



AVG File Server 2013

Kullanıcı Kılavuzu

Belge revizyonu 2013.01 (20.11.2012)

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.

Bu ürün sıkıştırma kitaplığı libbzip2 kullanır, Telif Hakkı (c) 1996-2002 Julian R. Seward.



İçindekiler

1. Giriş	3
2. AVG Yükleme Gereksinimleri	4
2.1 Desteklenen İşletim Sistemleri	4
2.2 Desteklenen Dosya Sunucuları	4
2.3 Önerilen Donanım Gereksinimleri	4
3. AVG Yükleme Süreci	5
3.1 Yükleme Başlatma	5
3.2 Lisans Sözleşmesi	6
3.3 Lisansınızı Etkinleştirin	6
3.4 Yükleme Türünü Seçin	7
3.5 Özel Yükleme - Özel Seçenekler	8
3.6 Yüklemeyi Tamamlama	9
4. Yüklemeden sonra	10
5. MS SharePoint için Belge Tarayıcı	12
5.1 Genel Bilgiler	12
5.2 Gelişmiş Ayarlar	14
6. SharePoint Portal Server için AVG	17
6.1 Program Bakımı	17
6.2 Virüslerden koruma ayarlarına erişim	17
6.3 Virüslerden koruma yapılandırması	18
7. SSS ve Teknik Destek	22



1. Giriş

Bu kullanıcı el kitabı, **AVG File Server 2013** için kapsamlı dokümantasyon sağlar.

AVG File Server 2013 programını satın aldığınız için tebrik ederiz!

AVG File Server 2013 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 File Server 2013**, 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.

Bu belge özel AVG File Server 2013 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 File Server 2013 aşağıdaki işletim sistemlerine sahip iş istasyonlarını/sunucuları koruma amaçlıdır:

- Windows 2003 Server ve Windows 2003 Server x64 Edition (Service Pack 1)
- Windows 2008 Server ve Windows 2008 Server x64 Edition

(ve belirli işletim sistemleri için daha yeni servis paketleri)

2.2. Desteklenen Dosya Sunucuları

Desteklenen dosya sunucuları:

- MS SharePoint 2003 Server sürümü
- MS SharePoint 2007 Server sürümü
- MS SharePoint 2010 Server sürümü

2.3. Önerilen Donanım Gereksinimleri

AVG File Server 2013 için önerilen donanım gereksinimleri:

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



3. AVG Yükleme Süreci

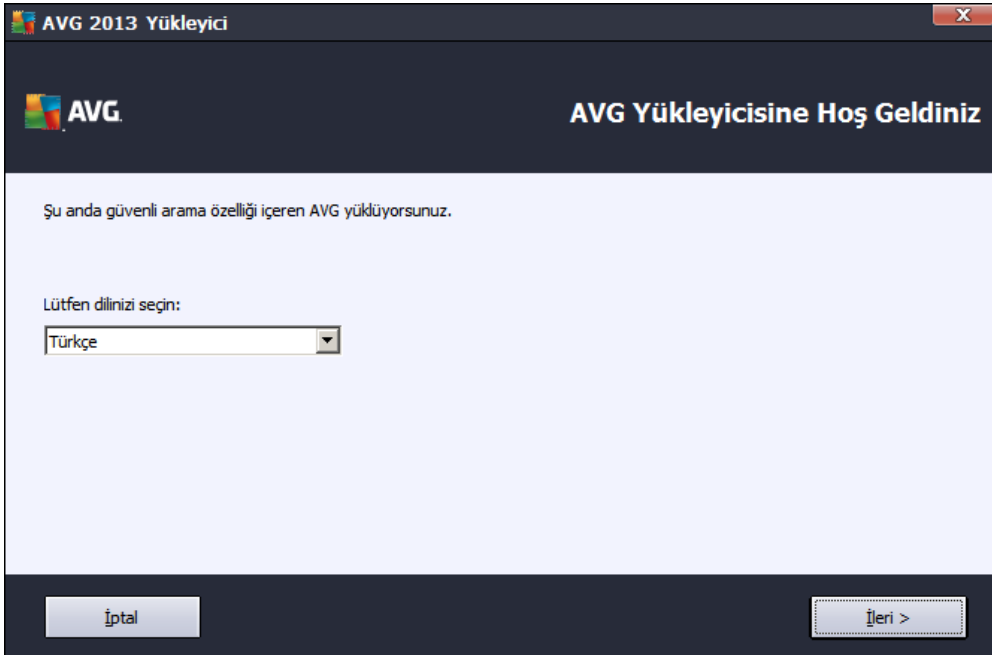
AVG'yi bilgisayarınıza kurmak için en güncel yükleme dosyasına ihtiyacınız vardır. Kutulu versiyonların içinden çıkan CD'de bulunan yükleme dosyasını da kullanabilirsiniz fakat söz konusu dosya güncel olmayabilir. Bu nedenle en güncel kurulum dosyasını çevrimiçi ortamdan indirmenizi öneriyoruz. Dosyayı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

Ürününüz için iki yükleme paketi seçeneği vardır: 32 bit işletim sistemleri için (x86 olarak belirtilir) ve 64 bit 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

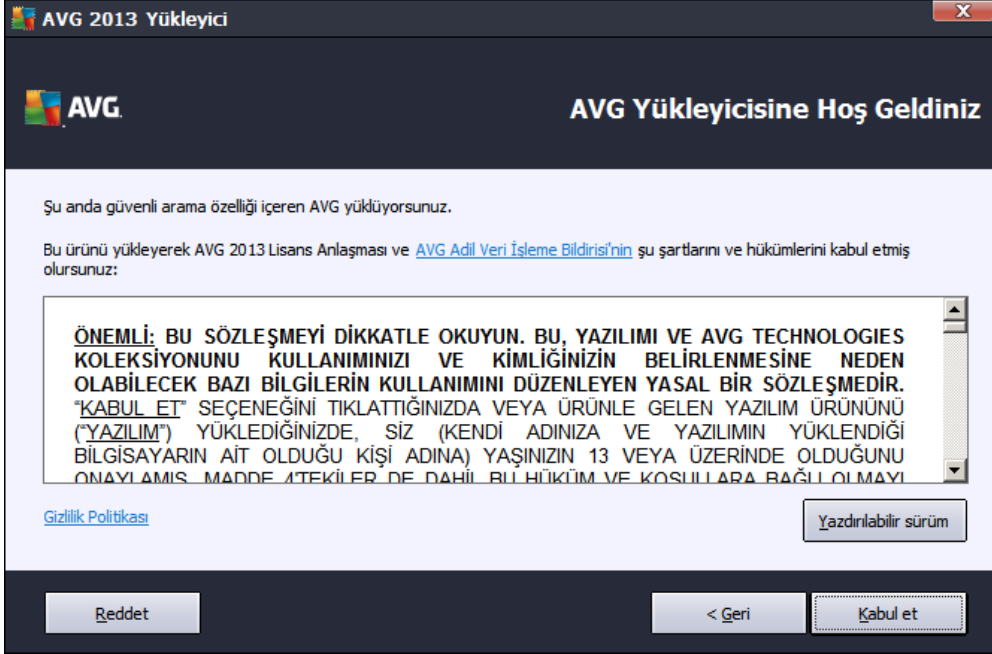


Yükleme işlemi **Hoş geldiniz** penceresiyle başlar. Burada yükleme için kullanılan dili seçer ve **İleri** düğmesini tıklarınız.

Daha sonra yükleme işlemi sırasında uygulama arayüzü için ek dilleri de seçebilirsiniz.



3.2. Lisans Sözleşmesi



Bu iletişim kutusu lisans koşullarını okumanıza olanak verir. Lisans metnini yeni bir pencerede açmak için **yazdırılabilir sürüm** düğmesini kullanın. Onaylamak ve bir sonraki iletişim kutusuna geçmek için **Kabul Ediyorum** düğmesine basın.

3.3. 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-postası ile gönderilecektir. Sayıları gösterildiği gibi girmelisiniz. Lisans numarasının dijital formu mevcut ise (e-postada) lisans numarasını girmek için kopyala ve yapıştır yönteminin kullanılması önerilmektedir.



AVG 2013 Yükleyici

AVG Lisansınızı Etkinleştirin

Lisans Numarası:

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

AVG 2013 yazılımınızı çevrimiçi satın aldıysanız, lisans numaranız e-posta ile gönderilmiştir. Yanlış yazmayı önlemek için numarayı 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.

3.4. Yükleme Türünü Seçin

AVG 2013 Yükleyici

AVG File Server Edition Yükleme türünü seçin

Ekspres Yükleme (önerilir)
Yazılımı standart yapılandırmasında yükler.

Özel Yükleme
Hangi uygulama özelliklerini yüklemek istediğinizi seçin. Gelişmiş kullanıcılar için önerilen seçim.

İptal < Geri İleri >

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

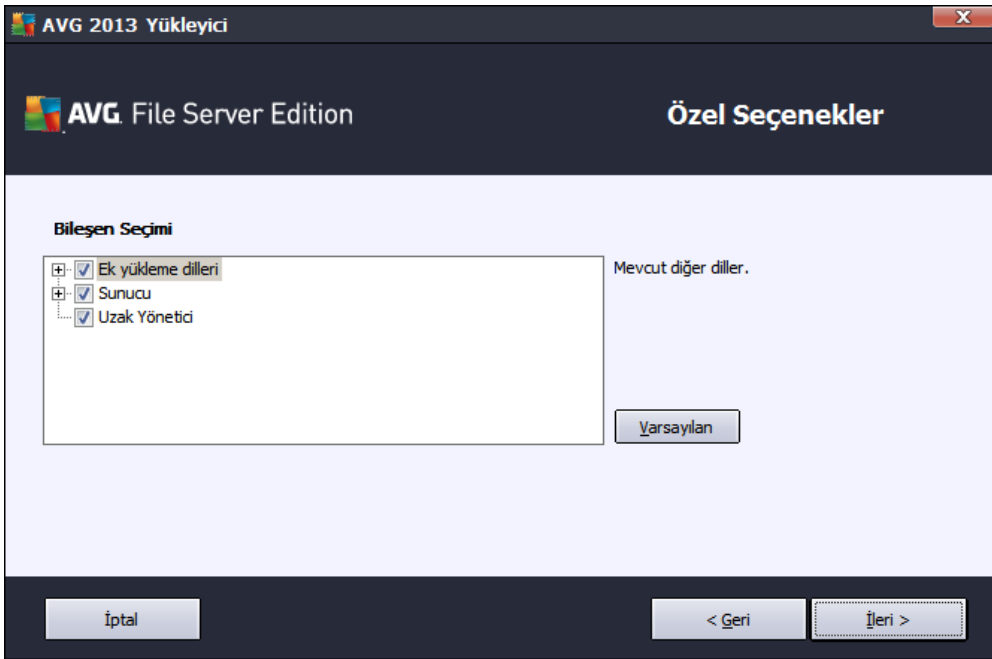
Kullanıcıların çoğu için AVG'yi program geliştiricisi tarafından önceden tanımlanmış ayarlarla tam otomatik modda yükleyen **Ekspres Yükleme** önerilmektedir. Bu yapılandırma, minimum kaynak kullanımı ile maksimum güvenliği bir araya getirir. Gelecekte söz konusu yapılandırmayı değiştirme ihtiyacı duyarsanız söz konusu işlemi doğrudan AVG uygulamasından yapabileceksiniz.



Özel Yükleme, AVG'yi standart olmayan ayarlarla yüklemek için geçerli bir nedeni olan deneyimli kullanıcılar tarafından kullanılmalıdır. Örn. belirli sistem gereksinimlerini karşılamak için.

Özel Yükleme seçildiğinde iletişim kutusunun alt bölümünde **Hedef klasör** kısmı görüntülenir. Burada AVG'nin yükleneceği konumu belirleyebilirsiniz. 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.

3.5. Özel Yükleme - Özel Seçenekler



Bileşen Seçimi bölümünde, yüklenebilecek tüm AVG bileşenlerinin genel bilgileri 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!

- **Uzaktan Yönetim** - AVG'yi bir AVG DataCenter'a (AVG Ağ Sürümleri) bağlamayı düşünüyorsanız bu seçeneği seçmeniz gerekir.
- **Ek yükleme dilleri** - AVG'de hangi dillerin yüklenmesi gerektiğini tanımlayabilirsiniz. **Ek yükleme dilleri** öğesini işaretleyin ve sonra ilgili menüden istediğiniz dilleri seçin.
- **Sunucu** - bu AVG sürümünde yalnızca **MS SharePoint için Belge Tarayıcı** sunucu bileşeni mevcuttur. MS SharePoint'te depolanan tüm belgeleri tarar ve tespit edilen tüm virüsleri siler.

İleri düğmesine basarak devam edin.



3.6. Yükleme Tamamlama

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

AVG 2013 Yükleyici

AVG File Server Edition **Tebrikler!**

AVG 2013 başarıyla yüklendi.

AVG Veri Merkezi belirtimi:

AVG [Gizlilik Politikası](#) politikasına uygun olarak AVG [ürün geliştirme programı](#) programına katılarak güvenliğimi geliştirmek istiyorum

Bitir

Bu iletişim kutusu yoluyla genel internet güvenliğini artırmak için tespit edilen tehditler hakkında anonim olarak bilgi toplayan Ürün Geliştirme Programı'na katılıp katılmamaya da karar verebilirsiniz. Bu bildirim kabul ediyorsanız lütfen **AVG Gizlilik Politikası'na uygun olarak AVG Ürün Geliştirme Programı'na katılarak güvenliğimi geliştirmek istiyorum** seçeneğini işaretli bırakın (*seçenek varsayılan olarak onaylanmıştır*).

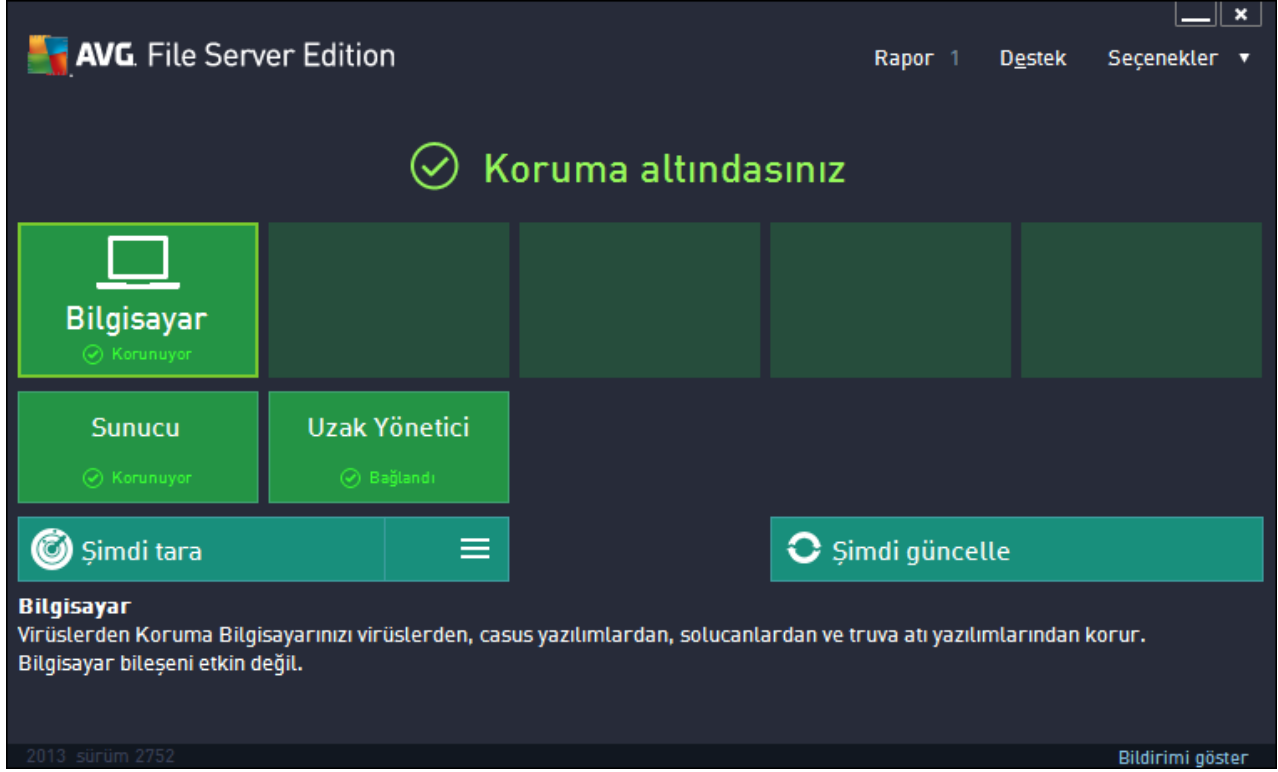
Bitir düğmesine basarak seçimlerinizi onaylayın.

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

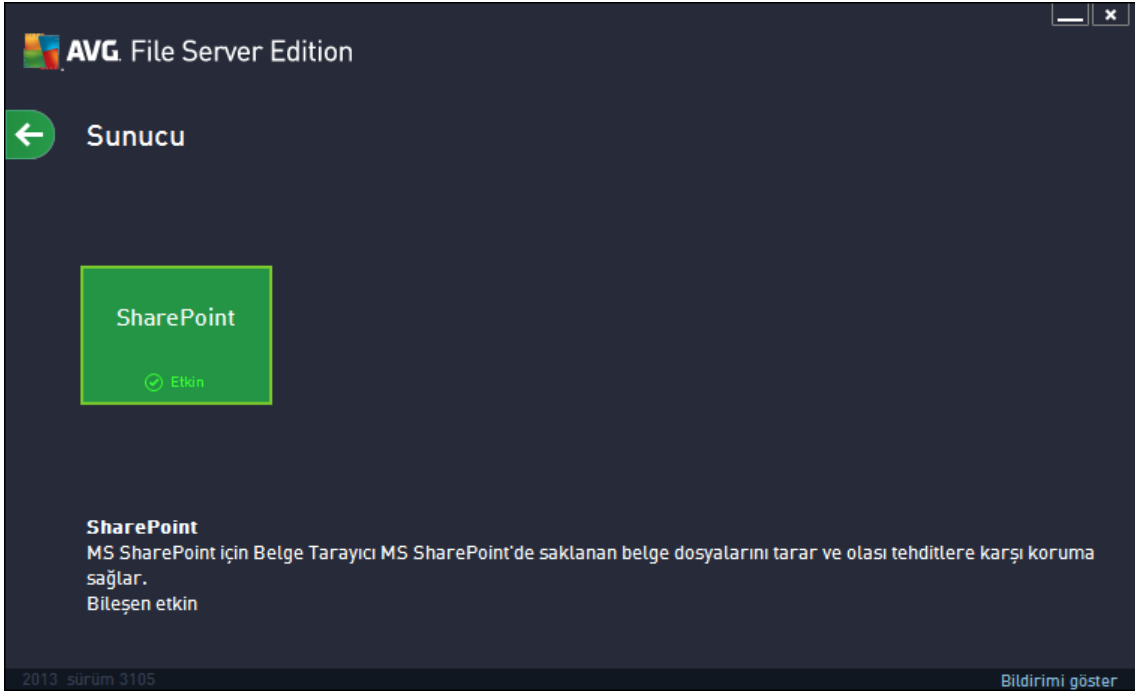


4. Yüklemeden sonra

Yükleme tamamlandıktan hemen sonra **AVG File Server 2013** ana ekranı görünür:



Bu kılavuzda yalnızca **AVG File Server 2013** ürününe özgü özellikler yer almaktadır; diğer tüm bileşenler ve ayarlar AVG Masaüstü kılavuzunda açıklanmaktadır. Ana sunucu bileşenleri iletişim kutusuna erişmek için **Sunucu** düğmesini tıklayın. Aşağıdaki ekranı görürsünüz:



Dosya sunucunuz için korumayı bağımsız olarak ayarlamak için ilgili bölümü izleyin:

- [MS SharePoint için Belge Tarayıcı](#)
- [SharePoint Portal Server için AVG](#)

5. MS SharePoint için Belge Tarayıcı

5.1. Genel Bilgiler

MS SharePoint Server 2003/2007/2010 için AVG yapılandırma seçenekleri, sunucu bileşenleri ekranı yoluyla AVG File Server 2013 içine tamamen entegre edilmiştir.



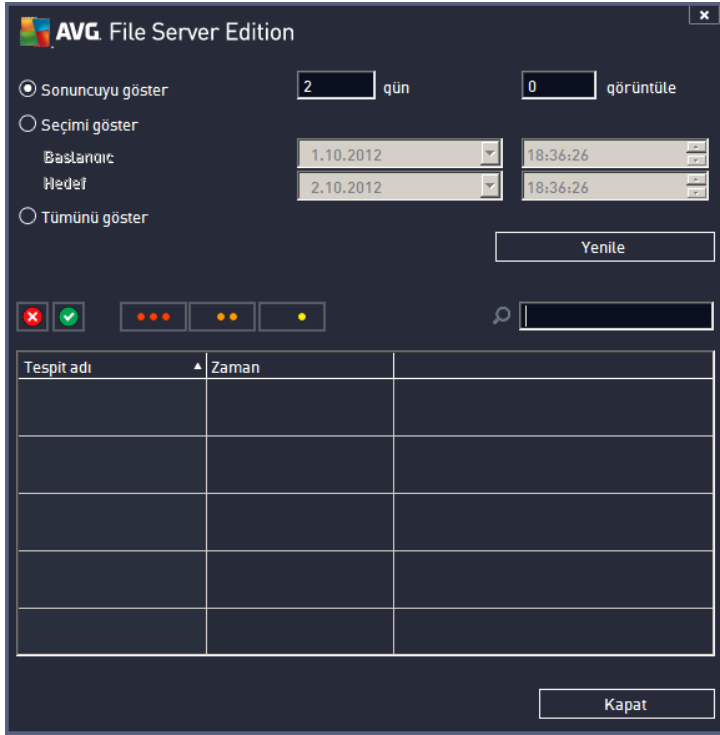
MS SharePoint için Belge Tarayıcı sunucu bileşenin amacı (bu AVG sürümündeki tek bileşendir) MS SharePoint'te depolanan belgelerin taranmasıdır. Herhangi bir virüs algılanırsa, Virüs Kasası'na taşınır veya tamamen kaldırılır.

Microsoft SharePoint, gelişen bileşen 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.

Genel arayüz bilgileri:

- **Tarama Sonuçları**

Tarama sonuçlarını inceleyebileceğiniz yeni bir iletişim kutusu açar:



AVG File Server Edition

Sonuncuyu göster 2 gün 0 görüntü

Seçimi göster

Başlangıç: 1.10.2012 18:36:26

Hedef: 2.10.2012 18:36:26

Tümünü göster

Yenile

Tespit adı	Zaman	

Kapat

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

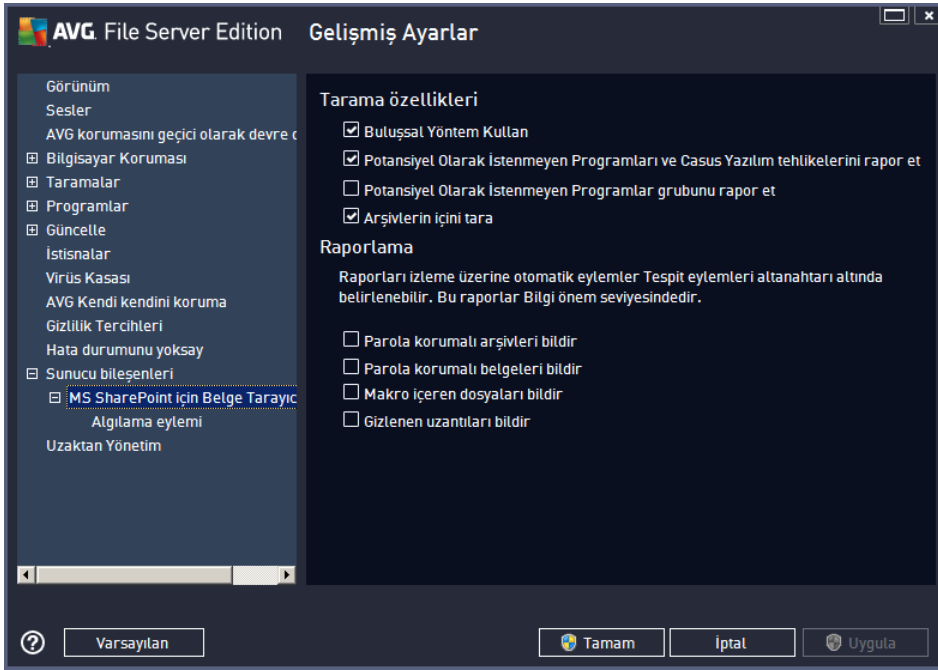
Ayarlar çalışma düğmesi tıklatıldığında seçilen bileşenin gelişmiş ayarları açılır (aşağıdaki bölümlerde tüm bileşenlerin ayarları hakkında daha fazla bilgi bulabilirsiniz).

5.2. Gelişmiş Ayarlar

5.2.1. Genel ayarlar

MS SharePoint için Belge Tarayıcı ayarlarını açmak için, bileşenin arayüzünden **Ayarlar** düğmesini seçin.

Sunucu bileşenleri listesinden **MS SharePoint için Belge Tarayıcı** öğesini seçin:



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

Raporlama bölümü tarama sırasında hangi öğelerin raporlanması gerektiğini seçmenize izin verir. Bu, **Algılama eylemleri** bölümü, **Bilgi** kısmında (aşağıya bakın) kolaylıkla değiştirilebilen varsayılan

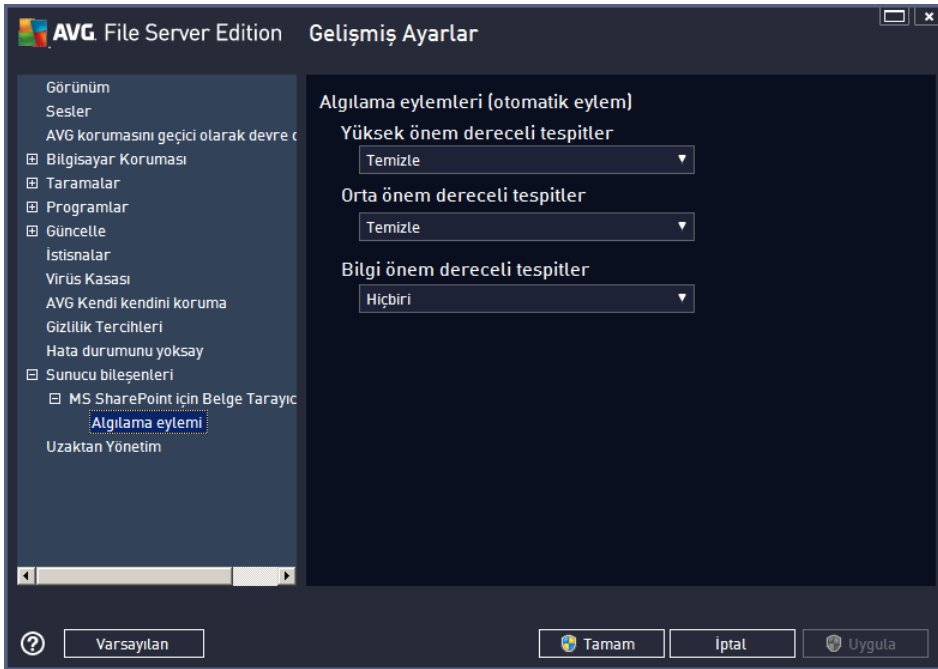
yapılandırma yapılmamıştır.

Aşağıdaki seçenekler mevcuttur:

- **Parola korumalı arşivleri bildir** - parolayla korunan arşivlerin (ZIP, RAR vb.) virüs için taranması mümkün değildir; bunların potansiyel olarak tehlikeli olduklarını bildirmek için kutuyu işaretleyin.
- **Parola korumalı belgeleri bildir** - parolayla korunan belgelerin virüs için taranması mümkün değildir; bunların potansiyel olarak tehlikeli olduklarını bildirmek 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. Makro içeren dosyaların şüpheli olarak bildirilmesini sağlamak için kutuyu işaretleyebilirsiniz.
- **Gizlenen uzantıları bildir** - gizli uzantılar şüpheli bir çalıştırılabilir dosyayı (örn. "birşey.txt.exe") zararsız bir düz metin dosyası gibi (örn. "birşey.txt") gösterebilir; bunları potansiyel olarak tehlikeli olarak bildirmek için kutuyu işaretleyin.

Ayrıca aşağıdaki ağaç yapısında [Algılama eylemleri](#) alt öğesi mevcuttur (aşağıdaki bölüme bakın).

5.2.2. Algılama eylemi



Bu iletişim kutusunda, **MS SharePoint için Belge Tarayıcı** bileşenin bir tehlike tespit ettiğinde nasıl davranması gerektiğini yapılandırabilirsiniz. Tehditler üç kategoriye ayrılır:

- **Yüksek önem dereceli tehditler** - Kendilerini kopyalayan ve yayan zararlı kodlar zarar verene kadar genellikle anlaşılmaz.
- **Orta önem dereceli tehditler** - bu tür programlar genellikle gizliliğinizi tehdit eden ciddi tehlikelerden yalnızca potansiyel tehlikelere kadar çok çeşitli olabilir.



- **Bilgi önem dereceli tehditler** - algılanan ancak yukarıdaki kategorilerin hiçbirinde yer almayan tüm potansiyel tehditleri içerir.

Her biri için otomatik bir işlem seçmek üzere aşağı açılır menüleri kullanın:

- **Hiçbiri** - bu tür bir tehdit içeren bir belge yalnız bırakılacaktır.
- **Temizle** - bulaşmış dosyayı/belgeyi temizlemeye çalışır.
- **Kasaya Taşı** - virüs bulaşmış olan her belge Virüs Kasası karantina ortamına taşınacaktır.
- **Kaldır** - virüsün algılandığı her belge silinecektir.



6. SharePoint Portal Server için AVG

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

6.1. Program Bakımı

SharePoint Portal Server için AVG, sunucunuzun olası virüs bulaşmalarına 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 veritabanı (*SharePoint Portal Sunucusunun yanı sıra*) web tabanlıdır ve Windows **Başlat** menüsünün **Programlar/Microsoft Office Sunucusu** klasöründen **SharePoint merkezi Yönetim** seçeneğini kullanarak (*SharePoint Portal Sunucusunun* sürümüne de bağlıdır) veya **Yönetimsel Araçlar** öğesine gidip **Sharepoint Merkezi Yönetim** seçeneğini belirleyerek açabilirsiniz.

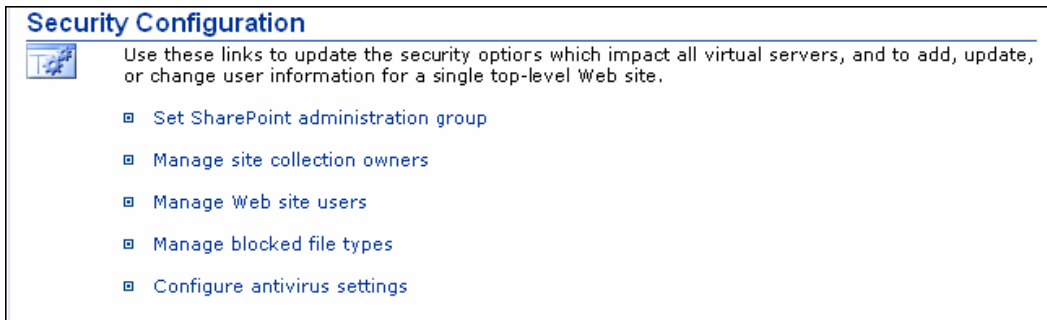
Uygun erişim haklarını ve URL'yi kullanarak da **SharePoint Portal Sunucusu Merkezi Yönetim** web sayfasına ulaşabilirsiniz.

6.2. Virüslerden koruma ayarlarına erişim

SharePoint Portal Server Central Administration arayüzünde, **SharePoint Portal Server için AVG** tarayıcısının performans parametrelerini ve eylemlerini kolayca yapılandırabilirsiniz. Ancak, virüslerden koruma ayarları tüm desteklenen SharePoint sürümleriyle aynı olmasına rağmen, yapılandırma iletişim kutusuna erişim yolu her birinde biraz farklılık gösterir. Lütfen aşağıdaki kısa genel bilgilerde sürümünüzü bulun:

MS SharePoint 2003 Server

Merkezi Yönetim ana ekranında **İşlemler**'i seçin. Yeni bir iletişim kutusu görünecektir. Şimdi, **Virüslerden Koruma Ayarlarını Yapılandır** öğesini seçerek (**Güvenlik Yapılandırması** bölümünde, aşağıdaki ekran resmine bakın) **Virüslerden Koruma Ayarları** iletişim kutusunu açın.



MS SharePoint 2007 Server

Merkezi Yönetim ana ekranında **İşlemler**'i seçin. Yeni bir iletişim kutusu görünecektir. Şimdi, **Virüslerden**



Koruma ögesini seçerek (**Güvenlik Yapılandırması** bölümünde, aşağıdaki ekran resmine bakın) [Virüslerden Koruma](#) iletişim kutusunu açın.

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

MS SharePoint 2010 Server

Merkezi Yönetim ana ekranında **Güvenlik**'i seçin. Yeni bir iletişim kutusu görünecektir:

The screenshot shows the Microsoft SharePoint 2010 Central Administration interface. The breadcrumb path is "SharePoint 2010 Central Administration > Security". The left navigation pane includes "Central Administration", "Application Management", "System Settings", "Monitoring", "Backup and Restore", "Security" (highlighted), "Upgrade and Migration", "General Application Settings", and "Configuration Wizards". The main content area is divided into three sections: "Users" (Manage the farm administrators group, Approve or reject distribution groups, Specify web application user policy), "General Security" (Configure managed accounts, Configure service accounts, Configure password change settings, Specify authentication providers, Manage trust, Manage antivirus settings, Define blocked file types, Manage web part security, Configure self-service site creation), and "Information policy" (Configure information rights management, Configure Information Management Policy).

Virüslerden koruma ayarlarını yönet ögesini seçerek (**Genel Güvenlik** bölümünde) [Virüslerden Koruma](#) iletişim kutusunu açın.

6.3. Virüslerden koruma yapılandırması

Aşağıdaki genel bilgilerde Virüslerden Koruma (veya Virüslerden Koruma Ayarları) iletişim kutusunun farklı SharePoint sürümlerinde nasıl görüldüğü gösterilmektedir:

MS SharePoint 2003 Server



Windows SharePoint Services

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



MS SharePoint 2007 Server

Central Administration > Operations > Antivirus

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

MS SharePoint 2010 Server

Central Administration > 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.](#)

Central Administration

- Application Management
- System Settings
- Monitoring
- Backup and Restore
- Security
- Upgrade and Migration
- General Application Settings
- Configuration Wizards

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:

Yapılandırma seçenekleri, görünümünden bağımsız olarak desteklenen tüm SharePoint sürümlerinde tamamen aynıdır:

- **Yüklemede belgeleri tara** - belgelerin yüklenirken taranmasını etkinleştirin/devre dışı bırakın
 - **İndirmede belgeleri tara** - belgelerin indirilirken taranmasını etkinleştirin/devre dışı bırakın
 - **Kullanıcıların bulaşmış belgeleri indirmesine izin ver** - kullanıcıların bulaşmış belgeleri indirmesine izin verin/yasaklayın
 - **Bulaşmış belgeleri temizlemeye çalış** - virüslü belgelerin otomatik olarak silinmesini etkinleştirin/devre dışı bırakın (mümkünse)
-
- **Zaman aşımı süresi (saniye cinsinden)** - tek bir başlatmadan sonra virüs tarama sürecinin çalışacağı maksimum saniye sayısı (belgeler taranırken sunucunun yanıtı yavaş görünüyorsa değeri azaltın)
-
- **İş parçacığı sayısı** - aynı anda çalıştırılabilen virüs tarama iş parçacığı sayısını belirtebilirsiniz. Sayıyı artırmak aynı anda çalışan tarama sayısını artıracığı için taramayı hızlandırabilir, ancak öte yandan sunucunun yanıt süresini artırabilir



7. 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.