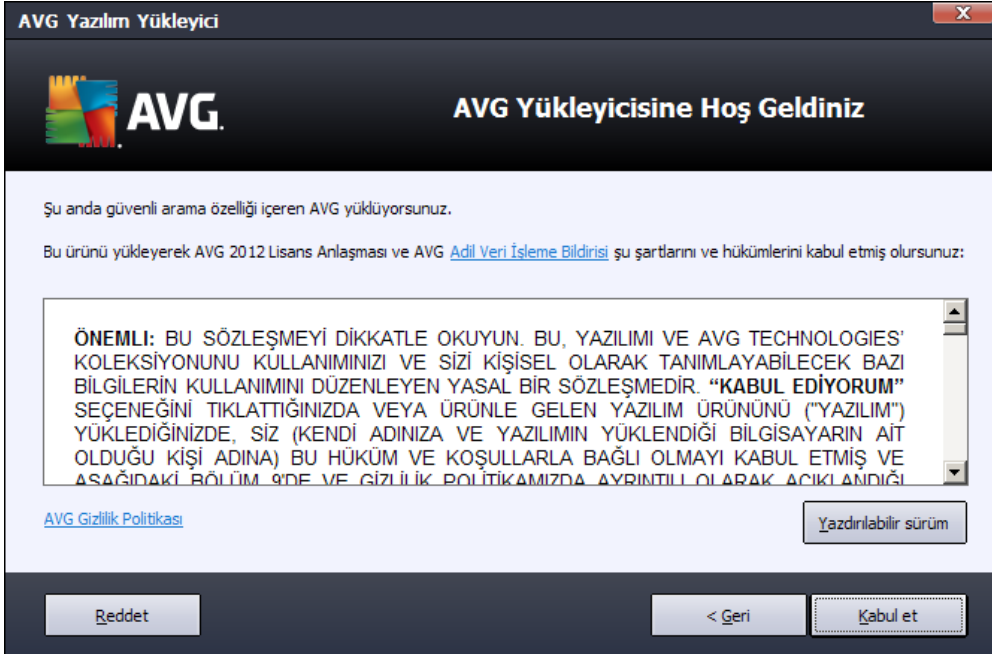
AVG'yi bilgisayarınıza kurmak için en güncel yükleme dosyasına ihtiyacınız vardır. Kutulu versiyonların içinden çıkan CD'de bulunan yükleme dosyasını da kullanabilirsiniz fakat söz konusu dosya güncel olmayabilir. Bu nedenle en güncel kurulum dosyasını çevrimiçi ortamdan indirmenizi öneriyoruz. Dosyayı [AVG web sitesinden](http://www.avg.com/download?prd=msw) indirebilirsiniz (<http://www.avg.com/download?prd=msw> web sitesinde)

Not: Ürününüz için iki yükleme paketi seçeneği vardır - 32bit işletim sistemleri için (x86 olarak belirtilir) ve 64bit işletim sistemleri için (x64 olarak belirtilir). İşletim sisteminiz için doğru yükleme paketini kullandığınızdan emin olun.

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

Yükleme dosyasını sabit disk sürücünüze indirme ve kaydetme işlemini tamamladıktan sonra yükleme işlemini başlatabilirsiniz. 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:

3.1. Yükleme Başlatma



Yükleme işlemi **Hoş geldiniz** penceresiyle başlar. Burada, yükleme sürecinde kullanılacak dili seçebilirsiniz ve lisans koşullarını okuyabilirsiniz. Lisans metnini yeni bir pencerede açmak için **yazdırılabilir sürüm** düğmesini kullanın. Onaylamak ve bir sonraki iletişim kutusuna geçmek için **Kabul Ediyorum** düğmesine basın.

Dikkat: Ayrıca, daha sonra yükleme süreci sırasında uygulama arayüzü için ek dilleri de



seçebilirsiniz.

3.2. Lisansınızı Etkinleştirin

Lisansınızı Etkinleştirin iletişim kutusuna lisans bilgilerinizi girmeniz gerekir.

Lisans numaranızı **Lisans Numarası** alanına girin. Lisans numarası, AVG'nizi çevrimiçi ortamda satın aldıktan sonra gönderilen onaylama e-postasıyla gönderilecektir. Sayıları gösterildiği gibi gitmelisiniz. Lisans numarasının dijital formu mevcut ise (e-postada) lisans numarasını girmek için kopyala ve yapıştır yönteminin kullanılması önerilmektedir.

AVG Yazılım Yükleyici

Lisansınızı Etkinleştirin

Lisans Numarası:

Örnek: IQNP6-9BCA8-PUQU2-A5HCK-GP338L-93OCB

AVG 2012 yazılımınızı çevrimiçi satın aldıysanız, lisans numaranız e-posta ile gönderilmiştir. Yanlış yazmayı önlemek için numaray e-postanızdan kopyalayarak bu ekrana yapıştırmanızı öneririz.

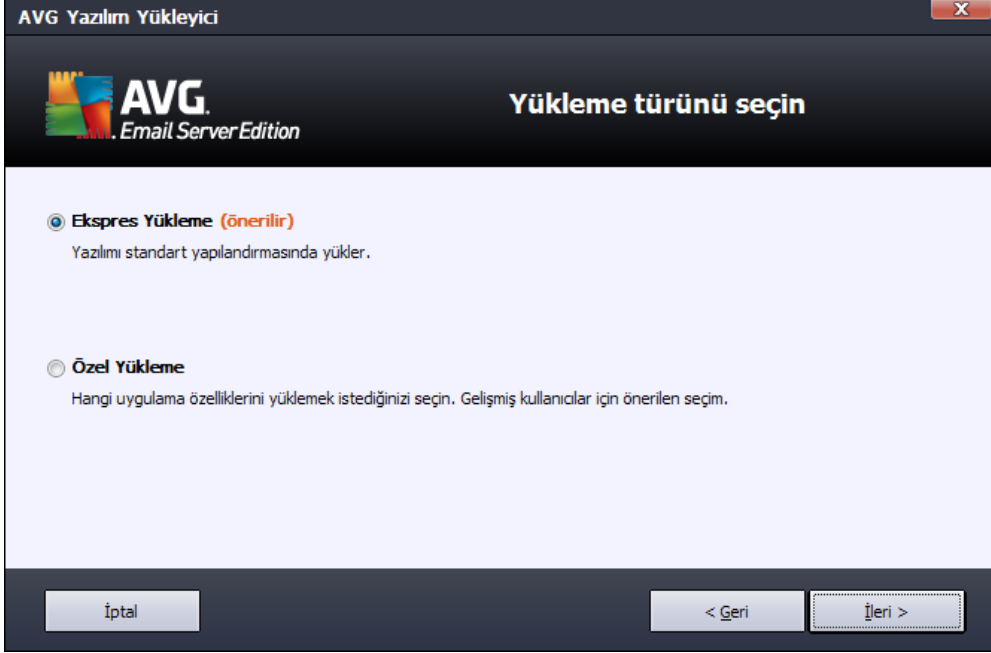
Yazılımı bir mağazadan satın aldıysanız, lisans numarasını paketin içindeki ürün kayıt kartı üzerinde bulabilirsiniz. Numarayı doğru biçimde kopyaladığınızdan emin olun.

İptal < Geri İleri >

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



3.3. Yükleme Türünü Seçin

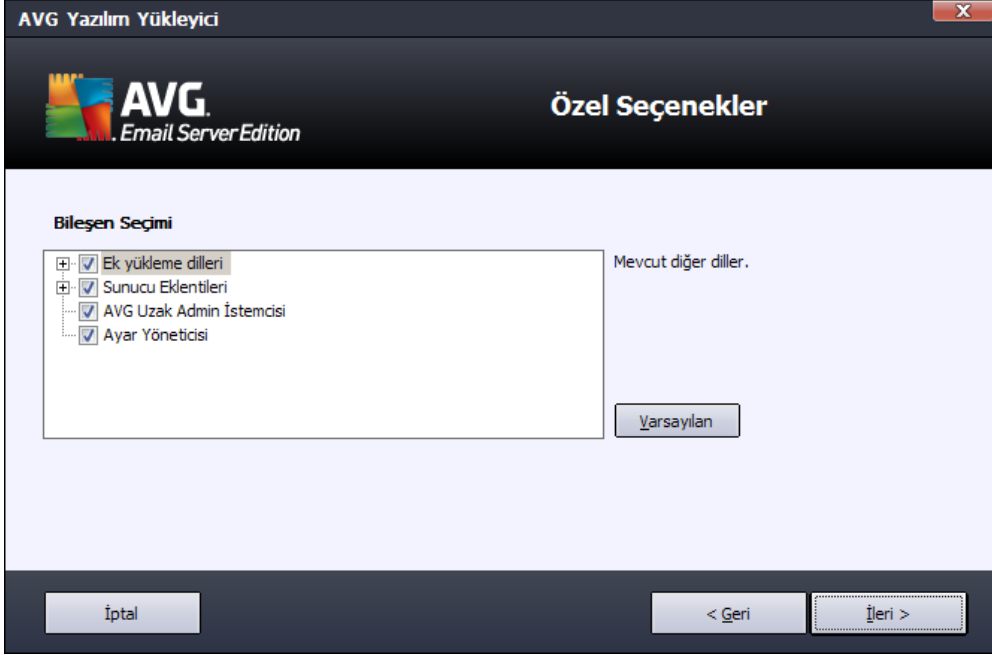


Yükleme türünü seçin iletişim kutusu iki yükleme seçeneği sunar: **Hızlı Yükleme** ve **Özel Yükleme**.

Kullanıcıların çoğu için AVG'yi program geliştiricisi tarafından önceden tanımlanmış ayarlarla tam otomatik modda yükleyen **Hızlı 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 yüklemek için geçerli bir nedeni olan deneyimli kullanıcılar tarafından kullanılmalıdır. Öm. belirli sistem gereksinimlerini karşılamak için.

3.4. Özel Yükleme - Özel Seçenekler



Hedef Klasör iletişim kutusu, AVG'nin yükleneceği konumu seçebilmenize olanak verir. Varsayılan olarak AVG, C: Sürücüsü üzerindeki program dosyaları klasörüne yüklenecektir. Bu konumu değiştirmek istiyorsanız, sürücü yapısını görüntülemek ve ilgili klasörü seçmek için **Gözet** düğmesini kullanın.

Bileşen Seçimi bölümünde, yüklenebilecek tüm AVG bileşenlerinin genel görünümü görüntülenir. Varsayılan ayarların size uygun olmaması halinde belirli bileşenleri kaldırabilir ya da ekleyebilirsiniz.

Diğer bir yandan sadece satın aldığınız AVG sürümü kapsamında bulunan bileşenler arasından seçim yapabilirsiniz. Bileşen Seçimi iletişim kutusunda yalnızca yüklenecek söz konusu bileşenler sunulur!

- **AVG Uzaktan Yönetim İstemcisi** - AVG'yi bir AVG DataCenter'a (AVG Ağ Sürümleri) bağlamayı düşünüyorsanız bu seçeneği belirlemeniz gerekir.
- **Ayar Yöneticisi** - temel olarak ağ yöneticilerinin AVG yapılandırmasını kopyalayabilmesi, düzenleyebilmesi ve dağıtabilmesi için uygun bir araçtır. Yapılandırma taşınabilir bir cihaza kaydedilebilir (USB flash sürücü vb.) ve seçili istasyonlara sonra manuel olarak veya başka bir yolla uygulanır.
- **Ek Yükleme Dilleri** - AVG'de hangi dillerin yüklenmesi gerektiğini tanımlayabilirsiniz. **Ekstra yüklenen diller** öğesini işaretleyin ve sonra ilgili menüden istediğiniz dilleri seçin.

Ayrı sunucu bileşenlerinin temel genel görünümü (**Sunucu Eklentileri**):

- **MS Exchange için Anti-Spam Sunucusu**

Tüm gelen e-posta iletilerini kontrol eder ve istenmeyen e-postaları İSTENMEYEN E-POSTA



olarak işaretler. Her e-posta iletilisini işlemek için çeşitli inceleme yöntemleri kullanır ve istenmeyen postalara karşı mümkün olan en üst seviyede koruma sağlar.

- **MS Exchange için E-posta Tarayıcısı (Taşıma Ajanını yönlendirme)**

MS Exchange HUB rolü üzerinden tüm gelen, giden ve dahili e-posta iletilerini denetler.

MS Exchange 2007/2010 için kullanılabilir ve yalnızca HUB rolü için yüklenebilir.

- **MS Exchange için E-posta Tarayıcısı (SMTP Taşıma Aracısı)**

MS Exchange SMTP arayüzü üzerinden gelen tüm e-posta iletilerini denetler.

Yalnızca MS Exchange 2007/2010 için kullanılabilir ve hem EDGE hem de HUB rolleri için yüklenebilir.

- **MS Exchange için E-posta Tarayıcısı (VSAPI)**

Kullanıcıların posta kutularında depolanan tüm e-posta iletilerini denetler. Herhangi bir virüs algılanırsa, Virüs Kasası'na taşınır veya tamamen kaldırılır.

Not: MS Exchange için farklı seçenekler mevcuttur.

İleri düğmesine basarak devam edin.



3.5. Yüklemeyi Tamamlama

Modül seçimi sırasında **Uzaktan Yönetim Bileşeni** modülünü seçerseniz, son ekran AVG DataCenter'ınıza bağlanmak için bağlantı dizesini tanımlamanıza olanak verir.

AVG Yazılım Yükleyici

 **AVG**
Email Server Edition

Yükleme başarılı oldu

AVG 2012 ürününü yüklediğiniz için teşekkür ederiz.

AVG Veri Merkezi belirtimi:

[Gizlilik Politikası](#) bağlantısındaki ilkelere göre (AVG sizi kişisel olarak tanımlayabilecek bilgileri saklamayacak ve sizinle hiçbir şekilde iletişime geçmeyecektir) [ürün geliştirme programı](#) bölümüne katılarak güvenliğimi artırmak istiyorum

Bitir

AVG artık bilgisayarınıza yüklenmiştir ve doğru çalışmaktadır. Program arka planda tam otomatik moda çalışır.

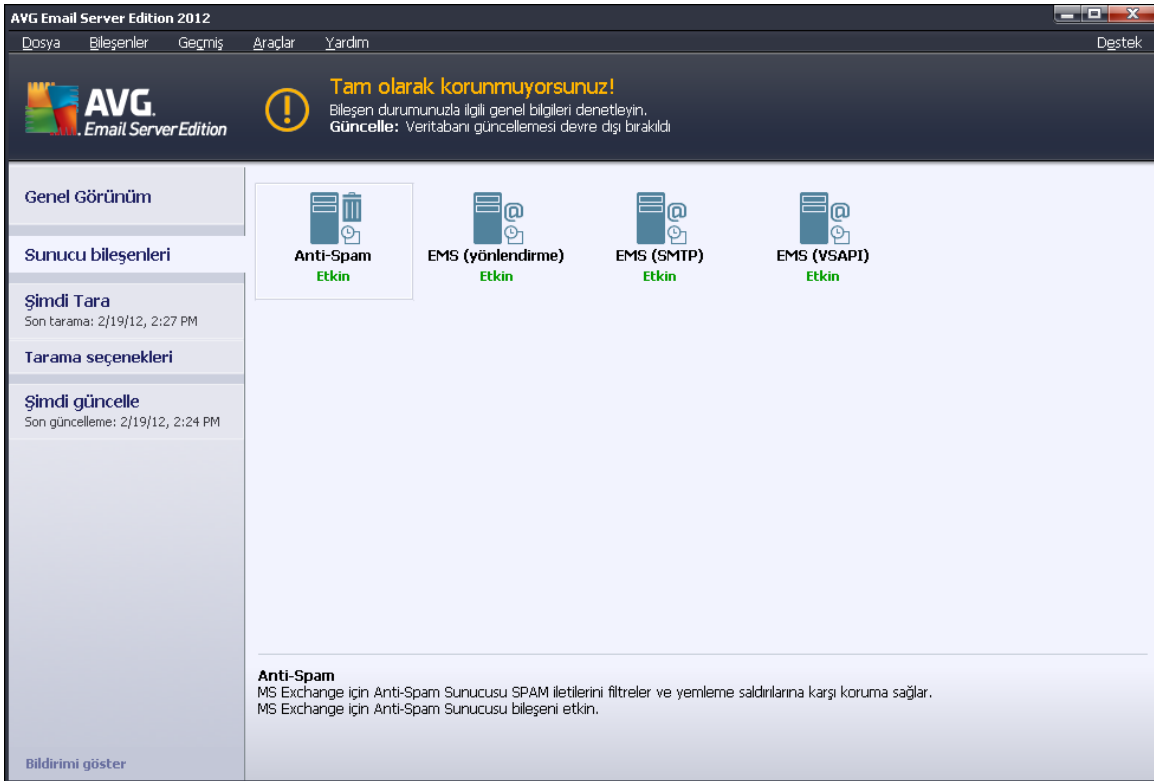
E-posta sunucunuz için korumayı bağımsız olarak ayarlamak için ilgili bölümü izleyin:

- [MS Exchange Server 2007/2010 için E-posta Tarayıcısı](#)
- [MS Exchange Server 2003 için E-posta Tarayıcısı](#)
- [Kerio MailServer için AVG](#)

4. MS Exchange Server 2007/2010 için E-posta Tarayıcısı

4.1. Genel Görünüm

MS Exchange Server 2007/2010 için AVG yapılandırma seçenekleri, sunucu bileşenleri olarak AVG Email Server Edition 2012 içine tamamen entegre edilmiştir.



Sunuculara ayrı ayrı temel genel bakış:

- [**Anti-Spam - MS Exchange için Anti-Spam Sunucusu**](#)

Tüm gelen e-posta iletilerini denetler ve istenmeyen e-postaları İSTENMEYEN E-POSTA olarak işaretler. Her e-posta iletilisini işlemek için çeşitli inceleme yöntemleri kullanır ve istenmeyen postalara karşı mümkün olan en üst seviyede koruma sağlar.

- [**EMS \(yönlendirme\) - MS Exchange için E-posta Tarayıcısı \(Taşıma Ajanını yönlendirme\)**](#)

MS Exchange HUB rolü üzerinden tüm gelen, giden ve dahili e-posta iletilerini denetler.

MS Exchange 2007/2010 için kullanılabilir ve yalnızca HUB rolü için yüklenebilir.

- [**EMS \(SMTP\) - MS Exchange için E-posta Tarayıcısı \(SMTP Taşıma Ajanı\)**](#)



MS Exchange SMTP arayüzü üzerinden gelen tüm e-posta iletilerini denetler.

Yalnızca MS Exchange 2007/2010 için kullanılabilir ve hem EDGE hem de HUB rolleri için yüklenebilir.

- **[EMS \(VSAPI\) - MS Exchange için E-posta Tarayıcısı \(VSAPI\)](#)**

Kullanıcıların posta kutularında depolanan tüm e-posta iletilerini denetler. Herhangi bir virüs algılanırsa, Virüs Kasası'na taşınır veya tamamen kaldırılır.

Önemli not: VSAPI'yı Hub Exchange rolüne dolaşım Aktarım aracı ile birlikte yüklemeye karar verirsiniz, e-posta iletileriniz iki kez taranacaktır. Bunu engellemek için, lütfen VSAPI kutusundaki **Giden iletileri tarama (MS Exchange 2007/2010)** kutusunu işaretleyin (daha fazla bilgi için [burayı](#) tıklayın).

Arayüzünü açmak için gerekli bir bileşeni tıklayın. Anti-Spam haricinde, tüm bileşenler aşağıdaki ortak kontrol düğmelerini ve bağlantılarını içerir:

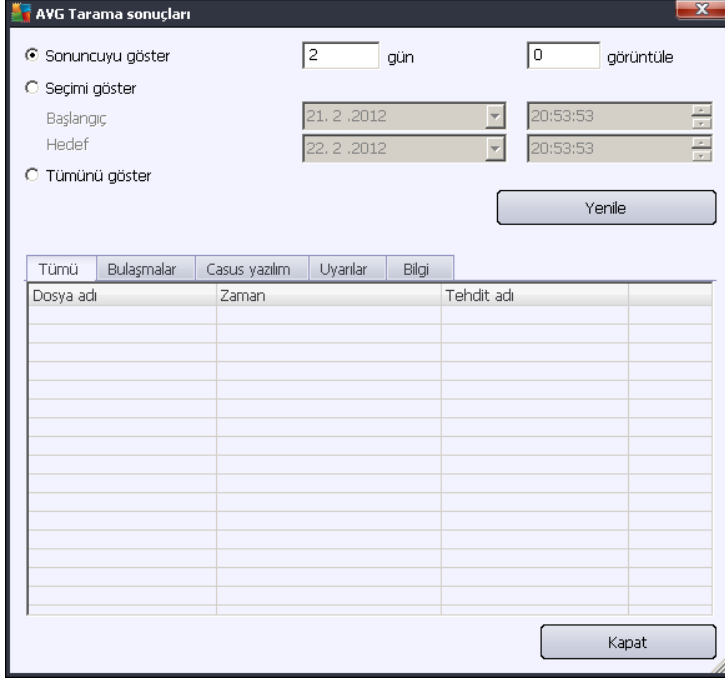
The screenshot shows the AVG Email Server Edition 2012 interface. The main window is titled "MS Exchange için E-mail Scanner (VSAPI) Bileşeni". It displays the following information:

- Genel Görünüm:** MS Exchange için E-mail Scanner (VSAPI) Bileşeni
- Sunucu bileşenleri:** MS Exchange için E-mail Scanner (VSAPI)
- Şimdi Tara:** Son tarama: 2/19/12, 2:27 PM
- Tarama seçenekleri:** Başlangıç: 2/19/2012, 2:22 PM; Kontrol edilen e-posta kısımları: 1604
- Şimdi güncelle:** Son güncelleme: 2/19/12, 2:24 PM
- Statistikler:**
 - Algılanan tehditler: 0
 - Algılanan bulaşmalar: 0
 - Algılanan uyarılar: 0
 - Virüs Kasasına Taşındı: 0
 - Silindi: 0
 - Göz ardı edildi: 0
 - Algılanan PUP: 0
 - Algılanan bilgiler: 0

Buttons for "Ayarlar" (Settings) and "Geri" (Back) are visible at the bottom.

- **Tarama Sonuçları**

Tarama sonuçlarını inceleyebileceğiniz yeni bir iletişim kutusu açar:



Burada, önemlerine göre birkaç sekmeye ayrılmış iletileri kontrol edebilirsiniz. Önem derecelerini düzeltmek ve raporlamak için tek tek bileşenlerin yapılandırılmalarını görün.

Varsayılan olarak yalnızca son iki günün sonuçları görüntülenir. Görüntülenen dönemi aşağıdaki seçenekleri kullanarak değiştirebilirsiniz:

- **Sonuncuyu göster** - Tercih edilen günleri ve saatleri girin.
- **Seçimi göster** - özel bir saat ve tarih aralığı seçin.
- **Tümünü göster** - Tüm zaman dönemi için sonuçları görüntüler.

Sonuçları yeniden yüklemek için **Yenile** düğmesini kullanın.

- **İstatistik değerlerini yenile** - yukarıda görüntülenen istatistikleri günceller.
- **İstatistik değerlerini sıfırla** - tüm istatistikleri sıfır olarak sıfırlar.

Çalışan düğmeler aşağıda belirtilmektedir:

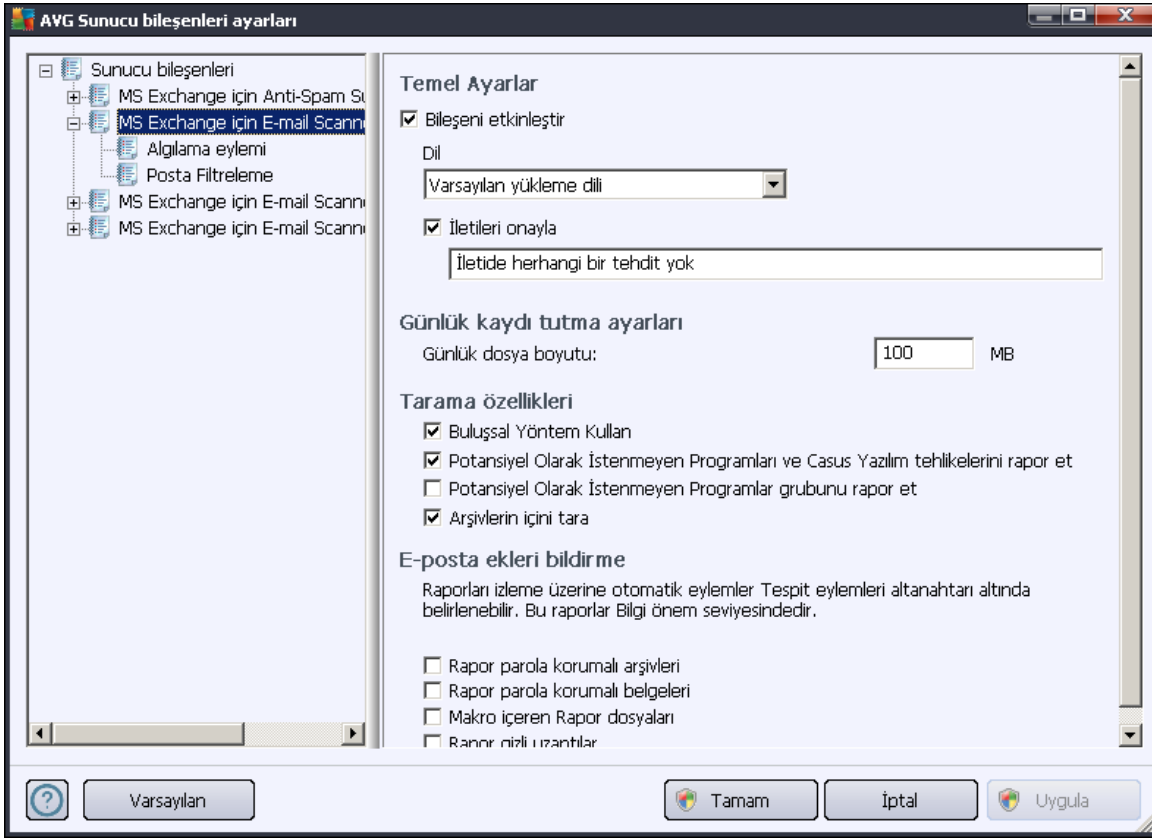
- **Ayarlar** - bu düğmeyi bileşenin ayarlarını açmak için kullanın.
- **Geri** - Sunucu bileşenleri genel görünümüne geri dönmek için bu düğmeye basın.

Aşağıdaki bölümde tüm bileşenlerin tek tek ayarları hakkında daha fazla bilgi bulabilirsiniz.

4.2. MS Exchange için E-posta Tarayıcısı (Aktarım Ajanını yönlendirme)

MS Exchange için E-Posta Tarayıcısı (yönlendirme aktarım ajanı) ayarlarını açmak için, bileşenin arayüzünden **Ayarlar** düğmesini seçin.

Sunucu bileşenleri listesinden **MS Exchange için E-posta Tarayıcısı (yönlendirme TA)** öğesini seçin:



Temel Ayarlar kısmı aşağıdaki seçenekleri içerir:

- **Bileşeni etkinleştir** - bileşenin tamamını devre dışı bırakmak için işaretini kaldırın.
- **Dil** - tercih edilen bileşen dilini seçin.
- **İletileri onayla** - taranan tüm iletilere bir sertifika notu eklemek istiyorsanız bunu işaretleyin. İletiyi bir sonraki alanda özelleştirebilirsiniz.

Günlük ayarları bölümü:

- **Günlük dosyası boyutu** - tercih edilen bir günlük dosyası boyutu seçin. Varsayılan değer: 100 MB.

Tarama özellikleri bölümü:



- **Buluşsal Analiz Yöntemlerini Kullan** - bu kutuyu tarama sırasında buluşsal analiz yöntemini etkinleştirmek için işaretleyin.
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et** - bu seçeneği potansiyel olarak istenmeyen programların ve casus yazılımın varlığını bildirmek için işaretleyin.
- **Geliştirilmiş bir Potansiyel Olarak İstenmeyen Program dizisi bildirin** - ayrıntılı bir casus yazılım (spyware) paketi tespit etmek için işaretleyin: doğrudan üreticiden sağlandığında mükemmel durumda ve zararsız olan ancak daha sonra kötü amaçlar için kullanılabilir programlar veya her zaman zararsız olan ancak istenmeyebilecek programlar (çeşitli araç çubukları vs.). Bu ek önlem, bilgisayarınızın güvenliğini ve rahatlığını daha da artırır, ancak yasal programları engellemesi de olasıdır ve bu nedenle varsayılan olarak kapatılır. Not: Bu algılama özelliği, bir önceki seçeneğe ektir. Bu nedenle, temel casus yazılım (spyware) türlerinden korunmak istiyorsanız, bir önceki kutuyu daima seçili halde bırakın.
- **Arşivlerin içeriğini tara** - bu seçeneği tarayıcının arşivi dosyaların (zip, rar vb.) içine de bakmasını sağlamaya izin vermek için işaretleyin.

E-posta eklerini bildirme bölümü, tarama sırasında hangi öğelerin seçileceğine izin vermenize olanak verir. İşaretliyse, böyle bir öğe içeren her e-postanın ileti konusunda [BİLGİ] etiketini bulacaktır. Bu, **Algılama eylemleri bölümü**, **Bilgi** kısmında (aşağıya bakın) kolaylıkla istenebilen varsayılan yapılandırmadır.

Aşağıdaki seçenekler mevcuttur:

- **Parola korumalı arşivleri bildir**
- **Parola korumalı belgeleri bildir**
- **Makro içeren dosyaları bildir**
- **Gizli uzantıları bildir**

Ayrıca aşağıdaki ağaç yapısında bu alt öğeler de bulunur:

- [Tespit işlemleri](#)
- [Posta filtreleme](#)

4.3. MS Exchange için E-posta Tarayıcısı (SMTP TA)

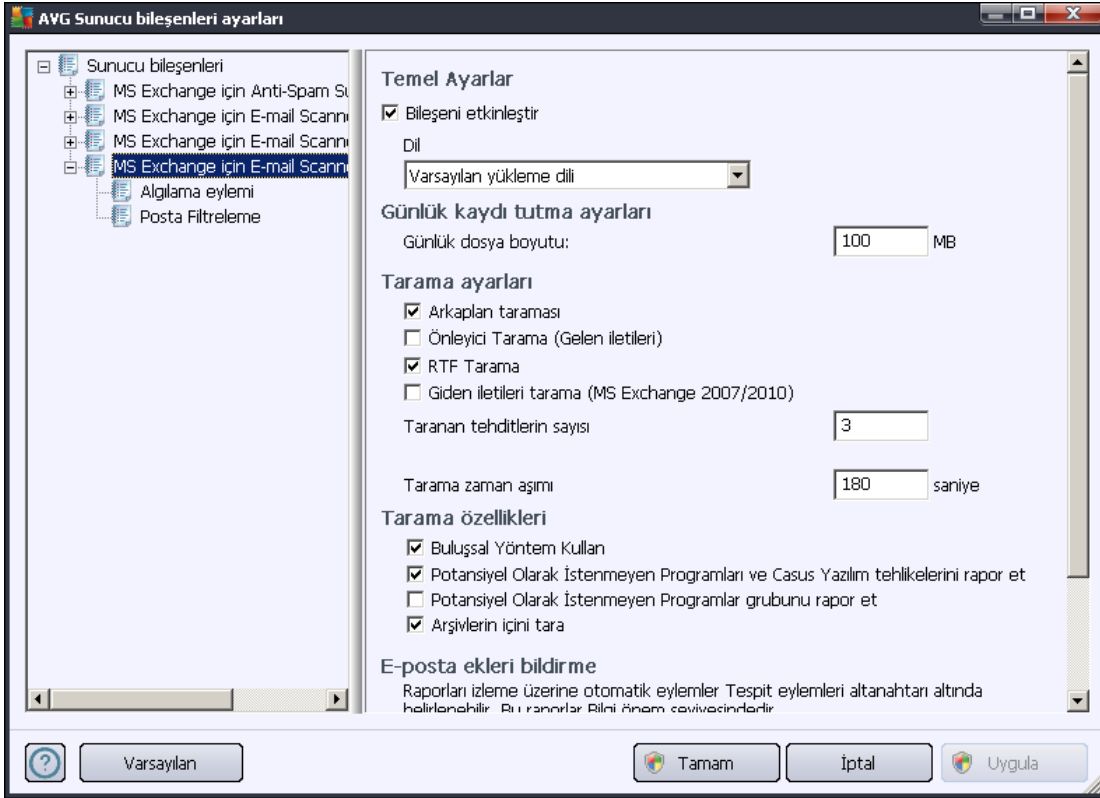
MS Exchange için E-posta Tarayıcısı (SMTP Aktarım Ajansı) yapılandırması aktarım ajanını yönlendirme durumuyla tamamen aynıdır. Daha fazla bilgi için lütfen yukarıdaki [MS Exchange için E-posta Tarayıcısı \(Aktarım Ajansı yönlendirme\)](#) bölümüne bakın.

Ayrıca aşağıdaki ağaç yapısında bu alt öğeler de bulunur:

- [Tespit işlemleri](#)
- [Posta filtreleme](#)

4.4. MS Exchange için E-posta Tarayıcısı (VSAPI)

Bu öge, **MS Exchange için E-posta Tarayıcısı (VSAPI)** ayarlarını içerir.



Temel Ayarlar bölümü aşağıdaki seçenekleri içerir:

- **Bileşeni etkinleştir** - bileşenin tamamını devre dışı bırakmak için işaretini kaldırın.
- **Dil** - tercih edilen bileşen dilini seçin.

Günlük ayarları bölümü:

- **Günlük dosyası boyutu** - tercih edilen bir günlük dosyası boyutu seçin. Varsayılan değer: 100 MB.

Tarama ayarları bölümü:

- **Arka Plan Tarama** - arka plan tarama işlemini buradan etkinleştirebilir veya devre dışı bırakabilirsiniz. Arka plan tarama, VSAPI 2.0/2.5 uygulama arayüzü özelliklerinden biridir. Exchange Mesaj Veritabanlarının iş parçacıklı taranmasını sağlar. Kullanıcının posta kutusunda, en son AVG virüs veritabanı güncellemesiyle taranmamış bir ögeyle karşılaşılması durumunda, ilgili öge taranması için Exchange Server için AVG'ye gönderilir. İncelenmeyen nesnelerin taranması ve aranması paralel olarak çalışır.

Diğer görevleri garantileyen özel bir düşük öncelikli iş parçacığı her veritabanı için kullanılır



(örn. Microsoft Exchange veritabanında e-posta iletilerinin saklanması) ve her zaman isteğe bağlı olarak gerçekleşir.

- **Proaktif Tarama (gelen iletiler)**

VSAPI 2.0/2.5 proaktif tarama işlevini buradan etkinleştirebilir veya devre dışı bırakabilirsiniz. Bu tarama bir öge klasöre teslim edildiğinde ancak istemci tarafından bir istek yapılmadığında oluşur.

İletiler Exchange deposuna gönderilir gönderilmez, global tarama kuyruğuna düşük öncelikli olarak girerler (maksimum 30 öge). İlk giren ilk çıkar (FIFO) temelinde taranırlar. Hala kuyrukta olan bir ögeye erişilirse, bu öge yüksek öncelikli olarak değişir.

Not: Taşma iletileri taranmamış deposuna gider.

Not: Hem Arka Plan Tarama hem de Proaktif Tarama seçeneklerini devre dışı bıraksanız bile, bir kullanıcı MS Outlook istemcisiyle bir ileti indirmeye çalıştığında tarayıcıya erişim yine de aktif olacaktır.

- **RTF Tara** - burada RTF dosyası türünün taranması gerekip gerekmediğini belirtebilirsiniz.
- **Giden iletileri tarama (MS Exchange 2007/2010)** - Hem VSAPI hem de Yönlendirme Aktarma Aracısı ([yönlendirme TA](#)) sunucu bileşenleri yüklüken (tek bir sunucuda veya iki farklı sunucuda olması fark etmez), giden posta iki kez taranabilir. İlk tarama VSAPI Erişim tarayıcısı ile yapılırken, ikincisi Yönlendirme Aktarım Aracısı tarafından yapılır. Bu durum bazı sunucuların yavaşlamasına ve e-postaların gönderiminde kısmi yavaşlamaya neden olabilir. Her iki sunucu bileşeninin yüklü ve etkin olup olmadığından emin değilseniz, bu kutuyu işaretleyerek ve VSAPI Erişim tarayıcısını devre dışı bırakarak giden e-postaların iki kez taranmasını önleyebilirsiniz.
- **Taranan İş Parçacıklarının Sayısı** - Tarama işlemi varsayılan olarak tüm tarama performansını belirli bir paralelizm düzeyinde artırmak için iş parçacığı olarak oluşturulur. İş parçacığı sayısını buradan değiştirebilirsiniz.

Varsayılan iş parçacığı sayısı 2 kere 'işlemci_sayısı' + 1 olarak hesaplanır.

Minimum iş parçacığı sayısı ('işlemci sayısı'+1) bölü 2 olarak hesaplanır.

Maksimum iş parçacığı sayısı 'işlemci Sayısı' çarpı 5 + 1 olarak hesaplanır.

Değer minimum veya daha küçük değerse veya maksimum veya daha büyük değerse varsayılan değer kullanılır.

- **Tarama Zaman Aşımı** - bir iş parçacığının taranmakta olan iletiye erişmesi için (saniye cinsinden) maksimum süreli aralık (varsayılan değer 180 saniyedir).

Tarama özellikleri bölümü:

- **Buluşsal Analiz Yöntemlerini Kullan** - bu kutuyu tarama sırasında buluşsal analiz yöntemini etkinleştirmek için işaretleyin.
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et** - bu seçeneği potansiyel olarak istenmeyen programların ve casus yazılımın varlığını bildirmek için işaretleyin.



- **Geliştirilmiş bir Potansiyel Olarak İstenmeyen Program dizisi bildirin** - ayrıntılı bir casus yazılım (spyware) paketi tespit etmek için işaretleyin: doğrudan üreticiden sağlandığında mükemmel durumda ve zararsız olan ancak daha sonra kötü amaçlar için kullanılacak programlar veya her zaman zararsız olan ancak istenmeyebilecek programlar (çeşitli araç çubukları vs.). Bu ek önlem, bilgisayarınızın güvenliğini ve rahatlığını daha da artırır, ancak yasal programları engellemesi de olasıdır ve bu nedenle varsayılan olarak kapatılır. Not: Bu algılama özelliği, bir önceki seçeneğe ektir. Bu nedenle, temel casus yazılım (spyware) türlerinden korunmak istiyorsanız, bir önceki kutuyu daima seçili halde bırakın.
- **Arşivlerin içeriğini tara** - bu seçeneği tarayıcının arşivi dosyaların (zip, rar vb.) içeriğini de bakmasını sağlamaya izin vermek için işaretleyin.

E-posta eklerini bildirme bölümü, tarama sırasında hangi öğelerin seçileceğine izin vermenize olanak verir. Varsayılan yapılandırma **Tespit işlemleri bölümü**, **Bilgi** kısmında (yukarı bakın) kolaylıkla istenebilir.

Aşağıdaki seçenekler mevcuttur:

- **Parola korumalı arşivleri bildir**
- **Parola korumalı belgeleri bildir**
- **Makro içeren dosyaları bildir**
- **Gizli uzantıları bildir**

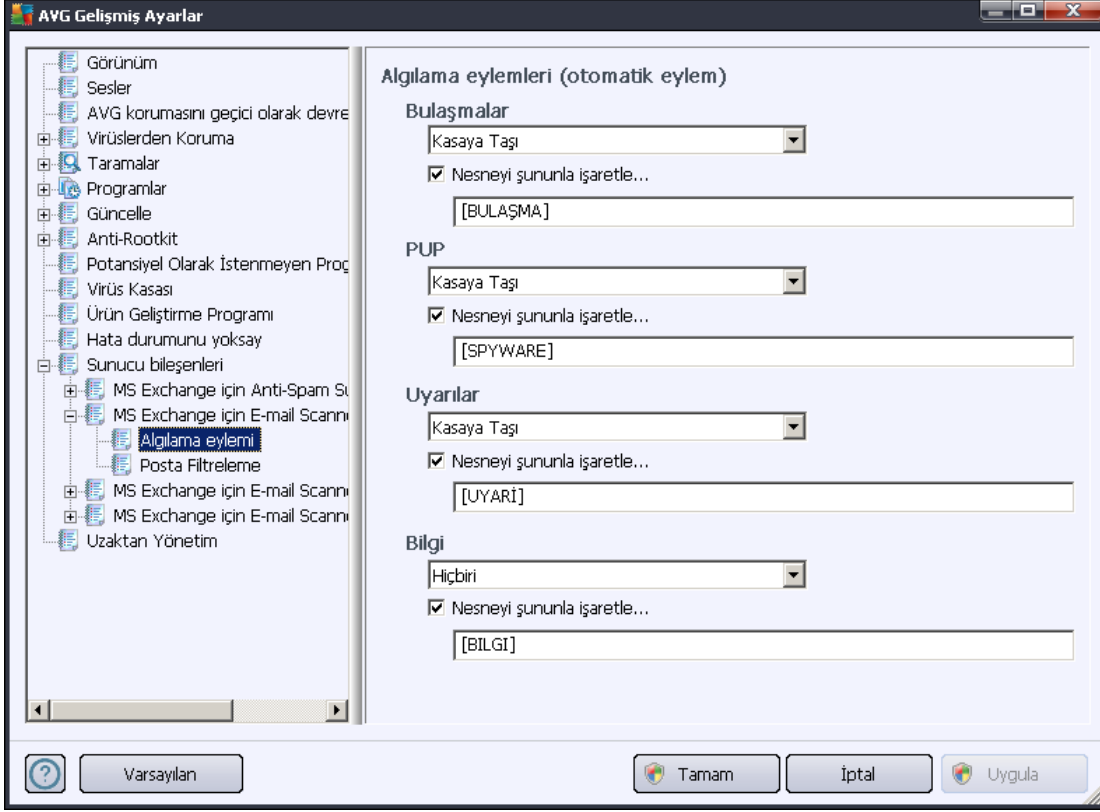
Genel olarak, bu özelliklerden bazıları Microsoft VSAPI 2.0/2.5 uygulama arayüzü hizmetlerinin kullanıcı uzantılarıdır. VSAPI 2.0/2.5 hakkında ayrıntılı bilgiler için lütfen aşağıdaki bağlantılara (ve ayrıca, başvuru alanlardan erişilen bağlantılar) bakın:

- <http://support.microsoft.com/default.aspx?scid=kb:en-us:328841&Product=exch2k> - Exchange ve virüsten koruma yazılımı etkileşimi hakkında bilgi için
- <http://support.microsoft.com/default.aspx?scid=kb:en-us:823166> - Exchange 2003 Server uygulamasında ek VSAPI 2.5 özellikleri hakkında bilgi için.

Ayrıca aşağıdaki ağaç yapısında bu alt öğeler de bulunur:

- [Tespit işlemleri](#)
- [Posta filtreleme](#)

4.5. Algılama Eylemleri



Algılama eylemleri alt ögesinde, tarama işlemi sırasında yapılması gereken otomatik eylemleri seçebilirsiniz.

Eylemler aşağıdaki öğeler için kullanılabilir:

- **Bulaşmalar**
- **PUP (Potansiyel Olarak İstenmeyen Programlar)**
- **Uyarılar**
- **Bilgi**

Her öğe için bir eylem seçmek için açılır menüyü kullanın:

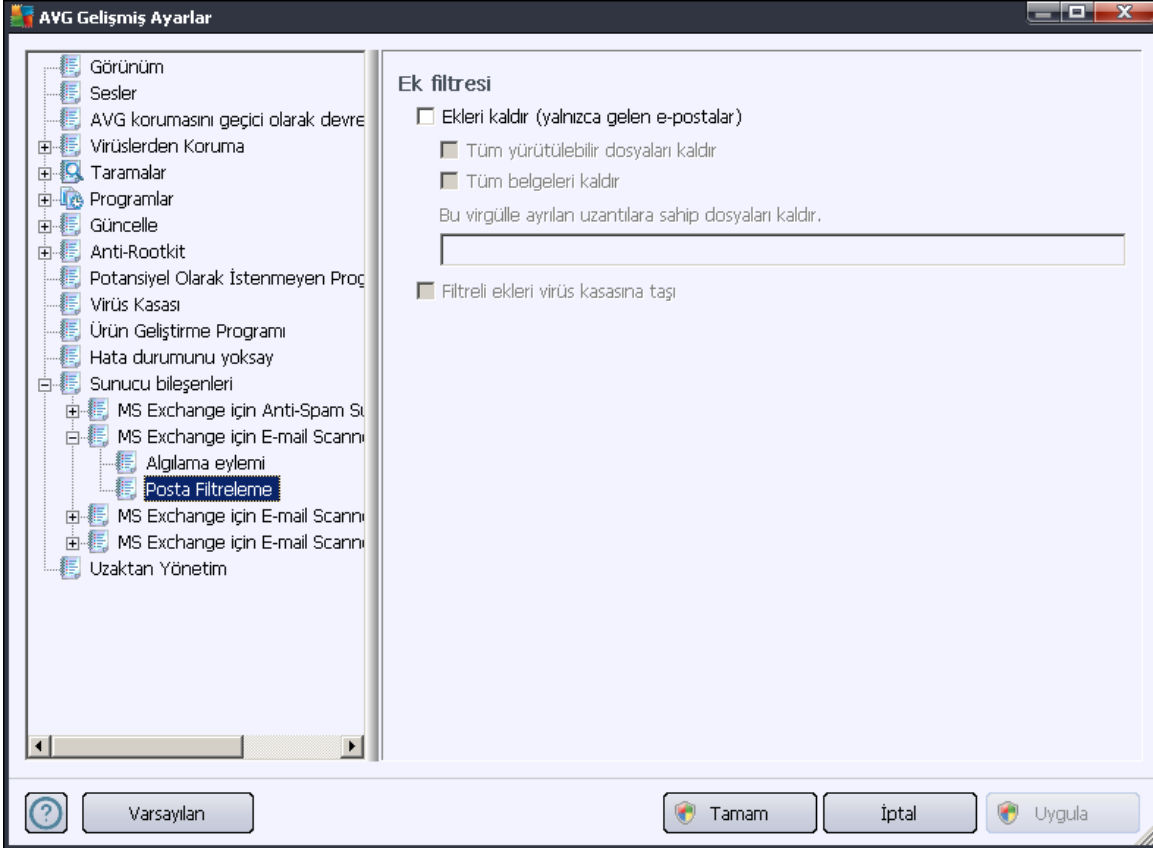
- **Hiçbiri** - hiçbir eylem yapılmaz.
- **Kasaya Taşı** - verilen tehlike Virüs Kasasına taşınacaktır.
- **Kaldır** - verilen tehlike kaldırılacaktır.

Verilen öğeyi/tehlikeyi içeren iletileri için özel bir konu metni seçmek için, **Konuyu şununla işaretle...** kutusunu işaretleyin ve tercih edilen değeri doldurun.



Not: En son bahsedilen özellik MS Exchange VSAPI için E-posta Tarayıcısı'nda kullanılamaz.

4.6. Posta Filtreleme



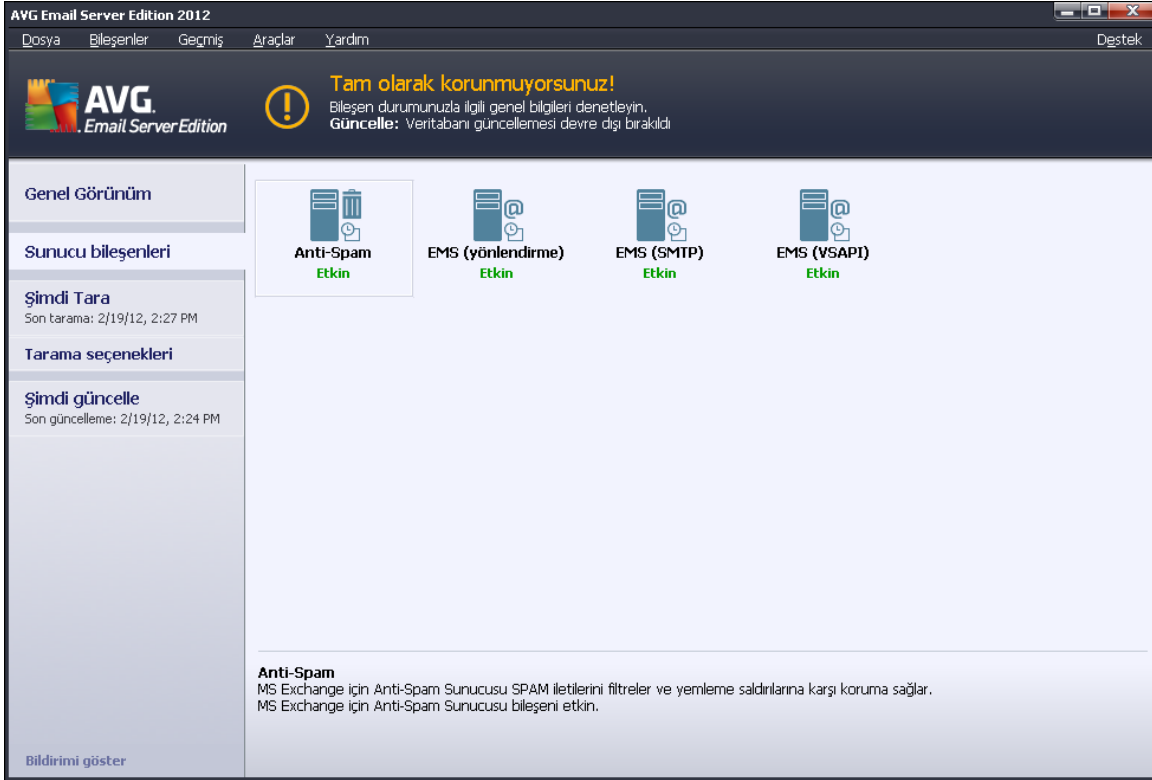
Posta Filtreleme alt ögesinde, hangi eklerin (varsa) otomatik olarak kaldırılacağını seçebilirsiniz. Aşağıdaki seçenekler mevcuttur:

- **Ekleri kaldır** - bu kutuyu özelliği etkinleştirmek için işaretleyin.
- **Tüm çalıştırılabilir dosyaları kaldır** - tüm çalıştırılabilirleri kaldırır.
- **Tüm belgeleri kaldır** - tüm belge dosyalarını kaldırır.
- **Bu virgülle ayrılan uzantılara sahip dosyaları kaldır** - kutuyu otomatik olarak kaldırılmalarını istediğiniz dosya uzantılarıyla doldurun. Uzantıları virgülle ayırın.
- **Filtrelenmiş ekleri virüs kasasına taşı** - Filtrelenmiş eklerin tamamen kaldırılmamasını istemeniz durumunda işaretleyin. Bu kutu işaretlendiğinde, bu iletişim kutusunda seçilen tüm ekler otomatik olarak Virüs Kasası karantina ortamına taşınır. Burası, potansiyel olarak zararlı dosyaları saklamak için güvenli bir yerdir - Dosyaları sisteminizi tehlikeye sokmadan görüntüleyebilir ve inceleyebilirsiniz. Virüs Kasasına **AVG Email Server Edition 2012** ana arayüzünün üst menüsünden erişebilirsiniz. **Geçmiş** ögesini sol tıklatıp bağlam menüsünden **Virüs Kasası** ögesini seçmeniz yeterlidir.

5. MS Exchange Server 2003 için E-posta Tarayıcı

5.1. Genel Görünüm

MS Exchange Server 2003 için E-posta Tarayıcısı, yapılandırma seçenekleri bir sunucu bileşeni olarak AVG Email Server Edition 2012 içinde tamamen entegre edilmiştir.



Sunucu bileşenleri şunları içerir:

Tek tek sunuculara temel genel bakış:

- [**Anti-Spam - MS Exchange için Anti-Spam Sunucusu**](#)

Tüm gelen e-posta iletilerini denetler ve istenmeyen e-postaları İSTENMEYEN E-POSTA olarak işaretler. Her e-posta iletilisini işlemek için çeşitli inceleme yöntemleri kullanır ve istenmeyen postalara karşı mümkün olan en üst seviyede koruma sağlar.

- [**EMS \(VSAPI\) - MS Exchange için E-posta Tarayıcısı \(VSAPI\)**](#)

Kullanıcıların posta kutularında depolanan tüm e-posta iletilerini denetler. Herhangi bir virüs algılanırsa, Virüs Kasası'na taşınır veya tamamen kaldırılır.

Arayüzünü açmak için gerekli bir bileşeni tıklatın. **Anti-Spam bileşeni**, [ayrı bir bölümde](#) açıklanan özel bir ekrana sahiptir. **MS Exchange için E-posta Tarayıcısı (VSAPI)** arayüzünde aşağıdaki



kontrol düğmeleri ve bağlantılar bulunur:

The screenshot shows the AVG Email Server Edition 2012 interface. The main window displays the status of the MS Exchange için E-mail Scanner (VSAPI) component. A warning message at the top indicates that the component is not fully protected and that the database update is out of date. The component is currently active (Etkin). The last scan was performed on 2/19/12 at 2:27 PM. The scan options include scanning for threats, attachments, and warnings. The scan results show zero detected threats, attachments, or warnings. The interface includes a sidebar with navigation options like 'Genel Görünüm', 'Sunucu bileşenleri', 'Şimdi Tara', 'Tarama seçenekleri', and 'Şimdi güncelle'. There are also buttons for 'Ayarlar' and 'Geri'.

MS Exchange için E-mail Scanner (VSAPI) Bileşeni

Tam olarak korunmuyorsunuz!
Bileşen durumunuzla ilgili genel bilgileri denetleyin.
Güncelle: Veritabanı güncellemesi devre dışı bırakıldı

MS Exchange için E-mail Scanner (VSAPI) kullanıcıların posta kutularında saklanan tüm e-posta iletilerini denetler. Algılandığında, virüsler Virüs Kasası öğesine taşınır veya tamamen kaldırılır.

Etkin

Başlangıç: **2/19/2012, 2:22 PM**
Kontrol edilen e-posta kısımları: **1604**

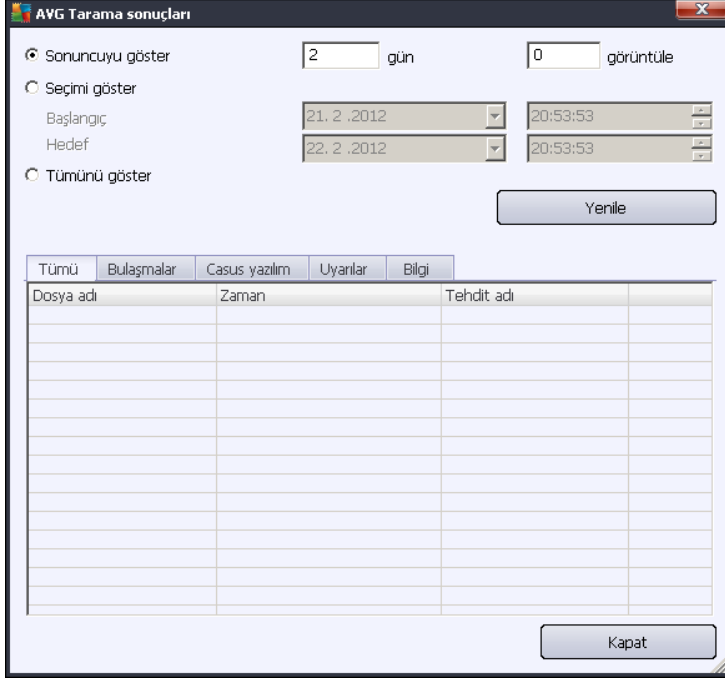
Algılanan tehditler:	0	Algılanan PUP:	0
Algılanan bulaşmalar:	0	Algılanan bilgiler:	0
Algılanan uyarılar:	0		
Virüs Kasasına Taşındı:	0		
Silindi:	0		
Göz ardı edildi:	0		

[Tarama sonuçları](#), [İstatistik değerlerini yenile](#), [İstatistik değerlerini sıfırla](#)

[Bildirim göster](#) [Ayarlar](#) [Geri](#)

- **Tarama Sonuçları**

Tarama sonuçlarını inceleyebileceğiniz yeni bir iletişim kutusu açar:



Burada, önemlerine göre birkaç sekme ayrılmış iletileri kontrol edebilirsiniz. Önem derecelerini düzeltmek ve raporlamak için tek tek bileşenlerin yapılandırılmalarını görün.

Varsayılan olarak yalnızca son iki günün sonuçları görüntülenir. Görüntülenen dönemi aşağıdaki seçenekleri kullanarak değiştirebilirsiniz:

- **Sonuncuyu göster** - Tercih edilen günleri ve saatleri girin.
- **Seçimi göster** - özel bir saat ve tarih aralığı seçin.
- **Tümünü göster** - Tüm zaman dönemi için sonuçları görüntüler.

Sonuçları yeniden yüklemek için **Yenile** düğmesini kullanın.

- **İstatistik değerlerini yenile** - yukarıda görüntülenen istatistikleri günceller.
- **İstatistik değerlerini sıfırla** - tüm istatistikleri sıfır olarak sıfırlar.

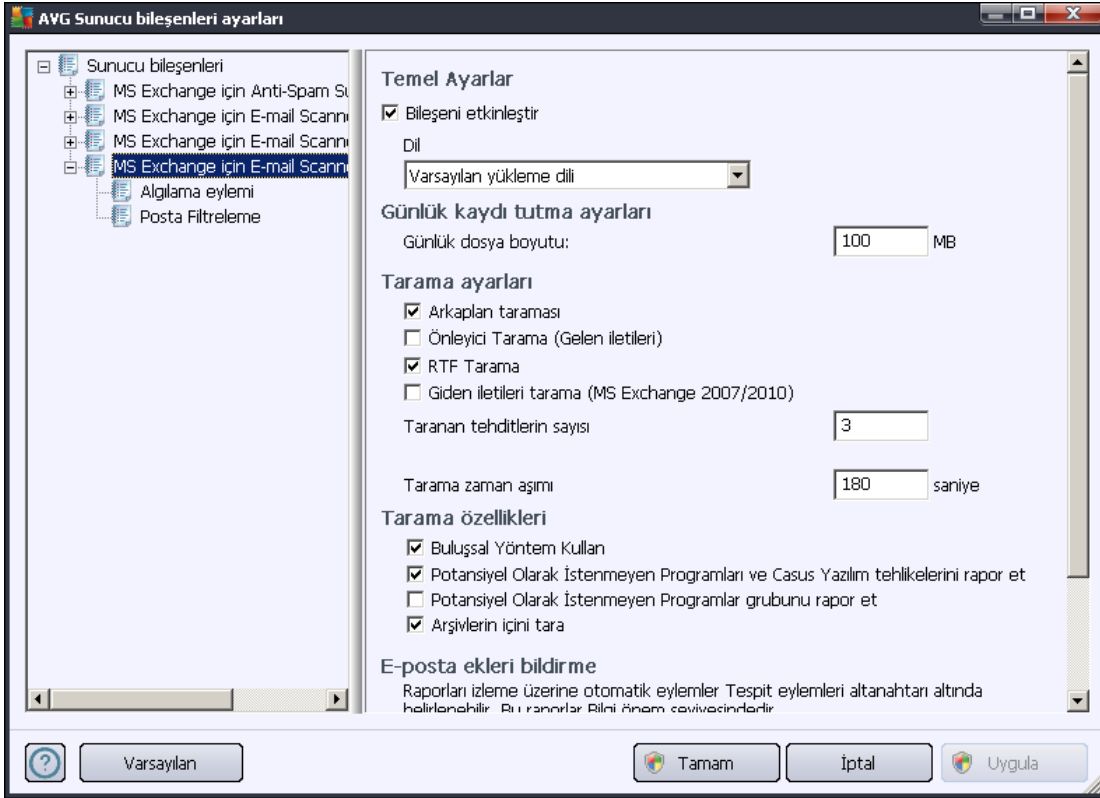
Çalışan düğmeler aşağıda belirtilmektedir:

- **Ayarlar** - bu düğmeyi bileşenin ayarlarını açmak için kullanın.
- **Geri** - Sunucu bileşenleri genel görünümüne geri dönmek için bu düğmeye basın.

Aşağıdaki bölümde tüm bileşenlerin tek tek ayarları hakkında daha fazla bilgi bulabilirsiniz.

5.2. MS Exchange için E-posta Tarayıcısı (VSAPI)

Bu öge, **MS Exchange için E-posta Tarayıcısı (VSAPI)** ayarlarını içerir.



Temel Ayarlar bölümü aşağıdaki seçenekleri içerir:

- **Bileşeni etkinleştir** - bileşenin tamamını devre dışı bırakmak için işaretini kaldırın.
- **Dil** - tercih edilen bileşen dilini seçin.

Günlük ayarları bölümü:

- **Günlük dosyası boyutu** - tercih edilen bir günlük dosyası boyutu seçin. Varsayılan değer: 100 MB.

Tarama ayarları bölümü:

- **Arka Plan Tarama** - arka plan tarama işlemini buradan etkinleştirebilir veya devre dışı bırakabilirsiniz. Arka plan tarama, VSAPI 2.0/2.5 uygulama arayüzü özelliklerinden biridir. Exchange Mesaj Veritabanlarının iş parçacıklı taranmasını sağlar. Kullanıcının posta kutusunda, en son AVG virüs veritabanı güncellemesiyle taranmamış bir ögeyle karşılaşılması durumunda, ilgili öge taranması için Exchange Server için AVG'ye gönderilir. İncelenmeyen nesnelere taranması ve aranması paralel olarak çalışır.

Diğer görevleri garantileyen özel bir düşük öncelikli iş parçacığı her veritabanı için kullanılır



(örn. Microsoft Exchange veritabanında e-posta iletilerinin saklanması) ve her zaman isteğe bağlı olarak gerçekleşir.

- **Proaktif Tarama (gelen iletiler)**

VSAPI 2.0/2.5 proaktif tarama işlevini buradan etkinleştirebilir veya devre dışı bırakabilirsiniz. Bu tarama bir öge klasöre teslim edildiğinde ancak istemci tarafından bir istek yapılmadığında oluşur.

İletiler Exchange deposuna gönderilir gönderilmez, global tarama kuyruğuna düşük öncelikli olarak girerler (maksimum 30 öge). İlk giren ilk çıkar (FIFO) temelinde taranırlar. Hala kuyrukta olan bir ögeye erişilirse, bu öge yüksek öncelikli olarak değişir.

Not: Taşma iletileri taranmamış deposuna gider.

Not: Hem Arka Plan Tarama hem de Proaktif Tarama seçeneklerini devre dışı bıraksanız bile, bir kullanıcı MS Outlook istemcisiyle bir ileti indirmeye çalıştığında tarayıcıya erişim yine de aktif olacaktır.

- **RTF Tara** - burada RTF dosyası türünün taranması gerekip gerekmediğini belirtebilirsiniz.
- **Taranan İş Parçacıklarının Sayısı** - Tarama işlemi varsayılan olarak tüm tarama performansını belirli bir paralelizm düzeyinde artırmak için iş parçacığı olarak oluşturulur. İş parçacığı sayısını buradan değiştirebilirsiniz.

Varsayılan iş parçacığı sayısı 2 kere 'işlemci_sayısı' + 1 olarak hesaplanır.

Minimum iş parçacığı sayısı ('işlemci sayısı'+1) bölü 2 olarak hesaplanır.

Maksimum iş parçacığı sayısı 'İşlemci Sayısı' çarpı 5 + 1 olarak hesaplanır.

Değer minimum veya daha küçük deçerse veya maksimum veya daha büyük deçerse varsayılan deçer kullanılır.

- **Tarama Zaman Aşımı** - bir iş parçacığının taranmakta olan iletiye erişmesi için (saniye cinsinden) maksimum sürekli aralık (varsayılan deçer 180 saniyedir).

Tarama özellikleri bölümü:

- **Buluşsal Analiz Yöntemlerini Kullan** - bu kutuyu tarama sırasında buluşsal analiz yöntemini etkinleştirmek için işaretleyin.
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et** - bu seçeneği potansiyel olarak istenmeyen programların ve casus yazılımın varlığını bildirmek için işaretleyin.
- **Geliştirilmiş bir Potansiyel Olarak İstenmeyen Program dizisi bildirin** - ayrıntılı bir casus yazılım (spyware) paketi tespit etmek için işaretleyin: doğrudan üreticiden sağlandığında mükemmel durumda ve zararsız olan ancak daha sonra kötü amaçlar için kullanılacak programlar veya her zaman zararsız olan ancak istenmeyebilecek programlar (çeşitli araç çubukları vs.). Bu ek önlem, bilgisayarınızın güvenliğini ve rahatlığını daha da artırır, ancak yasal programları engellemesi de olasıdır ve bu nedenle varsayılan olarak kapatılır. Not: Bu algılama özelliği, bir önceki seçeneğe ektir. Bu nedenle, temel casus yazılım (spyware)



türlerinden korunmak istiyorsanız, bir önceki kutuyu daima seçili halde bırakın.

- **Arşivlerin içeriğini tara** - bu seçeneği tarayıcının arşivi dosyaların (zip, rar vb.) içine de bakmasını sağlamaya izin vermek için işaretleyin.

E-posta eklerini bildirme bölümü, tarama sırasında hangi öğelerin seçileceğine izin vermenize olanak verir. Varsayılan yapılandırma **Tespit işlemleri bölümü**, **Bilgi** kısmında (yukarı bakın) kolaylıkla istenebilir.

Aşağıdaki seçenekler mevcuttur:

- **Parola korumalı arşivleri bildir**
- **Parola korumalı belgeleri bildir**
- **Makro içeren dosyaları bildir**
- **Gizli uzantıları bildir**

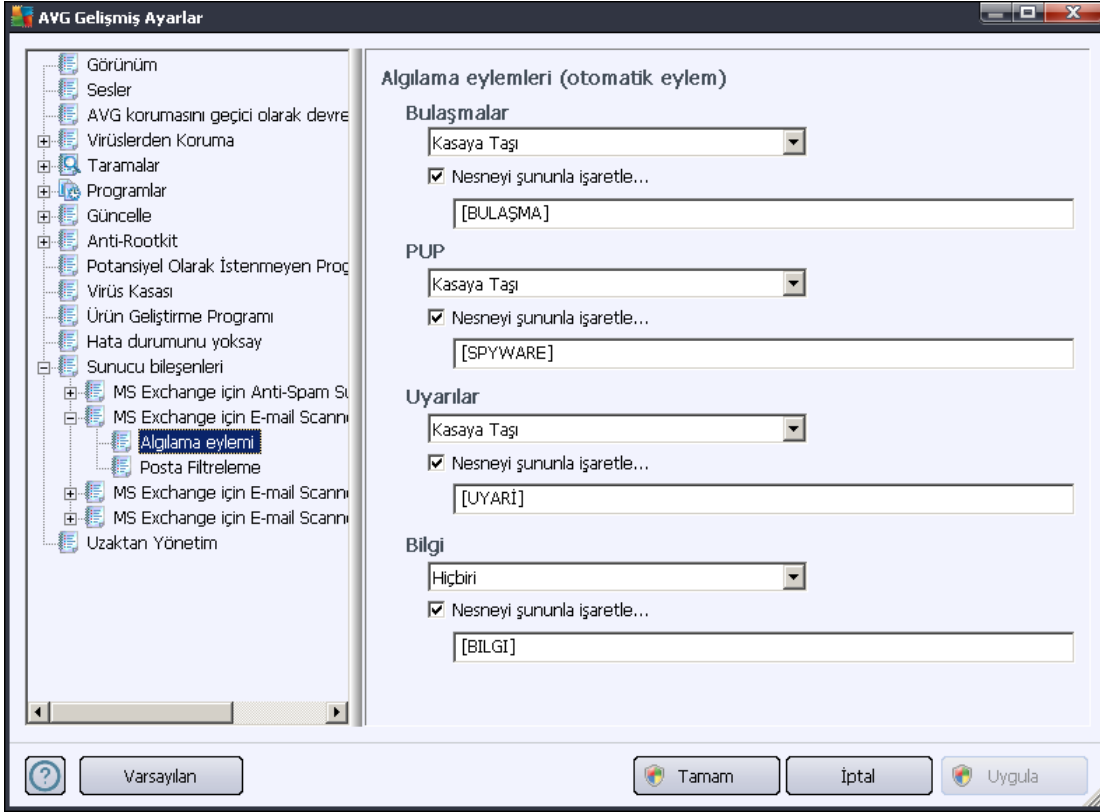
Genel olarak, bu özelliklerin tümü Microsoft VSAPI 2.0/2.5 uygulama arayüzü hizmetlerinin kullanıcı uzantılarıdır. VSAPI 2.0/2.5 hakkında ayrıntılı bilgiler için lütfen aşağıdaki bağlantılara (ve ayrıca, başvurulanlardan erişilen bağlantılar) bakın:

- <http://support.microsoft.com/default.aspx?scid=kb:en-us:328841&Product=exch2k> - Exchange ve virüsten koruma yazılımı etkileşimi hakkında bilgi için
- <http://support.microsoft.com/default.aspx?scid=kb:en-us:823166> - Exchange 2003 Server uygulamasında ek VSAPI 2.5 özellikleri hakkında bilgi için.

Ayrıca aşağıdaki ağaç yapısında bu alt öğeler de bulunur:

- [Tespit işlemleri](#)
- [Posta filtreleme](#)

5.3. Algılama Eylemleri



Algılama eylemleri alt ögesinde, tarama işlemi sırasında yapılması gereken otomatik eylemleri seçebilirsiniz.

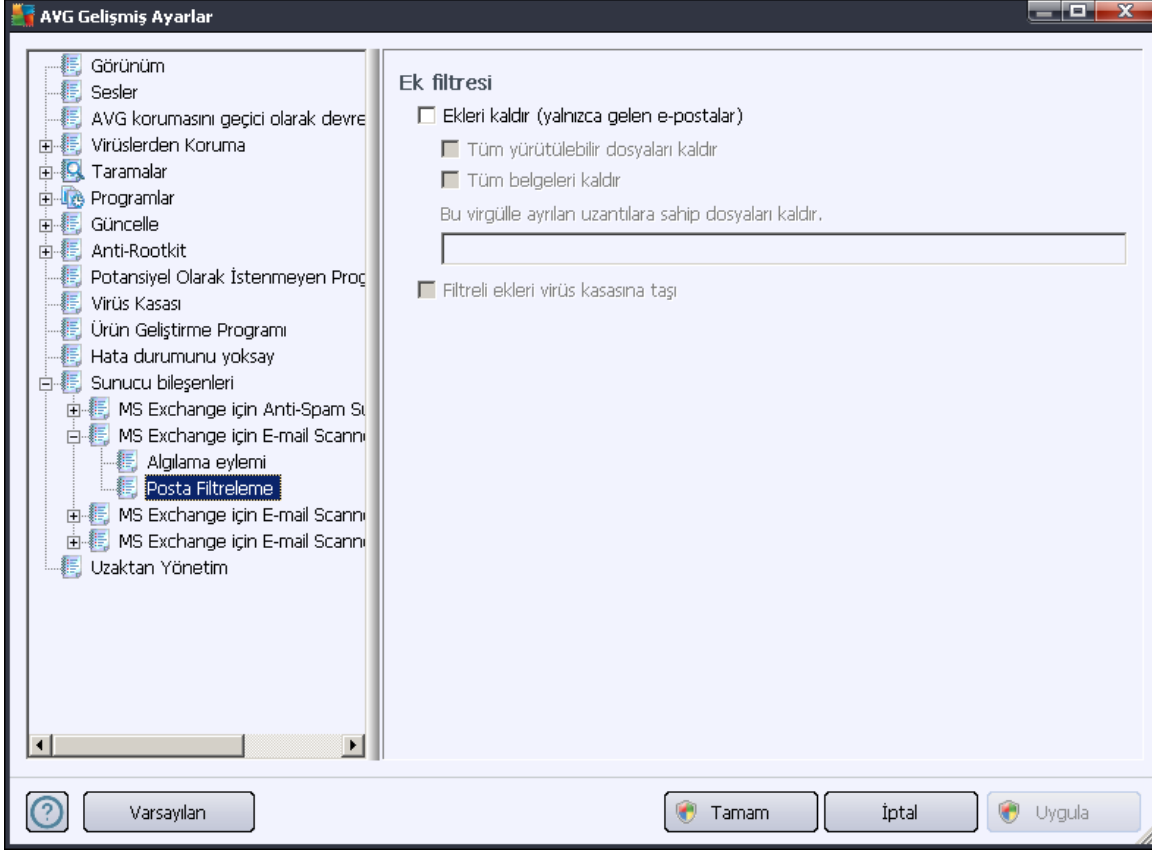
Eylemler aşağıdaki öğeler için kullanılabilir:

- **Bulaşmalar**
- **PUP (Potansiyel Olarak İstenmeyen Programlar)**
- **Uyarılar**
- **Bilgi**

Her öğe için bir eylem seçmek için açılır menüyü kullanın:

- **Hiçbiri** - hiçbir eylem yapılmaz.
- **Kasaya Taşı** - verilen tehlike Virüs Kasasına taşınacaktır.
- **Kaldır** - verilen tehlike kaldırılacaktır.

5.4. Posta Filtreleme



Posta Filtreleme alt ögesinde, hangi eklerin (varsa) otomatik olarak kaldırılacağını seçebilirsiniz. Aşağıdaki seçenekler mevcuttur:

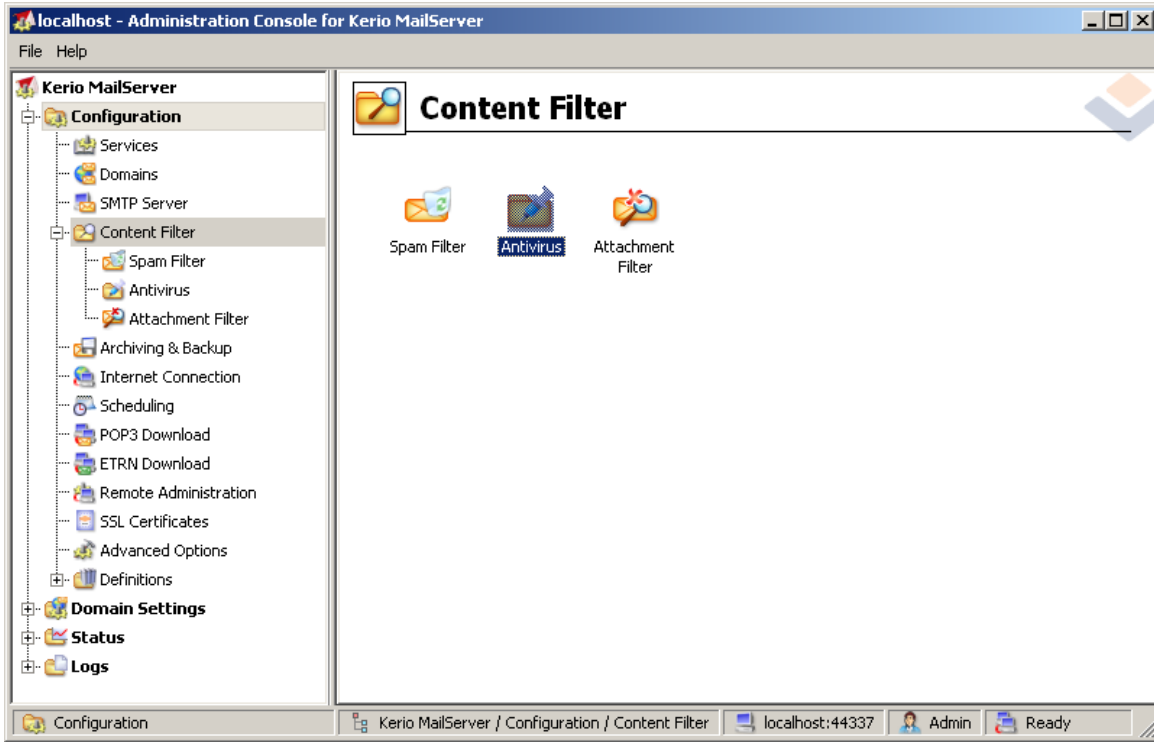
- **Ekleri kaldır** - bu kutuyu özelliği etkinleştirmek için işaretleyin.
- **Tüm çalıştırılabilir dosyaları kaldır** - tüm çalıştırılabilirleri kaldırır.
- **Tüm belgeleri kaldır** - tüm belge dosyalarını kaldırır.
- **Bu virgülle ayrılan uzantılara sahip dosyaları kaldır** - kutuyu otomatik olarak kaldırılmalarını istediğiniz dosya uzantılarıyla doldurun. Uzantıları virgülle ayırın.
- **Filtrelenmiş ekleri virüs kasasına taşı** - Filtrelenmiş eklerin tamamen kaldırılmamasını istemeniz durumunda işaretleyin. Bu kutu işaretlendiğinde, bu iletişim kutusunda seçilen tüm ekler otomatik olarak Virüs Kasası karantina ortamına taşınır. Burası, potansiyel olarak zararlı dosyaları saklamak için güvenli bir yerdir - Dosyaları sisteminizi tehlikeye sokmadan erişebilir ve inceleyebilirsiniz. Virüs Kasasına **AVG Email Server Edition 2012** ana arayüzünün üst menüsünden erişebilirsiniz. **Geçmiş** ögesini sol tıklatıp bağlam menüsünden **Virüs Kasası** ögesini seçmeniz yeterlidir.



6. Kerio MailServer için AVG

6.1. Yapılandırma

Virüsten koruma mekanizması doğrudan Kerio MailServer uygulamasına entegredir. AVG tarama motoruyla Kerio MailServer e-posta korumasını etkinleştirmek için, Kerio Administration Paneli uygulamasını başlatın. Uygulama penceresinin sol tarafındaki kontrol ağacında Yapılandırma dalının İçerik Filtresi alt dalını seçin:



İçerik Filtresi öğesi tıklatıldığında üç öğe içeren bir iletişim kutusu görüntülenir:

- ***İstenmeyen Posta Filtresi***
- ***Virüsten koruma*** (bkz. ***Virüsten koruma*** bölümü)
- ***Ek Filtresi*** (bkz. ***Ek Filtresi*** bölümü)

6.1.1. Virüsten koruma

Kerio MailServer için AVG'yi etkinleştirmek için, Harici virüsten korumayı kullan onay kutusunu seçin ve yapılandırma penceresinin Virüsten koruma çerçevesinde harici yazılım menüsünden AVG Email Server Edition öğesini seçin:



Antivirus usage

Use integrated McAfee® antivirus engine

Use external antivirus AVG Email Server Edition Options

Aşağıdaki kısımda virüslü veya filtrelili bir iletiye ne yapılacağını belirtebilirsiniz:

• ***İletide bir virüs bulunursa***

If a virus is found in a message

Discard the message

Deliver the message with the malicious code removed

Forward the original message to administrator address:

Forward the filtered message to administrator address:

Bu çerçeve, iletide bir virüs bulunduğunda veya ileti bir ek filtresiyle filtrelendiğinde yapılacak eylemi belirtir:

- ***İletiyi gözardı et*** - seçildiğinde, virüslü veya filtrelili ileti silinecektir.
- ***İletiyi zararlı kodu kaldırarak teslim et*** - seçiliyken, ileti alıcıya zararlı olabilecek ek olmadan teslim edilir.
- ***Orijinal iletiyi yönetici adresine ilet*** - seçiliyken virüs bulaştı iletisi adres metni alanında belirtilen adrese iletilir
- ***Filtrelili iletiyi yönetici adresine ilet*** - seçiliyken, filtrelili ileti adres metni alanında belirtilen adrese iletilir

• ***İletinin bir kısmı taranamıyorsa (örn. şifreli veya bozuk dosya)***

If a part of message cannot be scanned (e.g. encrypted or corrupted file)

Deliver the original message with a prepended warning

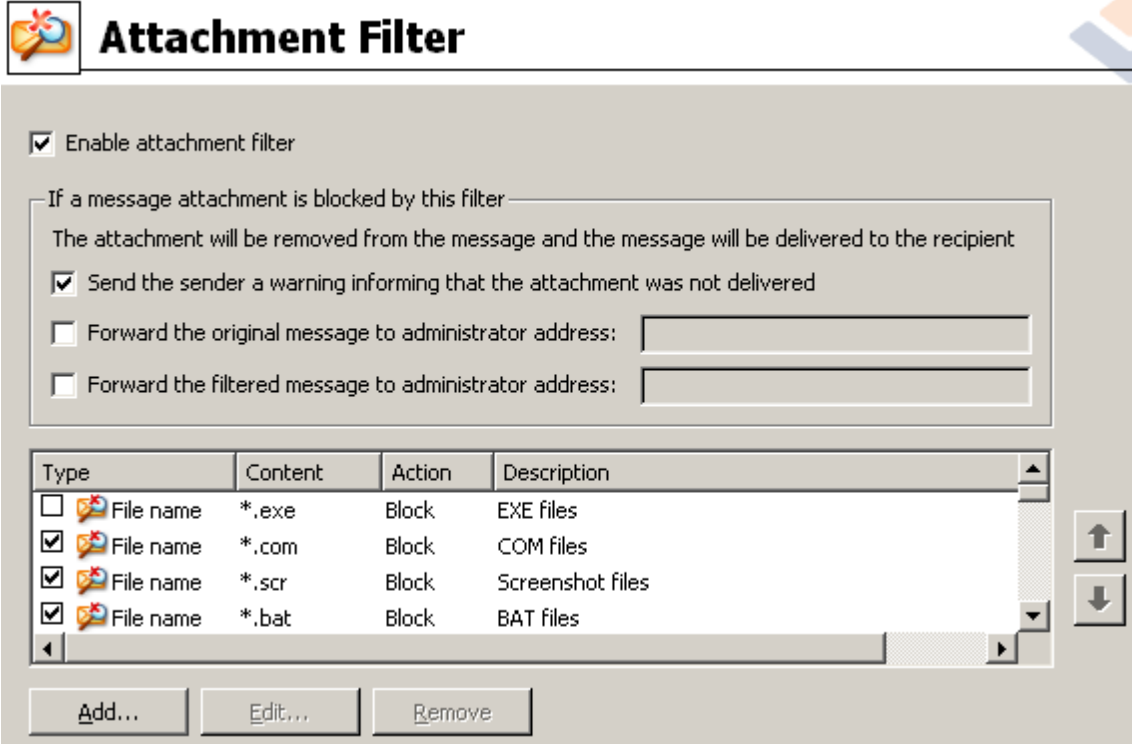
Reject the message as if it was a virus (use the settings above)

Bu çerçeve iletinin veya ekin bir kısmı taranamadığında yapılacak eylemi belirtir:

- ***Orijinal iletiyi hazırlanmış uyarıyla teslim et*** - ileti (veya ek) kontrol edilmeden teslim edilir. Kullanıcı iletinin hala virüs taşıyabileceği konusunda uyarılacaktır.
- ***İletiyi virüslüymüş gibi reddet*** - sistem, virüs algılandığında davrandığı şekilde davranır (örn. ileti ek olmadan teslim edilir veya reddedilir). Seçenek güvenlidir, ancak parola korumalı arşivler gönderme neredeyse imkansızdır.

6.1.2. Ek Filtresi

Ek Filtresi menüsünde çeşitli ek tanımlamalarının bir listesi bulunur:



Attachment Filter

Enable attachment filter

If a message attachment is blocked by this filter

The attachment will be removed from the message and the message will be delivered to the recipient

Send the sender a warning informing that the attachment was not delivered

Forward the original message to administrator address:

Forward the filtered message to administrator address:

Type	Content	Action	Description
<input type="checkbox"/>	File name *.exe	Block	EXE files
<input checked="" type="checkbox"/>	File name *.com	Block	COM files
<input checked="" type="checkbox"/>	File name *.scr	Block	Screenshot files
<input checked="" type="checkbox"/>	File name *.bat	Block	BAT files

Ek filtresini etkinleştir onay kutusunu seçerek posta eklerinin filtrelenmesini etkinleştirebilir/devre dışı bırakabilirsiniz. İsteğe bağlı olarak, aşağıdaki ayarları da değiştirebilirsiniz:

- ***Kullanıcıya ekin teslim edilmediğini bildiren bir uyarı gönder***

Gönderen virüslü veya engellenmiş eki olan bir ileti gönderdiğine dair Kerio MailServer'dan bir uyarı alacaktır.

- ***Orijinal iletiyi yönetici adresine ilet***

İleti ister yerel ister harici bir adres olsun, tanımlanan bir e-posta adresine iletilecektir (olduğu gibi - virüslü veya yasak ekle).

- ***Filtreli iletiyi yönetici adresine ilet***

İleti virüslü veya yasak ek olmaksızın (aşağıda seçilen eylemlerden hariç) belirtilen e-posta adresine iletilecektir. Bu, virüsten korumanın ve/veya ek filtresinin doğru çalıştığını doğrulamak için kullanılabilir.

Uzantılar listesinde, her öğenin dört alanı vardır:

- **Tür** - ekin türünü belirtme İçerik alanında verilen uzantıyla belirlenir. Olası türler Dosya adı veya MIME türüdür. Öğeyle ek filtrelemesi eklemek/çıkarmak için bu alandaki ilgili kutuyu

seçebilirsiniz.

- **İçerik** - filtrelenecek bir uzantı burada belirtilebilir. İşletim sistemi joker karakterlerini burada kullanabilirsiniz (örneğin "*.doc.*" dizesi .doc uzantılı herhangi bir dosya ve izleyen herhangi bir uzantı anlamına gelir).
- **Eylem** - belirli bir ekle gerçekleştirilecek eylemi tanımlayın. Olası eylemler Kabul et (eki kabul et) ve Engelle'dir (devre dışı bırakılan ekler listesinin üstünde tanımlandığı gibi bir eylem gerçekleştirilecektir).
- **Açıklama** - ekin açıklaması bu alanda tanımlanır.

Kaldır düğmesine basılarak bir öğe listeden kaldırılır. **Ekle...** düğmesine basarak başka bir öğeyi listeye ekleyebilirsiniz. Ya da **Düzenle...** düğmesine basarak varolan bir kaydı düzenleyebilirsiniz. Aşağıdaki pencere görünür:



- Açıklama alanında filtrelenecek ekin kısa bir açıklamasını yazabilirsiniz.
- Posta iletisi bir ek içeriyorsa alanında ekin türünü seçebilirsiniz (Dosya adı veya MIME türü). Ayrıca, sunulan uzantılar listesinden belirli bir uzantıyı seçebilirsiniz veya uzantı joker karakterini doğrudan yazabilirsiniz.

Sonra alanında tanımlanan eki engellemeyi veya kabul etmeyi seçebilirsiniz.



7. Anti-Spam Yapılandırması

7.1. İstenmeyen Posta Önleme Arayüzü

Anti-Spam sunucusu bileşeninin iletişim kutusunu **Sunucu Bileşenleri** kısmında (sol menü) bulabilirsiniz. Sunucu bileşeninin işlevselliği hakkında kısa bir bilgi, geçerli durumu hakkında bilgi (*MS Exchange bileşeni için Anti-Spam Sunucusu etkindir.*) ve bazı istatistikleri içerir.

Kullanılabilir bağlantılar:

- **Tarama Sonuçları**

Anti-spam tarama sonuçlarını gözden geçirebileceğiniz yeni bir iletişim kutusu açar:

AVG Tarama sonuçları

Sonuncuyu göster 2 gün 0 görüntüle

Seçimi göster

Başlangıç: 21. 2 .2012 20:53:53

Hedef: 22. 2 .2012 20:53:53

Tümünü göster

Yenile

Tümü	Bulaşmalar	Casus yazılım	Uyarılar	Bilgi
Dosya adı	Zaman	Tehdit adı		

Kapat

Burada, bir SPAM (istenmeyen iletiler) veya bir Yemleme girişimi (kişisel verilerinizi, banka ayrıntılarınızı, kimliğinizi vb. çalmaya çalışma) olarak algılanan iletileri kontrol edebilirsiniz. Varsayılan olarak yalnızca son iki günün sonuçları görüntülenir. Görüntülenen dönemi aşağıdaki seçenekleri kullanarak değiştirebilirsiniz:

- **Sonuncuyu göster** - Tercih edilen günleri ve saatleri girin.
- **Seçimi göster** - özel bir saat ve tarih aralığı seçin.
- **Tümünü göster** - Tüm zaman dönemi için sonuçları görüntüler.

Sonuçları yeniden yüklemek için **Yenile** düğmesini kullanın.

- **İstatistik değerlerini yenile** - yukarıda görüntülenen istatistikleri günceller.
- **İstatistik değerlerini sıfırla** - tüm istatistikleri sıfır olarak sıfırlar.

İletişim kutusunun **Anti-Spam ayarları** bölümünde tek bir **Anti-Spam'ı Etkinleştir** onay kutusu bulunur. Anti-Spam korumasını devre dışı bırakmak için onay kutusunun işaretini kaldırın (ör. tüm bileşeni devre dışı bırakın). Anti-Spam korumasını aynı onay kutusunu işaretleyerek veya [Anti-Spam ayarları](#) bölümündeki benzer onay kutusunu işaretleyerek yeniden açabilirsiniz.



Çalışan düğmeler aşağıda belirtilmektedir:

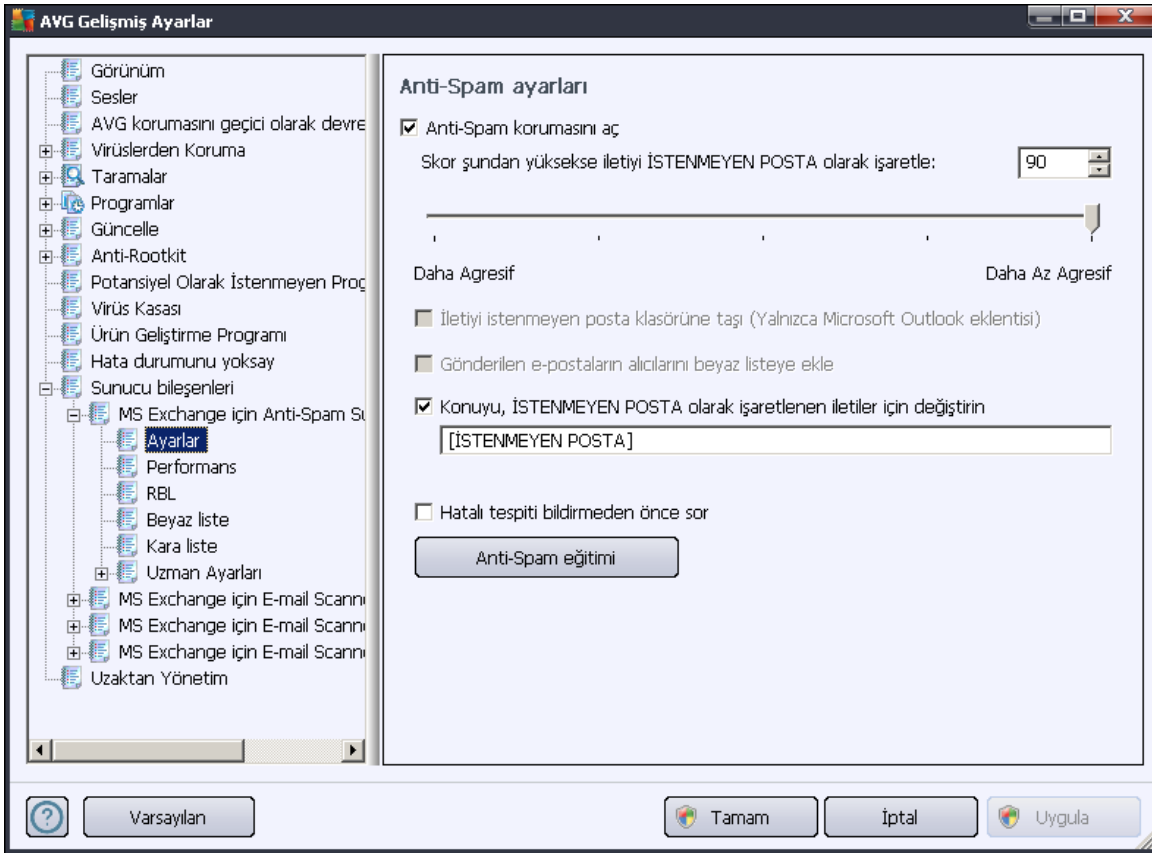
- **Ayarlar** - bu düğmeyi [Anti-Spam ayarlarını](#) açmak için kullanın.
- **Geri** - Sunucu bileşenleri genel görünümüne geri dönmek için bu düğmeye basın.

7.2. İstenmeyen Posta Önleme Prensipleri

Spam, ürün veya hizmet reklamı yapmak amacıyla bir kerede çok sayıda e-posta adresine toplu olarak gönderilen ve kullanıcıların posta kutularını dolduran istenmeyen e-postalardır. Spam, müşterinin kendi isteğiyle almayı kabul ettiği yasal ticari e-posta anlamına gelmez. Spam kişi için sıkıcı olmanın yanında genellikle aldatma, virüs veya saldırı amaçlı içerik de olabilir.

Anti-Spam, gelen tüm e-posta iletilerini denetler istenmeyen e-postaları SPAM (İSTENMEYEN) olarak işaretler. Her e-posta iletilisini işlemek için çeşitli inceleme yöntemleri kullanır ve istenmeyen postalara karşı mümkün olan en üst seviyede koruma sağlar.

7.3. Anti-Spam Ayarları



İstenmeyen Posta Önleme temel ayarları iletişim kutusunda **İstenmeyen Posta Önleme Korumasını Aç** onay kutusunu işaretleyerek e-posta iletişiminin istenmeyen posta önleme taramasına izin verebilir ya da engelleyebilirsiniz.



Bu iletişim kutusunda daha fazla ya da az agresif değerlendirme ölçütleri belirleyebilirsiniz. **İstenmeyen Posta Önleme** filtresi, çeşitli dinamik tarama teknikleri sayesinde mesajlardan her birine (*başka bir deyişle, mesajın içeriğinin İSTENMEYEN POSTA'ya ne kadar yakın olduğunu belirlemek üzere*) bir puan verir. **Puan, şu değere eşit veya bu bundan fazla ise iletiyi istenmeyen olarak işaretler** ayarını ya değeri girerek (50 ila 90) ya da kaydırma çubuğunu sola veya sağa hareket ettirerek ayarlayabilirsiniz.

Burada puan eşiği hakkında genel bilgi verilmektedir:

- **Değer 90** - Çoğu gelen e-posta mesajı normal olarak ([istenmeyen posta](#) olarak işaretlenmeden) alınacaktır. En kolay tanımlanabilir [istenmeyen postalar](#) filtrelenecek ancak belirli bir miktar [istenmeyen posta](#) alınmaya devam edecektir.
- **Değer 80-89** - [istenmeyen posta](#) olması muhtemel e-posta mesajları filtrelenecektir. İstenmeyen posta olmayan bazı postalar yanlışlıkla istenmeyen posta şeklinde etiketlenebilir.
- **Değer 60-79** - Oldukça etkili bir yapılandırma olarak değerlendirilir. [İstenmeyen posta](#) olması muhtemel e-posta mesajları filtrelenecektir. İstenmeyen posta olmayan mesajların da yakalanma ihtimali vardır.
- **Değer 50-59** - Çok agresif yapılandırma. İstenmeyen posta olmayan e-posta iletilerinin de gerçek [istenmeyen posta](#) iletileri ile birlikte yakalanma ihtimali çok yüksektir. Bu eşik aralığı normal kullanım için önerilmez.

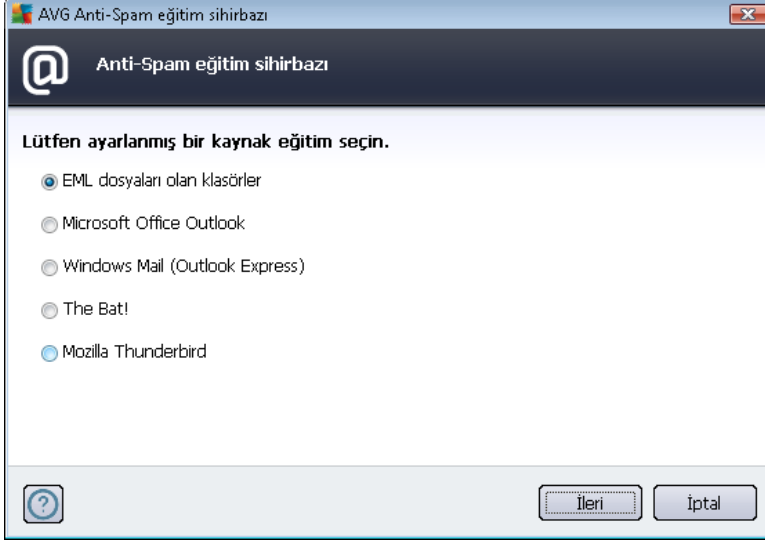
Algılanan [istenmeyen posta](#) e-posta iletilerine nasıl davranılacağını da tanımlayabilirsiniz:

- İstenmeyen posta olarak işaretlenmiş iletilerin konusunu değiştir - [istenmeyen posta](#) olarak işaretlenmiş e-postaların konu alanına belirli bir kelime ya da ibarenin yazılmasını istiyorsanız bu kutucuğu işaretleyin: istediğiniz metin, etkinleştirilen metin alanına girilebilir.
- **Hatalı tespiti bildirmeden önce sor** - yükleme süreci sırasında Ürün Geliştirme Programına katılmayı kabul etmeniz durumunda - bu program, en son tehditlerle ilgili en güncel bilgileri toplamamıza ve karşılığında korumayı herkes için iyileştirebilmemize yardımcı olur - yani, tespit edilen tehditlerin AVG'ye bildirilmesini kabul edersiniz. Bu raporlama otomatik olarak yapılır. Ancak, gerçekten istenmeyen posta olarak sınıflandırılması gerekip gerekmediğinden emin olmak için, tespit edilen istenmeyen posta AVG'ye bildirilmeden önce sorulmasını istediğinizi onaylamak için bu onay kutusunu işaretleyebilirsiniz.

Anti-Spam'ı Eğitin düğmesi, [bir sonraki bölümde](#) ayrıntılarla açıklanan [Anti-Spam eğitim sihirbazı](#) 'nı açar.

7.3.1. İstenmeyen Posta Önleme Eğitim Sihirbazı

İstenmeyen Posta Önleme Eğitim Sihirbazının ilk iletişim kutusu, eğitim için kullanmak istediğiniz e-posta iletileri kaynağını seçmenizi belirtir. Genellikle yanlışlıkla İSTENMEYEN POSTA olarak işaretlenen e-postaları ya da tanınmayan gereksiz mesajları kullanmak isteyeceksiniz.



Aşağıdaki seçenekler arasından seçim yapabilirsiniz:

- **Özel bir e-posta istemcisi** - listelenen e-posta istemcilerinden birini kullanıyorsanız (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*), sadece ilgili seçeneği seçin.
- **EML dosyalı Klasörler** - Başka bir e-posta programı kullanıyorsanız, öncelikle iletileri belirli bir klasöre kaydetmeniz (.eml biçiminde) veya e-posta istemcisi ileti klasörlerinin konumunu biliyor olmanız gerekir. Sonra, **EML dosyaları içeren klasör** seçeneğini seçin; bu, sonraki adımda istenen klasörü bulmanızı sağlayacaktır

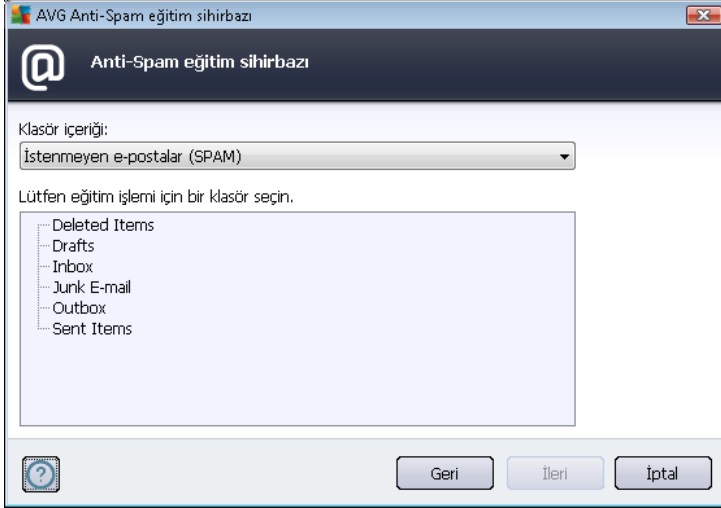
Eğitim sürecinin daha hızlı ve kolay olması için, klasörlerdeki e-postaları önceden sıralayabilirsiniz; böylece eğitim için kullanacağınız klasör yalnızca eğitim iletilerini (istenen veya istenmeyen) içerecektir. Ancak, e-postaları daha sonra filtreleyebileceğiniz için bu gerekli değildir.

Uygun seçeneği seçin ve sihirbaza devam etmek için **İleri** ögesini tıklayın.

7.3.2. Mesajların Olduğu Klasörü Seç

Bu adımda görüntülenen iletişim kutusu daha önceki seçimlerinize bağlıdır.

EML dosyalarının bulunduğu klasörler



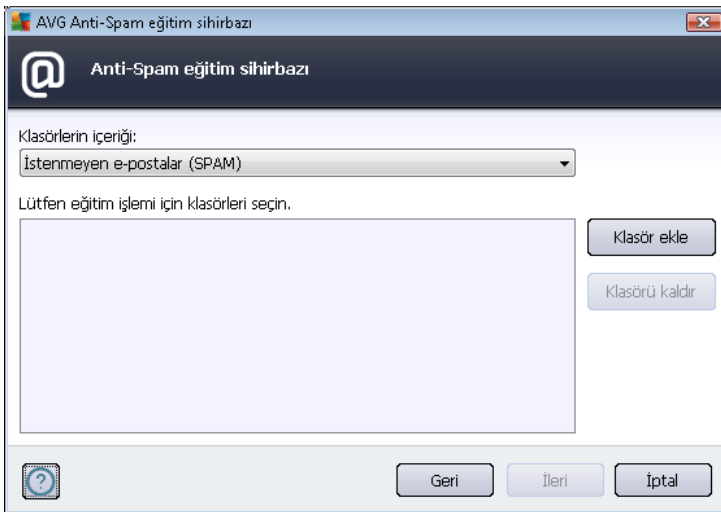
Bu iletişim kutusunda, eğitim için kullanmak istediğiniz iletilerin bulunduğu klasörün konumunu bulun. .eml dosyalarının (*kaydedilen e-posta iletileri*) bulunduğu klasörün konumunu seçmek için **Klasör ekle düğmesine basın**. Seçilen klasör, iletişim kutusunda görüntülenir.

Klasörlerin içeriği: açılır menüsünde, aşağıdaki iki seçenektten birini ayarlayın: seçilen klasör istenen (*HAM*) veya istenmeyen (*SPAM*) iletileri içerir. Bir sonraki adımda iletileri filtreleyebileceğinizi unutmayın; bu nedenle klasörün yalnızca eğitim e-postalarını içermesi zorunlu değildir. **Klasörü sil** düğmesine basarak istenmeyen klasörleri listeden silebilirsiniz.

Tamamladığınız zaman [Mesaj filtreleme seçenekleri](#) penceresine geçmek için **İleri** öğesini tıklayın.

Özel e-posta istemcileri

Seçeneklerden birini onayladığınız zaman yeni bir iletişim kutusu açılacaktır.



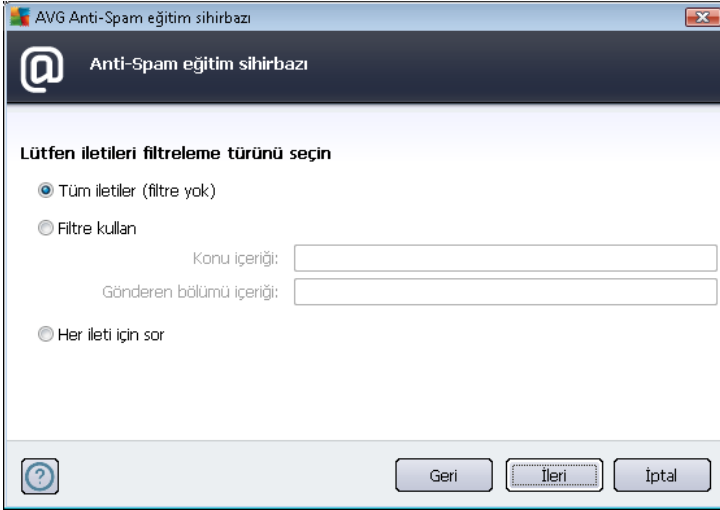
Not: Microsoft Office Outlook kullanıyor olmanız halinde ilk olarak MS Office Outlook profilini

seçmeniz istenecektir.

Klasörlerin içeriği: açılır menüsünde, aşağıdaki iki seçenektten birini ayarlayın: seçilen klasör istenen (*HAM*) veya istenmeyen (*SPAM*) iletileri içerir. Bir sonraki adımda iletileri filtreleyebileceğinizi unutmayın; bu nedenle klasörün yalnızca eğitim e-postalarını içermesi zorunlu değildir. Seçilen e-posta istemcisinin ağaç menüsü iletişim kutusunun ana bölümünde görüntülenir. Lütfen istediğiniz klasörü ağaç menüden bulun ve fareyle vurgulayın.

Tamamladığınız zaman **Mesaj filtreleme seçenekleri** penceresine geçmek için [İleri](#) ögesini tıklayın.

7.3.3. Mesaj filtreleme seçenekleri

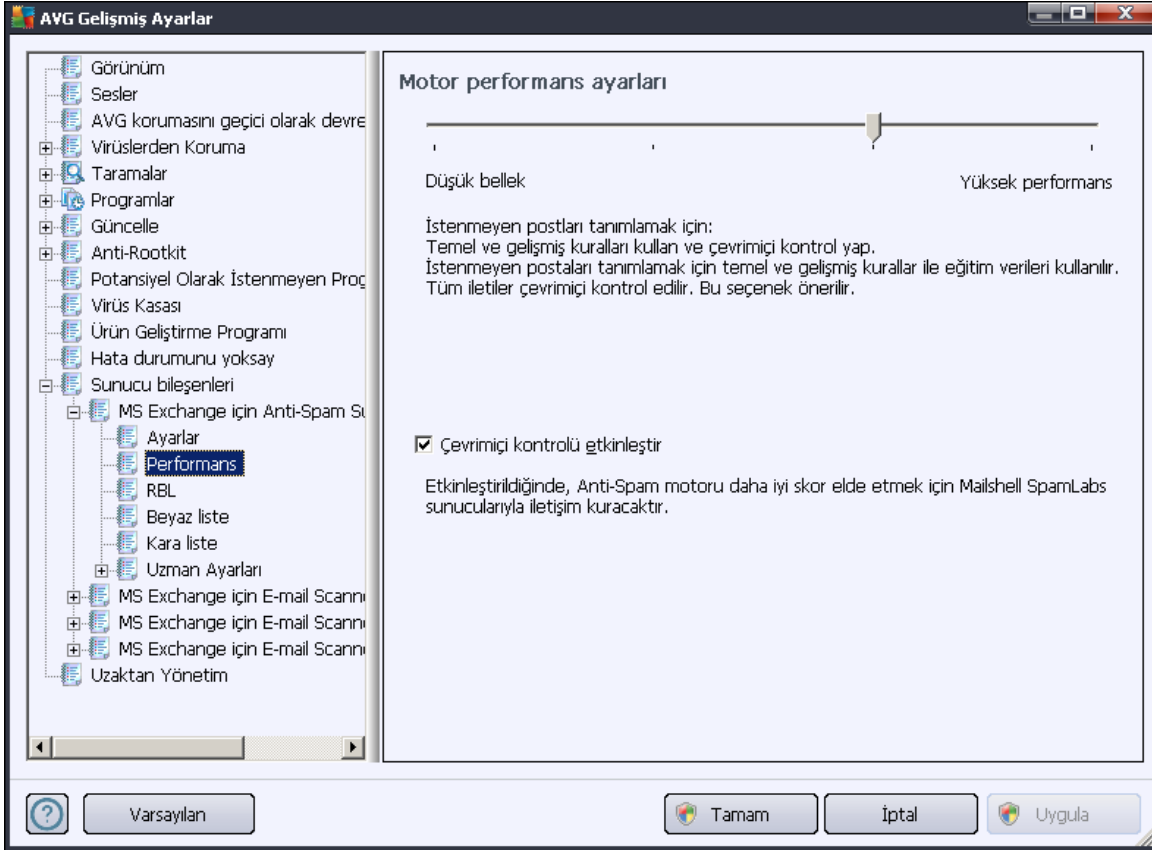


Bu iletişim kutusunda, e-posta iletileri filtrelemesini ayarlayabilirsiniz.

- **Tüm iletiler (filtre yok)** - Seçilen klasörün yalnızca eğitim için kullanmak istediğiniz iletileri içerdiğinden eminseniz, **Tüm iletiler (filtre yok)** seçeneğini işaretleyin.
- **Filtre kullan** - Daha gelişmiş filtreleme için **Filtre kullan** seçeneğini işaretleyin. E-posta konu ve/veya gönderici alanında arama yapmak için bir kelime (*ad*), bir kelime bölümü veya cümle parçası girebilirsiniz. Girilen kriterle tam olarak eşleşen tüm mesajlar, başka bir uyarı yapılmaksızın eğitim için kullanılacaktır. Her iki metin alanına da giriş yaptığınızda, yalnızca iki durumdan biriyle eşleşen adresler kullanılacaktır!
- **Her ileti için sor** - Klasörün içerdiği iletilerden emin değilseniz ve Sihirbazın her ileti için size sormasını istiyorsanız (*eğitim için kullanılıp kullanılmayacağını belirleyebilirsiniz*), **Her ileti için sor** seçeneğini işaretleyin.

Uygun seçenek seçildiği zaman **İleri** ögesine tıklayın. Bir sonraki iletişim kutusu tamamen bilgi amaçlıdır ve sihirbaz sizi işlem mesajları hakkında bilgilendirmeye hazırdır. Eğitime başlamak için yeniden **İleri** düğmesine basın. Daha önce seçtiğiniz koşullar doğrultusunda eğitim başlayacaktır.

7.4. Performans



Motor performans ayarları iletişim kutusu, (solda bulunan *dolaşım alanında Performans* ögesi altında bağlantısı verilen) **Anti-Spam** bileşeninin performans ayarlarının yapılmasını sağlar. Tarama performans seviyesini **Düşük bellek / Yüksek performans** modları arasında yapılandırmak için çubuğu sola ya da sağa kaydırın.

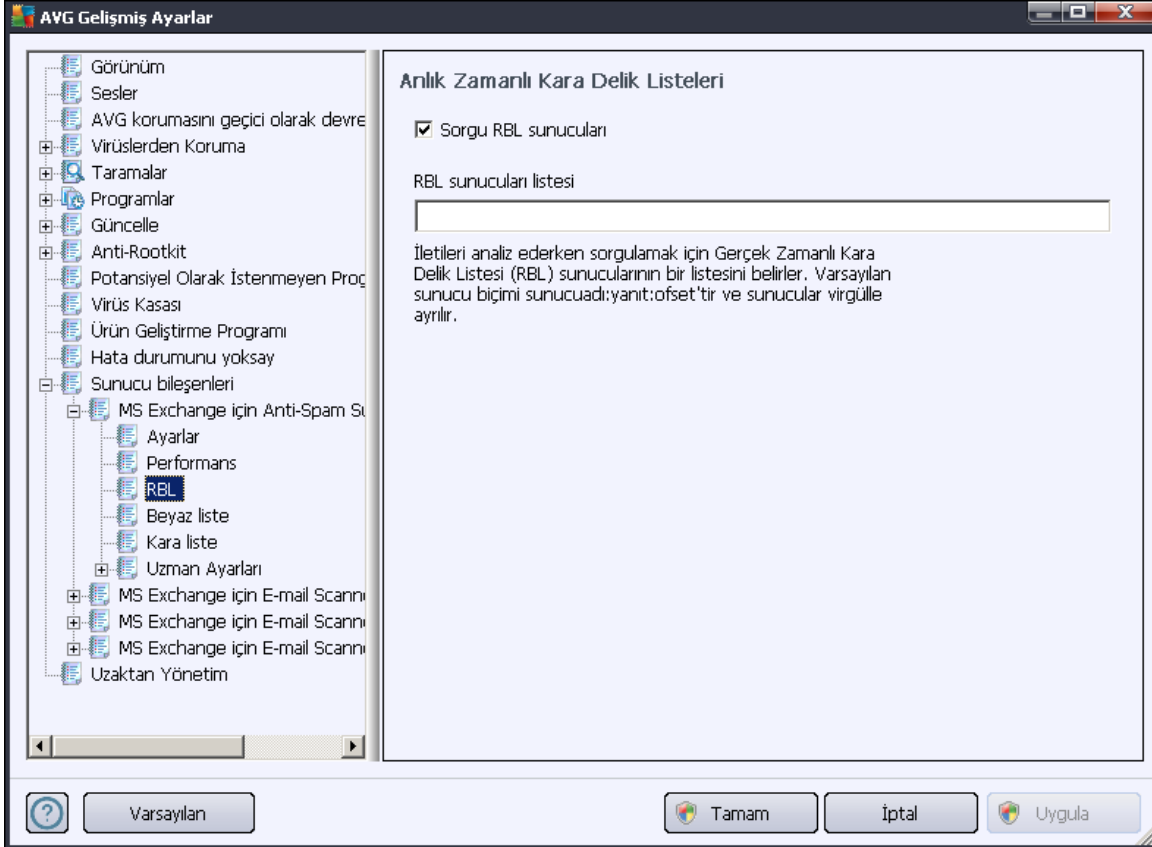
- **Düşük bellek** - tarama işlemi sırasında [istenmeyen postaların](#) tespit edilmesi için herhangi bir kural kullanılmayacaktır. Tanımlama için sadece eğitim verileri kullanılacaktır. Bu mod, bilgisayar donanımlarınız çok eski değil ise genel kullanım için önerilmemektedir.
- **Yüksek performans** - Bu mod, belleği oldukça yoğun şekilde kullanacaktır. Tarama işlemi sırasında [istenmeyen postaları](#) ayırt etmek için şu özellikler kullanılacaktır: kurallar ve [istenmeyen posta](#) veritabanı önbelleği, temel ve gelişmiş kurallar, istenmeyen postayı gönderenin IP adresi ve gönderici veritabanları.

Çevrimiçi taramayı etkinleştir ögesi varsayılan olarak açıktır. [Ana](#) sunucular ile iletişim kurmak vasıtasıyla [istenmeyen postaların](#) daha hassas şekilde tespit edilmesini sağlar. Diğer bir deyişle, taranan veriler çevrimiçi [Ana](#) veritabanları ile karşılaştırılacaktır.

Genellikle varsayılan ayarları kullanmanız ve geçerli bir nedeniniz varsa söz konusu ayarları değiştirmeniz önerilir. Yapılandırma sadece uzman kullanıcılar tarafından değiştirilmelidir!

7.5. RBL

RBL ögesi, **Gerçek Zamanlı Kara Delik Listesi** adlı bir düzenleme iletişim kutusu açar:



Bu iletişim kutusunda **RBL sorgu sunucularını** fonksiyonunu etkinleştirebilir ya da devreden çıkartabilirsiniz.

RBL (**Gerçek Zamanlı Kara Delik Listesi**) sunucusu, bilinen istenmeyen posta gönderen kişilerin kapsamlı bir veritabanının bulunduğu bir DNS sunucusudur. Bu özellik açıldığı zaman tüm e-posta mesajları RBL sunucusu veritabanı ile karşılaştırmalı olarak kontrol edilecek ve veritabanı girişlerinden herhangi biri ile aynı ise [istenmeyen posta](#) olarak etiketlenecektir.

RBL Sunucularının veritabanları en son güncel istenmeyen posta parmak izlerini içerir, en iyi ve en doğru [istenmeyen posta](#) tespit hizmetini sağlar. Bu özellik, normalde Anti-Spam motoru tarafından tespit edilmeyen büyük miktarlarda istenmeyen posta alan kullanıcılar için yararlıdır.

RBL sunucuları listesi belirli RBL sunucularının konumlarını tanımlayabilmenizi sağlar. Varsayılan olarak iki RBL sunucusu adresi belirtilmiştir. Deneyimli bir kullanıcı değilseniz ve bu ayarları gerçekten değiştirmeniz gerekmiyorsa varsayılan ayarları korumanızı öneririz!

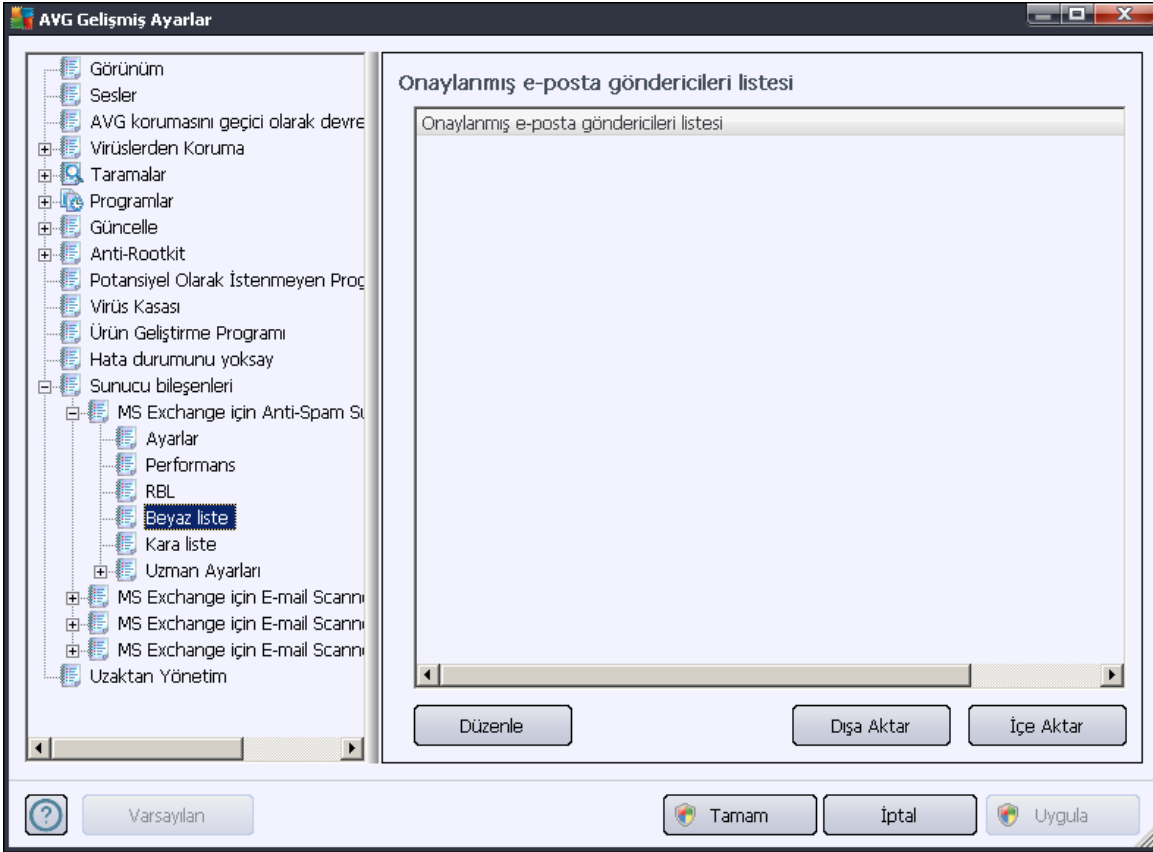
Not: Bazı sistem ve yapılandırmalarda bu özelliğin etkinleştirilmesi, e-posta işlemlerinin yavaşlamasına neden olabilir çünkü mesajların her birinin RBL sunucusu veritabanı ile karşılaştırılması gerekmektedir.



Sunucuya herhangi bir kişisel bilgi gönderilmez!

7.6. Beyaz Liste

Beyaz Liste öğesi, mesajları asla [gereksiz posta](#) olarak etiketlenmeyecek onaylı gönderici e-posta adresleri ve barındırma adlarından oluşan global bir liste içeren iletişim kutusu açar.



Düzenleme arayüzünde asla istenmeyen posta ([istenmeyen posta](#)) göndermeyecek göndericilerden oluşan bir liste düzenleyebilirsiniz. Bunun yanı sıra istenmeyen mesaj göndermediğini bildiğiniz barındırma isimlerinden de (Örn. [avg.com](#)) bir liste oluşturabilirsiniz.

Hazırlanan gönderen ve/veya etki alanı adı listesine sahip olduğunuzda, aşağıdaki yöntemlerden biriyle bunları girebilirsiniz: her e-posta adresini doğrudan girerek veya adreslerin tam listesini bir defada içe aktararak. Şu kontrol düğmeleri bulunur:

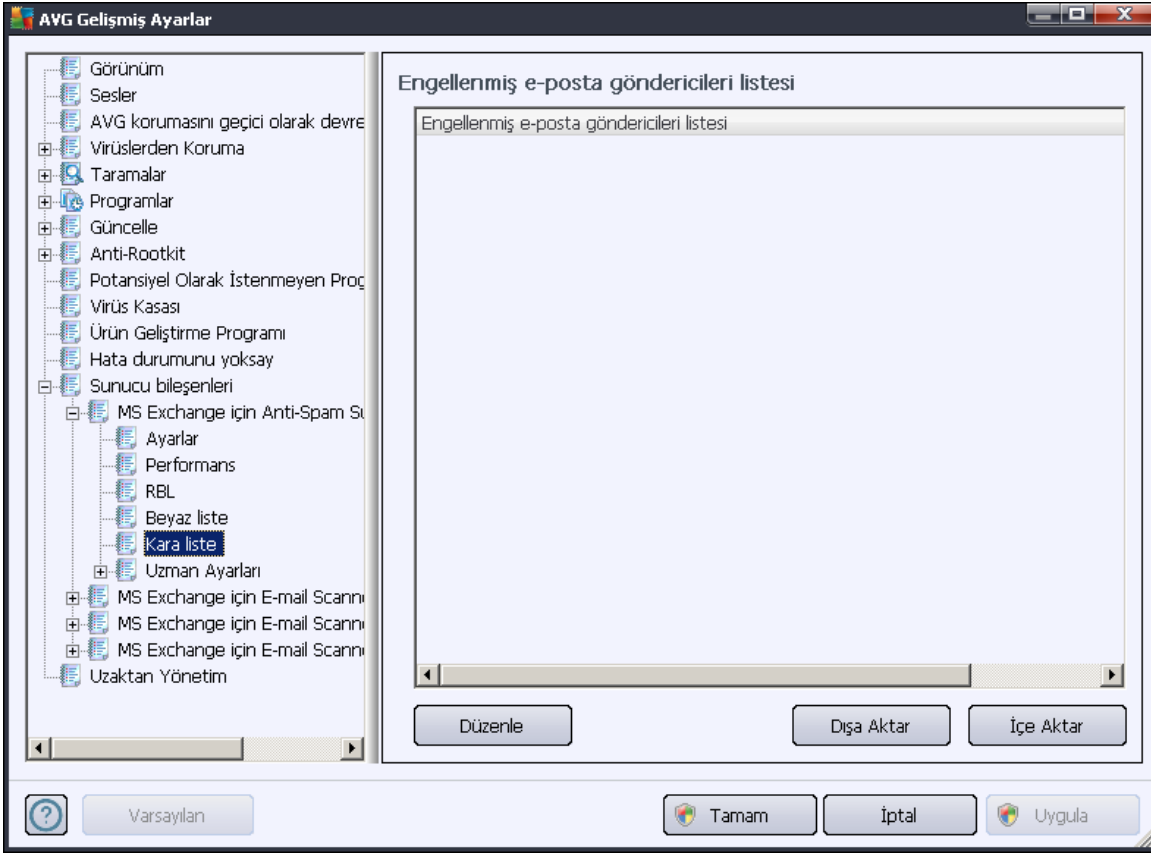
- **Düzenle** - adres listesini manuel olarak doldurabileceğiniz iletişim kutusunu açmak için bu düğmeye basın (bunun yanı sıra *kopyala ve yapıştır* yöntemini de kullanabilirsiniz). Satır başına bir öğe ekleyin (gönderen, etki alanı adı).
- **İçe Aktar** - bu düğmeyi seçerek mevcut e-posta adreslerinizi içe aktarabilirsiniz. Giriş dosyası metin dosyası (düz metin biçiminde ve içerik satır başına yalnızca bir öğe, adres, etki alanı adı içermelidir), WAB dosyası olabilir ya da içe aktarma işlemi Windows Adres Defterinden veya Microsoft Office Outlook'tan yapılabilir.



- **Dışa Aktar** - kayıtları belli bir amaçla dışa aktarmaya karar verirsiniz, bu düğmeye basarak dışa aktarabilirsiniz. Tüm kayıtlar düz bir metin dosyasına kaydedilecektir.

7.7. Kara Liste

Kara liste öğesi engellenmiş gönderici e-posta adresleri ve iletileri her zaman [istenmeyen posta](#) olarak işaretlenecek alan adlarının global bir listesinin bulunduğu bir iletişim kutusu açar.



Düzenleme arayüzünde, istenmeyen ileti [istenmeyen posta](#) göndermesini beklediğiniz göndericilerin bir listesini oluşturabilirsiniz. Ayrıca gereksiz iletiler beklediğiniz veya aldığınız tam etki alanı adlarının (örn. [istenmeyenpostagonderensirket.com](#)) bir listesini oluşturabilirsiniz. Listelenen adreslerden/alan adlarından gelecek tüm e-postalar istenmeyen posta olarak tanımlanacaktır.

Hazırlanan gönderen ve/veya etki alanı adı listesine sahip olduğunuzda, aşağıdaki yöntemlerden biriyle bunları girebilirsiniz: her e-posta adresini doğrudan girerek veya adreslerin tam listesini bir defada içe aktararak. Şu kontrol düğmeleri bulunur:

- **Düzenle** - adres listesini manuel olarak doldurabileceğiniz iletişim kutusunu açmak için bu düğmeye basın (bunun yanı sıra *kopyala ve yapıştır* yöntemini de kullanabilirsiniz). Satır başına bir öğe ekleyin (gönderen, etki alanı adı).
- **İçe Aktar** - bu düğmeyi seçerek mevcut e-posta adreslerinizi içe aktarabilirsiniz. Giriş dosyası metin dosyası (düz metin biçiminde ve içerik satır başına yalnızca bir öğe, adres, etki alanı adı



içermelidir), WAB dosyası olabilir ya da içe aktarma işlemi Windows Adres Defterinden veya Microsoft Office Outlook'tan yapılabilir.

- **Dışa Aktar** - kayıtları belli bir amaçla dışa aktarmaya karar vererseniz, bu düğmeye basarak dışa aktarabilirsiniz. Tüm kayıtlar düz bir metin dosyasına kaydedilecektir.

7.8. Uzman Ayarları

Genellikle varsayılan ayarları kullanmanız ve geçerli bir nedeniniz varsa söz konusu ayarları değiştirmeniz önerilir. Yapılandırma sadece uzman kullanıcılar tarafından değiştirilmelidir!

Anti-Spam yapılandırmasını uzman seviyede değiştirmeniz gerektiğini düşünüyorsanız lütfen kullanıcı arayüzünde belirtilen talimatları izleyin. Genellikle iletişim pencerelerinin her birinde belirli bir özellik bulursunuz ve söz konusu özelliği düzenleyebilirsiniz - ilgili özellik aynı iletişim kutusunda tanımlanır.

- **Önbellek** - parmak izi, etki alanı, LegitRepute
- **Eğitim** - maksimum kelime girişi, otomatik eğitim eşiği, ağırlık
- **Filtreleme** - dil listesi, ülke listesi, onaylanan IP'ler, engellenen IP'ler, engellenen ülkeler, engellenen karakter setleri, sahte göndericiler
- **RBL** - RBL sunucuları, çoklu eşleşme, eşik, zaman aşımı, maksimum IP'ler
- **İnternet bağlantısı** - zaman aşımı, proxy sunucusu, proxy sunucusu kimlik doğrulaması

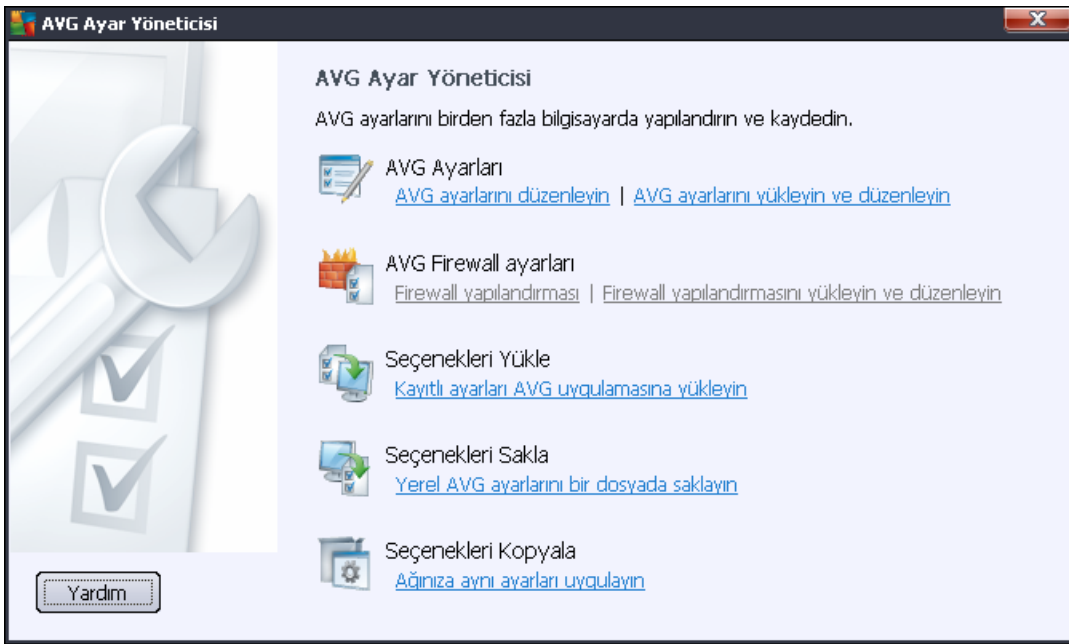


8. AVG Ayarları Yöneticisi

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 2012/AVG Ayar Yöneticisi



• AVG Ayarları

- **AVG Ayarlarını Düzenle** - Yerel AVG'nizin gelişmiş ayarlarını içeren iletişim kutusu açmak için bu bağlantıyı kullanın. Burada yapılan tüm ayarlar yerel AVG yüklemesine de yansıtılır.
- **AVG ayarlarını yükle ve düzenle** - AVG yapılandırma dosyanız (.pck) varsa, düzenlemek üzere açmak için bu düğmeyi kullanın. **Tamam** veya **Uygula** düğmesiyle değişiklikleri onayladıktan sonra, dosya yeni ayarlarla değiştirilir!

• AVG Firewall ayarları

Bu bölüm, yerel AVG yüklemenizin Güvenlik Duvarı ayarlarını değiştirmenize veya önceden hazırlanmış AVG yapılandırma dosyasındaki (.pck) Güvenlik Duvarı ayarlarını düzenlemenize olanak tanır. Ancak, AVG Email Server Edition 2012 ürününüzün Güvenlik Duvarı bileşenini içermemesi durumunda, her iki bağlantı da gri renkte gösterilir ve çalışmaz.

• Seçenekleri Yükle

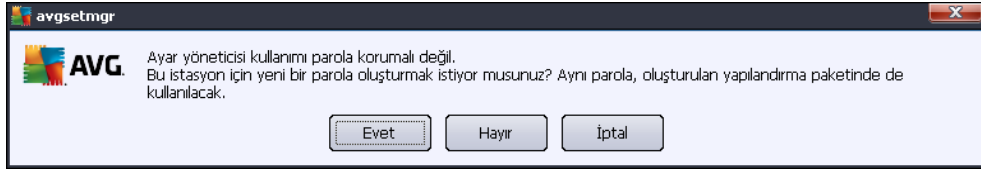
- **AVG'ye kayıtlı ayarları yükle** - AVG yapılandırma dosyasını (.pck) açmak için bu



bağlantıyı kullanın ve yapılandırmayı yerel AVG yüklemenize uygulayın.

- **Seçenekleri Sakla**

- **Yerel AVG ayarlarını dosyada sakla** - Yerel AVG yüklemenizin AVG yapılandırma dosyasını (.pck) kaydetmek için bu bağlantıyı kullanın. İzin Verilen işlemler için bir parola ayarlamadıysanız, aşağıdaki iletişim kutusuyla karşılaşabilirsiniz:



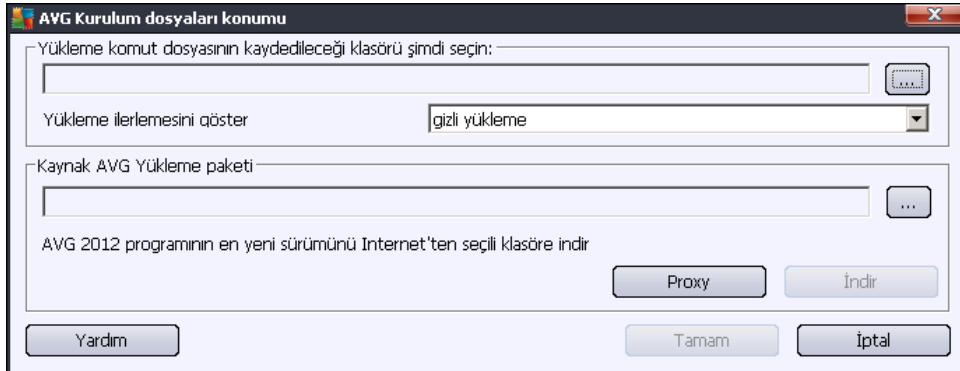
İzin verilen öğelere şimdi erişmek için parola ayarlamak istiyorsanız **Evet** yanıtını verip gerekli bilgileri doldurun ve seçiminizi onaylayın. Parola oluşturmayı atlamak ve yerel AVG yapılandırmasını bir dosyaya kaydetmek için **Hayır** yanıtını seçin.

- **Seçenekleri Kopyala**

- **Aynı ayarları ağa uygula** - Bu bağlantı özel seçeneklere sahip bir yükleme paketi oluşturarak yerel AVG yüklemenizin bir kopyasını almanızı sağlar. Çoğaltma işlemi, şunlar hariç olmak üzere AVG ayarlarının çoğunu içerir:

- ✓ Dil ayarları
- ✓ Ses ayarları
- ✓ Kimlik koruma bileşeninin izin verilenler listesi ve potansiyel olarak istenmeyen programlar istisnaları.

İlerlemek için, önce yükleme komut metninin kaydedileceği klasörü seçin.



Sonra, aşağı açılır menüden aşağıdakilerden birini seçin:

- ✓ **Gizli yükleme** - kurulum işlemi sırasında hiçbir bilgi görüntülenmez.
- ✓ **Yalnızca yükleme ilerlemesini göster** - yükleme kullanıcının dikkat etmesini



gerektirmez, ancak ilerleme tam olarak görülebilir.

- ✓ *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 ya **İndir** düğmesini kullanın ya da AVG yükleme paketini manuel olarak söz konusu klasöre yerleştirin.

Başarılı bir bağlantı için ağınız buna gereksinim duyuyorsa, proxy sunucusu ayarlarını tanımlamak için **Proxy** düğmesini kullanabilirsiniz.

Tamam düğmesini tıklattığınızda çoğaltma işlemi başlar ve kısa bir sürede bitmesi gerekir. Ayrıca İzin verilen öğeler için parola ayarlama hakkında size soru soran bir iletişim kutusuyla da karşılaşabilirsiniz (yukarıya bakın). Bittiğinde, seçili klasörde diğer dosyalarla birlikte **AvgSetup.bat** dosyası bulunmalıdır. **AvgSetup.bat** dosyasını çalıştırırsanız, AVG'yi yukarıda seçilen parametrelere göre yükler.



9. SSS ve Teknik Destek

İşletmenizde ya da teknik açıdan AVG ile herhangi bir sorun yaşarsanız lütfen <http://www.avg.com> adresinde bulunan AVG web sitesinin **SSS** bölümünü inceleyin.

Bu şekilde yardım alamazsanız teknik destek bölümüne e-posta ile başvurun. Lütfen **Yardım/Çevrimiçi yardım** al sistem menüsünden ulaşabileceğiniz iletişim formunu kullanın.