www.comodo.com

COMODO

Creating Trust Online™

Comodo İnternet Güvenliği 2011

Sürüm 5.0

Kullanıcı Rehberi

Comodo Security Solutions Inc.
525 Washington Bvld,
Jersey City, NJ 07310
United States

İçindekiler

1 Comodo İnternet Güvenliği'ne Giriş

Tanıtım

Comodo İnternet Güvenliği 2011 içeriden ve dışarıdan gelebilecek tehditlere karşı güçlü Antivirüs koruması, kurumsal seviyedeki güvenlik duvarı ve Savunma+ adındaki izinsiz saldırıları önleme sistemi ile tam koruma sağlar.

CIS Premium, Pro ve Complete olarak farklı baskıları vardır ve bunlarda ücretsiz sürümde bulunan çekirdek korumanın yanı sıra ek hizmetler de sunulmaktadır. Bu hizmetler LivePCSupport (Uzmanlar tarafından uzaktan bağlanılarak sistem onarımı); TrustConnect (Kablosuz açık ağlarda veri güvenliği); Online Backup (10GB çevrimiçi depolama alanı) ve Comodo Garanti (Sisteminiz zararlı saldırısı sonucu zarar görürse ve Comodo uzmanları bu hasarı düzeltip sisteminizi çalışır duruma getiremezlerse Comodo sisteminizin düzeltilmesi için gerekli maliyeti karşılayacaktır. Ayrıntılar için Şartlar ve Koşullara bakınız. Yalnızca ABD'de ikamet edenler içindir).

CIS 2011'deki yeni özellikler Bulut tabanlı antivirüs taramasını ve davranış analizini, kullanıcı dostu uygulama beyaz listesini, yeni casus yazılımı tarayıcısını ve geliştirilmiş kötücül yazılım temizliğini, oyun kipini, geliştirilmiş Savunma+ uygulama uyumluluğunu ve yeniden tasarlanmış arayüzü içermektedir.

Her bir ürün ayrı ayrı kullanıldığı zaman kendine özgü tehditlere karşı üst seviyede koruma sağlar. Beraber takım olarak kullanıldığı zaman ise bilgisayarınız için tam 'önleme, saptama ve iyileştirme' güvenlik sistemi sağlar.

Comodo İnternet Güvenliği Özellikleri:

- **Antivirüs –** Virüsleri, Solucanları ve Truva atlarını otomatik olarak bulan ve yok eden proaktif antivirüs sistemi.
- **Güvenlik Duvarı –** Sisteminizi gelen ve giden saldırılara karşı sürekli koruyan ve oldukça etkili paket süzen güvenlik duvarı.
- **Savunma+ -** Kural tabanlı saldırı önleme sistemi ile önemli işletim sistemi dosyalarınızı kötü niyetli işlemlerden korur, iç saldırıları ve bilinmeyen kötücül yazılımların kurulumunu engeller. Savunma+ şimdi ise bilinmeyen uygulamaları otomatik olarak Sandbox içinde çalıştırma özelliğini sunuyor. Sandbox, güvenilmeyen (zararsız) uygulamaların özgürce çalışmasını sağlarken güvenilmeyen (gerçek zararlıları) uygulamaların da bilgisayarınıza erişmesini ve bilgisayarınıza bulaşmasını engeller.
- **Live PC Support *(Yalnızca Pro ve Complete sürümler)*** - 24 x 7 çevrimiçi destek hizmeti ile ihtiyaç duyduğunuzda Comodo uzmanları uzaktan bilgisayarınıza erişerek aşağıdaki hizmetleri sağlarlar:

  Virüs Teşhisi / Temizliği;
  PC Ayarlama;
  İnternet Giriş Koruması;
  Eposta Hesap Ayarlaması;
  Yazılım Kurulumu;
  Yazıcı Kurulumu / Sorun Çözümü;
  Bilgisayarınızın güç seçeneklerini en uygun duruma getirme;
  Bilgisayar Sorunu Çözümü.

- **Secure Wireless Internet Connectivity (Yalnızca *Pro ve Complete sürümler*) -** TrustConnect halka açık kablosuz bağlantı noktalarından güvenli gezinti sağlar (10 GB aylık).
- **Comodo Guarantee (Yalnızca *Pro ve Complete sürümler*) –** Eğer sisteminiz zararlı saldırısı sonucu zarar görürse ve Comodo uzmanları bu hasarı düzeltip sisteminizi çalışır duruma getiremezlerse Comodo sisteminizin düzeltilmesi için gerekli maliyeti karşılayacaktır. Ayrıntılar için Şartlar ve Koşullara bakınız. Yalnızca ABD'de ikamet edenler içindir.
- **Online BackUp *(Yalnızca Complete sürümü)* -** Verilerinizi Comodo'nun güvenli sunucularına yedekleyebilirsiniz. Veriler şifrelenir ve verilere internet bağlantısı olan herhangi bir bilgisayardan yalnızca kullanıcı tarafından erişilebilir (10GB yedek alanı).

Comodo İnternet Güvenliği ek bir ayar gerektirmeden rahatlıkla acemi kullanıcılar tarafından da kullanılabilir.

Comodo İnternet Güvenliği kötücül yazılımların olası saldırı girişimlerinde veya sisteminize erişilmek istendiğinde uyarı gösterir. Uyarılar açılır pencere şeklindedir ve ekranın sağ alt köşesinde açılarak tanınmayan etkinliklere, işlemlere ve çalışan uygulamaların bağlantı girişimlerine (CIS artık tampon taşması saldırılarına karşı da koruma sağlıyor) izin vermenize veya engellemenize olanak sağlar.

Rehber Yapısı

Bu tanıtım Comodo İnternet Güvenliği'nin temellerini anlatmak için hazırlanmıştır ve tüm kullanıcıların ilgisini çekecektir.

•Giriş

•Özellikler

•Sistem Gereksinimleri

•Kurulum

•CIS Premium - Kurulum

•CIS Pro – Kurulum ve Etkinleştirme

•CIS Complete - Kurulum ve Etkinleştirme

•Comodo İnternet Güvenliği'nin Başlatılması

•Genel Gezinti

•Uyarıların Anlaşılması

Bu rehberin sonraki dört bölümü Comodo İnternet Güvenliği'nin her açıdan yapılandırılmasını kapsar. Son iki bölümü ise Live PC Support ve TrustConnect yapılandırılmasını ve teknik yardımını içerir.

•**Antivirüs Görev Merkezi**

•Bir Tarama Çalıştır

•Virüs Veritabanını Güncelle

•Karantinaya Alınmış Öğeler

•Antivirüs Olaylarını Göster

- Dosyaları Gönder
- Zamanlanmış Tarama
- Tarama Profilleri
- Tarayıcı Ayarları
- Gerçek Zamanlı Tarama
- Elle Taramam
- Zamanlanmış Tarama
- Hariç tutulanlar
- **Güvenlik Duvarı Görev Merkezi**
- Görev Arayüzünün Tanıtımı
- Güvenlik Duvarı Olaylarını Göster
- Yeni Güvenilen Uygulama Tanımla
- Yeni Engelli Uygulama Tanımla
- Ağ Güvenlik İlkeleri
- Genel Gezinti
- Uygulama Kuralları
- Genel Kurallar
- Öntanımlı İlkeler
- Ağ Bölgeleri
- Engellenmiş Bölgeler
- Port Setleri
- Etkin Bağlantıları Göster
- Port Gizleme Sihirbazı
- Güvenlik Duvarı Davranış Ayarları
- Genel Ayarlar
- Uyarı Ayarları
- Gelişmiş Ayarlar
- **Savunma+ Görev Merkezi**
- Görev Arayüzünün Tanıtımı
- Sandbox - Tanıtım
- Savunma+ Olaylarını Göster
- Güvenilir Dosyalar

- Tanınmayan Dosyalar
- Tanınmayan Dosyalar
- Gönderilmiş Dosyalar
- Bilgisayar Güvenlik İlkesi
- Bilgisayar Güvenlik İlkesi
- Öntanımlı İlkeler
- Her zaman Sandbox içinde Çalıştır
- Engellenmiş Dosyalar
- Korunan Dosyalar ve Klasörler
- Korunan Kayıt Defteri Anahtarları
- Korunan COM Bileşenleri
- Güvenilir Yazılım Sağlayıcıları
- Etkin İşlemler Listesini Göster
- Sandbox içinde Program Çalıştır
- Savunma+ Ayarları
- Genel Ayarlar
- Yürütme Denetimi Ayarları
- Sandbox Ayarları
- İzleyici Ayarları
- **Daha... Seçenekler**
- Tercihler
- Genel Ayarlar
- Dil Ayarları
- Ebeveyn Denetimi Ayarları
- Temalar
- Bağlantı Ayarları
- Güncelleme Ayarları
- Yapılandırmalarımı Yönet
- Hata Tanılayıcı
- Güncellemeleri Denetle
- Destek Forumlarına Göz At
- Yardım

1.1 Özellikler

Savunma+ Ana Makina Saldırı Önleme Sistemi

- **Sistemi rootkitlere, işlemler arası bellek enjeksiyonlarına (akıtma), tuş kaydedicilere ve daha birçok zararlı türüne karşı korur;**
- **Her programı bütünlüğünü bilgisayarın belleğine yüklenmeden önce doğrular;**
- **Anlık olarak kötücül yazılımların tespiti için Bulut Tabanlı Davranış Analizi gerçekleştirir;**
- **Bilinmeyen ve güvenilmeyen her uygulamanın çalışması veya kurulması girişimlerinde uyarı gösterir;**
- **Virüsleri, Truva Atlarını ve Casus Yazılımları sisteme bulaşmadan önce engeller;**
- **İşletim sisteminin önemli dosyalarında ve kayıt anahtarı girdilerinde yapılacak izinsiz değişiklikleri önler;**
- **Yeni Sandbox özelliği ile güvenilmeyen dosyaları sistemden izole eder**

Gelişmiş Ağ Güvenlik Duvarı Motoru

Comodo İnternet Güvenliği'nin Güvenlik Duvarı bileşeni içten ve dıştan gelen tehditlere karşı üst düzey güvenlik sunar. Böylece bilgisayar korsanlarına, kötücül yazılımlara ve bilgi hırsızlarına karşı güçlü bir koruma sağlar. Şimdi bu korumayı da yeni özellikler ekleyerek geliştirdik,

- **Port Gizleme özelliği ile fırsatçı port taramalarına karşı bilgisayarınızı tamamen görünmez yapabilirsiniz;**
- **Sihirbaz tabanlı otomatik saptanan güvenli bölgeler;**
- **Öntanımlı Güvenlik İlkeleri ile güvenlik kuralları hızlıcana oluşturabilirsiniz;**
- **Hata tanılayıcı ile sisteminizi olası çakışmalara ve daha birçok şeye göre analiz edebilirsiniz.**

Kapsamlı Antivirüs Koruması

- **Virüsleri saptar ve bilgisayarlarınızdan temizler;**
- **Bulut tabanlı Antivirüs Taraması gerçekleştirir;**
- **Sezgisel teknikler kullanarak bilinmeyen zararlıları tespit eder;**
- **Windows Kayıt Defterini ve Sistem Dosyalarını da olası casus yazılım bulaşmalarına karşı tarar ve onları temizler;**
- **Sürekli olarak gerçek zamanlı korur;**
- **Yapılandırılabilir Elle taraması ile herhangi bir dosyayı, klasörü veya sürücüyü anında denetlemenize izin verir;**
- **Windows işletim sistemine benzersiz bütünleşmesiyle belirli nesneleri anında taramanıza izin verir;**
- **Günlük, otomatik olarak virüs veritabanı tanımlarını günceller;**
- **Şüpheli dosyaları karantinaya alarak izole eder ve ilerideki bulaşmaları önler;**
- **Dahili zamanlayıcısı ile istediğiniz zaman ihtiyacınıza göre taramanıza izin verir;**
- **Kolay kullanımı – kur ve unut – ile arkaplanda sisteminiz korur.**

Grafiksel Kullanıcı Arayüzü

- **Özet ekranı ile bir bakışta güvenlik ayarlarınızı görebilirsiniz;**
- **Güvenlik Duvarı, Antivirüs ve Savunma+ bileşenleri arasında kolayca ve hızlıca gezebilirsiniz;**
- **Karışık olmayan seç ve tıkla yapılandırması;**
- **Yeniden tasarlanmış güvenlik kuralları arayüzü ile genel veya işlem başına erişim haklarını ve yetkilerini hızlıcana ayarlayabilirsiniz. Güvenlik Duvarı'nın içerdiği öntanımlı ilkeler ve sihirbazlar ile işlemler için kolaylıkla kurallar oluşturabilirsiniz.**

Live PC Support (Yalnızca Pro ve Complete sürümler)

Comodo İnternet Güvenliği, Pro ve Complete müşterileri LivePCSupport desteği alırlar. Destek hizmetleri Comodo güvenlik uzmanlarınca sisteminize uzaktan erişilerek verilir. Bilgisayarınızdaki sorunları çözerler. Bu hizmetler:

- **Virüs Teşhisi / Temizlenmesi**
- **PC Ayarları**
- **İnternet Giriş Koruması**
- **Eposta Hesabı Ayarlanması**
- **Yazılım Kurulumu**
- **Yazıcı Ayarlanması / Sorunu Çözümü**
- **Yeşil PC (güç ayarlamaları)**
- **Bilgisayar Sorunu Çözümü**

Lütfen tam ürün ayrıntıları için http://livepcsupport.com ziyaret ediniz. Lütfen CIS Pro paketine abone olmak için http://personalfirewall.comodo.com sayfasını ziyaret ediniz.

Comodo TrustConnect (Yalnızca Pro ve Complete sürümler)

Pro veya Complete aboneliklerine dahildir, Comodo TrustConnect webde sörfünüzü güvenli hale getiren hızlı, güvenli bir İnternet vekil sunucu hizmetidir -

- **Kafelerde, Otellerde ve Havaalanlarında;**
- **Diğer halka açık kablosuz noktalarda;**
- **Evde;**
- **İç ağlarına erişimde güvenlik gerektiren, uzaktan işçi çalıştıran Kurumlar için**

Comodo İnternet Güvenliği – Genişletilmiş Özellikler

Yapılandırılabilir Güvenlik Kuralları Arayüzü

Comodo İnternet Güvenliği öncekine göre daha fazla güvenlik seçeneği sunar. Kolay anlaşılabilir GKA ile genel ve uygulama başına erişim hakları ve yetkileri hızlıcana ayarlanabilir. Öntanımlı güvenlik ilkeleri ile birkaç tıklamayla güvenlik duvarı kuralları oluşturabilirsiniz.

Uygulama Davranış Analizi

Comodo İnternet Güvenliği protokol seviyesinde koruma özelliği ile kendi protokol sürücülerini kullanan zararlılara karşı da koruma sağlar.

Bulut Tabanlı Davranış Analizi

Comodo İnternet Güvenliği'nde bilinmeyen dosyaların bulut tabanlı analizi özelliği bulunur. Tanınmayan ve Comodo'nun beyaz listesinde bulunmayan dosyalar Comodo Anında Kötücül Yazılım Analizi (CIMA) sunucularına yollanarak davranış analizinden geçer. Her bir dosya Comodo sunucularındaki sanal ortamda çalıştırılır ve kötü niyetli kodlar içerip içermediğine bakılır. Sonuçlar bilgisayarınıza kısa sürede (15 dk) geri yollanır.

Olay günlükleyici

Comodo İnternet Güvenliği geliştirilmiş günlük yöneticisi bileşeni özelliğini bulundurur. Antivirüs, Güvenlik Duvarı ve

Savunma+ etkinliklerini kullanıcı tanımlı süzgeçler aracılığıyla görebilir ve dosyaya aktarabilirsiniz. Acemiler ve tecrübeli kullanıcılar bu özellikten oldukça yararlanabilirler.

Bellek Güvenlik Duvarı Bütünleştirmesi

Comodo İnternet Güvenliği, Comodo Memory Firewall'un hafıza taşma korumasını içerir. Hafıza taşırma saldırısı girişiminde CIS uyarı gösterir. Bu koruma, hafıza taşırma saldırı sonucu meydana gelebilecek veri hırsızlığına, bilgisayarın çökertilmesine ve sistem hasarına karşı koruma sağlar.

'Eğitim Kipi' ve 'Temiz PC' Kipi

Bu kipler ile güvenlik duvarı ve ana makina saldırı önleme sistemleri otomatik olarak güvendiğiniz uygulamalar için 'izin ver' kuralları oluşturur böylece, güvendiğiniz uygulamalardan gereksiz uyarılar almazsınız. Güvenlik Duvarı yalnızca şüpheli bir davranış olduğu zaman uyarır.

Uygulama Tanıma Veritabanı (Genişletilmiş güvenli uygulama listesi)

Güvenlik Duvarı 'Comodo Güvenli Liste Veritabanı' olarak bilinen genişletilmiş yürütülebilir güvenli dosyalar beyaz listesini içermektedir. Bu veritabanı her yürütülebilir dosyanın bütünlüğünü denetler ve zarar verebilecek olası uygulamalar kurulmadan önce uyarı verir. Bu koruma türü yenidir çünkü geleneksel güvenlik duvarları yalnızca bilinen kötücül yazılımları kara listeden saptar. Bilinmeyen yeni zararlıları – sıfırıncı gün saldırıları - genellikle kaçırırlar.

Güvenlik Duvarı'nın güvenli doyalar listesi sürekli olarak güncellenmektedir ve güvenlik endüstrisindeki en geniş güvenli dosyalar listesinden biridir.

Önemli İşlemlerin Sonlandırılmasına karşı Kendini Koruma

Zararlılar genelde saptanmadan işleyebilmek için bilgisayarınızdaki güvenlik uygulamalarını devre dışı bırakmaya çalışır. CIS kendi kayıt anahtarlarını, sistem dosyalarını ve işlemlerini koruyarak zararlılar tarafından kapatılmasını ve kurulumunun sabote edilmesini önler.

Güvenlik özelliği olarak Sandbox

Comodo İnternet Güvenliği'nin yeni sandbox özelliği bilinmeyen ve güvenilmeyen uygulamaları işletim ortamından izole eder. Bir uygulamanın sandbox içinde çalışması o uygulamanın diğer işlemler, programlar veya sistemdeki 'gerçek' veriler üzerinde kalıcı değişiklikler yapamayacağı anlamına gelir. Comodo, sandbox özelliğini güvenlik mimarisine doğrudan bütünleştirerek Güvenlik Duvarı, Savunma+ ve Antivirüs bileşenlerini güçlendirmiştir.

Şüpheli Dosyaların Comodo'ya Gönderilmesi

Yeni tür bir zararlının ilk kurbanı mı oldunuz? Kullanıcılar sıfırıncı gün tehditleriyle savaşmaya yardımcı olmak için dahili dosya gönder özelliğini kullanarak şüpheli dosyaları analiz için Comodo sunucularına gönderebilirler. Comodo olası tehditler için dosyayı analiz eder ve veritabanını tüm kullanıcılar için günceller.

1.2 Sistem Gereksinimleri

Comodo İnternet Güvenliği'nden en uygun performansı alabilmek için, lütfen bilgisayarınızın aşağıda belirtilen en düşük sistem gereksinimlerini karşıladığından emin olunuz:

- **Windows 7 (32-bit ve 64-bit sürümler), Windows Vista (32-bit ve 64-bit sürümler) veya Windows XP (32-bit ve 64-bit sürümler)**

- **Internet Explorer Sürüm 5.1 ve üzeri**
- **128 MB kullanılabilir Bellek**
- **210 MB sabit disk alanı, 32-bit ve 64-bit sürümler için**

1.3 Kurulum

Comodo İnternet Güvenliği'ni kurmadan önce, kurulum talimatlarını dikkatlice okuyun ve sistem gereksinimlerini gözden geçirin. LivePCSupport hesabının ve/veya Comodo Garanti'nin etkinleştirilmesi gibi ek hizmetler ve özellikler temel kurulum tamamlandıktan sonra gerçekleştirilir.

Lütfen dikkat – CIS yazılımı paket gözetmeksiniz tüm kullanıcılar için aynıdır. Tümü sürümler (ücretsiz de dahil) tüm güvenlik özelliklerini, teknolojilerini ve güncellemelerini içerir. Paketler arasındaki fark ek hizmetlerin kullanılabilirliğinde bulunmaktadır (LivePCSupport, TrustConnect, Online Storage ve Comodo Garanti). Ek hizmetlerin ve özelliklerin etkinleştirilmesi temel kurulum tamamlandıktan sonra gerçekleştirilir.

Ayrıntılı açıklamalar için aşağıdaki bağlantılara tıklayın:

•CIS Premium - Kurulum

•CIS Pro - Kurulum

•CIS Complete - Kurulum

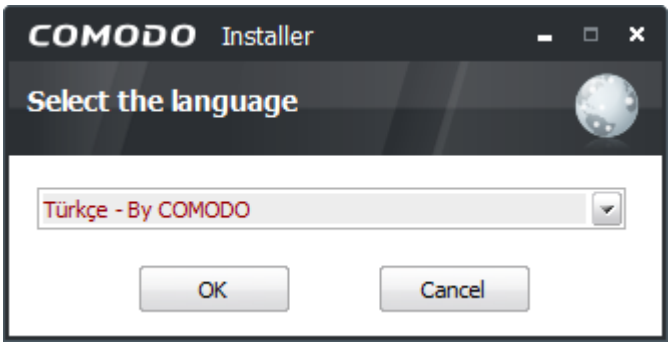
1.3.1 CIS Premium - Kurulum

Kurulum için, Comodo İnternet Güvenliği kurulum dosyalarını yerel diskinize indirin. (Kurulum dosyalarını bağlantıdaki sayfadan indirebilirsiniz - http://www.personalfirewall.comodo.com)

Comodo İnternet Güvenliği'nin kurulum dosyasını yerel diskinize indirdikten sonra, cispremium_installer.exe

dosyasına çift tıklayarak kurulum sihirbazını başlatabilirsiniz.

ADIM 1 – Arayüz Dilinin Seçimi

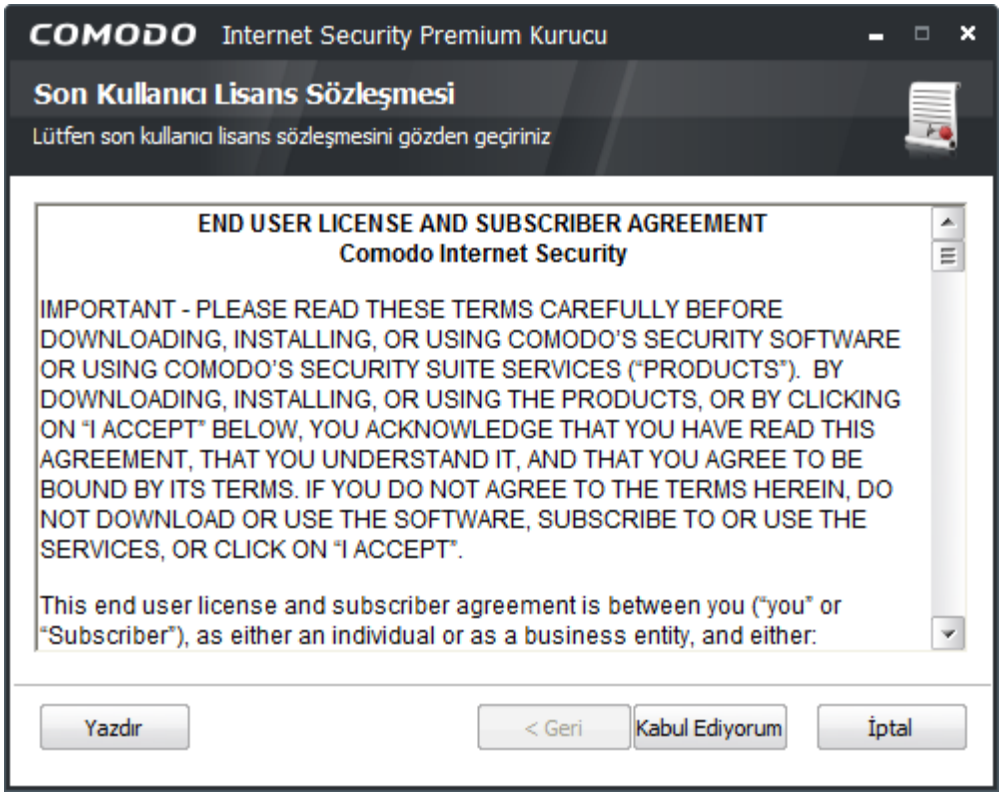


Kurulum sihirbazı otomatik olarak başlar ve 'Dil seçin (Select the language)' diyaloğu görünür. Comodo İnternet Güvenliği çeşitli dillerde bulunmaktadır.

- **Comodo İnternet Güvenliği'nin kurulmasını istediğiniz dili açılır listeden seçip 'Tamam (OK)' düğmesine tıklayın.**

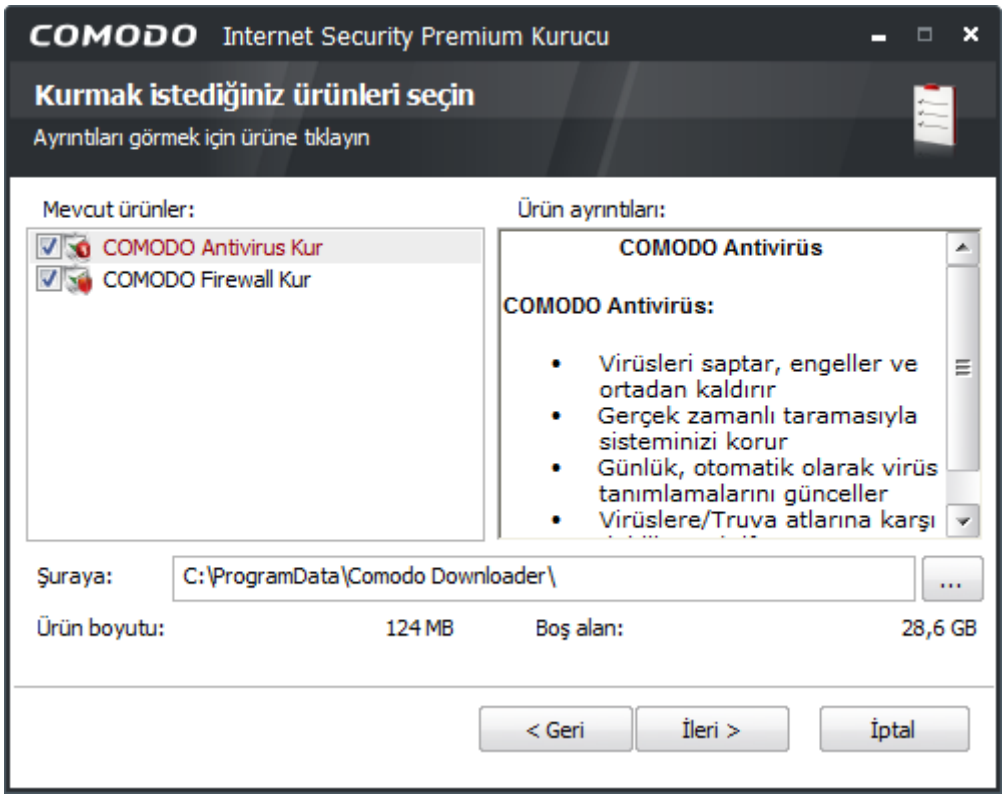
ADIM 2 – Son Kullanıcı Lisans Sözleşmesi

Son Kullanıcı Lisans Sözleşmesi diyaloğu görünecektir.



Kuruluma devam edebilmek için, Son Kullanıcı Lisans Sözleşmesini (EULA) okumalı sonra kabul etmelisiniz. Kuruluma devam etmek için 'Kabul ediyorum', bu aşamada kurulumdan çıkmak için 'İptal' düğmesine tıklamalısınız.

ADIM 3 – Kurulacak Bileşenlerin Seçimi



Sonraki adım hangi bileşenleri yükleyeceğinizi seçmektir. Comodo, en yüksek korumayı elde etmek için üçüncü parti antivirüs ve güvenlik duvarı yazılımlarının sistemden kaldırılıp Comodo Antivirüs ve Comodo Güvenlik Duvarı bileşenlerinin kurulmasını önermektedir. (Pro ve Complete müşterileri her iki bileşeni de kurmak zorundadırlar). CIS Pro ve Complete müşterilerinin hizmetlerden yararlanabilmesi için ayrıca Comodo TrustConnect uygulamasını da kurmaları gerekmektedir. (Ücretsiz ürün kullanan kullanıcılar için bu ürün seçime bağlıdır).

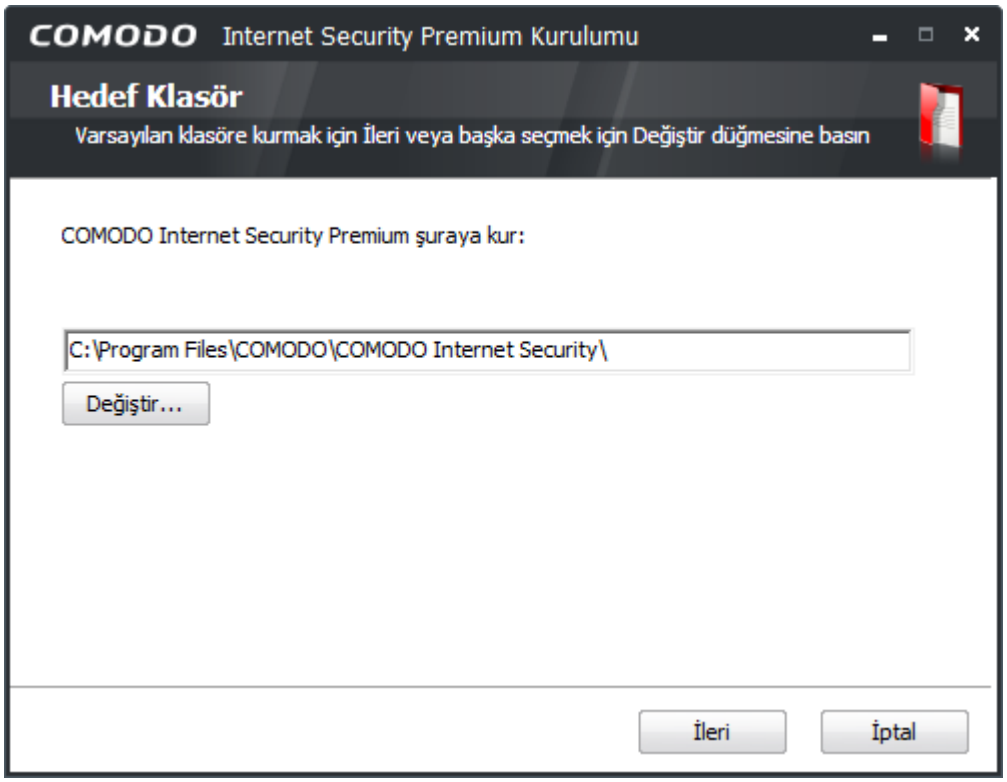
- **COMODO Firewall Kur** – Bu seçenekle birlikte Comodo Güvenlik Duvarı ve Savunma+ bileşenleri kurulur. Üçüncü parti güvenlik duvarı kullanıyorsanız bu seçenek işaretli olmasın. Comodo Güvenlik Duvarı Premium, Pro veya Complete müşterileri için zorunlu gereksinimdir. Eğer güvenlik duvarının kurulmasını seçer antivirüsü seçmezseniz ADIM 6'daki güvenlik duvarı ayarlarının yapılandırılması sorulacaktır.
- **COMODO Antivirus Kur** - Bu seçenekle birlikte Comodo Antivirüs ve Savunma+ bileşenleri kurulur. Üçüncü parti antivirüs kullanıyorsanız bu seçenek işaretli olmasın. Comodo Güvenlik Duvarı Premium, Pro veya Complete müşterileri için zorunlu gereksinimdir.

ADIM 4 – Dosyaların Çıkartılması

Kurucu seçilmiş bileşenlerin kurulum için gerekli dosyalarını çıkartacaktır.

ADIM 5 – Kurulum Klasörünün Seçimi

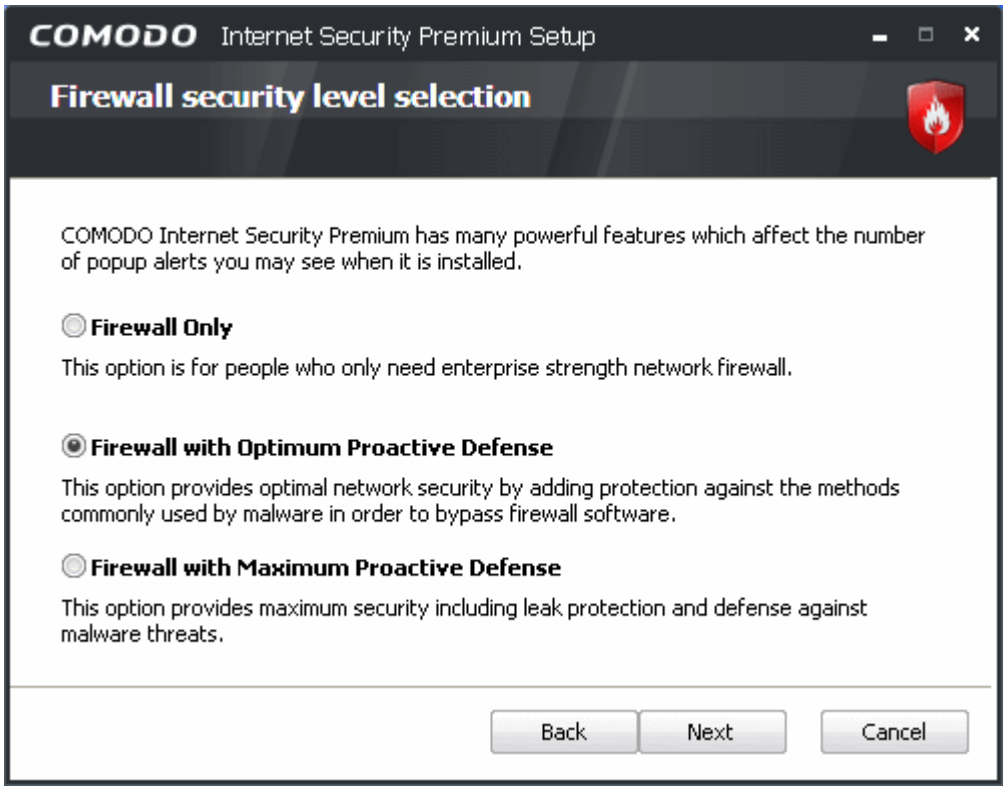
Sonraki ekran kurulumun yapılacağı klasörü seçmenize izin verir. Varsayılan yol *C:\Program Files\Comodo\Comodo Internet Security.*



Varsayılan klasöre kurmak için 'İleri' düğmesine tıklayın, eğer başka bir klasör seçmek istiyorsanız 'Değiştir' düğmesine tıklayarak başka bir konum seçin.

ADIM 6 – Güvenlik Duvarı Yapılandırması

Antivirüs bileşeninin kurulumunu seçmediğiniz için Güvenlik Duvarı'nın güvenlik seviyesini seçme diyaloğuna geçmiş oldunuz. Eğer her ikisini de seçmiş olsaydınız, sihirbaz Adım 7'ye geçecekti.



Seçenekler;

Yalnızca Güvenlik Duvarı – Bu seçenek sisteminde alternatif bir Ana Makina Saldırı Önleme yazılımı olan ***tecrübeli*** kullanıcılar içindir. Bu seçeneğin seçilmesi YALNIZCA paket süzen güvenlik duvarını kuracaktır ve Savunma+ kurulmayacaktır (Savunma+ solucanlar ve Truva atları gibi kötü niyetli yazılımların kuracakları bağlantı girişimlerini engellemek için gereklidir).

Güvenlik Duvarı ile birlikte Optimum Proaktif Savunma - Bu seçeneğin seçilmesi hem güvenlik duvarını hem de Savunma+ bileşenini kuracaktır. Savunma+ kurulumuyla birlikte güvenlik ayarlarının varsayılan yapılandırması da en uygun seviyeye ayarlanır. Varsayılan koruma seviyesi ile ilgili ayrıntılı bilgi için buraya tıklayın.

Güvenlik Duvarı ile birlikte Maksimum Proaktif Savunma – Bu seçenek en kapsamlı ve en iyi korumayı sağlar. Bu seçeneğin seçilmesi hem güvenlik duvarını hem de Savunma+ bileşenini kuracaktır. Savunma+ kurulumuyla birlikte güvenlik ayarlarının varsayılan yapılandırması da maksimum seviyeye ayarlanır. Varsayılan koruma seviyesi ile ilgili ayrıntılı bilgi için buraya tıklayın.

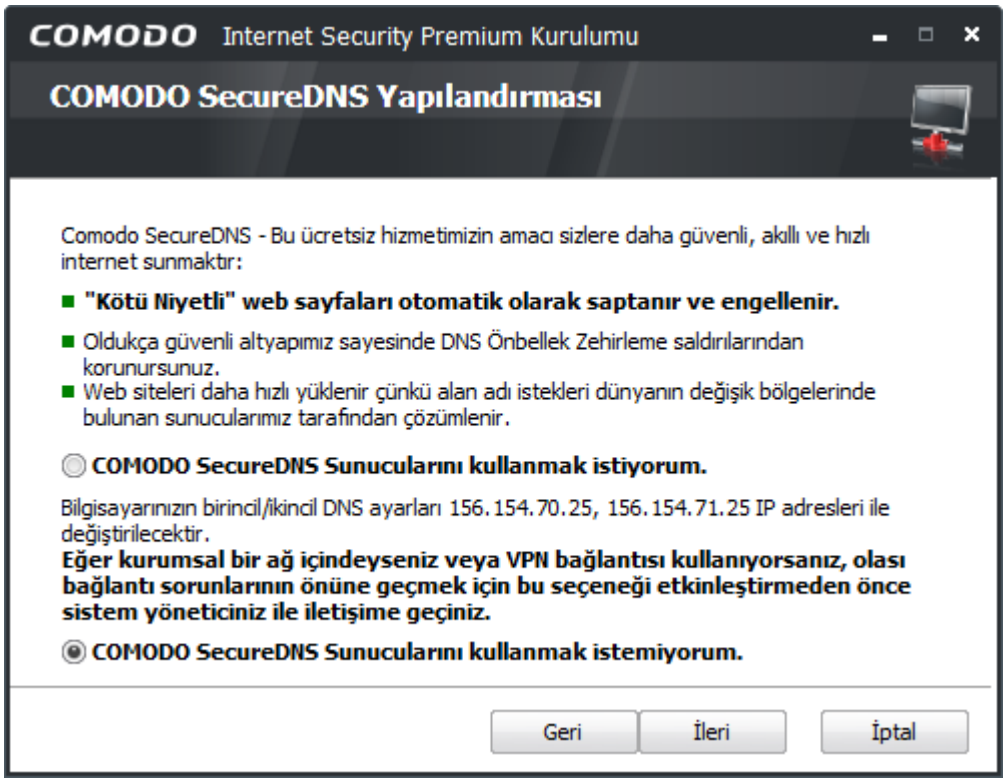
Seçiminizi yaptıktan sonra 'İleri' düğmesine tıklayın.

ADIM 7 - DNS Ayarlarının Yapılandırılması

Comodo Secure DNS hizmeti kullandığınız DNS sunucularını Comodo DNS sunucuları ile değiştirir ve onları kullanır. Comodo'nun dünya üzerine yayılmış sunucuları ile hızlı ve güvenli olarak İnternet gezintisi yaşarsınız. Bu hizmeti istediğiniz zaman devre dışı bırakarak önceki ayarlarınıza geri dönebilirsiniz.

Comodo Secure DNS Hizmeti hakkında daha fazla bilgi almak ve bu hizmetin nasıl etkinleştirileceğini veya devre

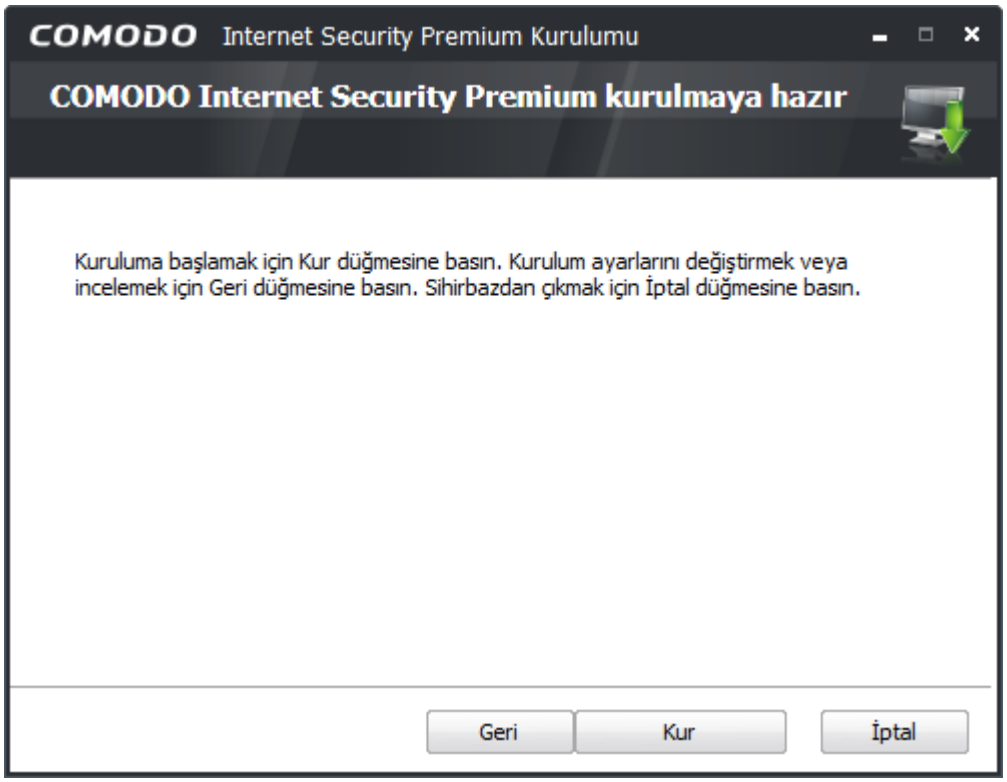
dışı bırakılacağını öğrenmek için, Ek 1 Comodo Secure DNS Hizmeti'ne bakın.



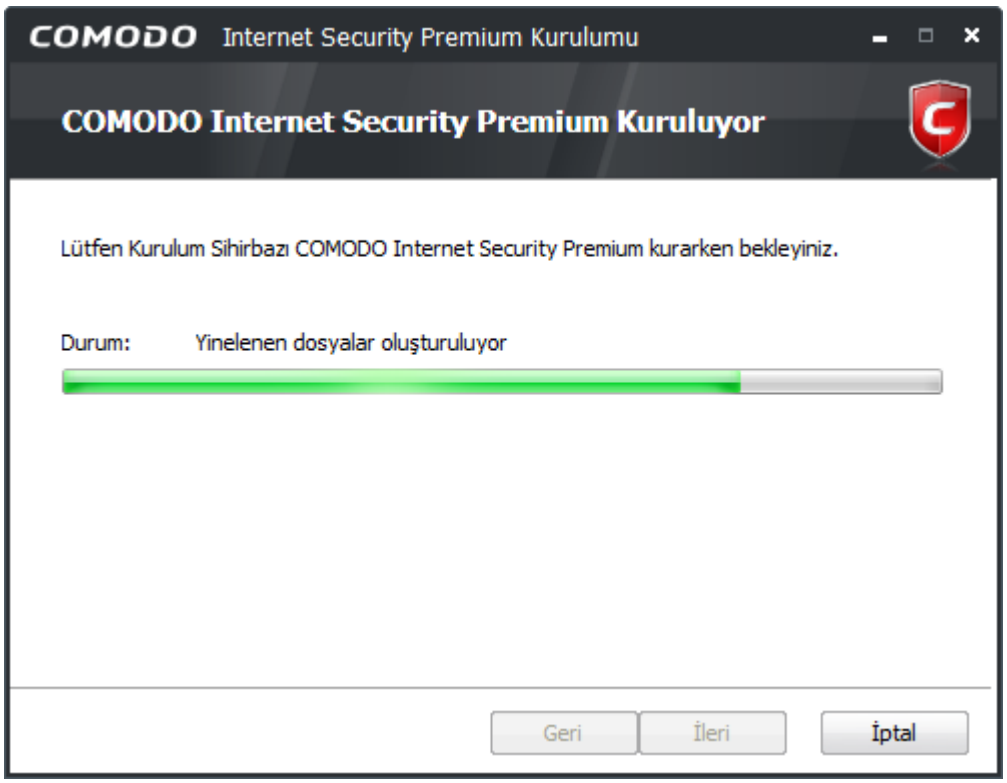
Comodo Secure DNS Hizmeti'ni etkinleştirmek için, **Comodo Secure DNS Hizmetini kullanmak istiyorum**'u seçin ve 'İleri' düğmesine tıklayın.

ADIM 8 – Kurulum İlerleyişi

Yapılandırma seçeneklerini tamamladıktan sonra kurucu sihirbaz size kurulum işlemini başlatma onayını soracaktır.

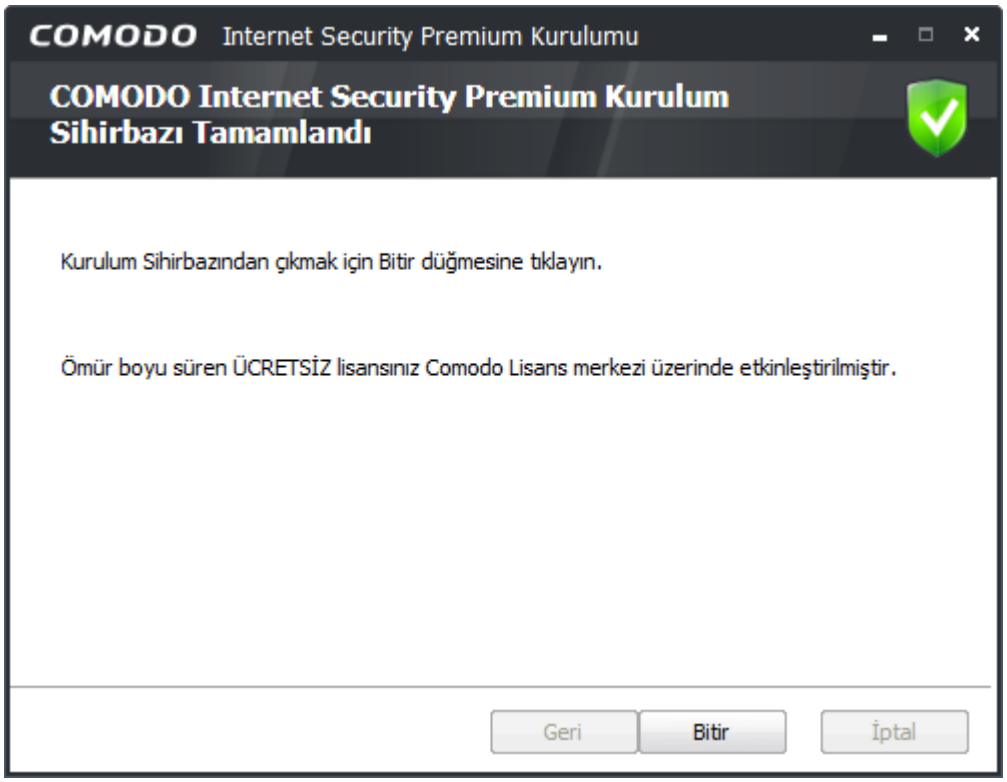


Önceden belirlediğiniz ayarların herhangi birini gözden geçirmek ve/veya değiştirmek için 'Geri' düğmesine tıklayın. Kuruluma başlamak için ise 'Kur' düğmesine tıklayın.



Kurulum ilerleyişi gösterilecektir...

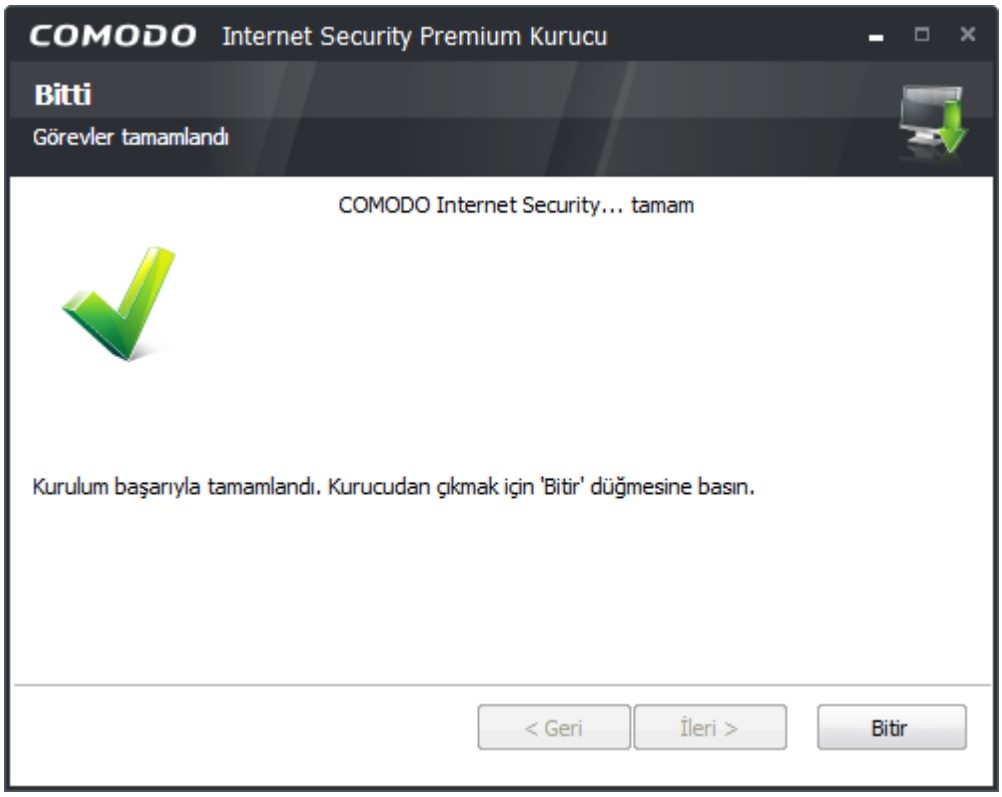
… ve tamamlandıktan sonra tamamlandı diyaloğu görünecektir.

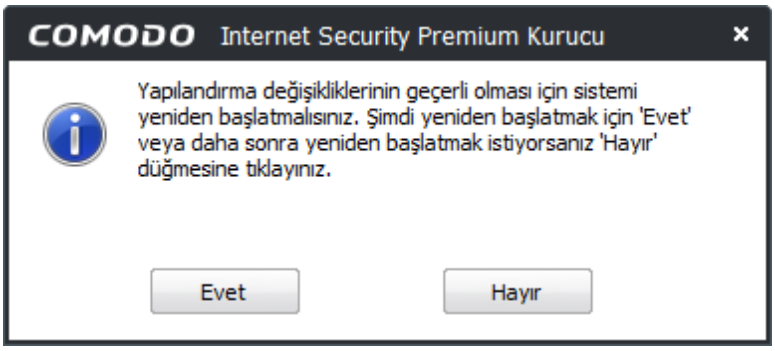


'Bitir' düğmesine tıklayın.

ADIM 9 – Kurulumun Tamamlanması ve Sistemin Yeniden Başlatılması

Başarılı kurulumdan sonra onay diyaloğu görüntülenecektir.





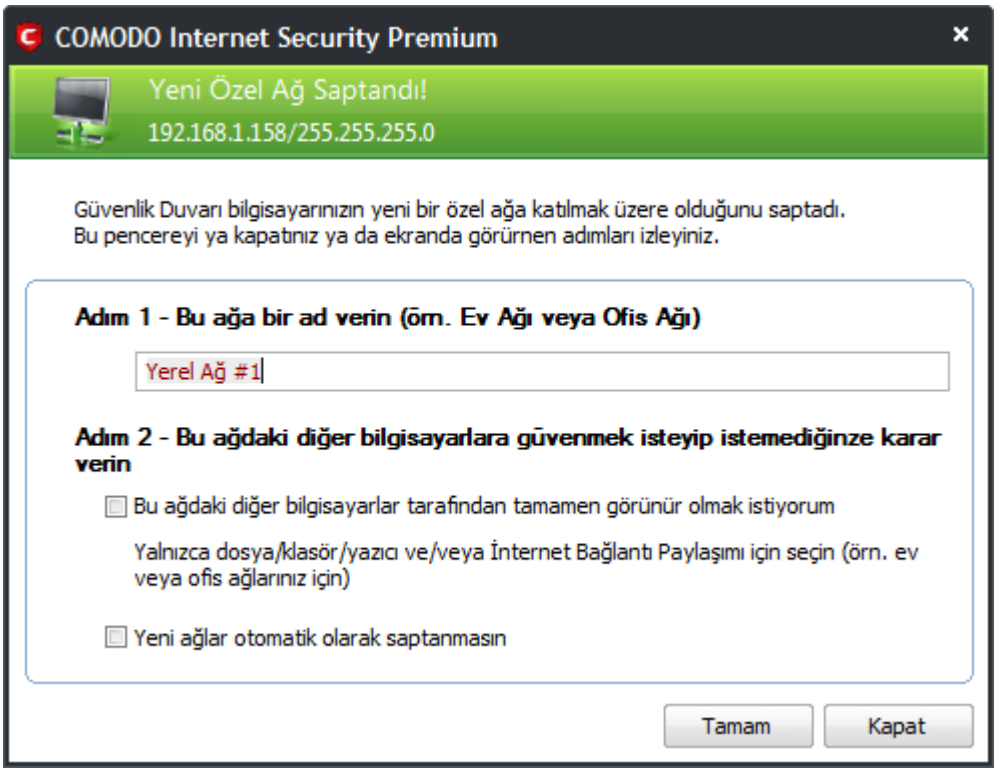
Bitir düğmesine tıklayın. Kurulumun etkili olabilmesi için bilgisayarınızın yeniden başlatılması gerekmektedir.

Kaydedilmemiş tüm verilerinizi kaydedin ve ‘Evet’ düğmesine tıklayarak sisteminizi yeniden başlatın. Daha sonra kendiniz yeniden başlatmak istiyorsanız ‘Hayır’ düğmesine tıklayın.

Not: Kurulum yalnızca sistem yeniden başlatıldıktan sonra etkili olacaktır.

STEP 10 - Sisteminizi Yeniden Başlattıktan Sonra

Sistem yeniden başladıktan sonra, eğer bilgisayarınız bir ağa bağlıysa ’Yeni Özel Ağ Saptandı’diyaloğu belirecektir ve yapılandırmanız istenecektir:



Adım 1: İnternete bağlanmak için tek bilgisayarlı ev kullanıcılarının bile ev ağı yapılandırması gereklidir. (Ağ bağlantınızın adı Adım 1'de metin alanında görünür). Çoğu kullanıcı bu adı kabul edebilir.

Adım 2: Bu ağdaki diğer bilgisayarlardan gelen bağlantıları kabul etmek istiyorsanız (örn. Çalışma veya Ev Ağı) veya yazıcı paylaşımı için 'Bu ağdaki diğer bilgisayarlar tarafından tamamen görünür olmak istiyorum' seçeneği işaretleyin. Bu ağ daha sonra güvenli ağ olur. Tek bilgisayarlı ev kullanıcıları bu seçeneği seçmekten kaçınmalıdırlar.

Tecrübeli bir kullanıcıysanız 'Yeni ağlar otomatik olarak saptanmasın' seçeneğini işaretleyerek gerektiğinde elle güvenli ağlar oluşturabilirsiniz. (Bunu 'Ağ Bölgelerinden' ve 'Port Gizleme Sihirbazı' aracılığıyla yapabilirsiniz)

Seçiminizi 'Tamam' düğmesine tıklayarak onaylamalısınız. Eğer 'Hayır' düğmesine tıklarsanız tüm ağ bağlantıları engellenecektir.

1.3.2 CIS Pro - Kurulum ve Etkinleştirilmesi

Comodo İnternet Güvenliği 2011 Pro'yu http://personalfirewall.comodo.com/internetsecuritypro/ sayfasından abone kaydı yaptırdıktan sonra indirebilirsiniz ve aşağıdaki hizmetleri içerir:

- **LivePCSupport** - Bilgisayar destek hizmeti Comodo uzmanlarınca uzaktan bağlanılarak verilir. Hizmet şunları içerir:

Virüs Teşhisi / Temizliği - Zararlı taramasını ve bulunan zararlıların kaldırılmasını içerir;

PC Ayarlanması – Uzamanlar tarafından bilgisayarınızın performansını etkileyen sorunlar belirlenerek değerlendirilir ve bu değerlendirmeye göre ince ayarlamalar yapılarak sistem kararlılığı ve hızı iyileştirilir;

İnternet Giriş Koruması – Bilgisayarınızın temel güvenlik ayarları etkinleştirilerek önemli bilgilerinizin kaybı önlenir;

Eposta Hesabı Ayarlanması – İnternet tabanlı eposta hesabınız ayarlanır – herhangi bir sağlayıcı, herhangi bir hesap. Yeni bilgisayarlar ve acemi eposta kullanıcıları için iyi;

Yazılım Kurulumu – Comodo ürünlerinin kurulumu ve en iyi koruma için özelleştirilmesi;

Yazıcı Ayarlanması ve Sorun Çözümü – Yazıcı sürücülerinin veya yazılımının güncellenmesi, mürekkep seviyesinin denetimi ve yazıcınızın kablolu veya kablosuz ağda çalışacak şekilde ayarlanması;

Yeşil PC – Bilgisayar kullanımınıza göre güç yönetim ayarlarının yapılandırılması sayesinde elektrik faturasından tasarruf edersiniz ve çevreyi korumuş olursunuz;

Bilgisayar orun Çözümü – Windows içindeki temel donanım çakışmalarının denetlenmesi.

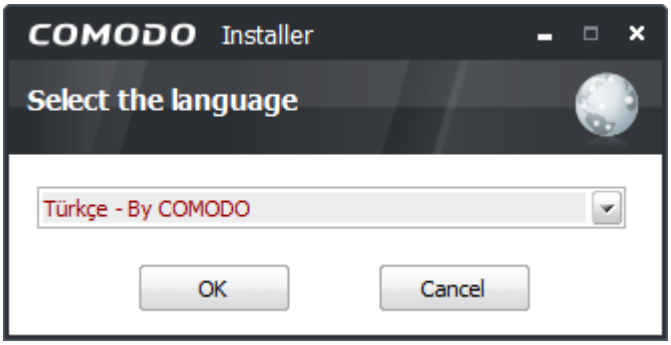
LivePCSupport hizmeti Comodo uzmanlarınca uzaktan bağlanılarak verilir. Daha fazla bilgi için Live PC support bölümüne bakın.

- **TrustConnect** - (Şifrelenmiş İnternet Vekil Sunucu Hizmeti). Trustconnect halka açık kablosuz ağlarda güvenli olarak gezinti yapmanızı sağlar.

Comodo Garanti - (Sisteminiz zararlı saldırısı sonucu zarar görürse ve Comodo uzmanları bu hasarı düzeltip sisteminizi çalışır duruma getiremezlerse Comodo sisteminizin düzeltilmesi için gerekli maliyeti karşılayacaktır. Ayrıntılar için Şartlar ve Koşullara bakınız.) Garanti yalnızca bilgisayarınız bazı ön koşulları sağlıyorsa etkinleştirilebilir. Sistemde zararlı olmamalı, belirli uygulamalar kurulu olmalı ve belirli CIS ayarları etkin olmalıdır. Bu ayarlar garanti etkinleştirilmesi işlemi sırasında sihirbaz tarafından test edilir ve etkinleştirilir. Daha fazla bilgi için 'Garanti Güvencesi'nin Etkinleştirilmesi' bölümüne bakın. Comodo Garanti yalnızca ABD'de ikamet edenler için mevcuttur.

Comodo İnternet Güvenliği'nin kurulum dosyasını yerel diskinize indirdikten sonra, cispro_installer.exe

dosyasına çift tıklayarak kurulum sihirbazını başlatabilirsiniz.



'Dil seçin (Select the language)' diyaloğu görünecektir.

Comodo İnternet Güvenliği çeşitli dillerde bulunmaktadır.

- **Comodo İnternet Güvenliği'nin kurulmasını istediğiniz dili açılır listeden seçip 'Tamam (OK)' düğmesine tıklayın.**

Aşağıdaki pencere görünecektir.

Comodo Internet Security 2011 Pro Kur – Eğer henüz CIS kurmadıysanız ilk olarak 'Comodo Internet Security 2011 Pro Kur' seçmelisiniz.

- **Comodo Internet Security 2011 Pro kurulumu hakkında daha fazla bilgi almak için buraya tıklayın**

TrustConnect Etkinleştirilmesi - TrustConnect hesabınızın ve Comodo Garanti'nizin etkinleştirilmesi işlemini başlatır. Lütfen başlamadan önce Lisans Anahtarınızı hazırlayın. Lisans Anahtarınız eposta yoluyla gönderilir. Geçerli bir anahtar girdikten sonra hesap kaydı işlemini başlatacak Comodo web-formuna yönlendirileceksiniz.

•**Hizmet etkinleştirilmesi hakkında tam bilgiye buraya tıklayarak ulaşabilirsiniz**

TrustConnect Kur - Comodo TrustConnect kur işlemini başlatır. TrustConnect kullanımınızı https://accounts.comodo.com sayfasından hesabınıza giriş yaparak yönetilebilirsiniz.

- **TrustConnect hakkında daha fazla bilgi için buraya tıklayın**
- **Comodo TrustConnect kurulumu hakkında daha fazla bilgi için buraya tıklayın.**

Dragon Web Browser Kur - Dragon web tarayıcısını kurar. Dragon kullanıcı dostu web tarayıcısıdır.

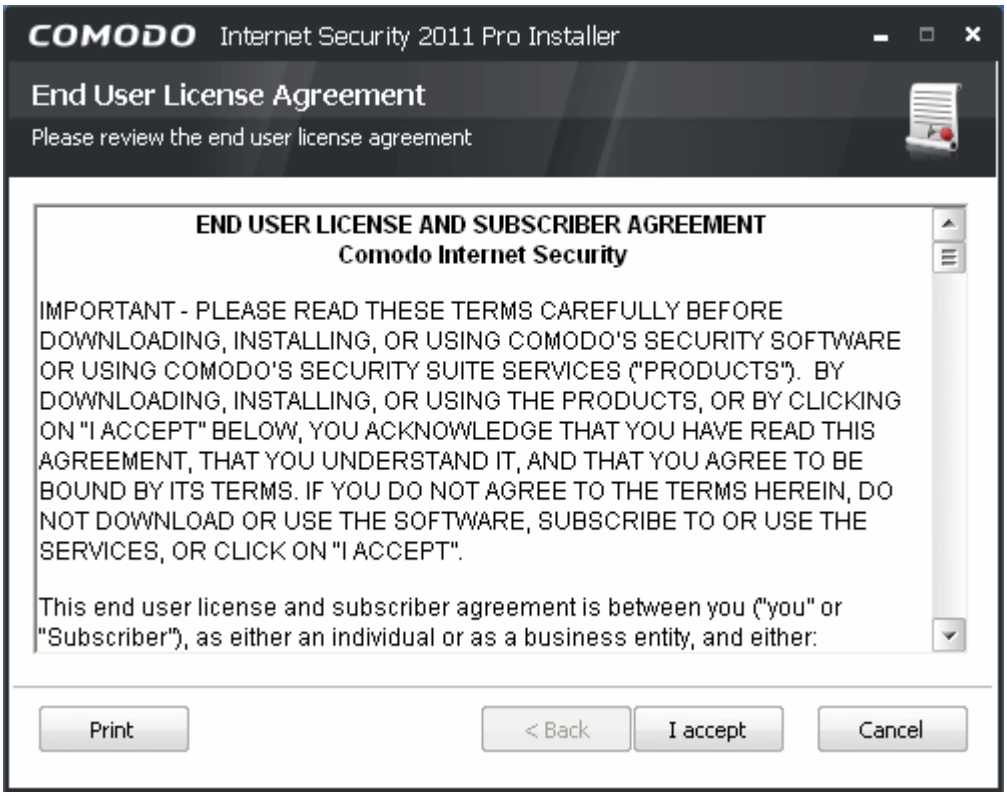
- Dragon web tarayıcısı hakkında daha fazla bilgi için buraya tıklayın

1.3.2.1 Comodo Internet Security 2011 Pro ve Live PC Support Kurulumu

Ana ekrandan 'COMODO Internet Security 2011 Pro Kur' düğmesine tıklayarak kurulumu başlatın. CIS 2011 ve Live PC Support kurulum sihirbazı başlayacaktır.

ADIM 1 – Son Kullanıcı Lisans Sözleşmesi

Son Kullanıcı Lisans Sözleşmesi diyaloğu görünecektir.



Kuruluma devam edebilmek için, Son Kullanıcı Lisans Sözleşmesini (EULA) okumalı sonra kabul etmelisiniz. Kuruluma devam etmek için 'Kabul ediyorum', bu aşamada kurulumdan çıkmak için 'İptal' düğmesine tıklamalısınız.

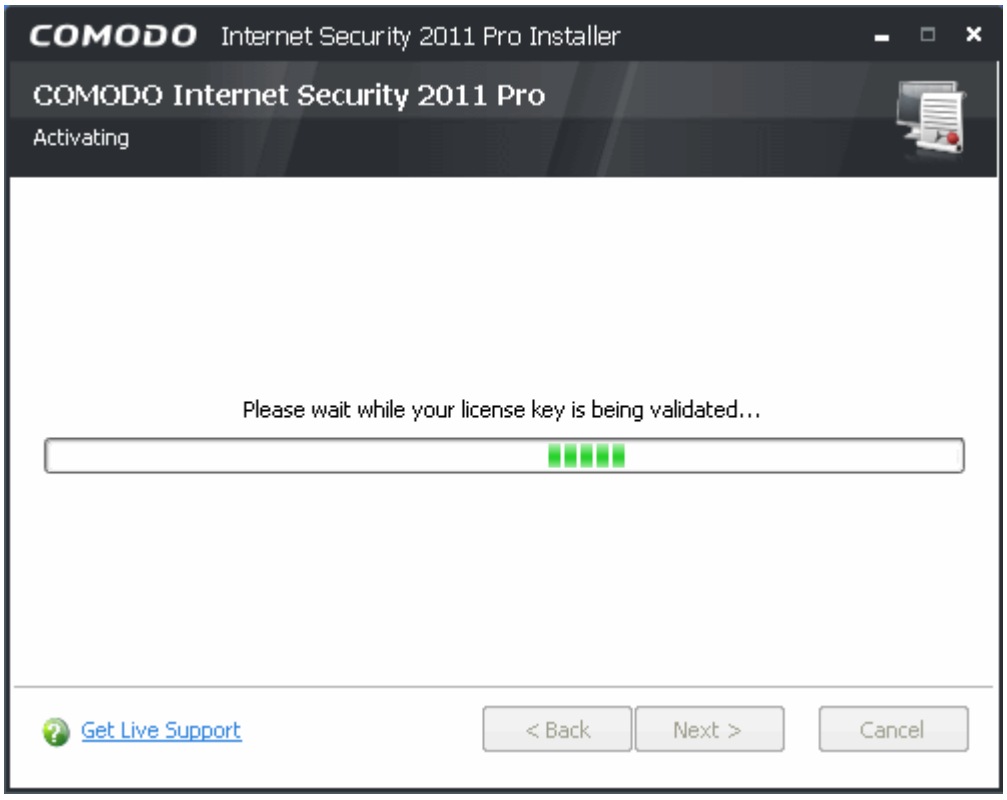
ADIM 2 – Lisansınızın Doğrulanması

Sonraki adım Lisans anahtarının girilmesidir. Anahtarınız eposta yoluyla gönderilir.

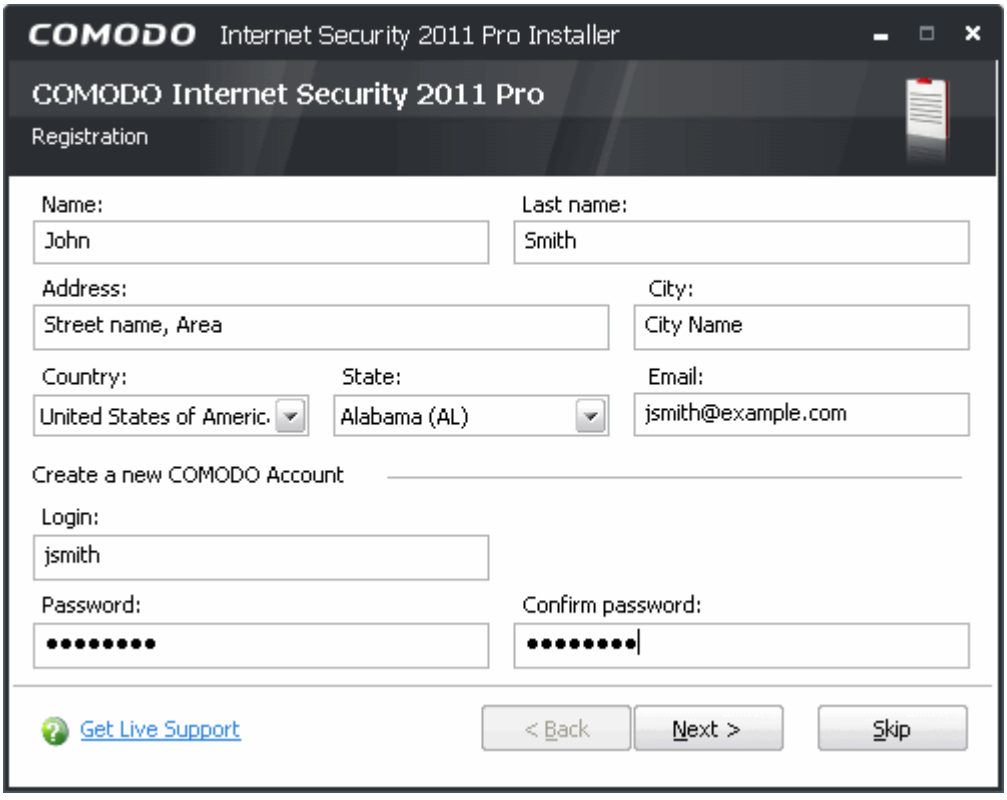
Anahtarı tam olarak girin ve 'İleri' düğmesine tıklayın.

İpucu: Kurulum sırasında anahtarınız yoksa bu adımı anahtar girmeden 'İleri' düğmesine tıklayarak geçebilirsiniz. Aboneliğiniz ve garantinizi daha sonra ana arayüzden etkinleştirebilirsiniz. Daha fazla bilgi için 'CIS Pro ve CIS Complete Hizmetlerinin Kurulumdan Sonra Etkinleştirilmesi' bölümüne bakabilirsiniz.

Lisans anahtarınız doğrulanacaktır.



Lisans anahtarınızın başarıyla doğrulanmasından sonra Comodo Hesapları Yöneticisi ile hesap kaydınızı yapmalısınız.



Gerekli bilgilerle kayıt formunu doldurun. Bu forma girdiğiniz giriş ve parola ile herhangi bir zamanda Comodo Hesapları Yöneticisine giriş yapmak için kullanabilirsiniz.

'İleri' düğmesine tıklayın.

Kaydınız etkinleştirilecektir.

Başarılı etkinleştirme sonrasında lisansınızın size sağladığı hakları içeren son bir onay ekranı çıkacaktır:

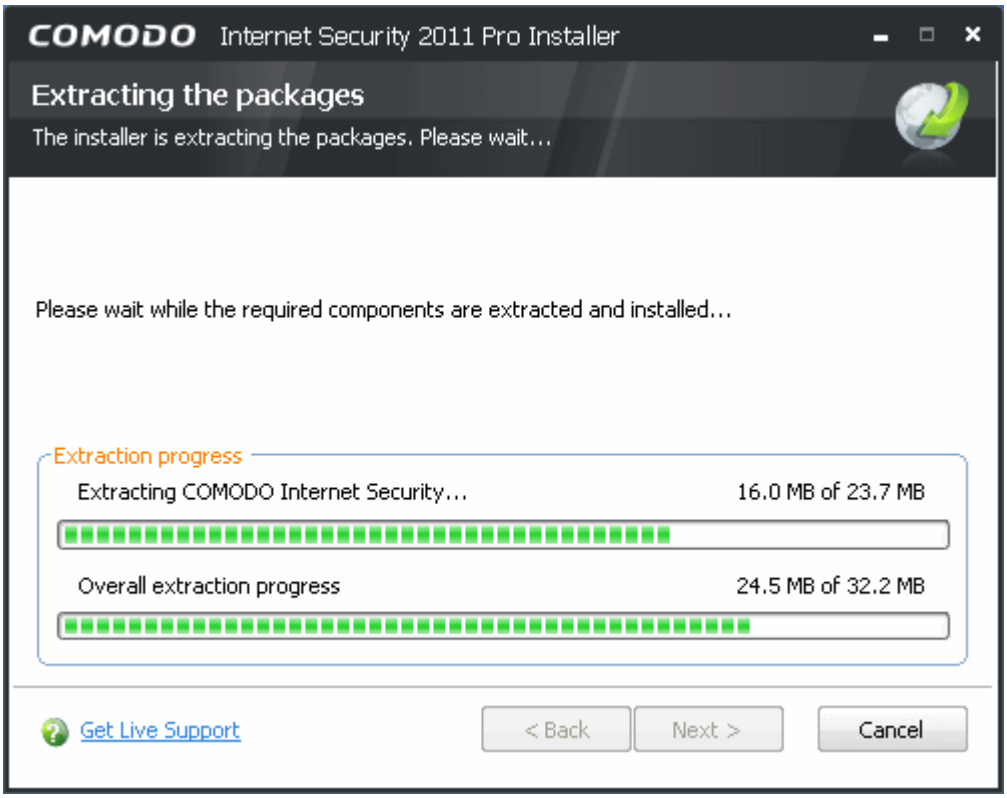
İleride kullanmak ve başka makinalara kurulum için lisans anahtarınızı saklayınız. (lisansınız 3 makinaya kadar geçerlidir).

Devam etmek için 'İleri' düğmesine tıklayın.

Önemli not: CIS kurulumundan sonra garantinizi etkinleştirmeniz gerekmektedir. Daha fazla bilgi için Garanti Güvencenizin Etkinleştirilmesi bölümüne bakın.

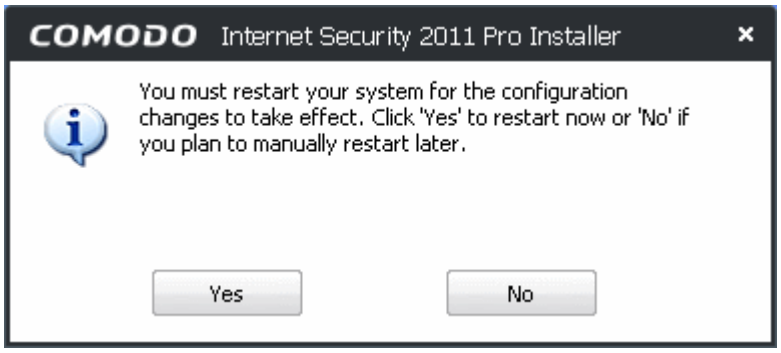
ADIM 3 –Kurulum İlerleyişi

Paketler çıkartılacaktır...



... ve kurulacaktır. Kurulum ilerleyişi görünecektir.

Başarılı kurulumdan sonra kurulumun etkili olabilmesi için yeniden başlatma onay diyaloğu görüntülenecektir.

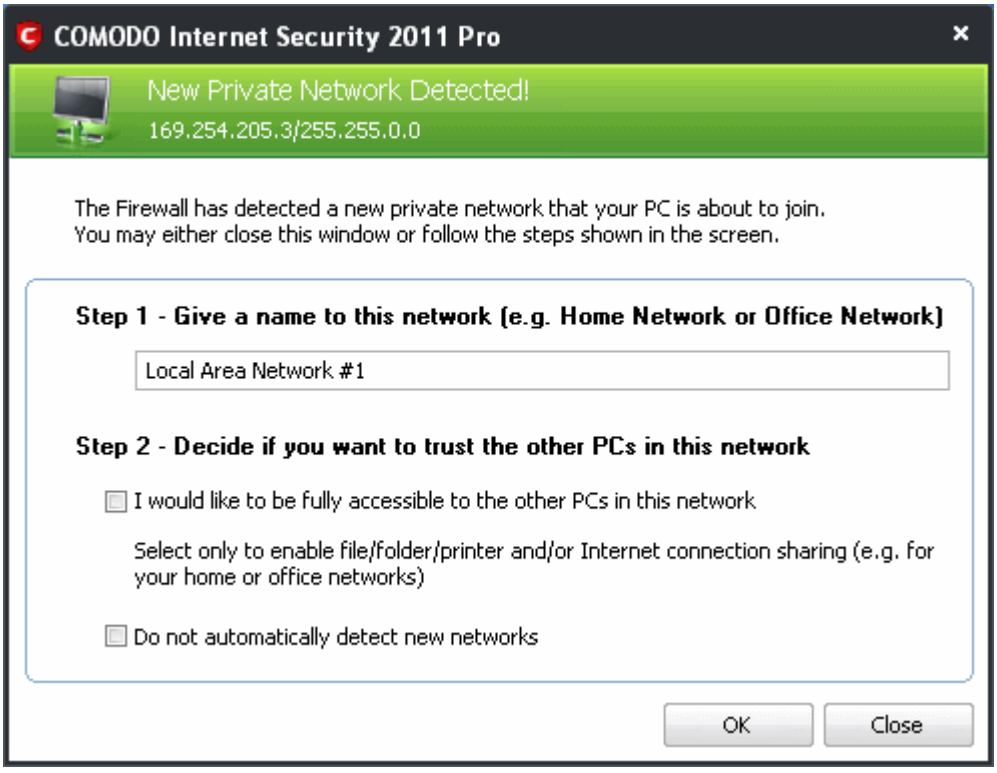


Kaydedilmemiş tüm verilerinizi kaydedin ve 'Evet' düğmesine tıklayarak sisteminizi yeniden başlatın. Daha sonra kendiniz yeniden başlatmak istiyorsanız 'Hayır' düğmesine tıklayın.

Not: Kurulum yalnızca sistem yeniden başlatıldıktan sonra etkili olacaktır.

ADIM 4 - Sisteminiz Yeniden Başladıktan Sonra

Sistem yeniden başladıktan sonra, eğer bilgisayarınız bir ağa bağlıysa 'Yeni Özel Ağ Saptandı' diyaloğu belirecektir ve yapılandırmanız istenecektir:



Adım 1: İnternete bağlanmak için tek bilgisayarlı ev kullanıcılarının bile ev ağı yapılandırması gereklidir. (Ağ

bağlantınızın adı Adım 1'de metin alanında görünür). Çoğu kullanıcı bu adı kabul edebilir.

Adım 2: Bu ağdaki diğer bilgisayarlardan gelen bağlantıları kabul etmek istiyorsanız (örn. Çalışma veya Ev Ağı) veya yazıcı paylaşımı için 'Bu ağdaki diğer bilgisayarlar tarafından tamamen görünür olmak istiyorum' seçeneği işaretleyin. Bu ağ daha sonra güvenli ağ olur. Tek bilgisayarlı ev kullanıcıları bu seçeneği seçmekten kaçınmalıdırlar.

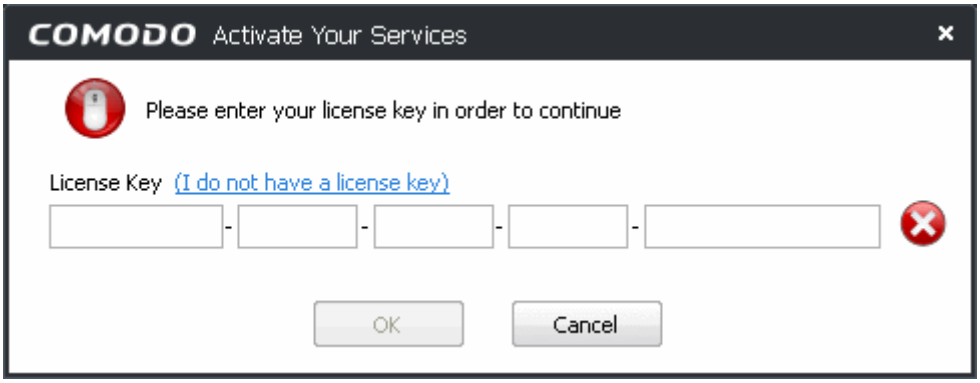
Tecrübeli bir kullanıcıysanız 'Yeni ağlar otomatik olarak saptanmasın' seçeneğini işaretleyerek gerektiğinde elle güvenli ağlar oluşturabilirsiniz. (Bunu 'Ağ Bölgelerinden' ve 'Port Gizleme Sihirbazı' aracılığıyla yapabilirsiniz)

Seçiminizi 'Tamam' düğmesine tıklayarak onaylamalısınız. Eğer 'Hayır' düğmesine tıklarsanız tüm ağ bağlantıları engellenecektir.

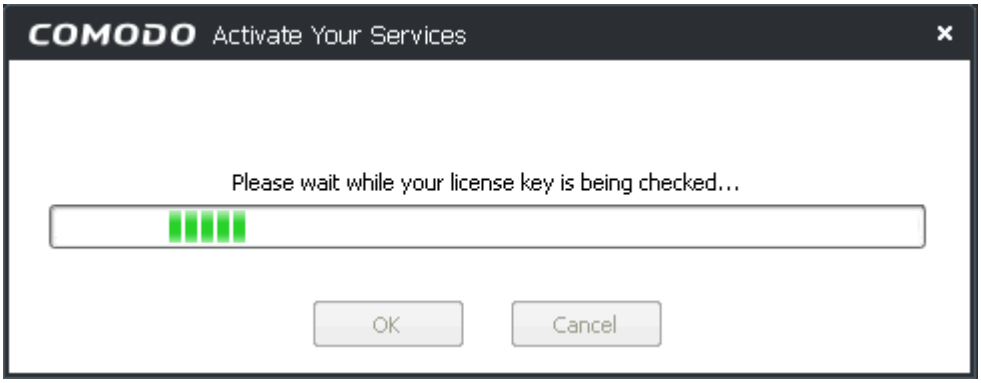
1.3.2.2 TrustConnect Hizmeti ve Garantinin Etkinleştirilmesi

TrustConnect hizmetlerinden ve garanti güvencesinden yararlanabilmek için hizmetleri etkinleştirmelisiniz. Bu işlemi başlatmadan önce anahtarınızı hazırlayın.

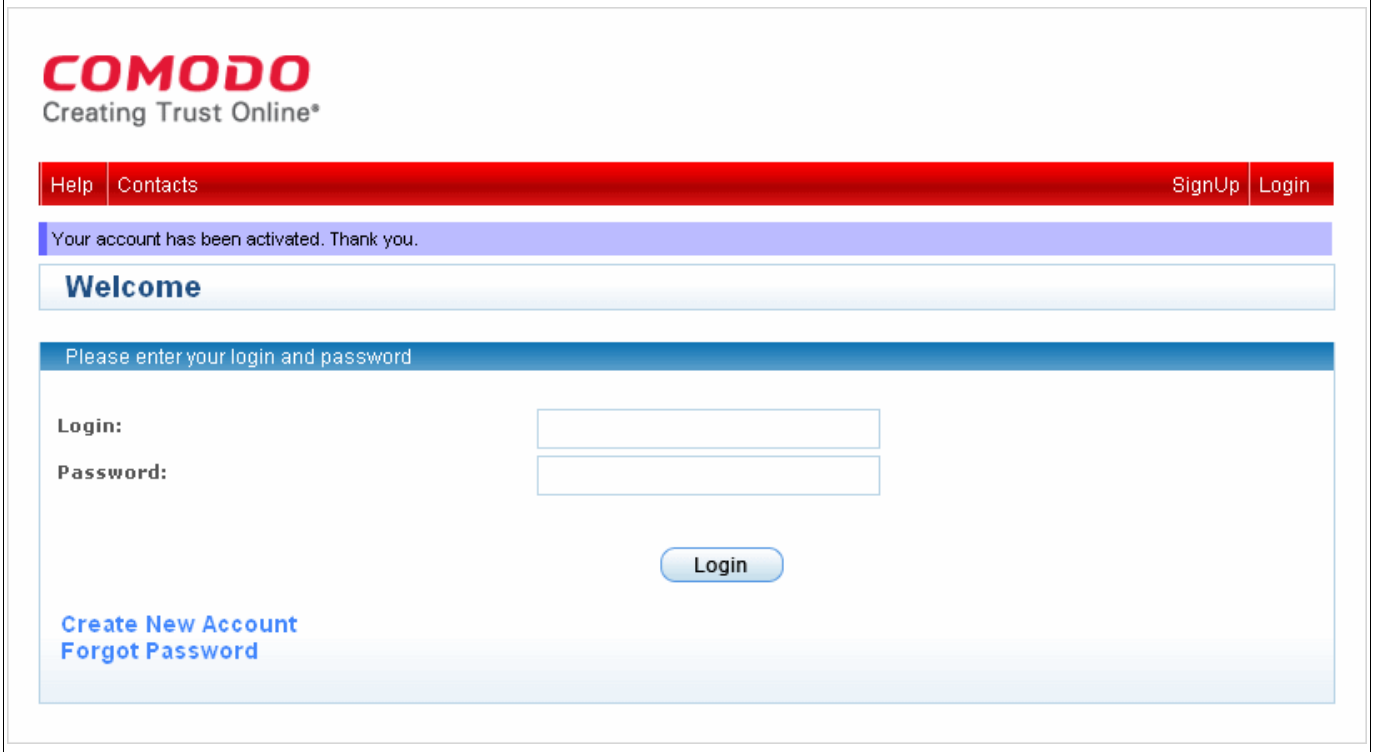
•Comodo Internet Security 2011 Pro kurucu ekranından 'TrustConnect etkinleştir' düğmesine tıklayın. Daha sonra çıkacak ekrandaki alanlara size gönderilen anahtarı girin.



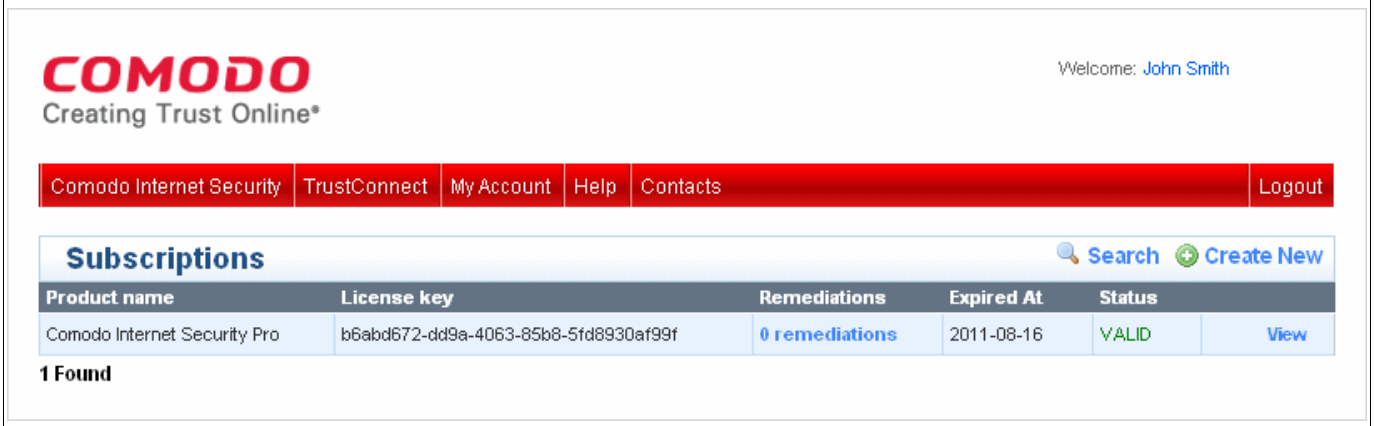
•Eposta ile gönderilen lisans anahtarını girin. Lisans anahtarı doğrulanacaktır.



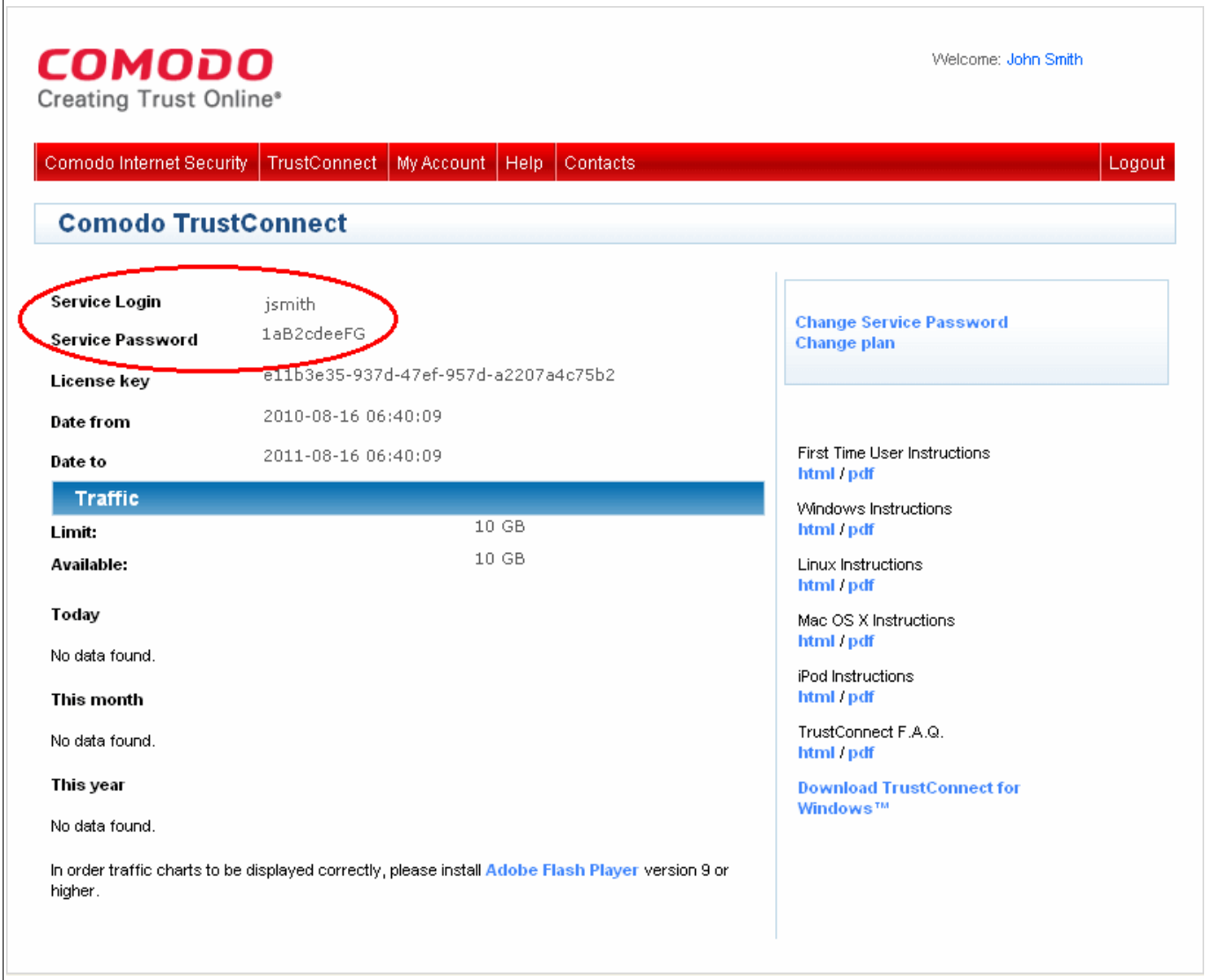
Lisans anahtarı doğrulandıktan sonra Comodo Hesapları Yöneticisi görüntülenecektir.



Lisansınızı etkinleştirirken tanımladığınız giriş kimliğini ve parolasını girin. (Adım 2'de kayıt yaparken tanımladığınız bilgiler). Hesap özeti görüntülenecektir..



'TrustConnect' sekmesine tıklayın. TrustConnect hesabı bilgileriniz görüntülenecektir.



•Bu sayfadaki hizmete giriş bilgilerinizi (giriş ve parola) bir yere not ediniz. Bu bilgiler TrustConnect Hizmetlerini kullanmak için gereklidir. Daha fazla bilgi için TrustConnect Tanıtımı bölümüne bakın.

1.3.3 CIS Complete – Kurulum ve Etkinleştirilmesi

Comodo Internet Security 2011 Complete DVD ile dağıtılır ve aşağıdaki hizmetleri içerir:

- **LivePCSupport** - Bilgisayar destek hizmeti Comodo uzmanlarınca uzaktan bağlanılarak verilir. Hizmet şunları içerir:

Virüs Teşhisi / Temizliği - Zararlı taramasını ve bulunan zararlıların kaldırılmasını içerir;

PC Ayarlanması – Uzamanlar tarafından bilgisayarınızın performansını etkileyen sorunlar belirlenerek değerlendirilir ve bu değerlendirmeye göre ince ayarlamalar yapılarak sistem kararlılığı ve hızı iyileştirilir;

İnternet Giriş Koruması – Bilgisayarınızın temel güvenlik ayarları etkinleştirilerek önemli bilgilerinizin kaybı önlenir;

Eposta Hesabı Ayarlanması – İnternet tabanlı eposta hesabınız ayarlanır – herhangi bir sağlayıcı, herhangi bir hesap. Yeni bilgisayarlar ve acemi eposta kullanıcıları için iyi;

Yazılım Kurulumu – Comodo ürünlerinin kurulumu ve en iyi koruma için özelleştirilmesi;

Yazıcı Ayarlanması ve Sorun Çözümü – Yazıcı sürücülerinin veya yazılımının güncellenmesi, mürekkep seviyesinin denetimi ve yazıcınızın kablolu veya kablosuz ağda çalışacak şekilde ayarlanması;

Yeşil PC – Bilgisayar kullanımınıza göre güç yönetim ayarlarının yapılandırılması sayesinde elektrik faturasından tasarruf edersiniz ve çevreyi korumuş olursunuz;

Bilgisayar sorunlarının Çözümü – Windows içindeki temel donanım çakışmalarının denetlenmesi.

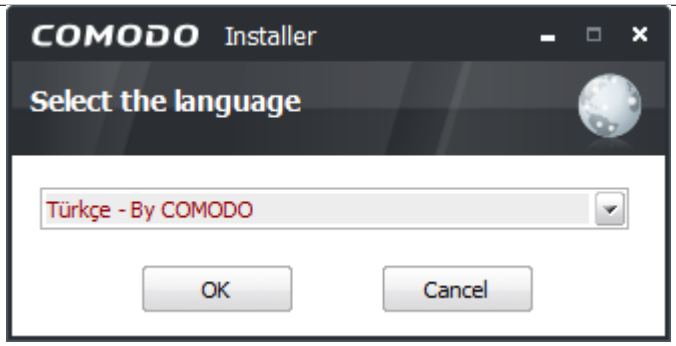
LivePCSupport hizmeti Comodo uzmanlarınca uzaktan bağlanılarak verilir. Daha fazla bilgi için Live PC support bölümüne bakın.

- **TrustConnect** - (Şifrelenmiş İnternet Vekil Sunucu Hizmeti). Trustconnect halka açık kablosuz ağlarda güvenli olarak gezinti yapmanızı sağlar.
- **10GB Çevrimiçi Depolama Alanı** – Comodo Backup ile verilerinizi Comodo'nun güvenli sunucularına yedekleyebilirsiniz. Veriler şifrelenir ve verilere internet bağlantısı olan herhangi bir bilgisayardan yalnızca kullanıcı tarafından erişilebilir (10GB yedek alanı).

Comodo Garanti - (Sisteminiz zararlı saldırısı sonucu zarar görürse ve Comodo uzmanları bu hasarı düzeltip sisteminizi çalışır duruma getiremezlerse Comodo sisteminizin düzeltilmesi için gerekli maliyeti karşılayacaktır. Ayrıntılar için Şartlar ve Koşullara bakınız.) Garanti yalnızca bilgisayarınız bazı ön koşulları sağlıyorsa etkinleştirilebilir. Sistemde zararlı olmamalı, belirli uygulamalar kurulu olmalı ve belirli CIS ayarları etkin olmalıdır. Bu ayarlar garanti etkinleştirilmesi işlemi sırasında sihirbaz tarafından test edilir ve etkinleştirilir. Daha fazla bilgi için 'Garanti Güvencesinin Etkinleştirilmesi' bölümüne bakın. Comodo Garanti yalnızca ABD'de ikamet edenler için mevcuttur.

DVD'yi yerleştirdikten sonra kurulum programı otomatik olarak başlayacaktır.

İpucu: Eğer kurulum otomatik olarak başlamazsa Başlat > Bilgisayarıma girin ve Windows Explorer penceresinden DVD sürücüsüne çift tıklayın.



'Dil seçin (Select the language)' diyaloğu görüntülenecektir.

Comodo İnternet Güvenliği çeşitli dillerde bulunmaktadır.

- **Comodo İnternet Güvenliği'nin kurulmasını istediğiniz dili açılır listeden seçip 'Tamam (OK)' düğmesine tıklayın**

Aşağıdaki pencere görünecektir.

Comodo Internet Security 2011 Complete Kur - Eğer henüz CIS kurmadıysanız ilk olarak 'Comodo Internet Security 2011 Complete Kur' seçmelisiniz.

- **Comodo Internet Security 2011 Complete kurulumu hakkında daha fazla bilgi için buraya tıklayın.**

Online Backup ve TrustConnect Etkinleştir – Çevrimiçi depolama alanınızın, TrustConnect hesabınızın ve Comodo Garanti'nizin etkinleştirilmesi işlemini başlatır. Lütfen başlamadan önce Lisans Anahtarınızı hazırlayın (Anahtarınız DVD üzerinde veya kutunun içinde yazılıdır). Geçerli bir anahtar girdikten sonra hesap kaydı işlemini başlatacak Comodo web-formuna yönlendirileceksiniz.

- **Hizmetlerin etkinleştirilmesi hakkında daha fazla için buraya tıklayın**

Online Backup Kur - Comodo BackUp kurulum işlemini başlatır. Kurulduktan sonra sabit veya ağ disklerinize yedeklerinizi zamanlayabileceksiniz. Ayrıca 10GB güvenli çevrimiçi yedek alanınız da olacak. (Comodo BackUp arayüzüne giriş adınızı ve parolanızı yazarak girebilirsiniz).

- **Comodo Backup kurulumu hakkında daha fazla bilgi için buraya tıklayın**
- **Comodo BackUp Kullanıcı Rehberini indirmek için buraya tıklayın**

TrustConnect Kur - Comodo TrustConnect kur işlemini başlatır. TrustConnect kullanımınızı https://accounts.comodo.com sayfasından hesabınıza giriş yaparak yönetilebilirsiniz.

- **TrustConnect hakkında daha fazla bilgi için buraya tıklayın**
- **Comodo TrustConnect kurulumu hakkında daha fazla bilgi için buraya tıklayın.**

Dragon Web Browser Kur - Dragon web tarayıcısını kurar. Dragon kullanıcı dostu web tarayıcısıdır.

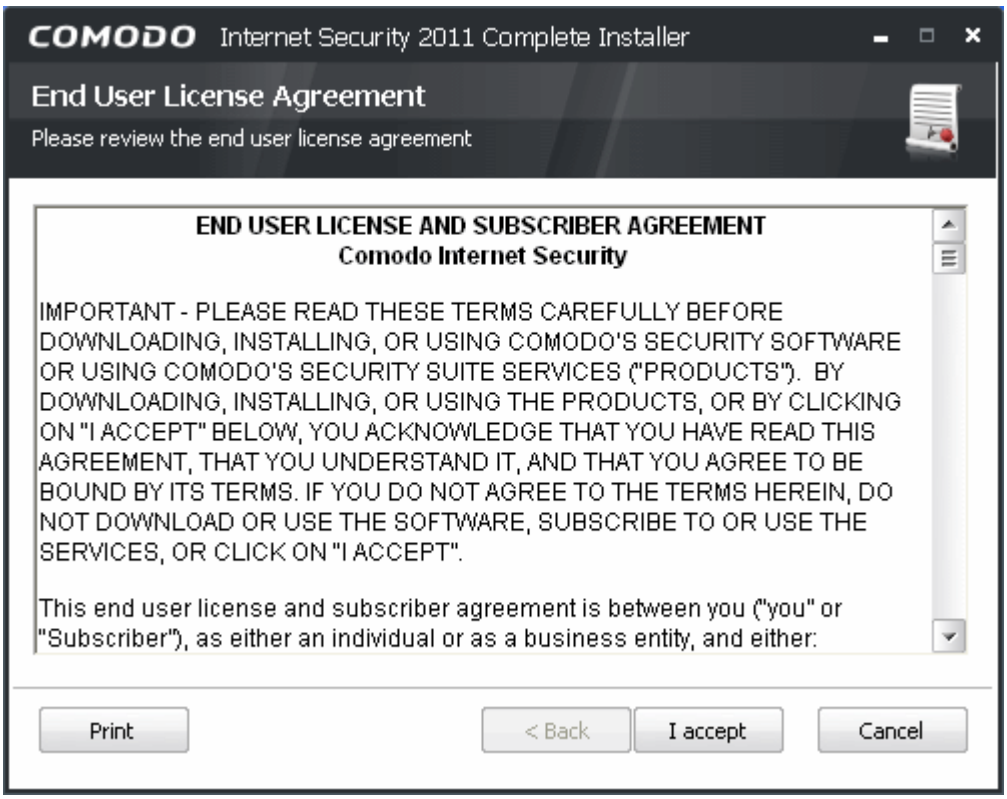
- **Dragon Web tarayıcı kurulumu hakkında daha fazla bilgi için buraya tıklayın**

1.3.3.1 Comodo Internet Security 2011 Complete ve Live PC Support Kurulumu

Ana ekrandan 'COMODO Internet Security 2011 Complete Kur' düğmesine tıklayarak kurulumu başlatın. CIS 2011 ve Live PC Support kurulum sihirbazı başlayacaktır.

ADIM 1 – Son Kullanıcı Lisans Sözleşmesi

Son Kullanıcı Lisans Sözleşmesi diyaloğu görünecektir.



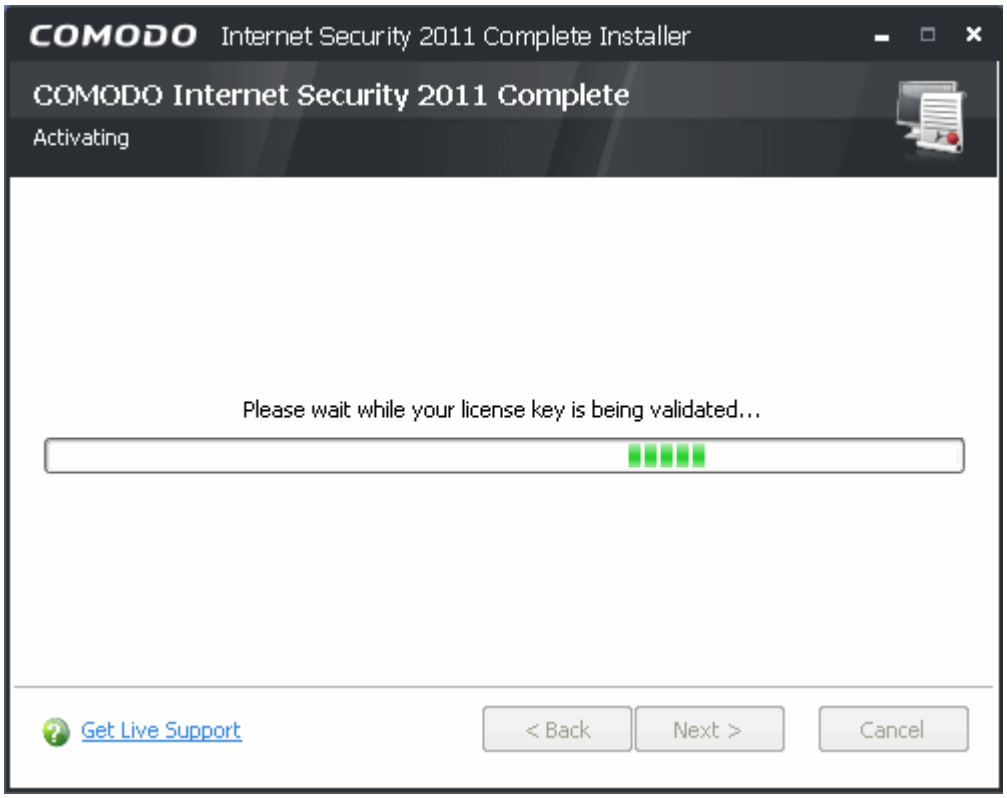
Kuruluma devam edebilmek için, Son Kullanıcı Lisans Sözleşmesini (EULA) okumalı sonra kabul etmelisiniz. Kuruluma devam etmek için 'Kabul ediyorum', bu aşamada kurulumdan çıkmak için 'İptal' düğmesine tıklamalısınız.

ADIM 2 – Lisansınızın Doğrulanması

Sonraki adım Lisans anahtarının girilmesidir. Anahtarınız paketin içinde yazılıdır.

İpucu: Kurulum sırasında anahtarınız yoksa bu adımı anahtar girmeden 'İleri' düğmesine tıklayarak geçebilirsiniz. Aboneliğiniz ve garantinizi daha sonra ana arayüzden etkinleştirebilirsiniz. Daha fazla bilgi için 'CIS Pro ve CIS Complete Hizmetlerinin Kurulumdan Sonra Etkinleştirilmesi' bölümüne bakabilirsiniz.

Anahtarı tam olarak girin ve 'İleri' düğmesine tıklayın. Lisans anahtarınız doğrulanacaktır.



Lisansınız doğrulandıktan sonra lisansınızın size sağladığı hakları içeren son bir onay ekranı çıkacaktır:

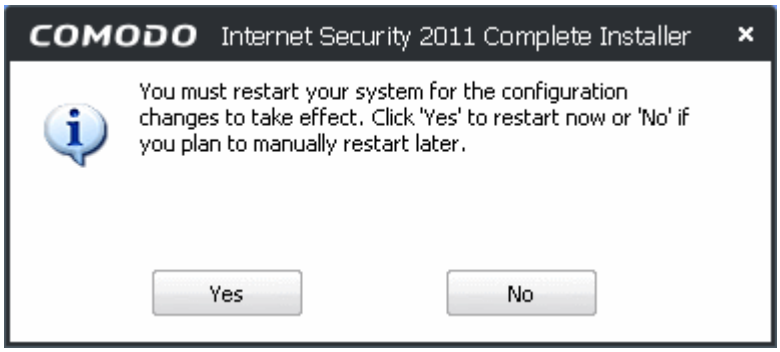
'İleri' düğmesine tıklayın.

ADIM 3 –Kurulum İlerleyişi

Paketler çıkartılacaktır...

... ve kurulacaktır. Kurulum ilerleyişi görüntülenecektir.

Başarılı kurulumdan sonra kurulumun etkili olabilmesi için yeniden başlatma onay diyaloğu görüntülenecektir.

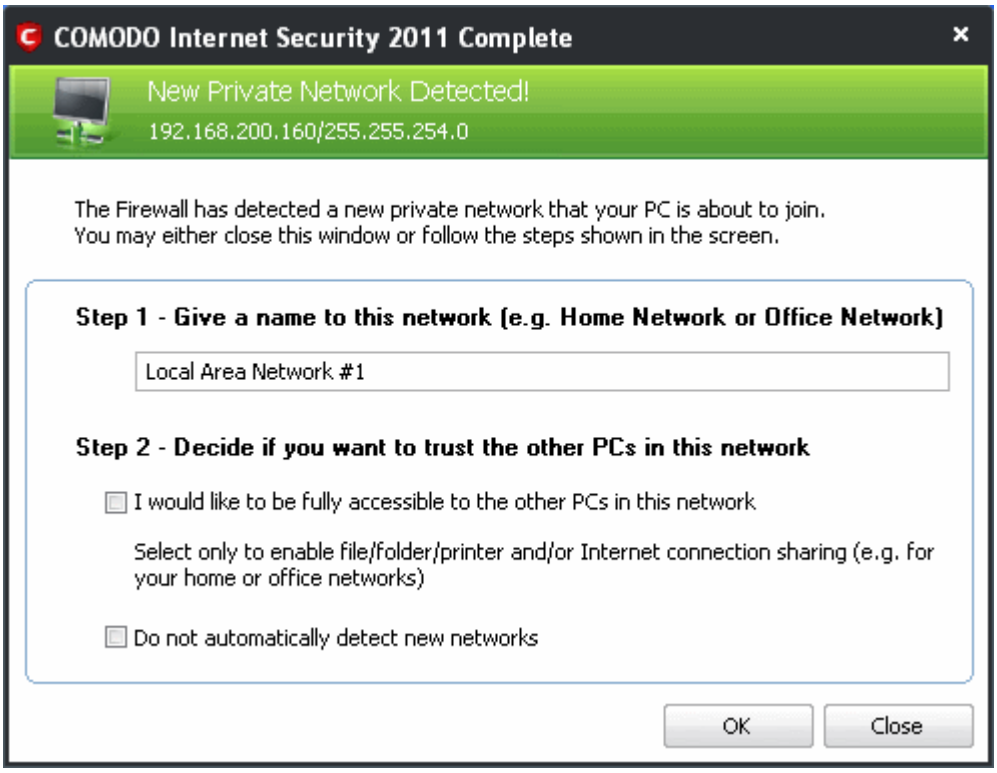


Kaydedilmemiş tüm verilerinizi kaydedin ve 'Evet' düğmesine tıklayarak sisteminizi yeniden başlatın. Daha sonra kendiniz yeniden başlatmak istiyorsanız 'Hayır' düğmesine tıklayın.

Not: Kurulum yalnızca sistem yeniden başlatıldıktan sonra etkili olacaktır.

ADIM 4 - Sisteminiz Yeniden Başladıktan Sonra

Sistem yeniden başladıktan sonra, eğer bilgisayarınız bir ağa bağlıysa 'Yeni Özel Ağ Saptandı' diyaloğu belirecektir ve yapılandırmanız istenecektir:



Adım 1: İnternete bağlanmak için tek bilgisayarlı ev kullanıcılarının bile ev ağı yapılandırması gereklidir. (Ağ bağlantınızın adı Adım 1'de metin alanında görünür). Çoğu kullanıcı bu adı kabul edebilir.

Adım 2: Bu ağdaki diğer bilgisayarlardan gelen bağlantıları kabul etmek istiyorsanız (örn. Çalışma veya Ev Ağı) veya yazıcı paylaşımı için 'Bu ağdaki diğer bilgisayarlar tarafından tamamen görünür olmak istiyorum' seçeneği işaretleyin. Bu ağ daha sonra güvenli ağ olur. Tek bilgisayarlı ev kullanıcıları bu seçeneği seçmekten kaçınmalıdırlar.

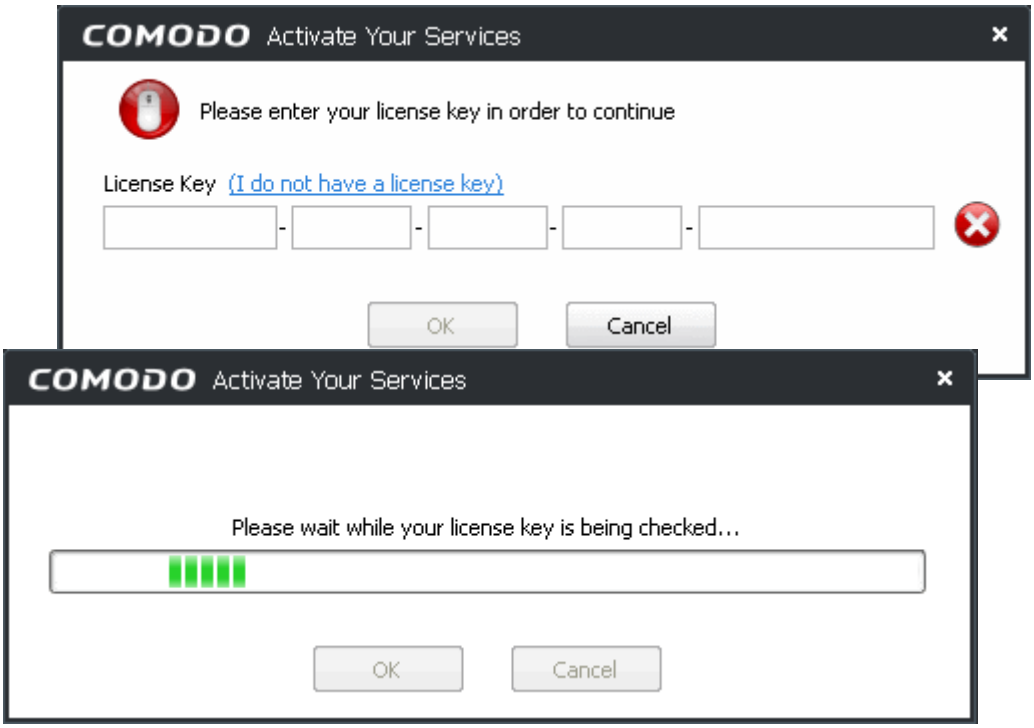
Tecrübeli bir kullanıcıysanız 'Yeni ağlar otomatik olarak saptanmasın' seçeneğini işaretleyerek gerektiğinde elle güvenli ağlar oluşturabilirsiniz. (Bunu 'Ağ Bölgelerinden' ve 'Port Gizleme Sihirbazı' aracılığıyla yapabilirsiniz)

Seçiminizi 'Tamam' düğmesine tıklayarak onaylamalısınız. Eğer 'Hayır' düğmesine tıklarsanız tüm ağ bağlantıları engellenecektir.

1.3.3.2 Online Backup, TrustConnect Hizmetleri ve Garanti Etkinleştirilmesi

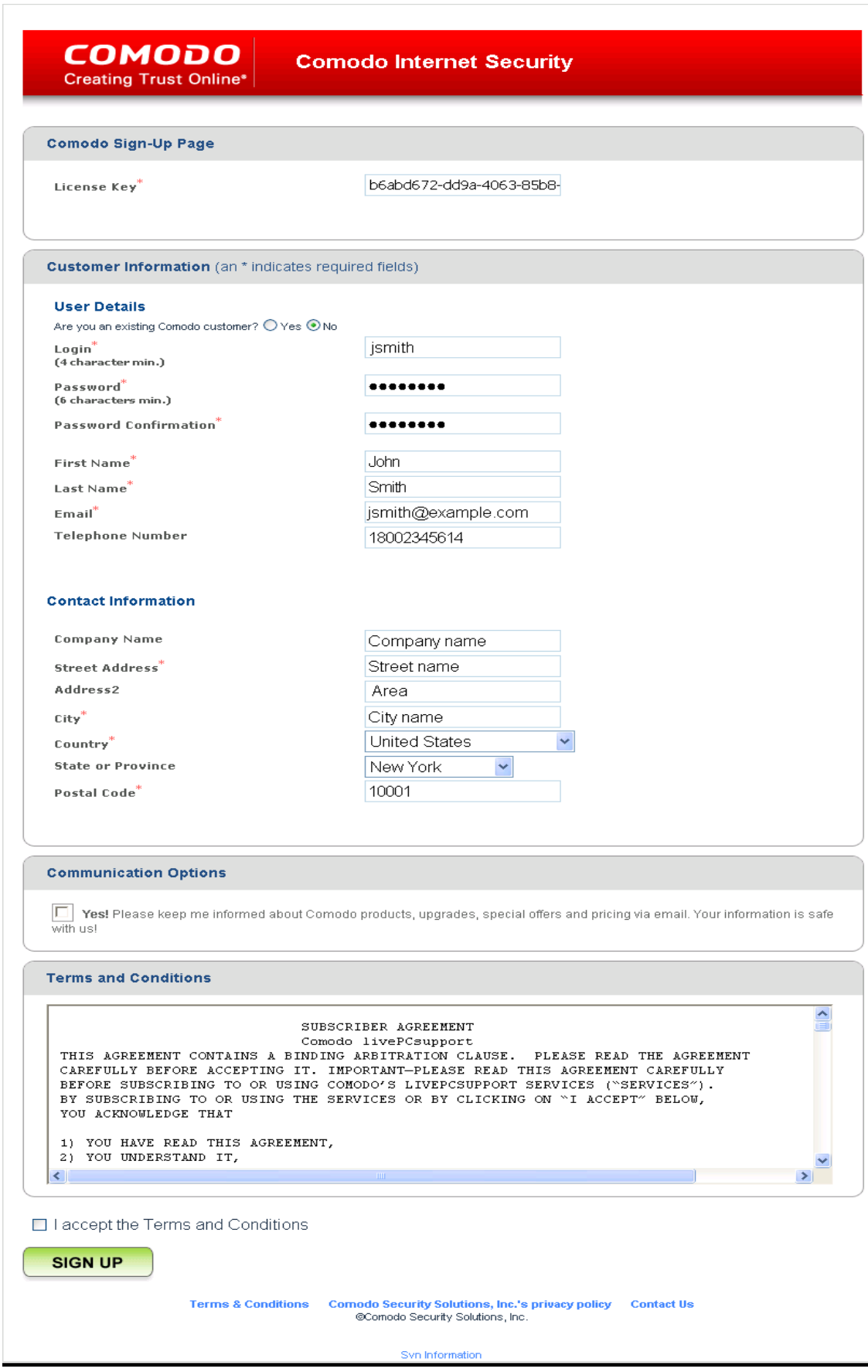
10GB çevrimiçi depolama alanından ve TrustConnect hizmetlerinden yararlanabilmek için hizmetleri etkinleştirmelisiniz. Bu işlemi başlatmadan önce anahtarınızı hazırlayın.

•DVD'yi yeniden takın ve Comodo Internet Security 2011 Complete ana ekranından 'Online Backup ve TrustConnect Etkinleştir' düğmesine tıklayın. Sunulan alana lisans anahtarınızı girmeniz istenecektir.



•CIS ürünüyle sağlanan lisans anahtarını girin. Lisans anahtarı doğrulanacaktır.

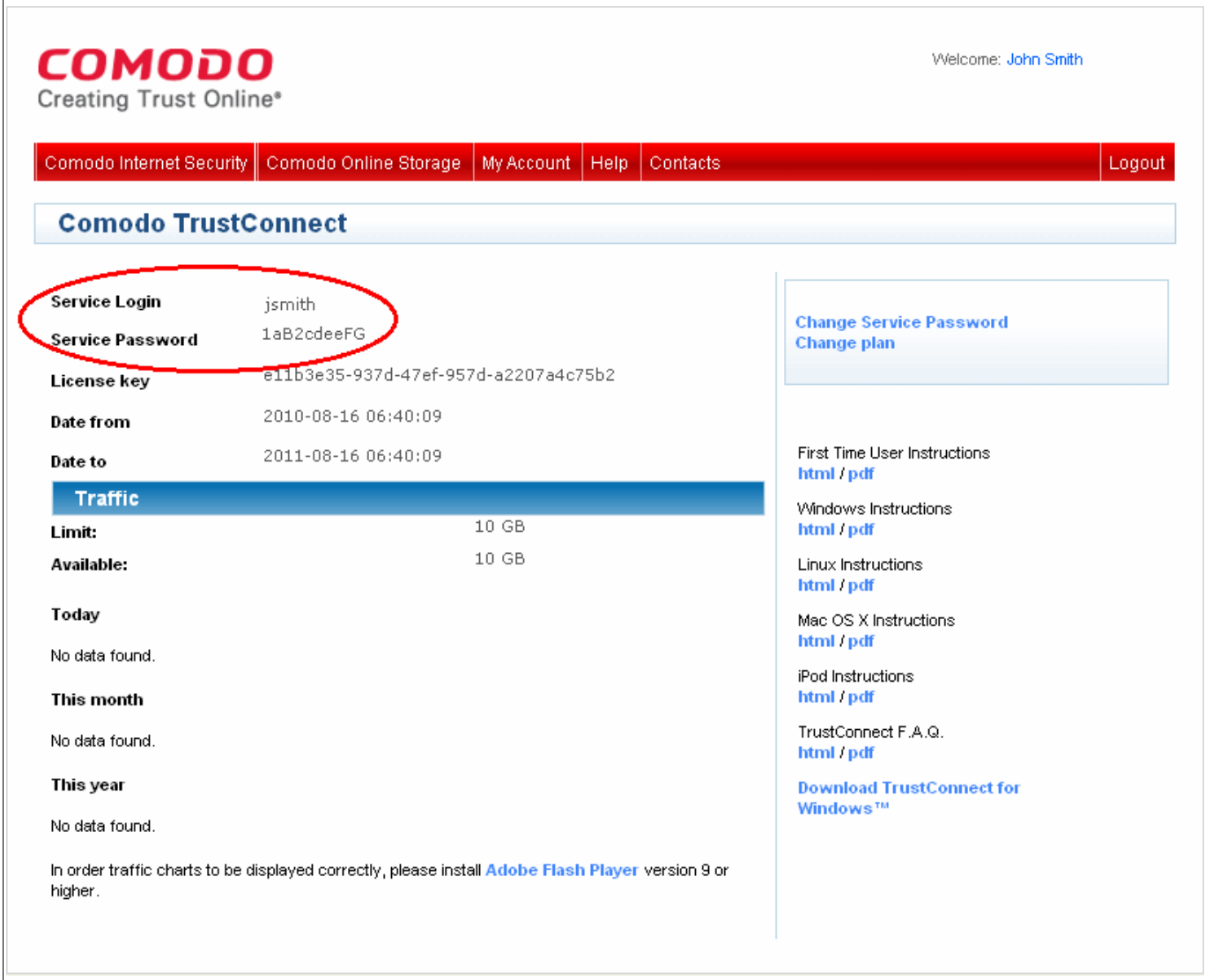
Lisans anahtarı doğrulandıktan sonra Comodo Kayıt Sayfası görüntülenecektir.


COMODO
Creating Trust Online®
Comodo Internet Security
Comodo Sign-Up Page
License Key*
b6abd672-dd9a-4063-85b8-
Customer Information (an * indicates required fields)
User Details
Are you an existing Comodo customer? Yes No
Login* (4 character min.)
jsmith
Password* (6 characters min.)
Password Confirmation*
First Name*
John
Last Name*
Smith
Email*
jsmith@example.com
Telephone Number
18002345614
Contact Information
Company Name
Company name
Street Address*
Street name
Address2
Area
City*
City name
Country*
United States
State or Province
New York
Postal Code*
10001
Communication Options
Yes! Please keep me informed about Comodo products, upgrades, special offers and pricing via email. Your information is safe with us!
Terms and Conditions
SUBSCRIBER AGREEMENT
Comodo livePCsupport
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT
CAREFULLY BEFORE ACCEPTING IT. IMPORTANT—PLEASE READ THIS AGREEMENT CAREFULLY
BEFORE SUBSCRIBING TO OR USING COMODO'S LIVEPCSUPPORT SERVICES ("SERVICES").
BY SUBSCRIBING TO OR USING THE SERVICES OR BY CLICKING ON "I ACCEPT" BELOW,
YOU ACKNOWLEDGE THAT
1) YOU HAVE READ THIS AGREEMENT,
2) YOU UNDERSTAND IT,
I accept the Terms and Conditions
SIGN UP
Terms & Conditions
Comodo Security Solutions, Inc.'s privacy policy
Contact Us
©Comodo Security Solutions, Inc.
Svn Information

Gerekli alanlara bilgilerinizi girin ve ‘Sign Up’ düğmesine ‘I accept the Terms and Conditions’ kutusunu işaretledikten sonra tıklayın. Sipariş Onayı sayfası görüntülenecektir. Hizmeti etkinleştirmek için ‘Confirm’ düğmesine tıklayın.

'Confirm' düğmesi sizin için oluşturulan faturayı görüntüler. Fatura kayıt olurken girdiğiniz bilgileri, sipariş ettiğiniz ürünleri, yazılımları indirmek için gerekli bağlantıları, lisans anahtarınızı ve diğer giriş bilgilerinizi görüntüler.

Kayıt sırasında girdiğiniz giriş bilgilerini kullanarak https://accounts.comodo.com adresinden hesabınıza giriş yapabilirsiniz.



•Bu bilgiler TrustConnect Hizmetlerini kullanmak için gereklidir. Daha fazla bilgi için TrustConnect Tanıtımı bölümüne bakın.

•Bu sayfadaki hizmete giriş bilgilerinizi (giriş ve parola) bir yere not ediniz.

•Çevrimiçi Depolama Hizmetlerini kullanmak için de aynı bilgileri kullanabilirsiniz. Daha fazla bilgi için Çevrimiçi Depolama Alanını Kullanmaya Başlayın bölümüne bakın.

1.3.3.3 Comodo Backup Kurulumu

Dosyalarınızı çevrimiçi yedekleyebilmek için Comodo Backup uygulaması sisteminizde kurulu olmalıdır.

Comodo Backup kurulumu için

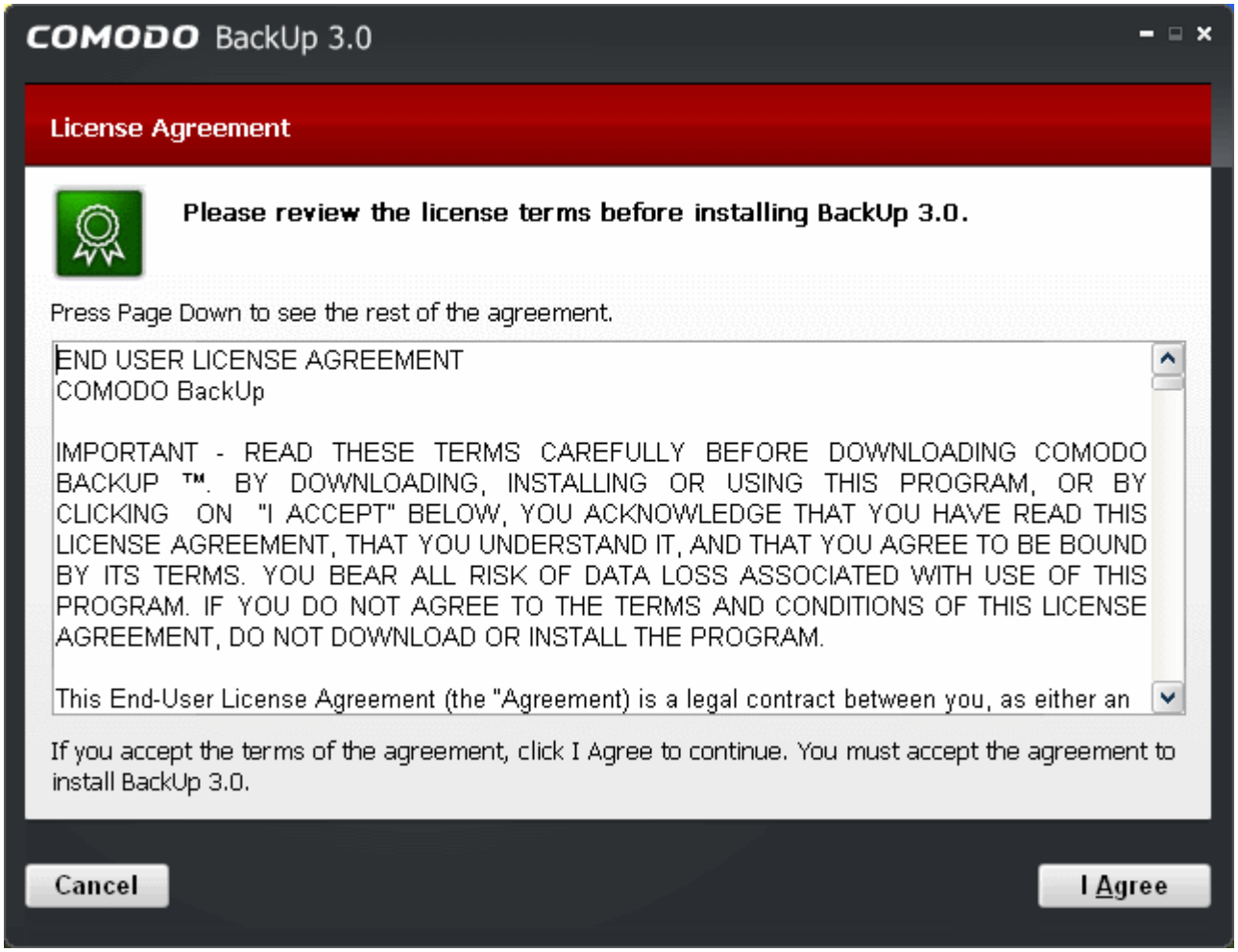
•DVD'yi yeniden takın ve Comodo Internet Security 2011 Complete ana ekranından 'Online Backup Kur' düğmesine tıklayın. Kurulum hemen başlayacaktır.

Adım 1 – Arayüz Dilinin Seçimi

Kurulum dili seçme diyaloğu görüntülenecektir. Comodo Online BackUp farklı dillerde mevcuttur.

Adım 2 – Son Kullanıcı Lisans Sözleşmesi

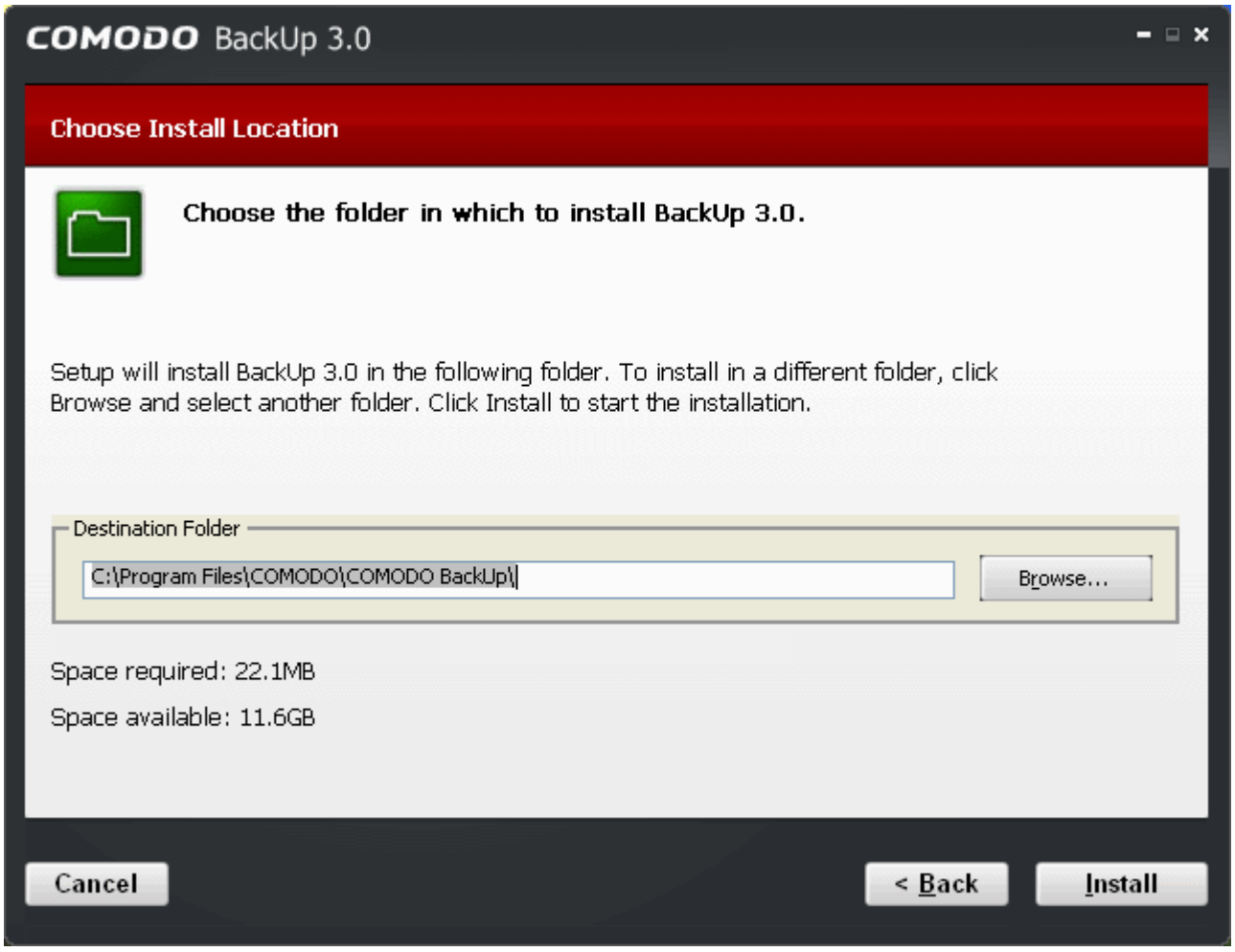
Başlangıç aşamasını tamamlamak için sözleşmeyi okuyup onaylayın.



- **Kuruluma devam etmek için 'Kabul Ediyorum' düğmesine tıklayın. Eğer kurulumu iptal etmek isterseniz 'İptal' düğmesine tıklayın.**

Adım 3 – Kurulum Klasörünün Seçimi

Sonraki ekranda kurulum klasörünü seçmenize izin verilecektir. Varsayılan yol *C:\Program Files\Comodo\Comodo BackUp.*

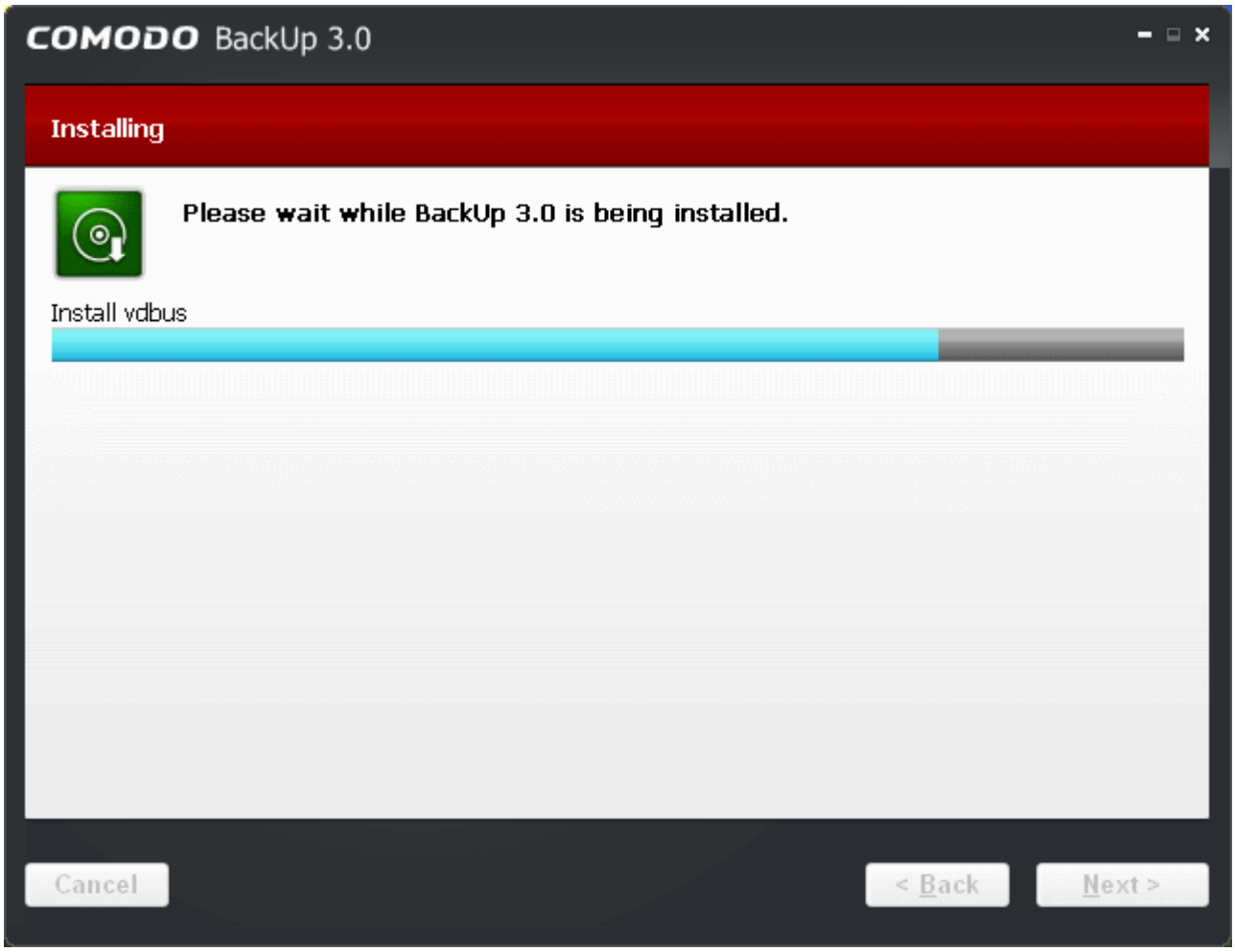


Uygulamayı farklı bir konuma yüklemek isterseniz 'Göz At' düğmesine tıklayarak farklı bir konum seçebilirsiniz.

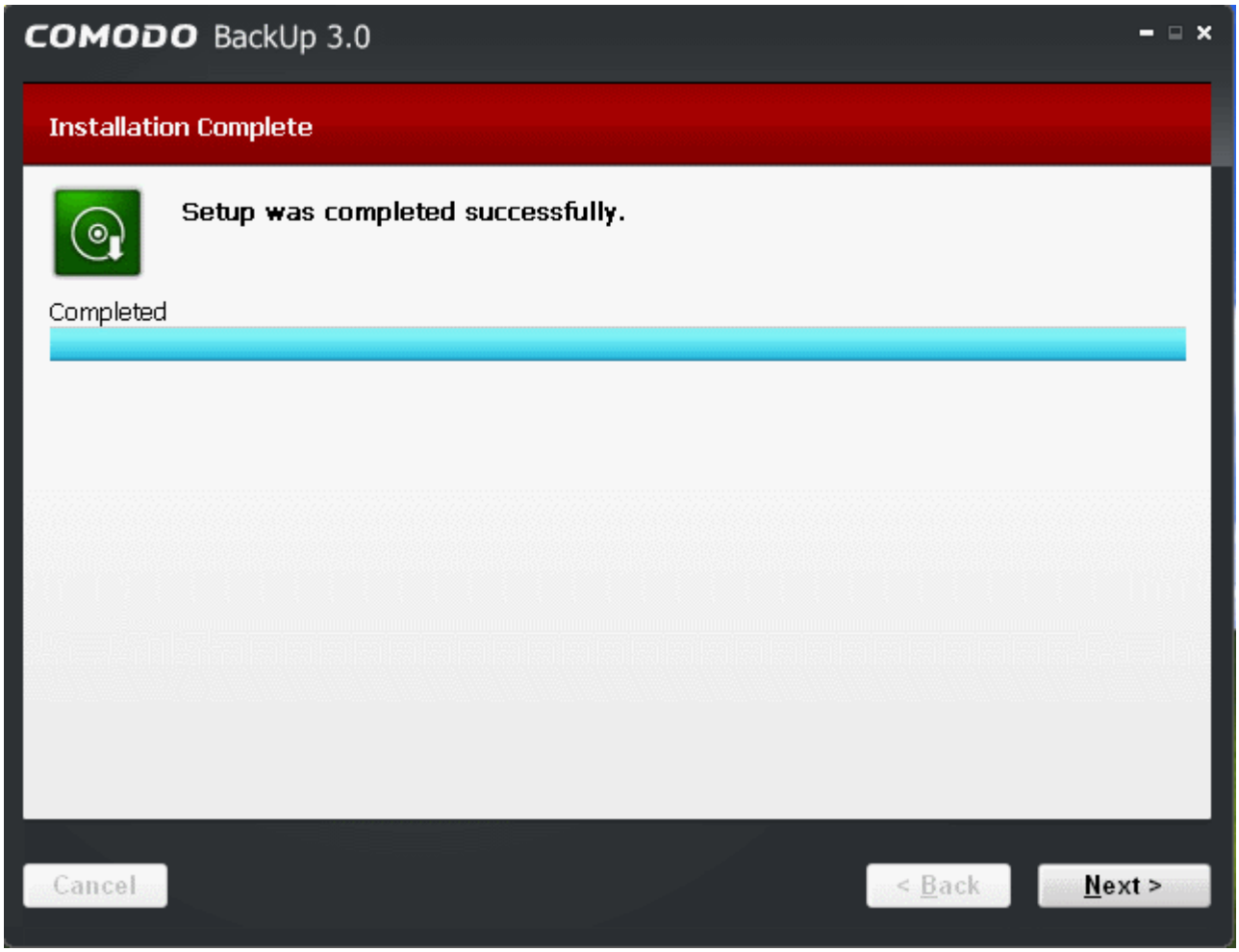
- **'Geri' düğmesine tıklayarak önceden belirlediğiniz ayarları gözden geçirebilir / değiştirebilirsiniz. Kurulum işlemine devam etmek için 'Kur' düğmesine tıklayın.**

Adım 4 – Kurulum İlerleyişi

Kurulum durum diyaloğu görüntülenecektir.



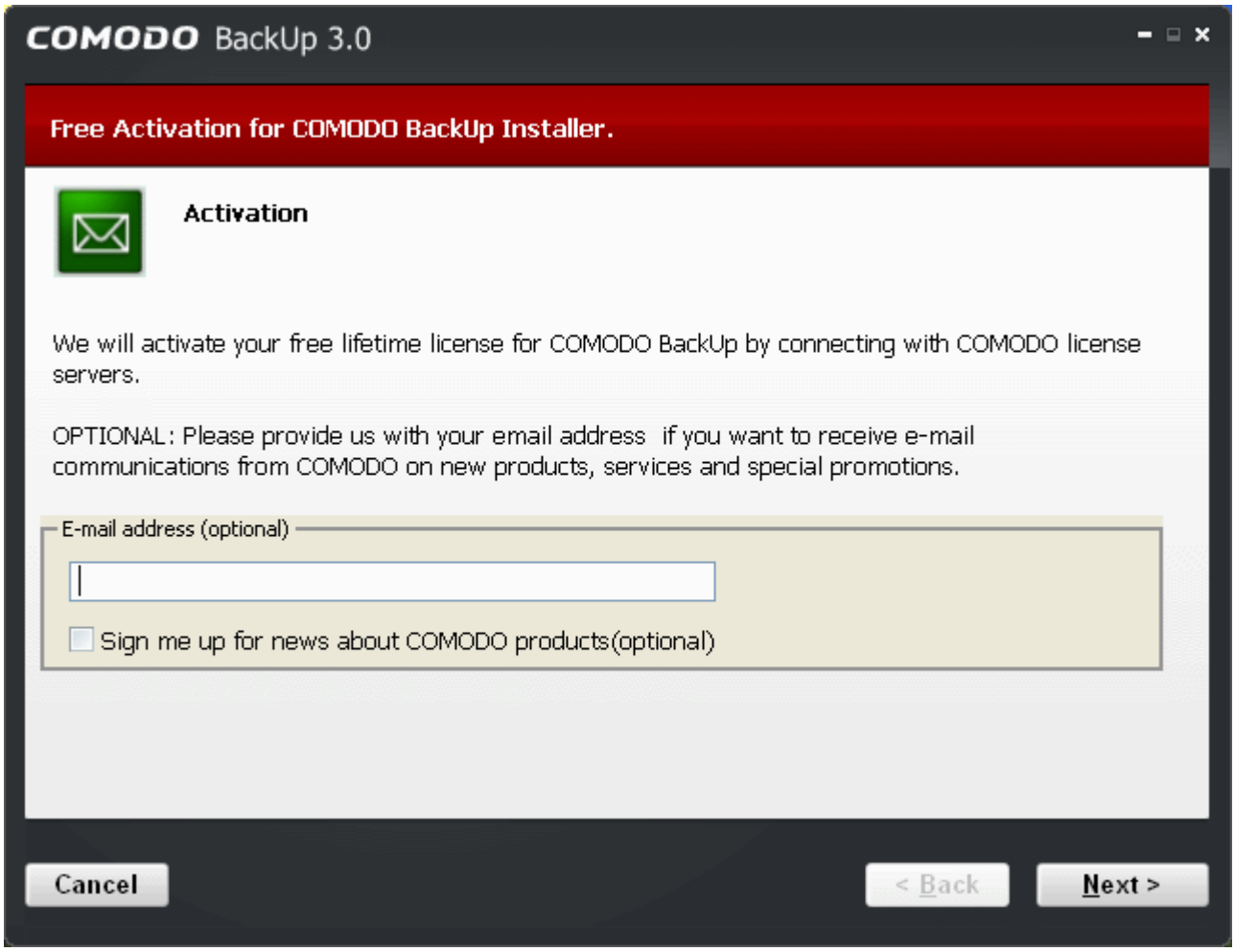
Tamamlandıktan sonra ‘Kurulum Tamamlandı’ diyaloğu görüntülenecektir.



Devam etmek için 'İleri' düğmesine tıklayın.

Adım 5 – Ürünün Etkinleştirilmesi

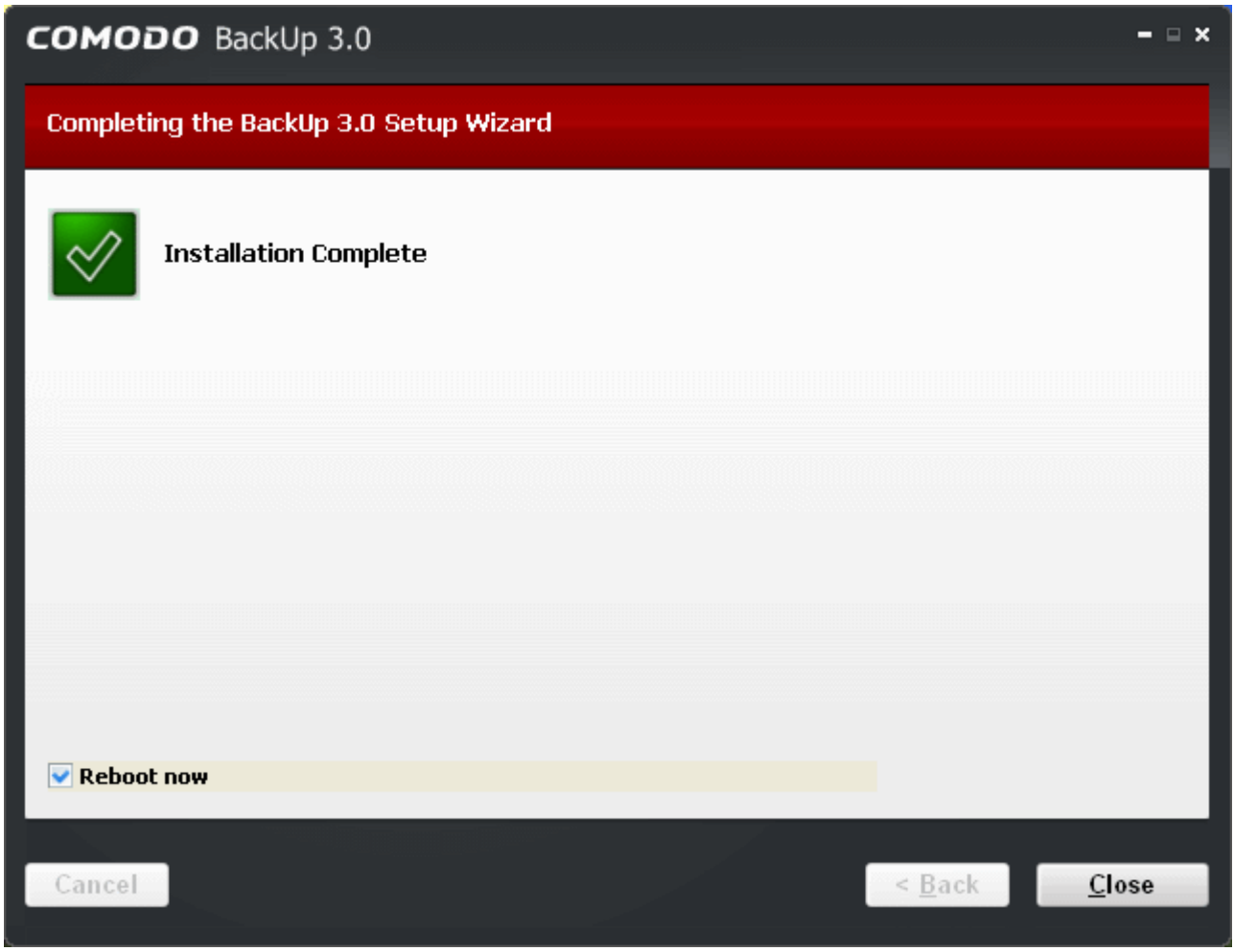
Kurulum tamamlandıktan sonra ürün Etkinleştirme diyaloğu görüntülenecektir. Comodo BackUp yazılımı ömür boyu kullanım için etkinleştirilecektir. Comodo ürünleri hakkında haberlere kaydolmak isterseniz eposta adresinizi çıkan alana girip **'Sign me up for news about Comodo products'** seçin.



Bu seçime bağlıdır. 'İleri' tıklayın.

Adım 6 – Kurulumun Tamamlanması

Başarılı kurulumdan sonra onay diyaloğu görüntülenecektir. Kurulumun etkili olabilmesi için bilgisayarınızın yeniden başlatılması gerekmektedir.

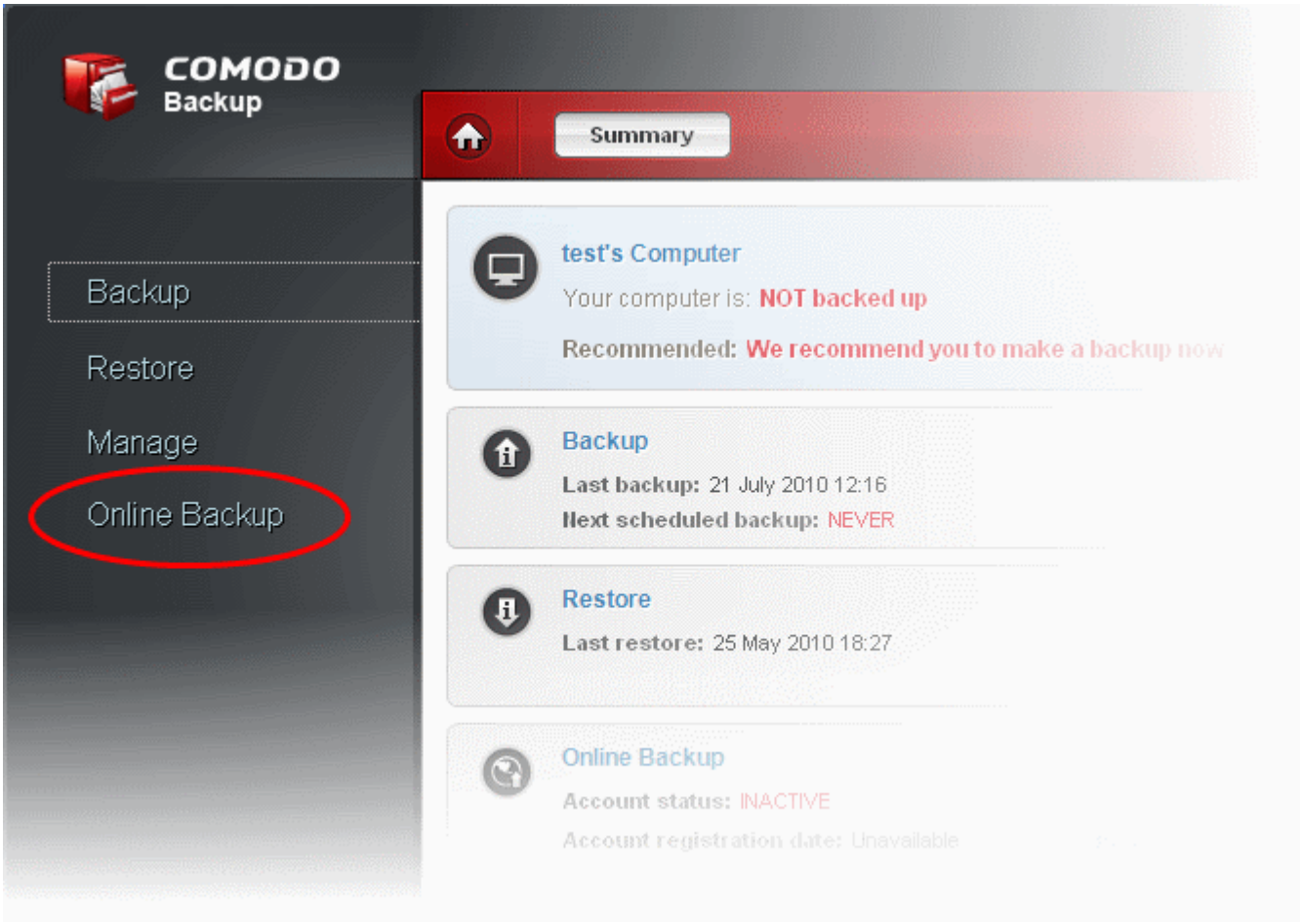


Lütfen kaydedilmemiş verilerinizi kaydedin, 'Reboot now' kutusu seçili kalsın ve ‘Close’ düğmesine tıklayın. Eğer sistemi sonradan elle yeniden başlatmak istiyorsanız 'Reboot now' kutusundan işareti kaldırın ve 'Close' düğmesine tıklayın.

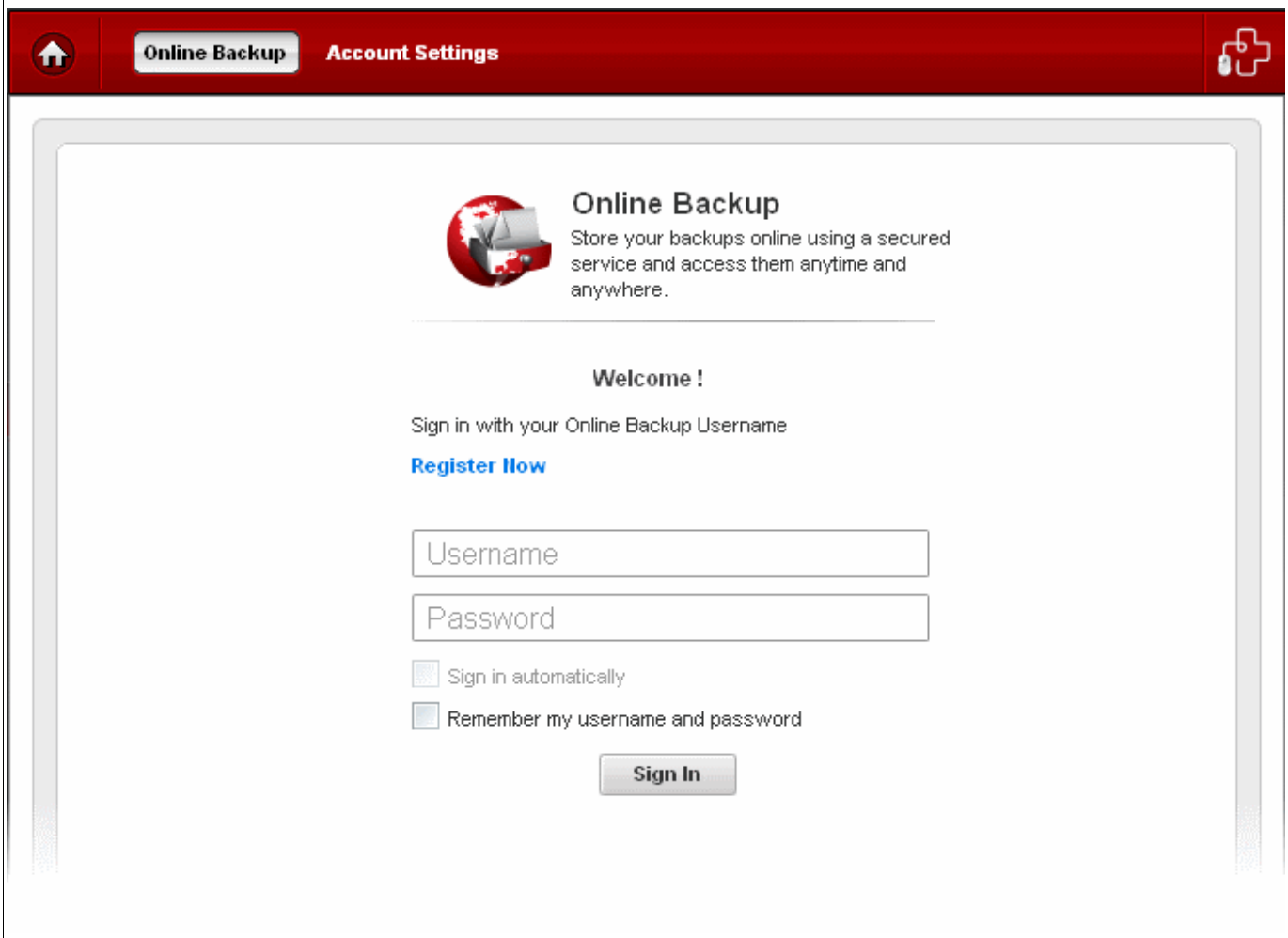
Not: Kurulum yalnızca bilgisayar yeniden başladıktan sonra etkili olacaktır.

Çevrimiçi Depolama Alanınızı Kullanmaya Başlayın

Comodo Backup’ın başarılı kurulumundan sonra uygulamayı başlatın ve soldaki menüden Online Storage bölümüne tıklayın.

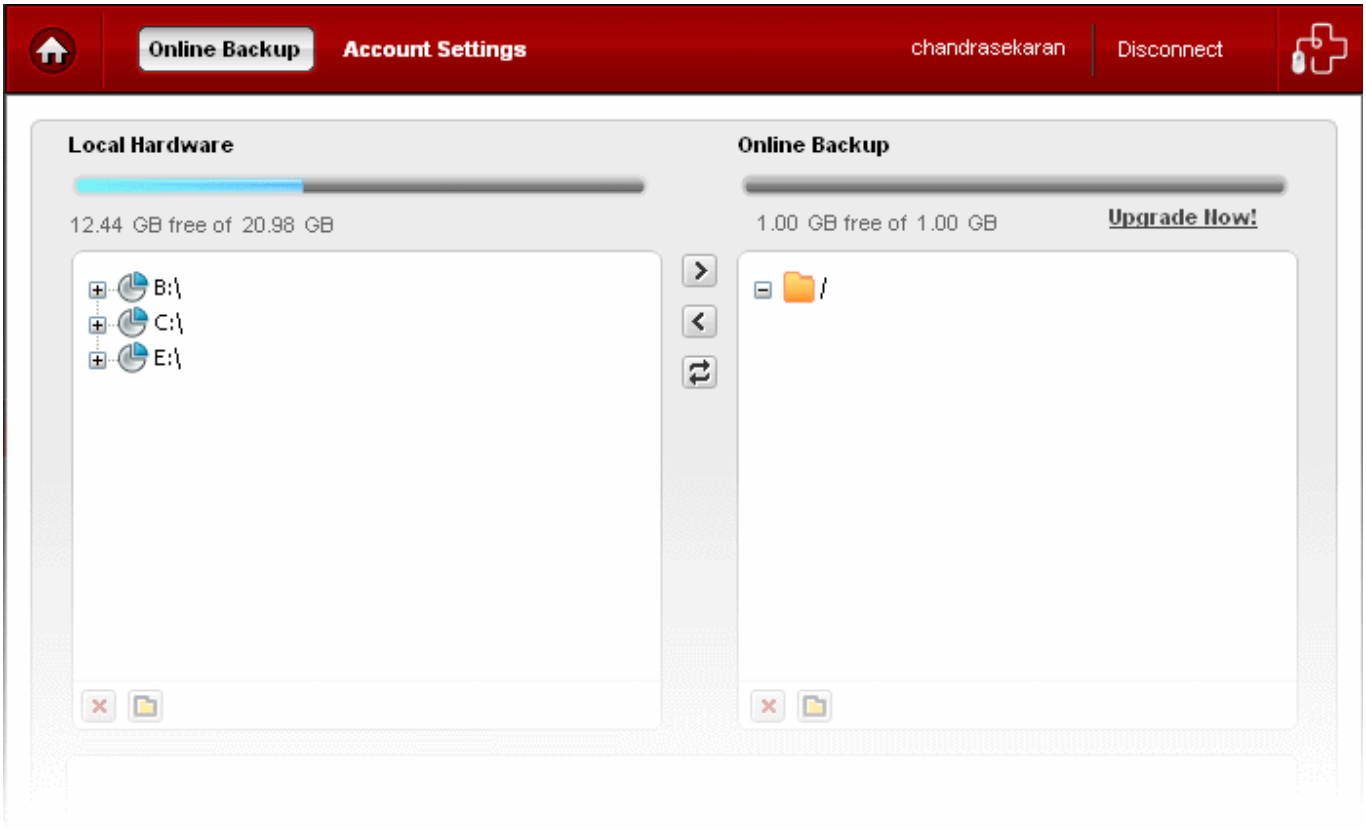


Online Backup arayüzü açılacaktır.



•Giriş adınızı ve parolanızı girip Sign In düğmesine tıklayın.

Başarılı giriş sonrasında kullanıcı adınız sekme bölümünde, sol panelde yerel dosya ve klasörleriniz ve sağ panelde çevrimiçi yedek alanınızdaki dosya ve klasörleriniz görünecektir. Bu paneller arasında dosya ve klasörlerinizi sürükleyip bırakabilirsiniz.



Daha fazla bilgi için http://backup.comodo.com/comodo_backup_user_manual.pdf adresindeki Comodo Backup Userguide dosyasına bakın.

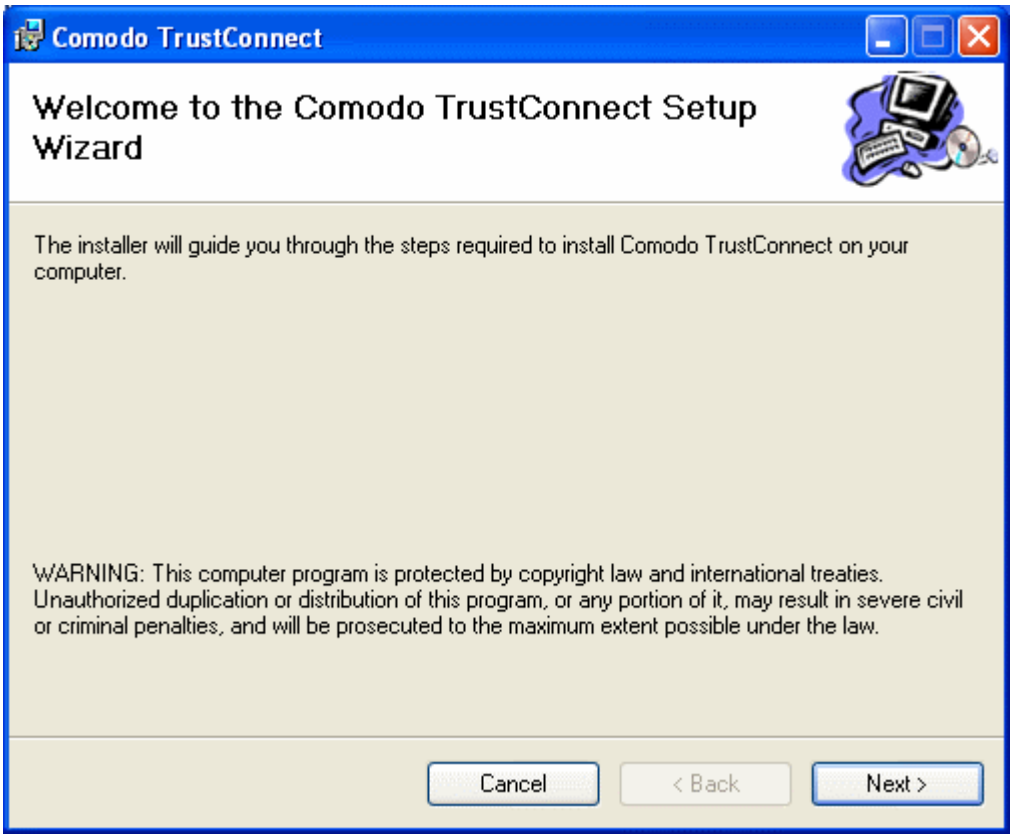
1.3.3.4 Comodo TrustConnect Kurulumu

Trustconnect halka açık kablosuz ağlarda güvenli olarak gezinti yapmanızı sağlar. Uygulamayı kurmak ve etkinleştirmek için lütfen ağağıdaki talimatları takip ediniz:

•Comodo Internet Security 2011 Pro/Complete kurucu ekranından 'TrustConnect Kur' düğmesine tıklayın. Comodo TrustConnect kurulum sihirbazı hemen başlayacaktır.

Adım 1 – Hoş Geldiniz Ekranı

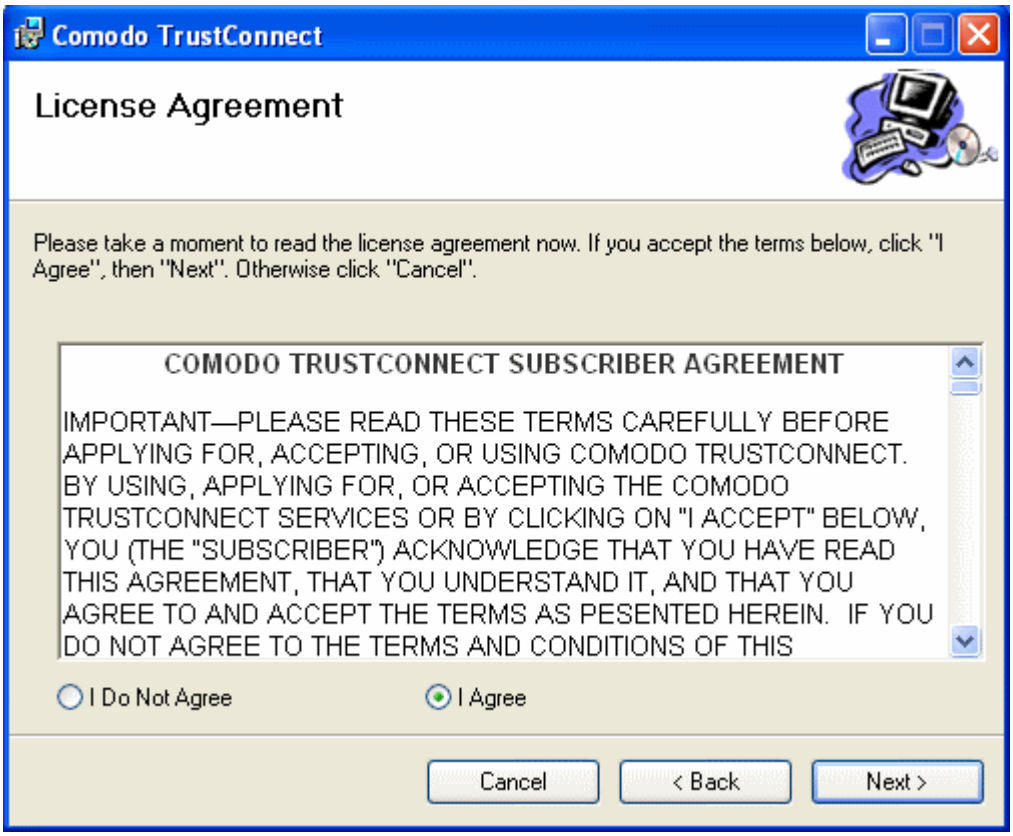
Hoş geldiniz ekranı görünecektir.



Devam etmek için 'İleri' düğmesine tıklayın.

Adım 2 – Abone Lisans Sözleşmesi

Lisans Sözleşmesini okuyup kabul ederek başlangıç aşamasını geçin.



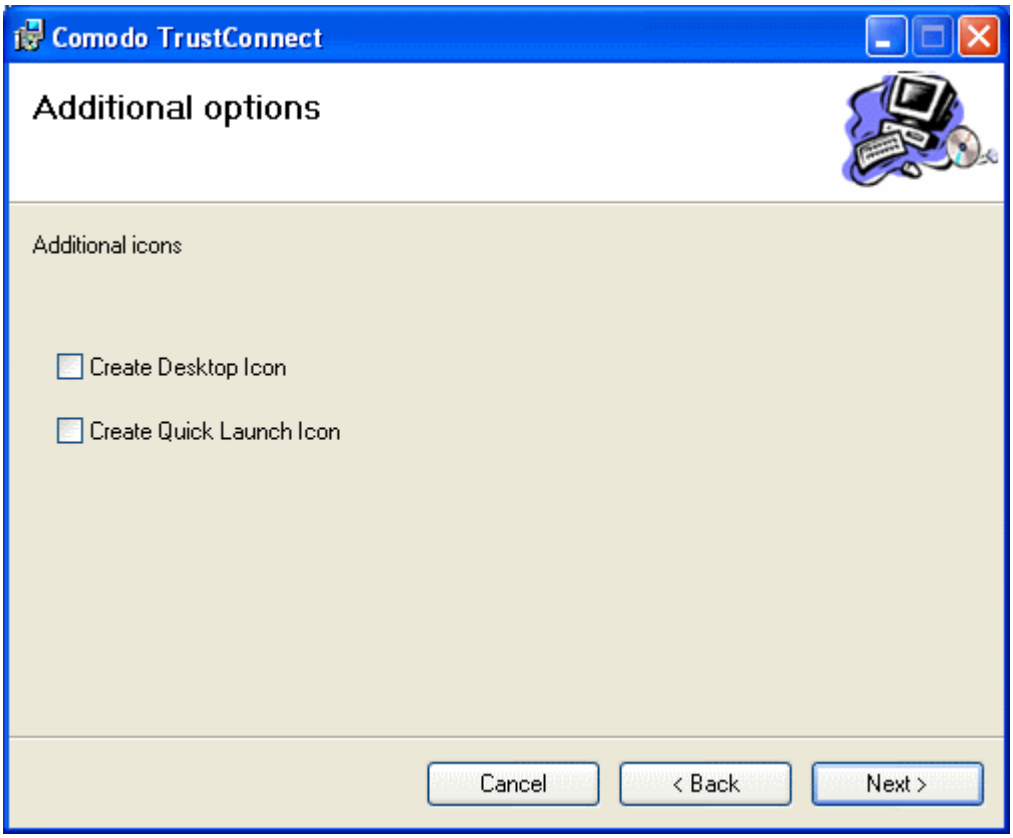
•Kuruluma devam etmek için 'I Agree' seçin.

•Kurulumdan çıkmak için 'I Do Not Agree' seçin.

Devam etmek için 'İleri' düğmesine tıklayın.

Adım 3 – Ek Seçenekler

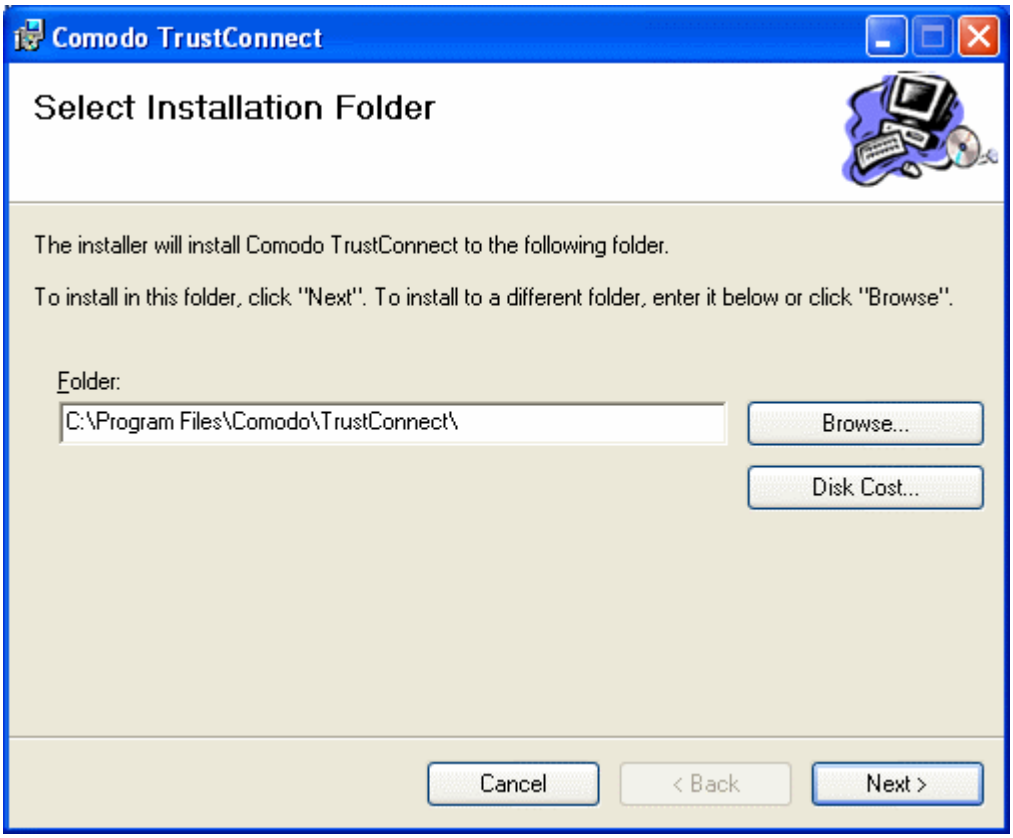
Sonraki adımda TrustConnect Masaüstü simgesini ve TrustConnect hızlı başlat simgesini seçebilirsiniz.



Seçiminizi yapın ve 'İleri' düğmesine tıklayın.

Adım 4 – Kurulum Klasörünün Seçimi

Sonraki ekrandan Comodo TrustConnect kurulum klasörünü seçebilirsiniz. Varsayılan yol *C:\Program Files\Comodo\TrustConnect.*

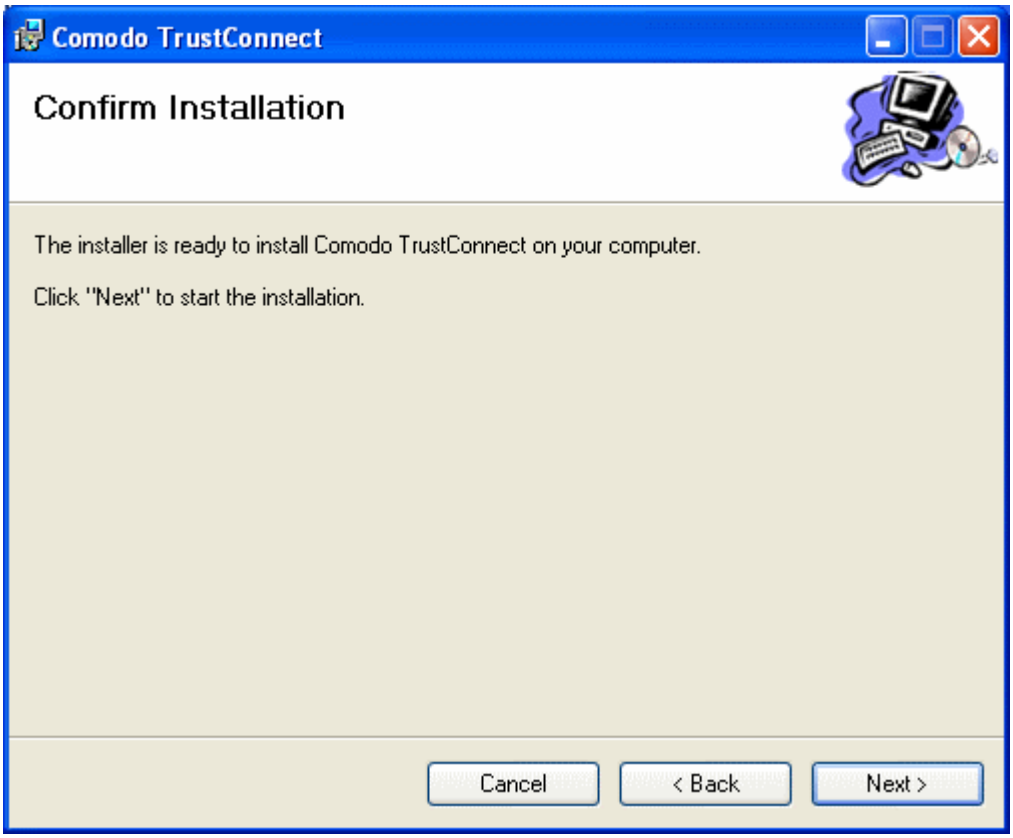


Eğer farklı bir konuma kurulum yapmak istiyorsanız 'Browse' düğmesine tıklayarak farklı bir konum seçin. Devam etmek için 'İleri' tıklayın.

.

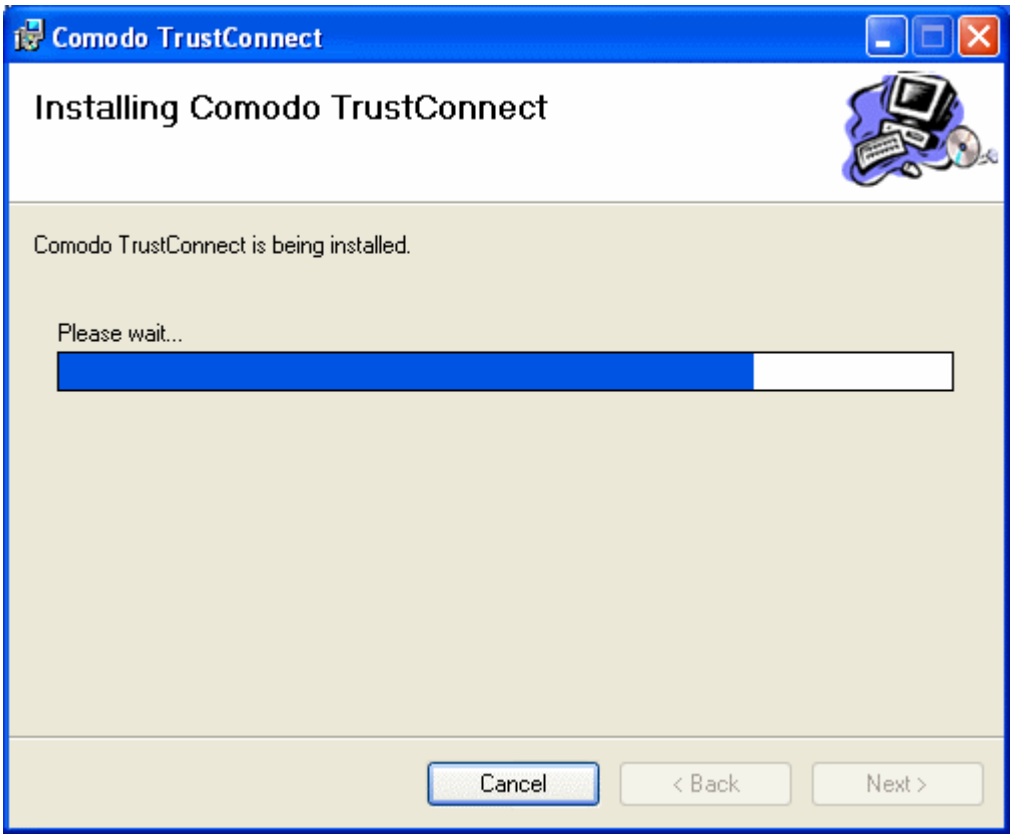
Adım 5 – Kurulum İlerleyişi

Yapılandırma seçeneklerini tamamladıktan sonra kurucu sihirbaz size kurulum işlemini başlatma onayını soracaktır.

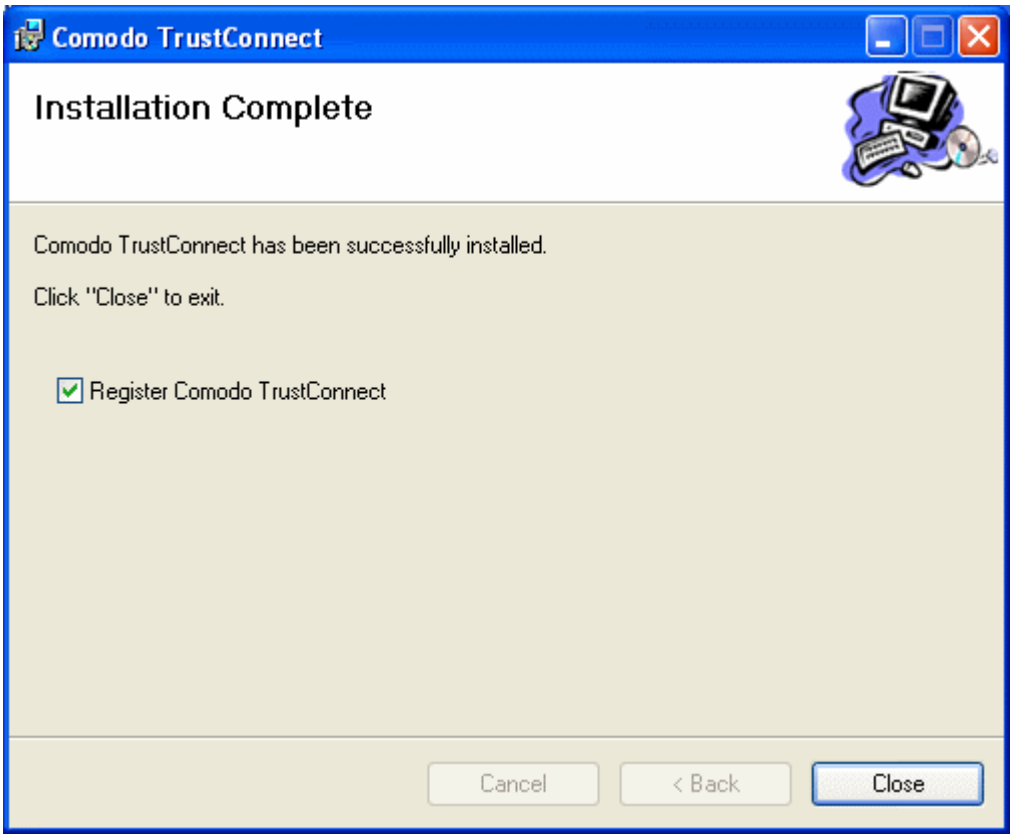


Önceden belirlediğiniz ayarların herhangi birini gözden geçirmek ve/veya değiştirmek için 'Geri' düğmesine tıklayın. Kuruluma başlamak için ise 'Kur' düğmesine tıklayın.

Kurulum ilerleyişi görüntülenecektir...

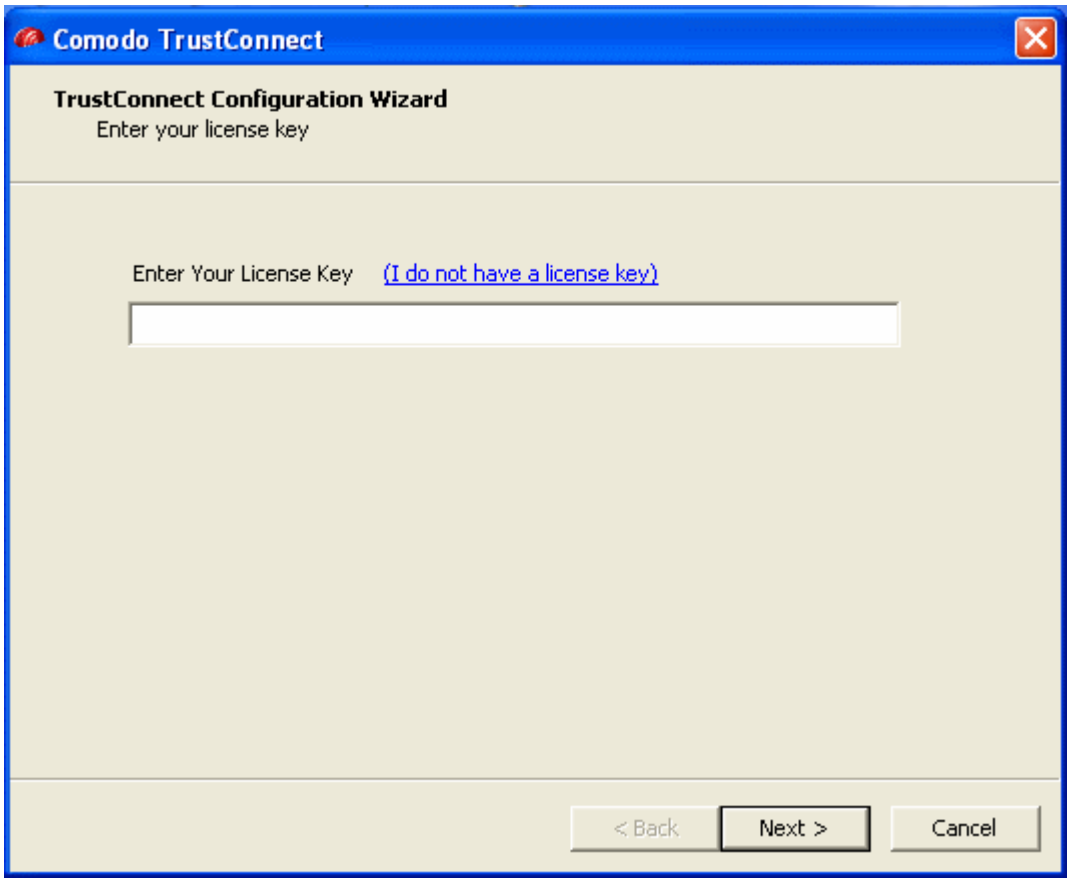


...ve tamamlandıktan sonra tamamlandı diyaloğu görüntülenecektir.



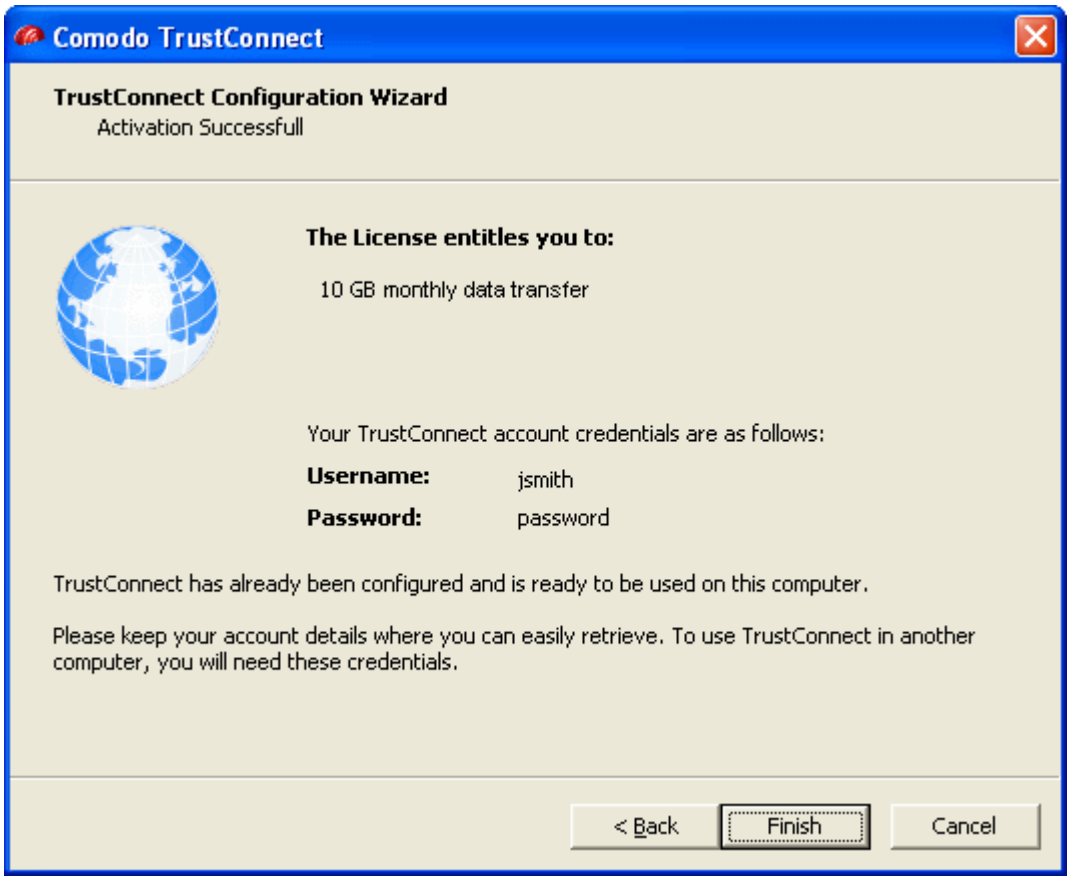
•TrustConnect hizmeti kaydını Online Backup ve TrustConnect etkinleştir üzerinden yaptıysanız, 'Register Comodo TrustConnect' kutusundaki işareti kaldırın ve Close düğmesine tıklayın. Kurulum tamamlanacaktır.

•TrustConnect hizmeti kaydını Online Backup ve TrustConnect etkinleştir üzerinden yapmadıysanız, Register Comodo TrustConnect kutusundaki işareti kaldırmayın ve Close düğmesine tıklayın. Kayıt diyaloğu görüntülenecektir.



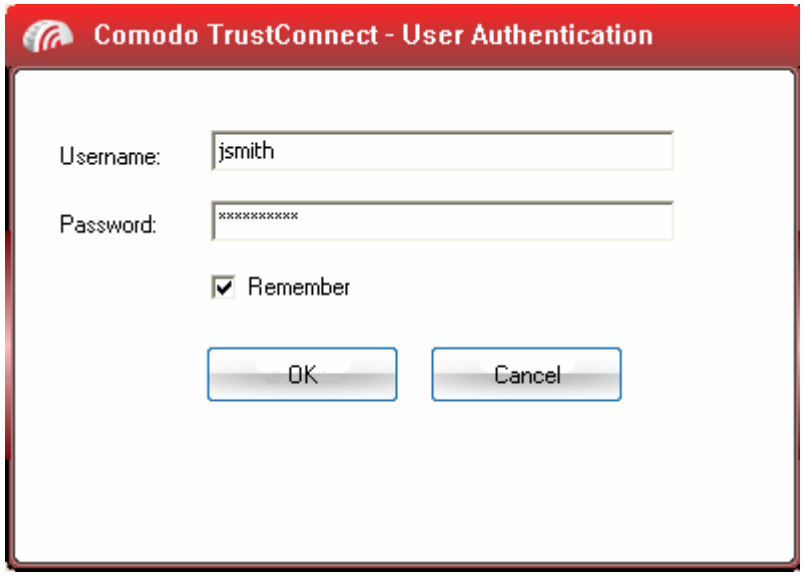
Lisans anahtarınızı girin ve İleri düğmesine tıklayın.

Anahtarınız doğrulanacaktır ve kayıt tamamlandı diyaloğu görüntülenecektir.



'Comodo TrustConnect' sisteminize başarıyla kuruldu.

Bitir düğmesine tıklayarak sihirbazdan çıkın ve TrustConnect uygulamasını kullanmaya başlayın.



Comodo TrustConnect kullanımı hakkında daha fazla bilgi için bu rehberin TrustConnect bölümüne bakın.

1.3.3.5 Comodo Dragon Tarayıcı Kurulumu

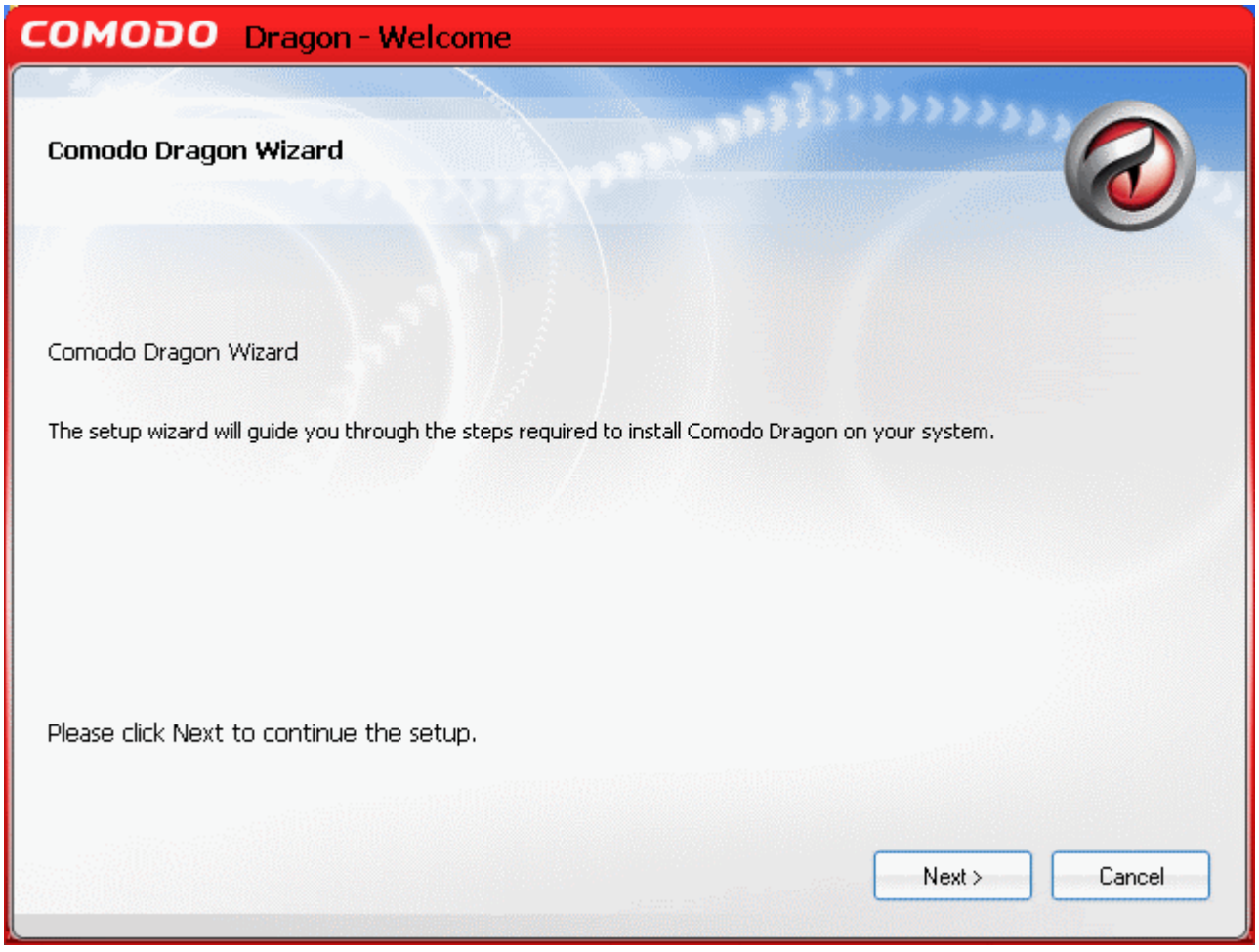
Comodo Dragon kullanıcı dostu bir tarayıcıdır ve Comodo tarafından geliştirilmiştir. CIS 2011 Pro/Complete ile birlikte ücretsiz olarak sunulmaktadır.

Comodo Dragon kurmak için

•Comodo Internet Security 2011 Pro/Complete kurucu ekranından 'Dragon Web Tarayıcı Kur' düğmesine tıklayın. Comodo Dragon kurulum sihirbazı hemen başlayacaktır.

Adım 1 – Hoş Geldiniz Ekranı

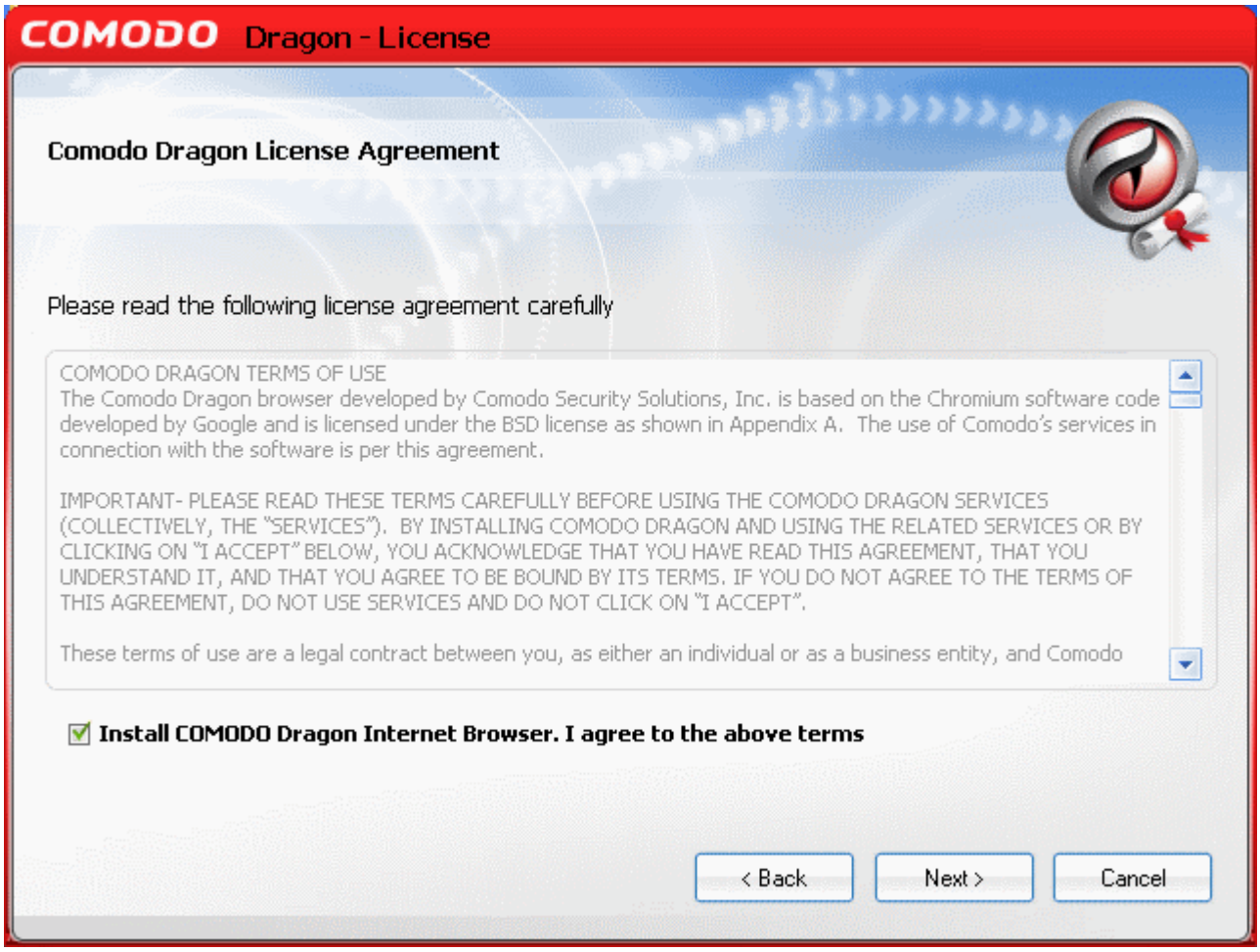
Hoş geldiniz ekranı görüntülenecektir.



Devam etmek için 'İleri' düğmesine tıklayın.

Adım 2 – Lisans Sözleşmesi

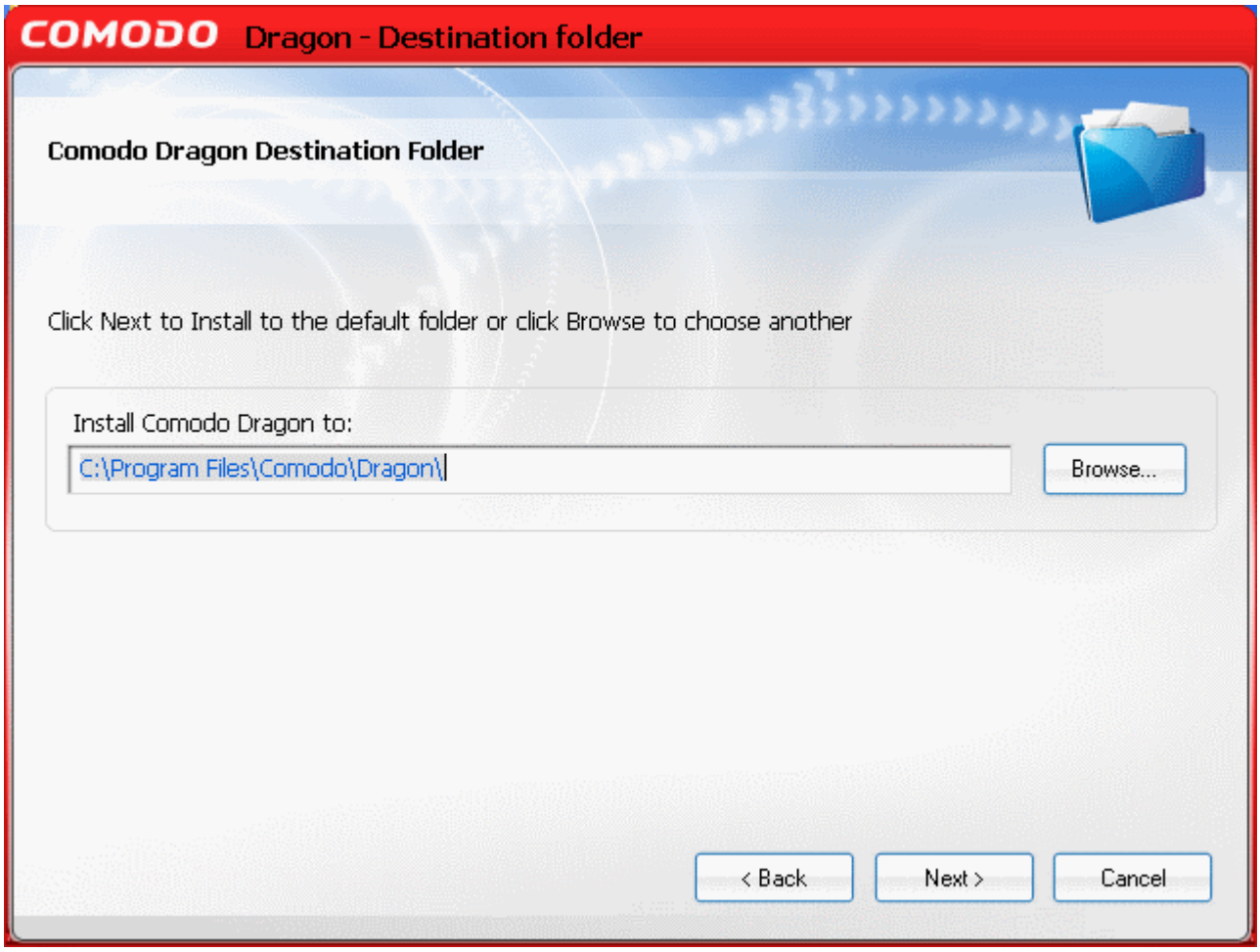
Lisans Sözleşmesini okuyup kabul ederek başlangıç aşamasını geçin.



'Comodo Dragon Internet Tarayıcısını Kur. I agree to the above terms' seçin ve 'İleri' tıklayın.

Adım 3 – Kurulum Klasörünün Seçimi

Sonraki ekrandan Comodo Dragon kurulum klasörünü seçebilirsiniz. Varsayılan yol *C:\Program Files\Comodo\Dragon.*

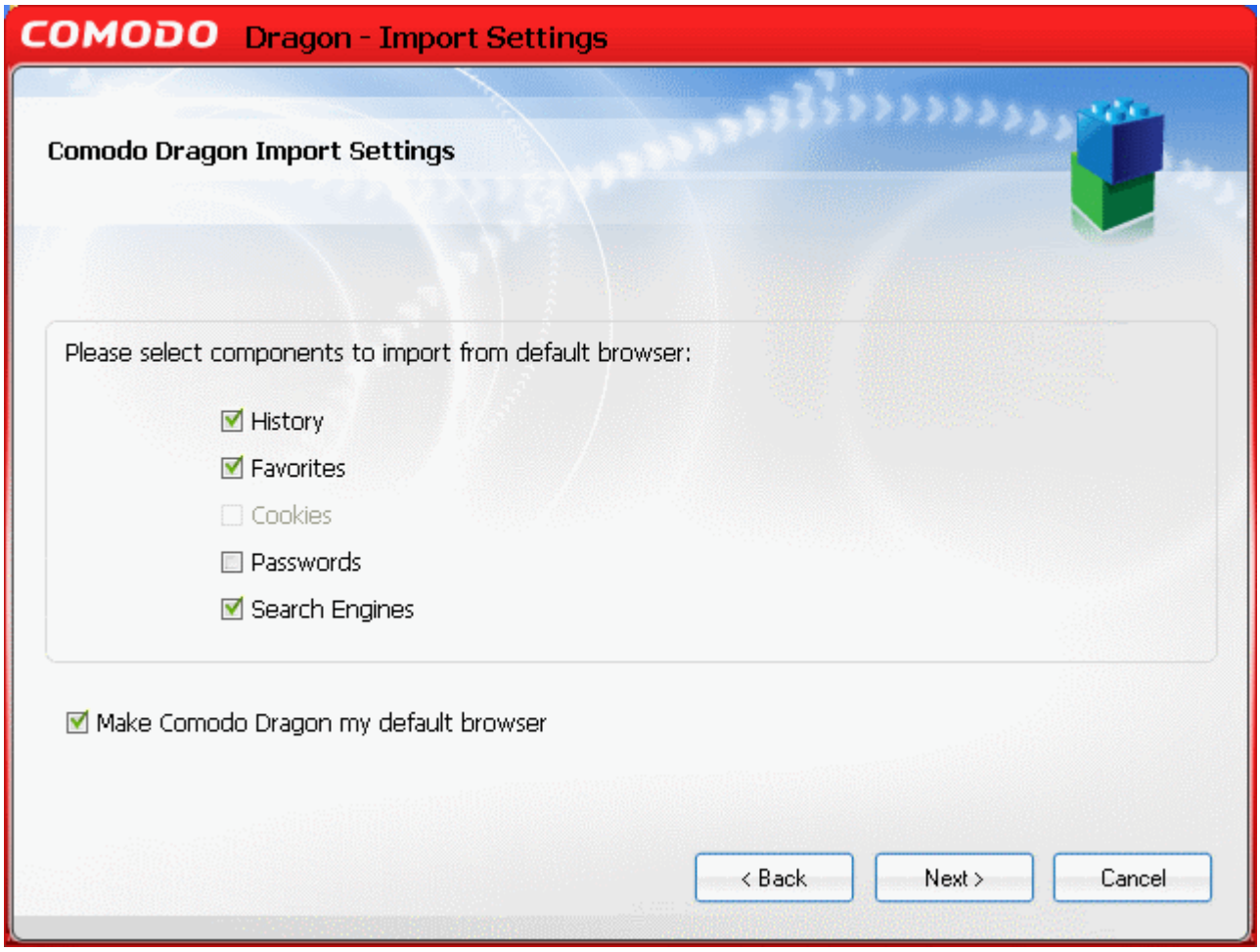


Farklı bir konuma kurulum yapmak için 'Browse' düğmesine tıklayın ve farklı bir konum seçerek kurulum yapın.

Devam etmek için 'İleri' tıklayın.

Adım 4 – Ayarların Alınması

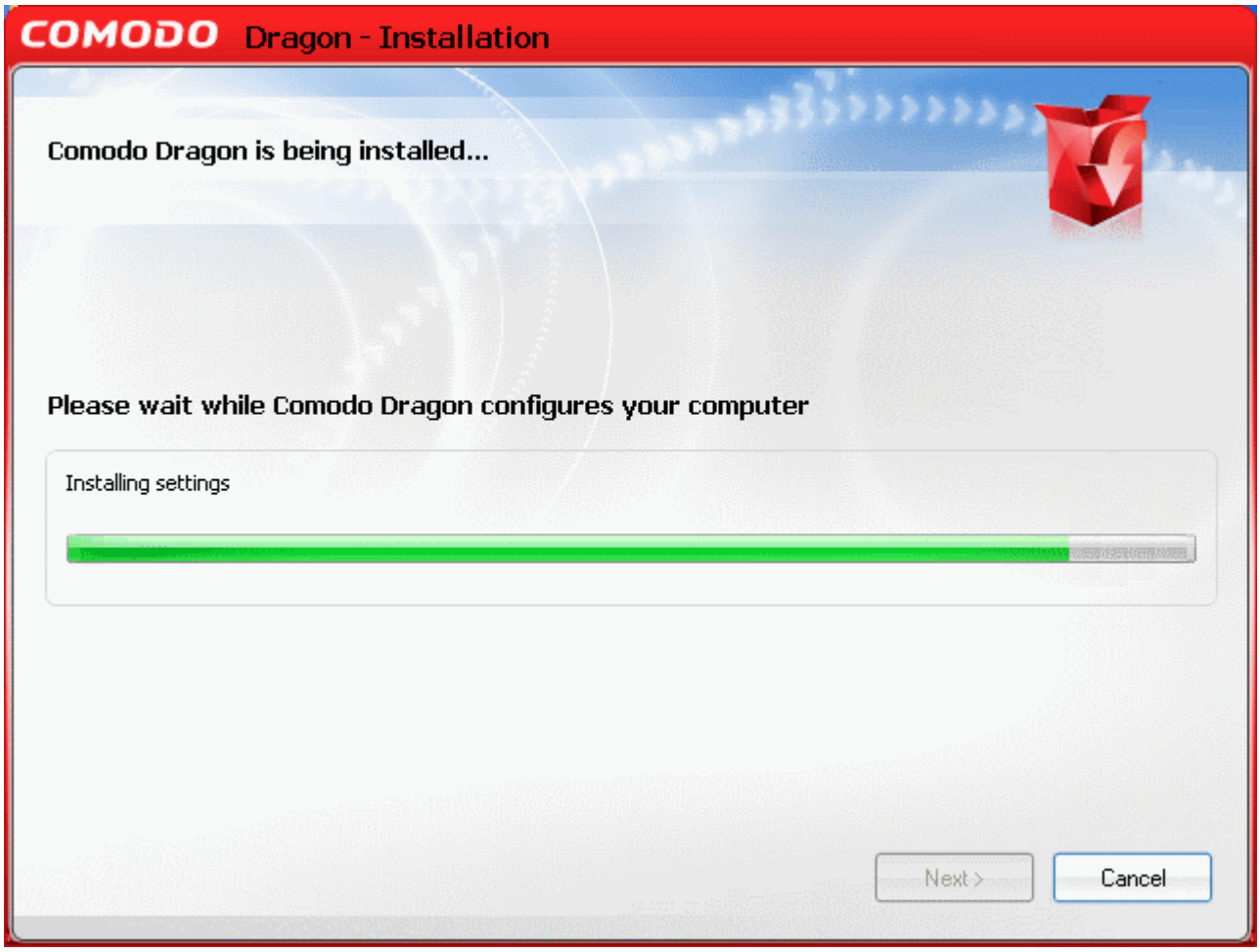
Sonraki adımda diğer tarayıcılardaki bilgilerinizi Dragon'a aktarabilirsiniz. Bu ayarlar; tarayıcı geçmişi, yer imleri, çerezler, parolalar, arama motorları gibi bilgileri kapsar. Ayrıca bu ekranı kullanarak Dragon'u varsayılan tarayıcınız olarak ayarlayabilirsiniz.



Seçimlerinizi yapın ve 'İleri' tıklayın.

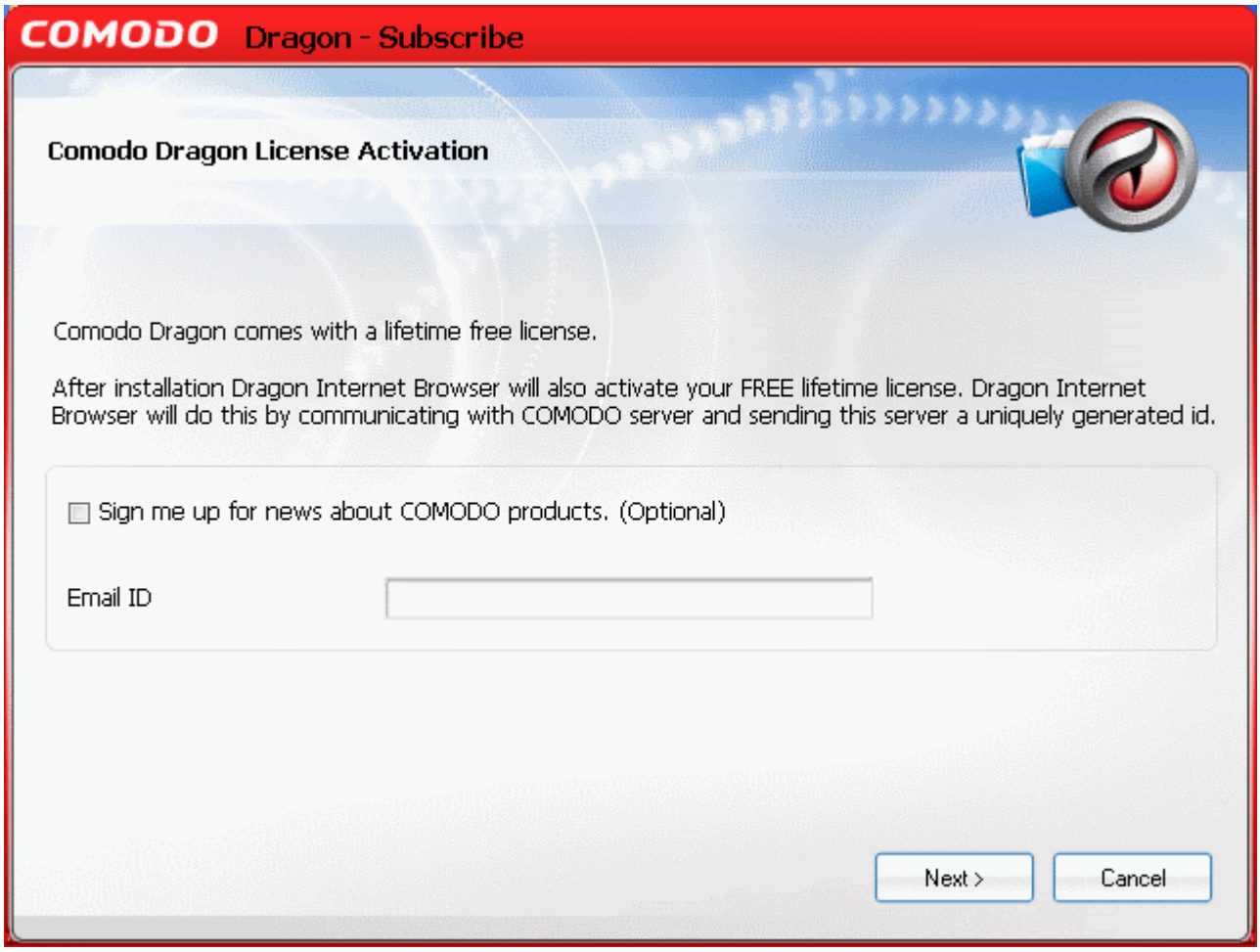
Adım 5 – Kurulum İlerleyişi

Sihirbaz kurulumu başlatır. Kurulum ilerleyişi görünecektir..



Adım 6 – Ürünün Etkinleştirilmesi

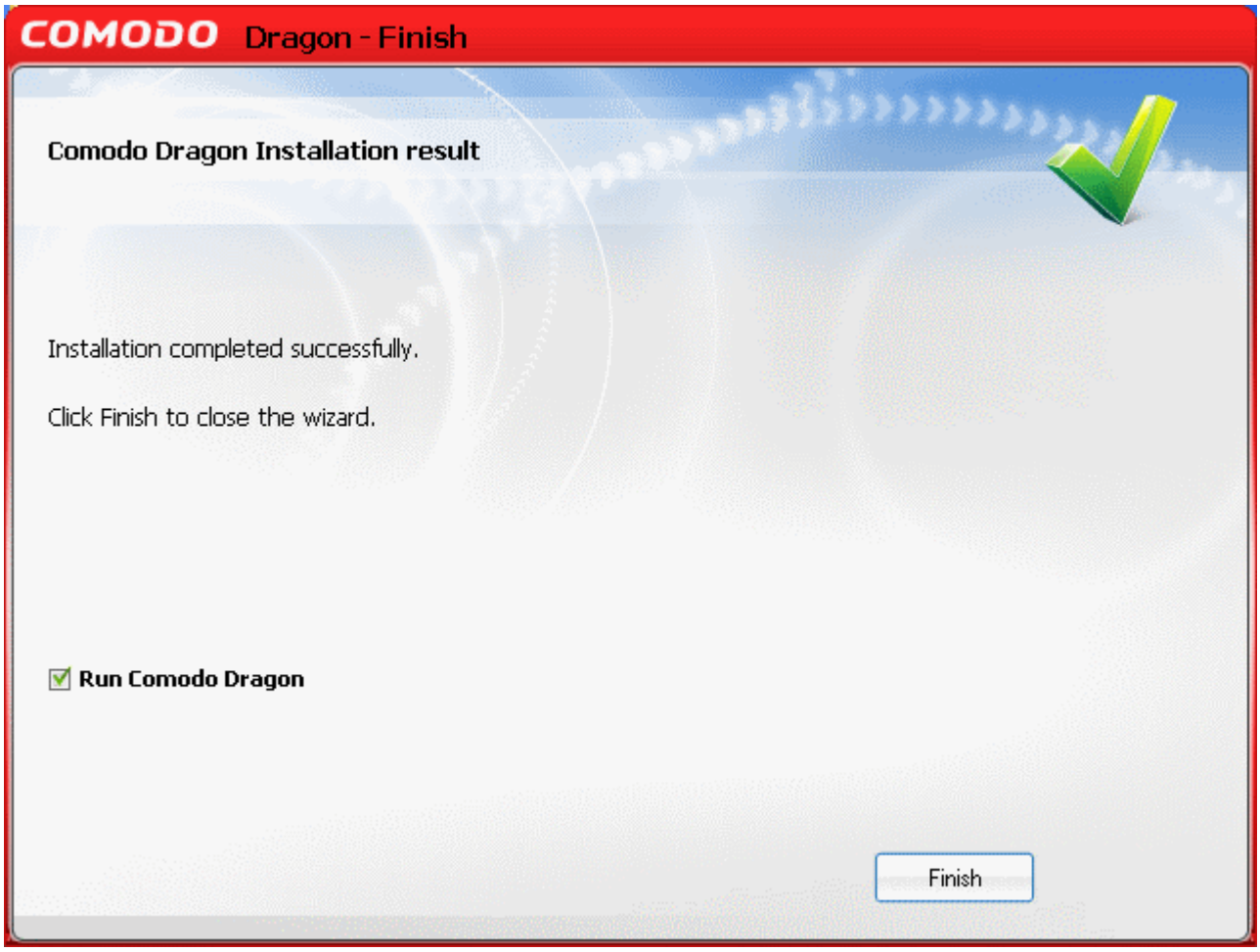
Kurulum tamamlandıktan sonra ürün Etkinleştirme diyaloğu görüntülenecektir. Comodo Dragon yazılımı ömür boyu kullanım için etkinleştirilecektir. Comodo ürünleri hakkında haberlere kaydolmak isterseniz eposta adresinizi çıkan alana girip **'Sign me up for news about Comodo products'** seçin.



Bu seçime bağlıdır. 'İleri' tıklayın.

Adım 7 – Kurulumun Tamamlanması

Başarılı kurulumdan sonra onay diyaloğu görüntülenecektir. Kurulumun etkili olabilmesi için bilgisayarınızın yeniden başlatılması gerekmektedir.



Kurulumdan hemen sonra Comodo Dragon Tarayıcısını başlatmak istiyorsanız 'Run Comodo Dragon' kutusu işaretli kalsın, istemiyorsanız kutudaki işareti kaldırıp 'Bitir' düğmesine basarak sihirbazı kapatın.

1.3.4 CIS Pro ve CIS Complete Hizmetlerinin Kurulumdan Sonra Etkinleştirilmesi

Kurulum sırasında bu hizmetleri etkinleştirmemiş olsanız da kurulumdan sonra etkinleştirebilirsiniz. Aşağıdaki bağlantılarda ayrıntılı açıklamaları bulabilirsiniz:

•Aboneliğinizin Etkinleştirilmesi;

•Garanti Güvencenizin Etkinleştirilmesi;

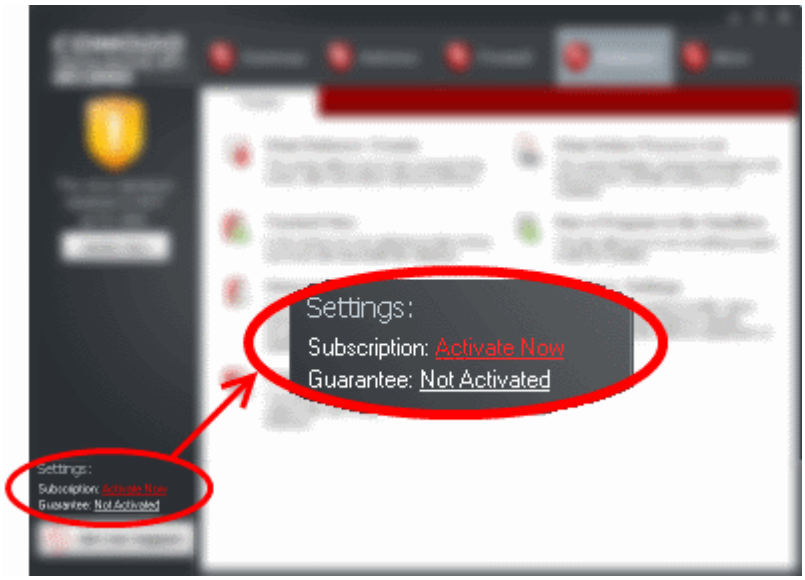
•Aboneliğinizin Yenilenmesi.

1.3.4.1 Aboneliğinizin Etkinleştirilmesi

•Comodo İnternet Güvenliği'nin Başlatılması bölümünde açıklandığı gibi Comodo İnternet Güvenliği'ni başlatın.

Ana ekranın sol alt köşesinde ‘Ayarlar’ alanını göreceksiniz.

•Abonelik yanındaki Şimdi Etkinleştir bağlantısına tıklayın:



Ürün Etkinleştirme Sihirbazı başlayacaktır.

•'Geçerli bir lisans anahtarına sahibim ve onu kullanmak istiyorum' kutusunu seçin ve ‘İleri’ düğmesine tıklayın.

Lisans anahtarınızı girin ve 'İleri' tıklayın. Sihirbaz lisans anahtarınızı doğrulamaya başlayacaktır.

Lisansınız doğrulandıktan sonra lisansınızın size sağladığı hakları içeren son bir onay ekranı çıkacaktır:

İleride kullanmak ve başka makinalara kurulum için lisans anahtarınızı saklayınız. (lisansınız 3 makinaya kadar geçerlidir).

Sihirbazı kapatmak için 'Bitir' düğmesine tıklayın.

1.3.4.2 Garanti Güvencenizin Etkinleştirilmesi

Garanti Güvencesi CIS Pro ve CIS Complete sürümlerini kullanan müşteriler için mevcuttur. Bu hizmeti kullanabilmek için öncelikle aboneliğinizi etkinleştirmeniz gerekmektedir. Aboneliğin etkinleştirilmesi hakkında daha ayrıntılı bilgilere CIS Pro – Kurulum ve Etkinleştirilmesi ve CIS Complete - Kurulum ve Etkinleştirilmesi bölümlerinde bulabilirsiniz.

- Comodo Garanti'yi kullanmak ve etkinleştirmek istiyorsanız Comodo İnternet Güvenliği'ni (Antivirüs ve Güvenlik Duvarı bileşenleriyle birlikte) ve Comodo LivePCSupport yazılımını kurmuş olmalısınız. Ayrıca Comodo Antivirüs ile tam sistem taraması gerçekleştirmelisiniz. Garanti yalnızca Birleşik Devletler'de ikamet edenler için mevcuttur.

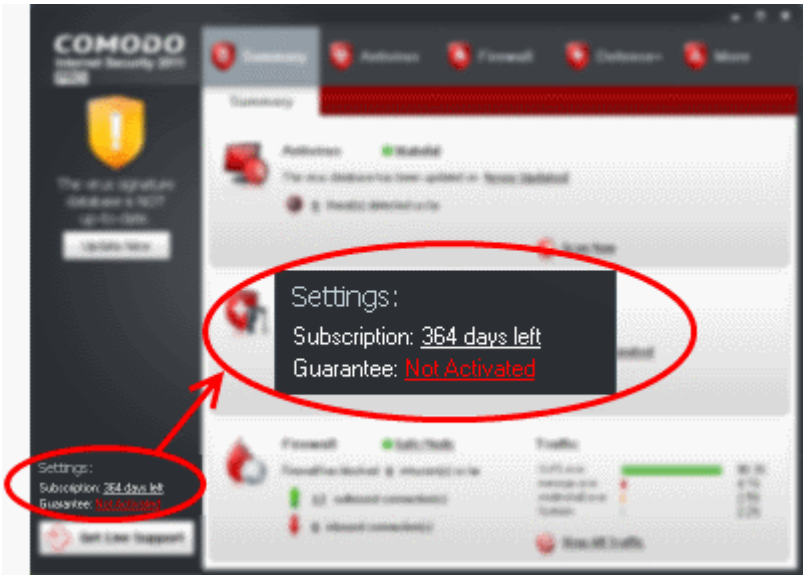
Limitler: Garanti en düşük olanla limitlidir**:**

- Bilgisayarın gerçek değeri;
- Tek bir lisans anahtarı altında tüm iddialar için toplam 500 $ 'lık ödeme, ve
- Comodo'nun belirlediği yetkili servis tarafından bilgisayarın işletilebilir duruma getirilmesinin maliyeti ("Garanti Limiti").

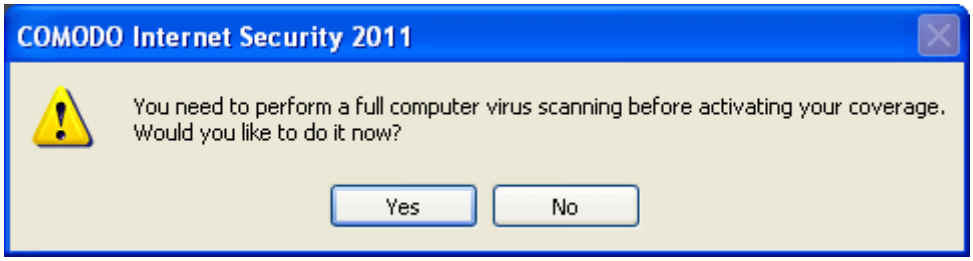
- **Garanti, bilgisayarın İnternet üzerinden işletilebilir duruma onarımı ile limitlidir ve kar kaybı, kaybolmuş veya bozulmuş veri, bozulmuş veya silinmiş iş veya kişisel dosyaların kaybı ve hasar görmesi iddialarını hariç tutar. Comodo herhangi bir dosya veya bilgi kaybına karşı garanti vermez. Garanti, Son Kullanıcı Lisans Sözleşmesi'nin (EULA) 3. bölümündeki işlemleri ihlal ederseniz veya Yazılımın kullanımı için gereken ödemeleri yapmazsanız geçersizdir.**
- **Comodo Garanti Güvencesi'nin Tam Şartlarını ve Koşullarını Son Kullanıcı Lisans Sözleşmesi'nin (EULA) 3. Bölümünde okuyabilirsiniz. (Step 1 of the Installation process of CIS Pro or CIS Complete).**

Önemli Not: Garantiyi etkinleştirmeden önce en son virüs tanımı güncellemelerini yapıp tam sistem taraması yaptırarak sisteminizin Garanti güvencesi için uygunluğundan emin olmalısınız. Antivirüs taramasıyla ilgili daha fazla bilgi için buraya tıklayın..

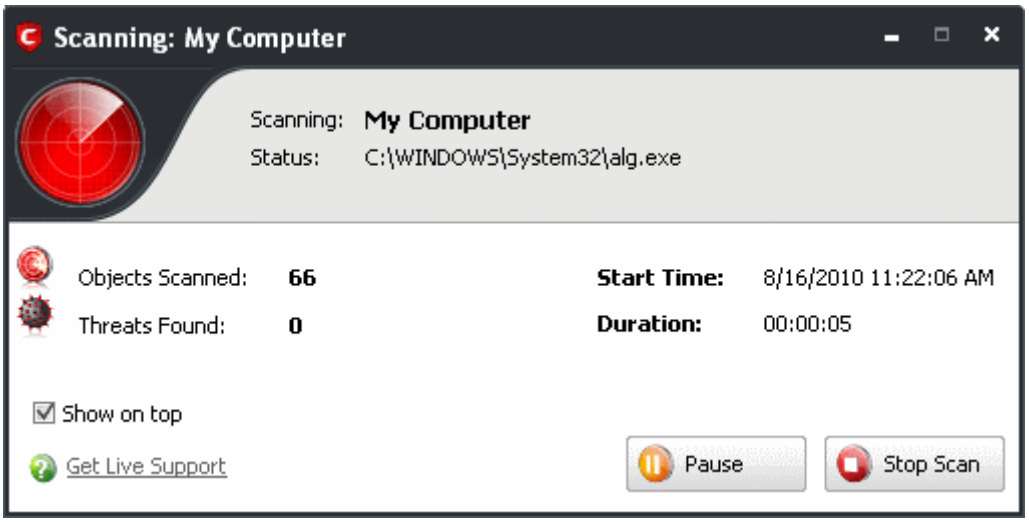
Adım 1: Garanti güvencenizi etkinleştirmek için ana ekranın sol alt köşesindeki "Garanti:" yazısının yanındaki 'Etkinleştirilmedi' bağlantısına tıklayın.



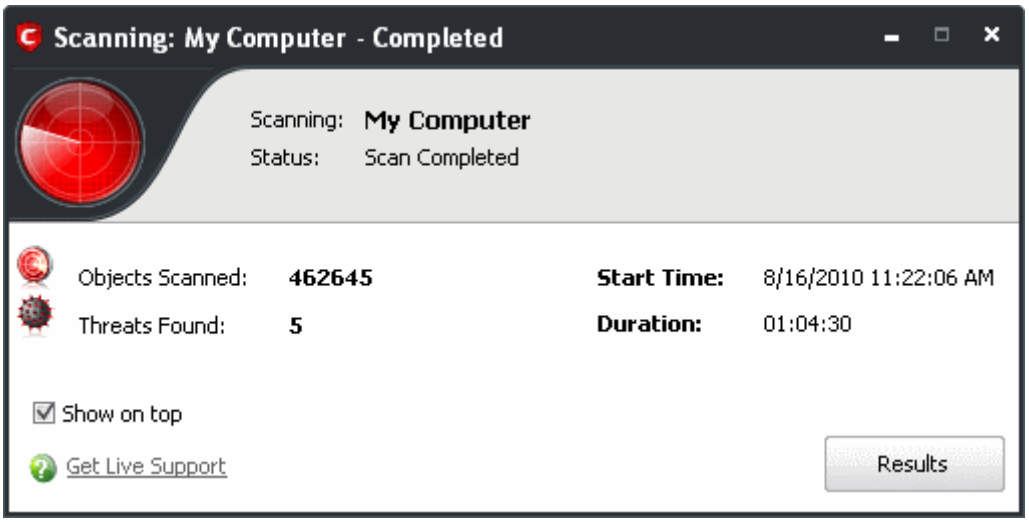
Eğer henüz tam sistem taraması gerçekleştirmediyseniz (yukarıda bahsedildiği gibi), gerçekleştirmeniz istenecektir. Tam sistem taraması bilinen zararlıların sisteminizden kaldırılması için zorunlu gerekliliktir. Eğer bu adımı zaten gerçekleştirdiyseniz (ve sisteminiz temiz ise) Adım 2'ye geçin.



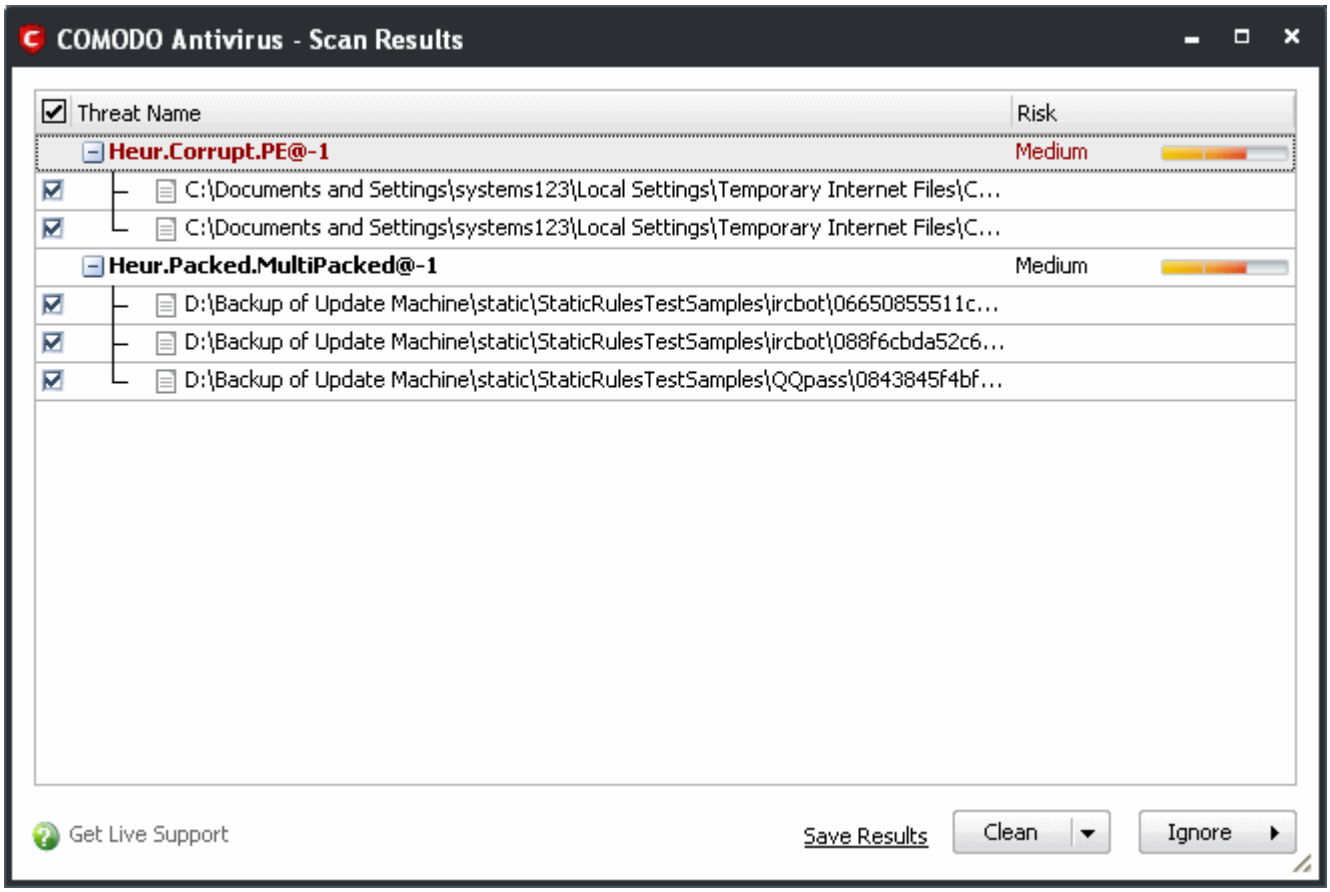
'Evet' düğmesine tıklayarak taramayı başlatın.



Tarama tamamlandığında 'tarama tamamlandı' penceresi görünecektir.

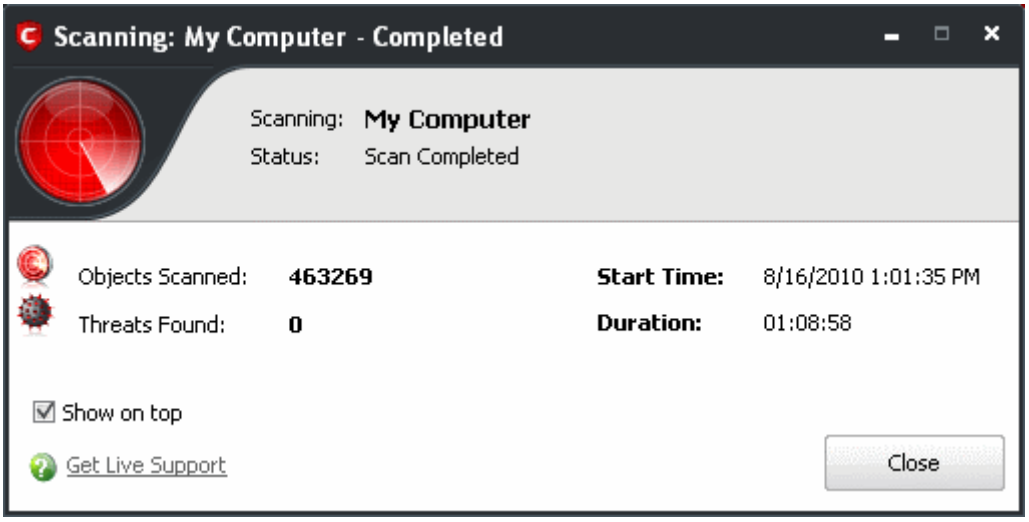


•Tarama Sonuçlarını görmek için 'Sonuçlar' düğmesine tıklatın. Eğer sisteminizde kötü niyetli yürütülebilirler saptanırsa tarama sonuç penceresinde ve bununla birlikte taranan nesne sayısı da görüntülenir.



•Tehditleri sisteminizden kaldırmak için Temizle düğmesine tıklayın.

- **Eğer hiç tehdit bulunmadıysa CIS arayüzüne geri dönmek için 'Kapat' düğmesine tıklayın.**



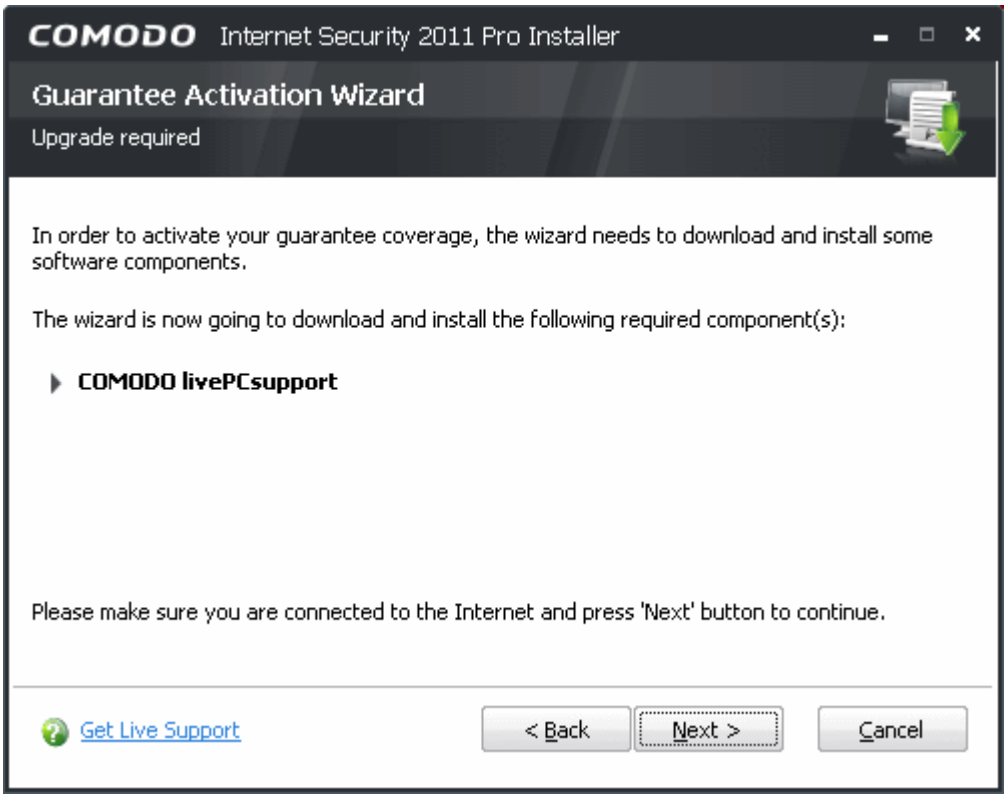
Adım 2: Sonraki adım Garanti Etkinleştirme Sihirbazını çalıştırmaktır.

•Ana ekranın sol alt köşesinde Ayarlar bölümündeki "Garanti:" yazısının yanındaki 'Etkinleştirilmedi' bağlantısına

tıklayın.

- **Devam etmek için İleri düğmesine tıklayın. Sihirbaz, sisteminizin garanti güvencesi için gereken ön koşulları sağlayıp sağlamadığını denetleyecektir. Ön koşullar:**
  - Comodo Internet Security 2011 (Pro veya Complete) tam olarak kurulu olmalıdır. (Güvenlik Duvarı ve Antivirüs)
  - Comodo LivePCSupport kurulu olmalıdır.
  - Sisteminiz en son virüs tanım güncellemeleri ile tam taramadan geçmiş olmalıdır

Eğer bunlardan eksik olanlar varsa bunlar sihirbaz tarafından uygulanacaktır. (örneğin, eksik bir bileşeni kurar ve tam virüs taraması gerçekleştirir). Tüm bileşenler kuruluysa Adım 3'e geçin.



- Devam etmek için ‘İleri’ düğmesine tıklayın. Sihirbaz otomatik olarak indirmeyi başlatacak ve bileşenleri kuracaktır.

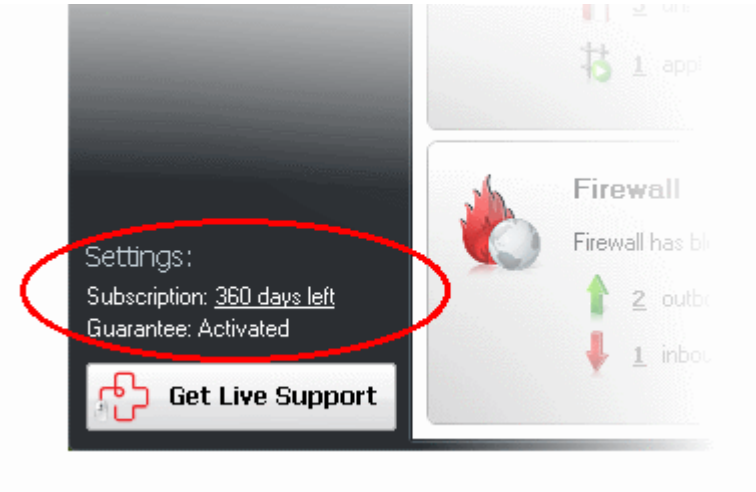
Adım 3: Garantinizin Kaydedilmesi

Garanti güvenceniz kaydedilecektir...

... ve tamamlandığında Garantinin başarılı olarak etkinleştirildiğini onaylayan son bir ekran çıkacaktır.

- **Etkinleştirme sihirbazını tamamlamak için 'Bitir' düğmesine tıklayın.**

Garantinizin başarılı etkinleştirilmesi 'Ayarlar' bölümünde görüntülenen bilgileri değiştirecektir:



1.3.4.3 Aboneliğinizin Yenilenmesi

CIS Pro veya CIS Complete aboneliğiniz bir yıllığına geçerlidir. Comodo hizmetlerinden yararlanmaya devam etmek için aboneliğinizi yenilemeniz gerekmektedir.

Aboneliğinizi yenilemek için ana ekranın sol alt köşesindeki Ayarlar bölümündeki 'Abonelik:' yanında bulunan 'Şimdi Etkinleştir' bağlantısına tıklayın.

Ürün Etkinleştirme Sihirbazı başlayacaktır.

•'Lisans anahtarına sahip değilim veya lisans anahtarımın süresi doldu' kutusunu işaretleyin ve 'İleri' düğmesine tıklayın.

https://accounts.comodo.com/cfp/management/signup adresine yönlendirileceksiniz.

•CIS Paketinizi seçin.

•'Mevcut müşteri misiniz?' sorusuna 'Evet' olarak cevap verin. Müşteri bilgi alanına giriş adınızı ve parolanızı yazın ve ödeme işlemlerini tamamlayın.

Abonelik anahtarı eposta yoluyla gönderilecektir. Yeni anahtar ile aboneliğinizi yenileyerek hizmetleri kullanmaya devam edebilirsiniz.

1.4 Comodo İnternet Güvenliği'nin Başlatılması

Kurulumdan sonra CIS Windows ile otomatik olarak başlar. CIS ayarlarını yapılandırmak veya görmek için yönetim arayüzüne erişmeniz gerekmektedir.

Yönetim arayüzüne erişmenin 3 ayrı yolu vardır:

•Windows Başlangıç Menüsü

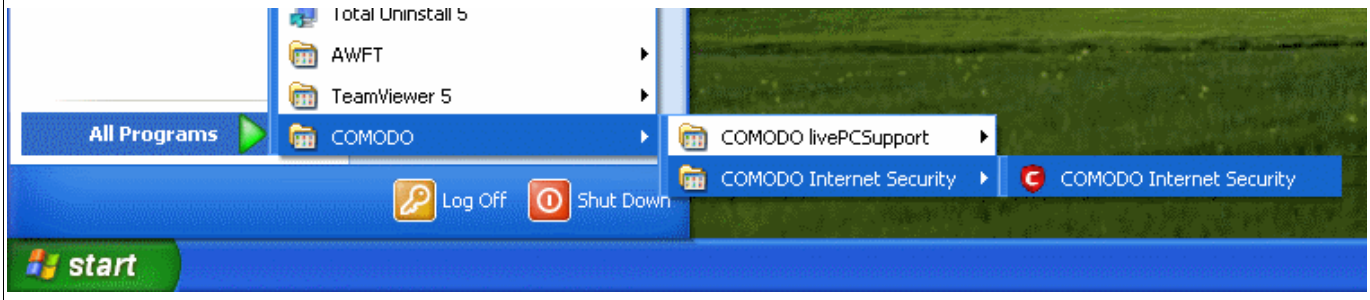
•Windows Masaüstü

•Bildirim Alanı Simgesi

Başlangıç Menüsü

CIS arayüzüne Windows Başlat Menüsünü kullanarak da erişebilirsiniz.

- Başlat'a tıklayın ve Tüm Programlar > Comodo > COMODO Internet Security > COMODO Internet Security seçin.



Windows Masaüstü

•Masaüstünde bulunan CIS simgesine çift tıklayın.

CIS Bildirim Alanı Simgesi

•Ana arayüzü açmak için bildirim alanındaki kalkan simgesine çift tıklayın.

Bildirim alanı simgesine sağ tıklayarak bileşenlerin güvenlik seviye ayarları kısayollarına erişebilirsiniz.

Antivirüs Güvenlik Seviyesi – Daha fazla bilgi için buraya tıklayın.

Güvenlik Duvarı Güvenlik Seviyesi – Daha fazla bilgi için buraya tıklayın.

Savunma+ Güvenlik Seviyesi – Daha fazla bilgi için buraya tıklayın.

Sandbox Güvenlik Seviyesi – Daha fazla bilgi için buraya tıklayın.

Yapılandırma – Daha fazla bilgi için buraya tıklayın.

Oyun Kipi – Oyun Kipi'ni açarak oyunlarınızı uyarılar ile bölünmeden oynayabilirsiniz. Bu kipin etkinleştirilmesiyle birlikte tüm CIS uyarıları bastırılacaktır, ek olarak virüs güncellemeleri ve zamanlanmış taramalar ertelenecektir. Oyun Kipi'nin devre dışı bırakılmasıyla birlikte virüs güncellemeleri ve zamanlanmış taramalar eski haline geri dönecektir.

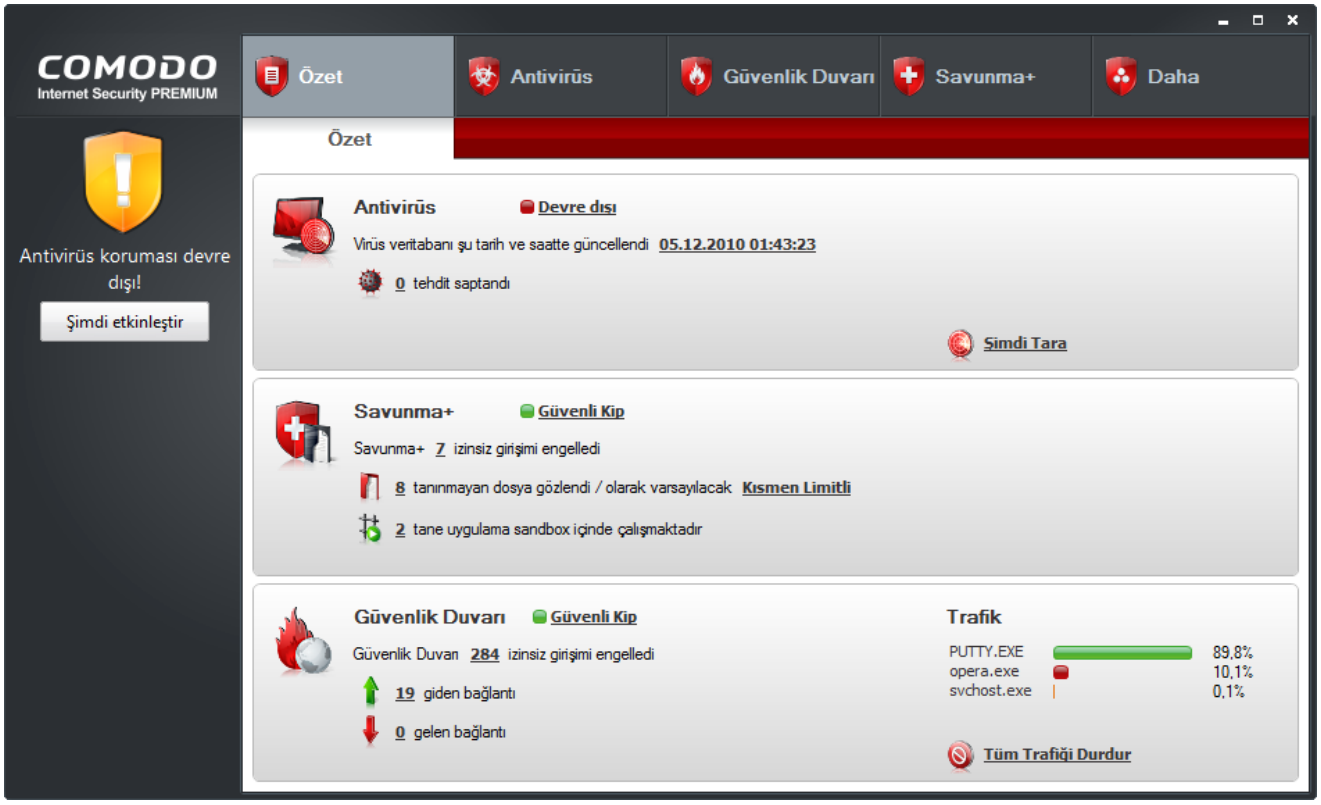
1.5 Özet Ekranlarının Tanıtımı

Varsayılan olarak yönetim arayüzünde 'Özet' bölümü görünür. İstediğiniz zaman Genel Gezinti bölümünden 'Özet' sekmesini seçerek erişebilirsiniz.

Bu bölümün yerleşimi kuruluma göre değişiklik gösterebilir. Aşağıda kurulumuza uygun taslak görünümleri tıklayarak görebilirsiniz:

- COMODO İnternet Güvenliği (Antivirüs ve Güvenlik Duvarı ile birlikte)
- COMODO Güvenlik Duvarı veya
- COMODO Antivirüs

1.5.1 Comodo İnternet Güvenliği – Özet



Özet ekranı aşağıdakileri gösterir

1. Sistem Durumu

Arayüzün sol tarafında uygulamanız önerilen eylemler görünür.

2. Antivirüs

Antivirüs özet kutusu şunları içerir:

i. Gerçek Zamanlı Tarayıcının Durumu

Örnekte görüldüğü gibi virüs tarayıcı ayarı Durumsal olarak görünüyor. Bu bağlantıya tıklayarak Virüs Tarayıcı Ayarlarına hızlıca erişebilirsiniz. Kaydırıcıyı hareket ettirerek Gerçek Zamanlı Tarama ayarını kolaylıkla değiştirebilirsiniz. Daha fazla bilgi için Tarayıcı Ayarları bölümüne bakın.

ii. Virüs Veritabanı En Son Ne Zaman Güncellendi

Son güncellenme tarihi ve saati bağlantı olarak görünür. Bu bağlantıya tıklayarak güncellemeleri denetleyebilirsiniz ve bu işlem tamamlandıktan sonra son güncellenme tarihi ve saati değişir.

iii. Saptanan Tehdit Sayısı

Açık oturumdaki tehdit sayısı bağlantı olarak görünür. Bu bağlantıya tıkladığınızda Antivirüs Olayları penceresi açılır. Daha fazla bilgi için Antivirüs Olaylarına bakın.

iv. Şimdi Tara

'Şimdi Tara' düğmesine tıklayarak bir tarama başlatabilirsiniz.

1. Savunma+

Savunma+ özet kutusu şunları içerir:

i. **Engellenmiş Şüpheli Girişim Sayısı**

Açık oturumdaki engellenmiş girişim sayısı bağlantı olarak görünür. Bu bağlantıya tıkladığınızda Savunma+ Olayları penceresi açılır. Daha fazla bilgi için Savunma+ Olaylarını Göster bölümüne bakın.

ii. **Savunma+ Güvenlik Seviyesi**

Savunma+ güvenlik seviyesi bağlantı olarak görünür (Örnekte Güvenli Kip göründüğü gibi). Bu bağlantıya tıklarsanız Savunma+ Ayarları açılır ve buradan kaydırıcı ile kolaylıkla seviye değiştirebilirsiniz. Daha fazla bilgi için Savunma+ Ayarları bölümüne bakın.

iii. **Tanınmayan Dosyaların Sayısı**

Bilgisayarınızda çalışan tanınmayan dosyaların sayısı sayısal bağlantı olarak görünür. Bu dosyalara nasıl davranılacağı Yürütme Denetimi Ayarlarına göre belirlenir. Sayısal bağlantıya tıkladığınızda **Tanınmayan Dosyalar** penceresi açılır.

Savunma+ içindeki Etkin İşlemler Listesinden çalışan tüm uygulamaların ayrıntılarını görebilirsiniz.

iv. Sandbox içinde Çalışan Uygulamaların Sayısı

Sandbox içinde çalışan uygulamaların sayısı görünür. Daha fazla bilgi için Her zaman Sandbox ve Sandbox içinde Program Çalıştır bölümlerine bakın.

1. Güvenlik Duvarı

Güvenlik Duvarı kutusu şunları içerir:

i. **Engellenmiş İzinsiz Girişlerin Sayısı**

Açık oturumdaki engellenmiş izinsiz girişimlerin sayısı bağlantı olarak görünür. Bu bağlantıya tıklayarak Güvenlik Duvarı Olayları penceresini açabilirsiniz. Daha fazla bilgi için Güvenlik Duvarı Olaylarını Göster bölümüne bakın.

ii. **Güvenlik Duvarı Seviyesi**

Güvenlik Duvarı güvenlik seviyesi bağlantı olarak görünür (Örnekte Güvenli Kip göründüğü gibi). Bu bağlantıya tıklayarak Güvenlik Duvarı Davranış Ayarları penceresini açabilirsiniz. Kaydırıcı ile kolaylıkla seviye değiştirebilirsiniz. Daha fazla bilgi için Güvenlik Duvarı Davranış Ayarları bölümüne bakın.

iii. **Gelen/Giden Bağlantılar**

Etkin gelen/giden bağlantıların sayısal bağlantısı görünür. Bu bağlantıya tıklayarak **Etkin Bağlantılar** penceresini açabilirsiniz. Daha fazla bilgi için Etkin Bağlantıları Göster bölümüne bakın..

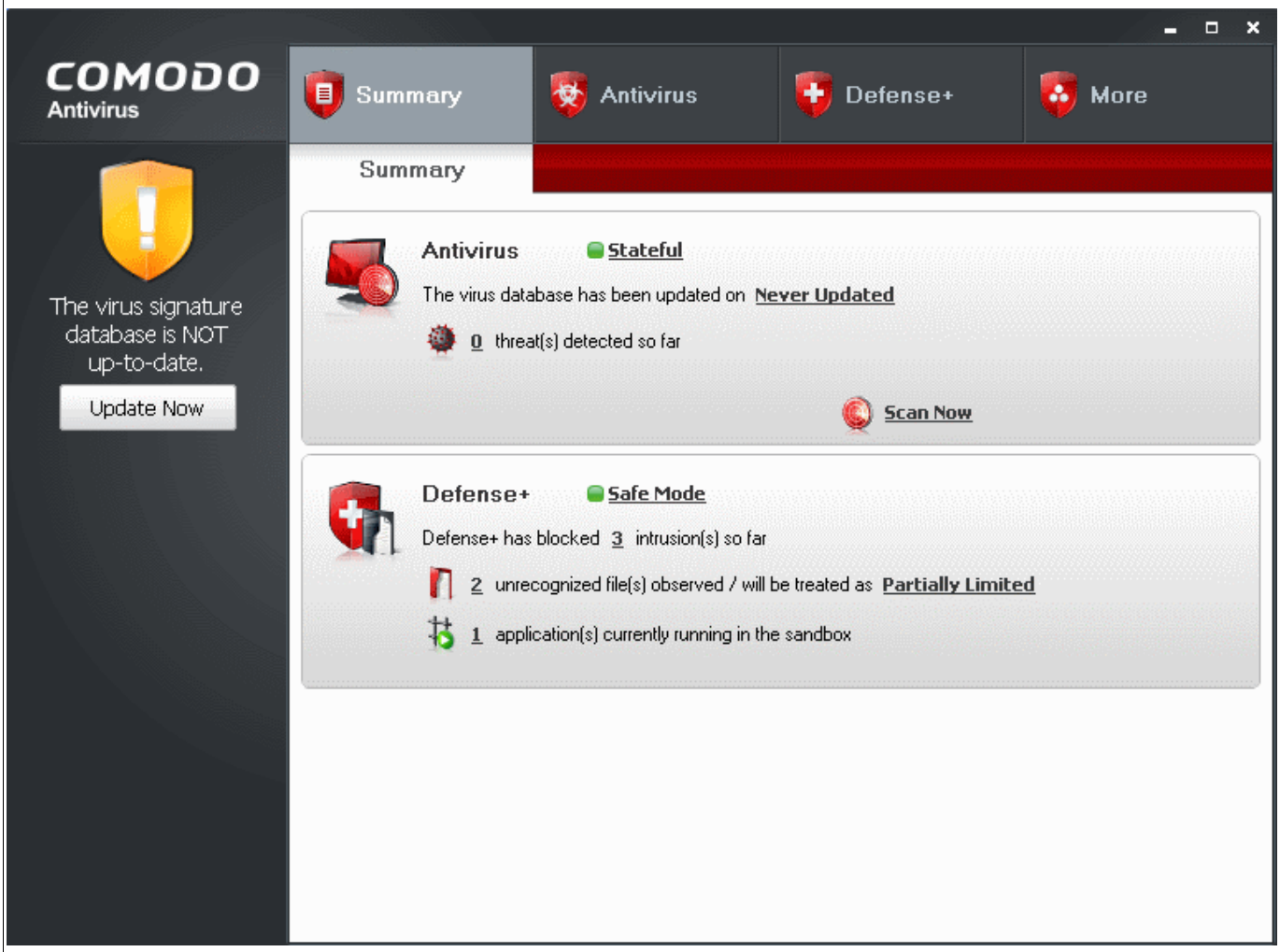
iv. **Trafik**

Trafik bölümünde internete bağlı olan uygulamalar çubuk grafik şeklinde görünür. Bunun yanında % olarak gerçekleştirdikleri trafik ve uygulama adı görünür. Uygulama adına tıklayarak Etkin Bağlantıları Göster arayüzüne erişebilirsiniz.

v. **Tüm Trafiği Durdur/Tüm Trafiği Eski Haline Getir**

Bu bağlantı ile ağ trafiğini açıp kapatabilirsiniz. **Tüm Trafiği Durdur** ile anında tüm ağ trafiğini engelleyebilirsiniz (Güvenlik Duvarı 'Tümünü Engelle' kipine geçer), **Tüm Trafiği Eski Haline Getir** ile önceki güvenlik seviyesine dönersiniz.

1.5.2 Comodo Antivirüs – Özet



Özet ekranı aşağıdakileri gösterir

1. Sistem Durumu

Arayüzün sol tarafında uygulamanız önerilen eylemler görünür.

2. Antivirüs

Antivirüs özet kutusu şunları içerir:

i. Gerçek Zamanlı Tarayıcının Durumu

Örnekte görüldüğü gibi virüs tarayıcı ayarı Durumsal olarak görünüyor. Bu bağlantıya tıklayarak Virüs Tarayıcı Ayarlarına hızlıca erişebilirsiniz. Kaydırıcıyı hareket ettirerek Gerçek Zamanlı Tarama ayarını kolaylıkla değiştirebilirsiniz. Daha fazla bilgi için Tarayıcı Ayarları bölümüne bakın.

ii. Virüs Veritabanı En Son Ne Zaman Güncellendi

Son güncellenme tarihi ve saati bağlantı olarak görünür. Bu bağlantıya tıklayarak güncellemeleri denetleyebilirsiniz

ve bu işlem tamamlandıktan sonra son güncellenme tarihi ve saati değişir.

iii. Saptanan Tehdit Sayısı

Açık oturumdaki tehdit sayısı bağlantı olarak görünür. Bu bağlantıya tıkladığınızda Antivirüs Olayları penceresi açılır. Daha fazla bilgi için Antivirüs Olaylarına bakın.

iv. Şimdi Tara

'Şimdi Tara' düğmesine tıklayarak bir tarama başlatabilirsiniz.

1. Savunma+

Savunma+ özet kutusu şunları içerir:

i. **Engellenmiş Şüpheli Girişim Sayısı**

Açık oturumdaki engellenmiş girişim sayısı bağlantı olarak görünür. Bu bağlantıya tıkladığınızda Savunma+ Olayları penceresi açılır. Daha fazla bilgi için Savunma+ Olaylarını Göster bölümüne bakın.

ii. **Savunma+ Güvenlik Seviyesi**

Savunma+ güvenlik seviyesi bağlantı olarak görünür (Örnekte Güvenli Kip göründüğü gibi). Bu bağlantıya tıklarsanız Savunma+ Ayarları açılır ve buradan kaydırıcı ile kolaylıkla seviye değiştirebilirsiniz. Daha fazla bilgi için Savunma+ Ayarları bölümüne bakın.

iii. **Tanınmayan Dosyaların Sayısı**

Bilgisayarınızda çalışan tanınmayan dosyaların sayısı sayısal bağlantı olarak görünür. Bu dosyalara nasıl davranılacağı Yürütme Denetimi Ayarlarına göre belirlenir. Sayısal bağlantıya tıkladığınızda **Tanınmayan Dosyalar** penceresi açılır.

Savunma+ içindeki Etkin İşlemler Listesinden çalışan tüm uygulamaların ayrıntılarını görebilirsiniz.

iv. Sandbox içinde Çalışan Uygulamaların Sayısı

Sandbox içinde çalışan uygulamaların sayısı görünür. Daha fazla bilgi için Her zaman Sandbox ve Sandbox içinde Program Çalıştır bölümlerine bakın.

1.5.3 Comodo Güvenlik Duvarı – Özet

Özet ekranı aşağıdakileri gösterir

1. Sistem Durumu

Arayüzün sol tarafında uygulamanız önerilen eylemler görünür.

2. Güvenlik Duvarı

Güvenlik Duvarı kutusu şunları içerir:

i. **Engellenmiş İzinsiz Girişlerin Sayısı**

Açık oturumdaki engellenmiş izinsiz girişimlerin sayısı bağlantı olarak görünür. Bu bağlantıya tıklayarak Güvenlik Duvarı Olayları penceresini açabilirsiniz. Daha fazla bilgi için Güvenlik Duvarı Olaylarını Göster bölümüne bakın.

ii. **Güvenlik Duvarı Seviyesi**

Güvenlik Duvarı güvenlik seviyesi bağlantı olarak görünür (Örnekte Güvenli Kip göründüğü gibi). Bu bağlantıya tıklayarak Güvenlik Duvarı Davranış Ayarları penceresini açabilirsiniz. Kaydırıcı ile kolaylıkla seviye değiştirebilirsiniz. Daha fazla bilgi için Güvenlik Duvarı Davranış Ayarları bölümüne bakın.

iii. **Gelen/Giden Bağlantılar**

Etkin gelen/giden bağlantıların sayısal bağlantısı görünür. Bu bağlantıya tıklayarak **Etkin Bağlantılar** penceresini açabilirsiniz. Daha fazla bilgi için Etkin Bağlantıları Göster bölümüne bakın..

iv. **Trafik**

Trafik bölümünde internete bağlı olan uygulamalar çubuk grafik şeklinde görünür. Bunun yanında % olarak gerçekleştirdikleri trafik ve uygulama adı görünür. Uygulama adına tıklayarak Etkin Bağlantıları Göster arayüzüne erişebilirsiniz.

v. **Tüm Trafiği Durdur/Tüm Trafiği Eski Haline Getir**

Bu bağlantı ile ağ trafiğini açıp kapatabilirsiniz. **Tüm Trafiği Durdur** ile anında tüm ağ trafiğini engelleyebilirsiniz (Güvenlik Duvarı 'Tümünü Engelle' kipine geçer), **Tüm Trafiği Eski Haline Getir** ile önceki güvenlik seviyesine dönersiniz.

1. Savunma+

Savunma+ özet kutusu şunları içerir:

i. **Engellenmiş Şüpheli Girişim Sayısı**

Açık oturumdaki engellenmiş girişim sayısı bağlantı olarak görünür. Bu bağlantıya tıkladığınızda Savunma+ Olayları penceresi açılır. Daha fazla bilgi için Savunma+ Olaylarını Göster bölümüne bakın.

ii. **Savunma+ Güvenlik Seviyesi**

Savunma+ güvenlik seviyesi bağlantı olarak görünür (Örnekte Güvenli Kip göründüğü gibi). Bu bağlantıya tıklarsanız Savunma+ Ayarları açılır ve buradan kaydırıcı ile kolaylıkla seviye değiştirebilirsiniz. Daha fazla bilgi için Savunma+ Ayarları bölümüne bakın.

iii. **Tanınmayan Dosyaların Sayısı**

Bilgisayarınızda çalışan tanınmayan dosyaların sayısı sayısal bağlantı olarak görünür. Bu dosyalara nasıl davranılacağı Yürütme Denetimi Ayarlarına göre belirlenir. Sayısal bağlantıya tıkladığınızda **Tanınmayan Dosyalar** penceresi açılır.

Savunma+ içindeki Etkin İşlemler Listesinden çalışan tüm uygulamaların ayrıntılarını görebilirsiniz.

iv. Sandbox içinde Çalışan Uygulamaların Sayısı

Sandbox içinde çalışan uygulamaların sayısı görünür. Daha fazla bilgi için Her zaman Sandbox ve Sandbox içinde Program Çalıştır bölümlerine bakın.

1.6 Comodo İnternet Güvenliği – Gezinti

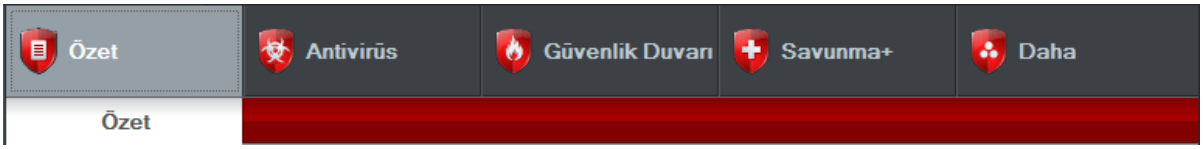
Kurulumdan sonra CIS yüklendiği bilgisayarı otomatik olarak korumaya başlar. Ek olarak bir ayar yapmanıza gerek yoktur.

Ana arayüze nasıl erişileceğini bilmiyorsanız Comodo İnternet Güvenliği'nin Başlatılması bölümüne bakın.

Gezinti

CIS, 5 ayrı bölüme ayrılmıştır.

- Özet
- Antivirüs
- Güvenlik Duvarı
- Savunma+
- Daha.



Bu alanların her biri alt bölümler içerir ve bu bölümler güvenlik yazılımının yapılandırılması üzerinde tam denetim sağlar.

- **Özet – Önemli ayarların ayrıntılarını, etkinlikleri ve diğer bilgileri içerir. Özet ekranı kuruluma göre değişiklik gösterir:**
  - Comodo İnternet Güvenliği
  - Comodo Antivirüs
  - Comodo Güvenlik Duvarı

Bu bölüm hakkında daha fazla bilgi için Özet Ekranlarının Tanıtımı bölümüne bakın.

- **Antivirüs – Bu simgeye tıklayınca Antivirüs Görevleri yapılandırma ekranı açılır.**
- **Güvenlik Duvarı - Bu simgeye tıklayınca Güvenlik Duvarı Görevleri yapılandırma ekranı açılır. Tecrübeli kullanıcılara ilke ve kural oluşumu için öncelikle Ağ Güvenlik İlkeleri bölümüne bakmalarını öneririz.**
- **Savunma+ - Bu simgeye tıklayınca Savunma+ Görevleri yapılandırma ekranı açılır. Tecrübeli kullanıcılara ilke, kural oluşumu ve Sandbox için öncelikle Bilgisayar Güvenlik İlkeleri bölümüne bakmalarını öneririz.**
- **Daha - Bu simgeye tıklayınca Daha... ekranı açılır ve bu bölümde CIS için çeşitli yapılandırma ayarları bulunur.**

1.7 Uyarıların Anlaşılması

CIS ilk kurulumundan sonra birkaç uyarı görebilirsiniz. Bu normaldir ve güvenlik yazılımının uygulamaların davranışlarını öğrendiğini gösterir. Her bir uyarı karar vermenize yardımcı olacak bilgiler içerir. Buna ek olarak benzer uyarılara ileride nasıl cevap verilmesi gerektiğini de belirleyebilirsiniz.

Hafıza Taşırma Koruması Özelliği – Hafıza taşırma saldırısı kötü niyetli programların veya betiklerin kendi belleklerine alabileceğinden daha çok veri göndermeleriyle oluşur. Savunma+ çoğu hafıza taşırma saldırılarına karşı koruma sağlar ve bu tür saldırı girişimlerinde uyarı gösterir. Daha fazla bilgi için Savunma+ Ayarları > Yürütme Denetimi Ayarları > Kabuk kodu enjeksiyonlarını belirle bölülerine bakın.

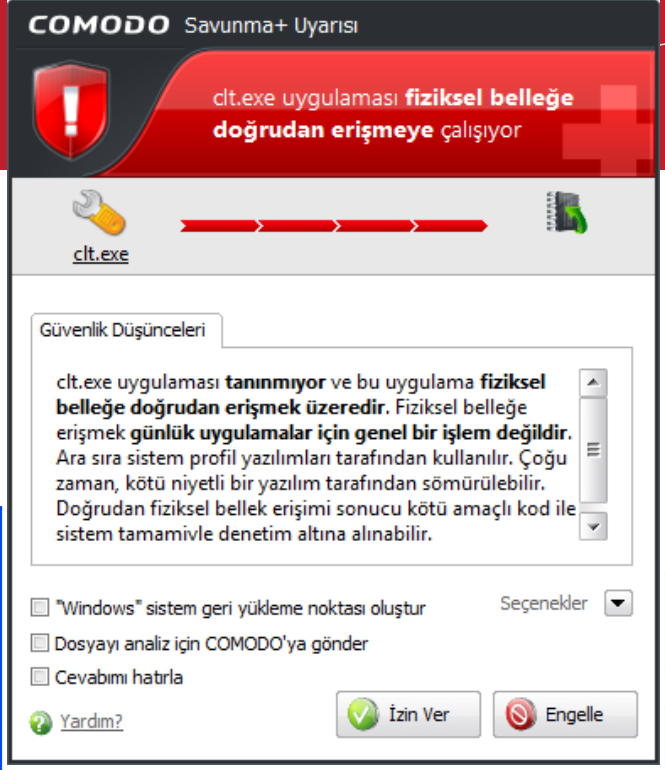
Uyarıların Tanıtımı

CIS uyarıları 4 ana türe ayrılır:

- **Antivirüs Uyarıları**
- **Güvenlik Duvarı Uyarıları**
- **Savunma+ Uyarıları (Yükseltilmiş Ayrıcalık Uyarıları dahil)**
- **Sandbox Uyarıları**

Antivirüs uyarıları sisteminizde bir zararlı yürütüldüğü zaman, Güvenlik Duvarı uyarıları ağ bağlantı girişimlerinde ve Savunma+ uyarıları uygulama davranışları hakkında sizi bilgilendirir. Her üç durumda da uyarılar önemli güvenlik uyarısı içerebilir veya en basitinden bir uygulamayı ilk defa çalıştırdığınız için çıkmış olabilir. Bu uyarılara uyarının içeriğinde bulunan bilgiye göre tepki göstermelisiniz.

Örnek bir uyarı aşağıda göründüğü gibidir.



Renk uyarının önemini belirtir

Güvenlik Duvarı ve Savunma+ uyarılarının her ikisi de risk seviyesine göre renklendirilmiştir

Etkinliğin veya bağlantı girişiminin açıklaması

Simgeler ile hangi uygulamaların hangi yöntemlerin uyarıda bulunduğu hızlıca bilgilendirilir. Yürütülebilirin adına tıklanarak daha fazla bilgi alınabilir.

Bilgi alanında kullanıcının uyarıya nasıl tepki vermesi gerektiği önerilir.

Gerektiği gibi bu seçimleri yapın. Aşağıda açıklanacaktır.

Fazla Seçenek ile görünmeneyen diğer seçenekleri de görebilirsiniz.

Bu düğmelere tıklayarak isteğe izin verebilir veya engelleyebilirsiniz.

Önem Seviyesi

Savunma+ ve Güvenlik Duvarı uyarılarının üst kısımları risk seviyesine göre renklendirilmiştir. Bu bir bakışta uyarının önemini anlamanızı sağlar. Bu rağmen 'Güvenlik Düşünceleri' bölümünü okuyarak bilgi doğrultusunda etkinliğe izin verin veya engelleyin.

Not: Antivirüs uyarıları bu yolla renklendirilmemiştir. Her zaman kırmızı renklidir.

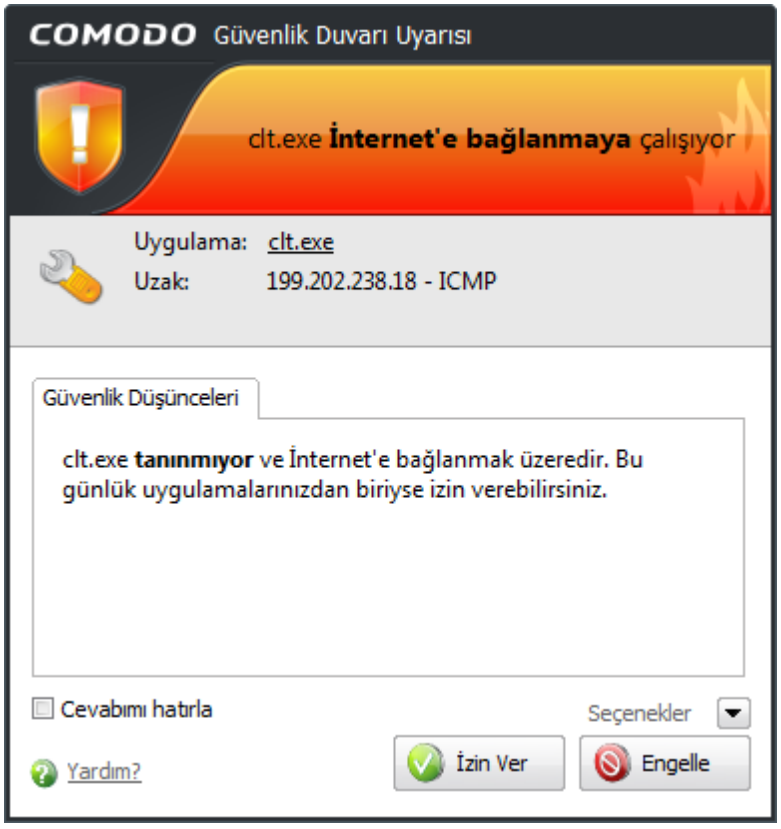
- **Sarı Uyarılar – Düşük Önemde – Çoğu zaman bu renkteki bağlantı isteklerine onay verebilirsiniz. 'Cevabımı hatırla' güvenli uygulamalar için varsayılan olarak seçilidir.**
- **Turuncu Uyarılar – Orta Önemde – 'Güvenlik Düşünceleri' bölümünü karar vermeden önce dikkatlice okuyun. Bu uyarılar zararsız bir işlem veya güvenli program etkinliği sonucunda veya kötücül yazılım saldırı belirtisi olarak çıkabilir. Uygulamayı güvenli olarak biliyorsanız uyarıya izin**

verebilirsiniz. Tanınmayan bir uygulamanın gerçekleştirdiği etkinlik veya bağlantı isteği ise engellemelisiniz.

- **Kırmızı Uyarılar – Yüksek Önemde – Bu uyarılar oldukça şüpheli davranışlar sonucunda çıkar. İzin vermeye karar verdiğinizde bunu bilgilendirmeyi iyicene okumadan yapmayın.**

Uyarıdaki Bilgilendirme

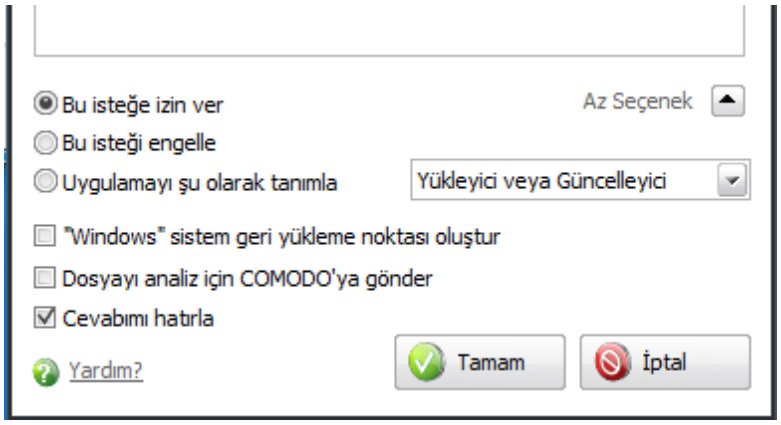
Güvenlik Düşünceleri: Bu alanda uyarıyla ilgili ayrıntılar yer alır. Uyarıya yol açan yazılımın/yürütülebilirin adını; gerçekleştirmeye çalıştığı eylemi ve bu eylemin sisteminizi nasıl etkileyeceğini söyler. Nasıl cevap vermeniz gerektiği hakkında yardımcı öneriler de içerir.



- **Cevabımı hatırla – Güvenlik Duvarı'ndan ileride aynı istekler için uyarı almak istemiyorsanız bu seçeneği işaretleyin.**

Daha Fazla Seçenek

Bu bağlantıya tıklayarak diğer seçenekleri de görünür yapabilirsiniz.



İlk üç seçenek istenilen etkinliğe veya bağlantı isteğine tepki vermenize olanak sağlar.

- **Bu isteğe izin ver – İstenilen etkinliğe veya bağlantı girişimine izin verir.**
- **Bu isteği engelle - İstenilen etkinliği veya bağlantı girişimini engeller.**

- **Uygulamayı olarak tanımla – Söz konusu uygulamaya öntanımlı güvenlik ilkesi seçilmesine olanak sağlar. Bunu seçerek uygulamanın güvenirliğine göre öntanımlı ilke seçebilirsiniz.**

Daha fazla bilgi için Öntanımlı Güvenlik Duvarı İlkeleri ve Öntanımlı Bilgisayar Güvenlik İlkeleri bölümlerine bakabilirsiniz.

- **Dosyaları analiz için COMODO'ya gönder – Şüphelendiğiniz uygulama kötücül yazılım uyarısı verdiyse bu seçeneği seçin. Comodo Internet Security izin ver veya engelle cevabınıza bakmaksızın uygulamayı gönderir. Comodo uygulamayı analiz eder ve duruma göre beyaz veya kara listeye alır.**
- **"Windows" sistem geri yükleme noktası oluştur – Bu seçenek ile Windows'un geri yükleme noktası oluşturması sağlanır. Bu isteğe izin vermenizden veya engellemenizden kaynaklanan bir sıkıntı oluşursa güvenli olarak sistemi önceki noktaya geri döndürebilirsiniz.**
  - Eğer Comodo Time Machine (CTM) kuruluysa CIS, Time Machine geri yükleme noktası oluşturur.
  - Eğer Comodo Time Machine kurulu değilse CIS, normal Windows geri yükleme noktası oluşturur.

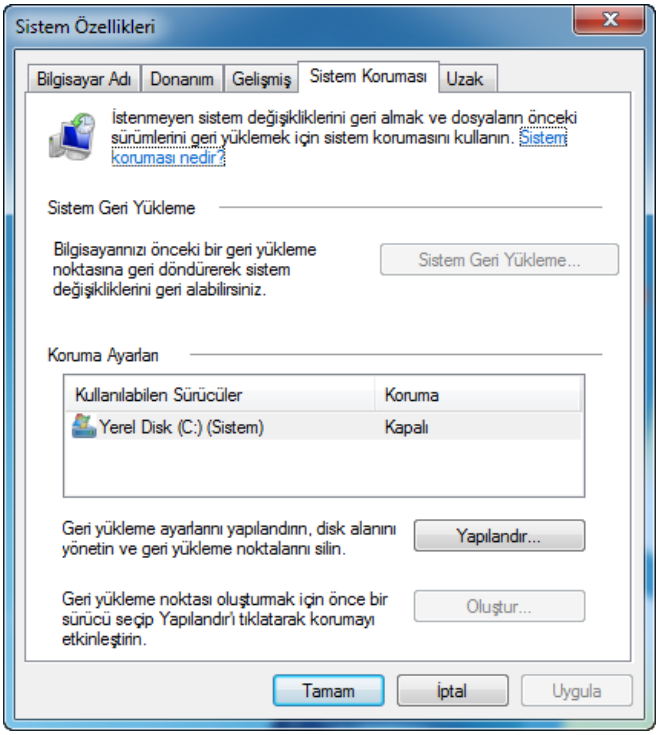
Not: Bu seçenek yalnızca Windows Geri Yükleme etkinse görünür. Windows Denetim Masası'ndan geri yükleme durumunu kontrol edebilirsiniz:

- Windows 7 kullanıyorsanız buraya tıklayın
- Windows Vista kullanıyorsanız buraya tıklayın
- Windows XP kullanıyorsanız buraya tıklayın

Windows 7

Windows sistem geri yüklemenin etkin olduğundan emin olmak için

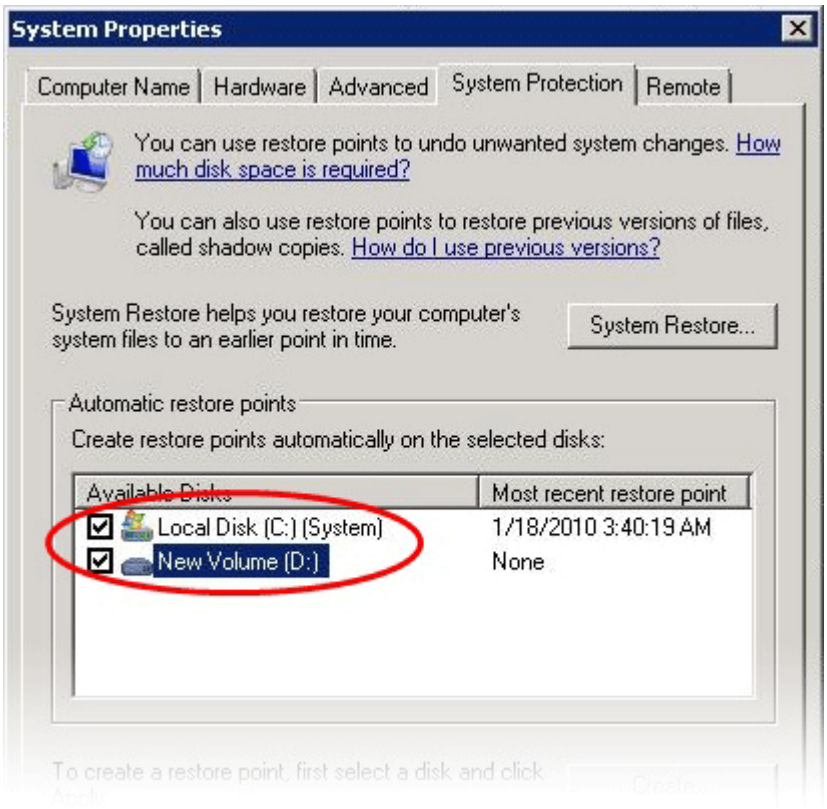
1. Başlangıç > Denetim Masası > Sistem > Sistem Koruması
2. 'Koruma Ayarları' altında disk bölümünün korumasının 'Açık' olduğundan emin olun.



Windows Vista

Windows sistem geri yüklemenin etkin olduğundan emin olmak için

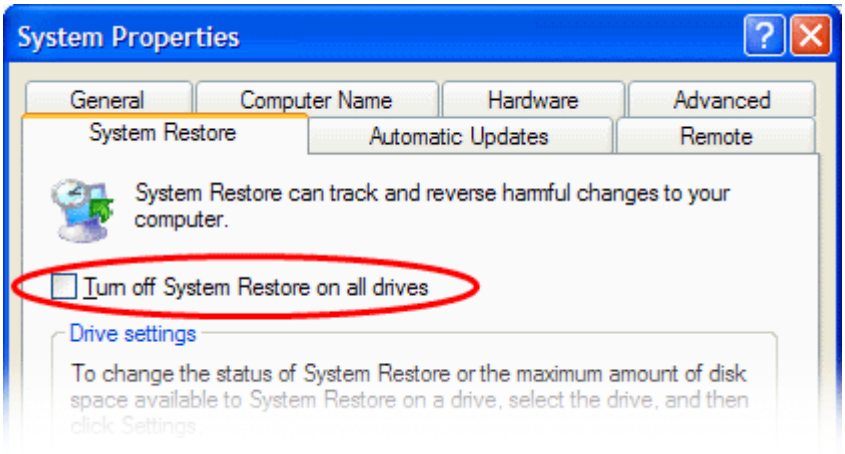
1. Başlangıç > Denetim Masası > Sistem > Sistem Koruması
2. 'Koruma Ayarları' altında disk bölümünün yanındaki kutuların işaretli olduğundan emin olun.



Windows XP

Windows sistem geri yüklemenin etkin olduğundan emin olmak için

1. Başlangıç > Denetim Masası > Sistem > Sistem Geri Yükleme
2. 'Tüm disklerde sistem geri yüklemeyi devre dışı bırak' kutusunun seçili olmadığından emin olun.



Eğer sisteminizde Comodo Time Machine (CTM) kuruluysa Windows Sistem Geri Yüklemenin durumuna

bakılmaksızın geri yükleme noktası oluşturulur.

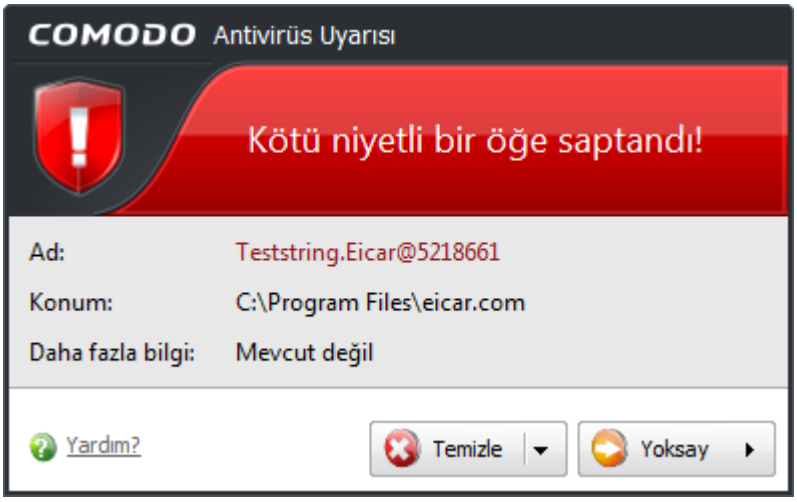
Not: Comodo Time Machine sisteminizi önceki durumuna hızlıca geri döndürmenize olanak sağlayan güçlü bir sistem geri yükleme aracıdır. Daha fazla bilgi ve uygulamayı indirmek için http://www.comodo.com/home/data-storage-encryption/data-recovery.php adresine bakın.

Uyarıları ana hatlarıyla anlattık ve şimdi de onlara nasıl tepki vermeniz gerektiğine bakalım:

Antivirüs Uyarılarının Cevaplanması

Comodo Internet Security bir virüs veya kötücül yazılım bilginiz dışında kopyalanmaya veya çalıştırılmaya çalışılırsa Antivirüs uyarı çıkartır ve ekranın sağ alt köşesinde belirir. Bu uyarılar kullanıcının uygulanması gereken eylemler hakkında değerli bilgiler içerir.

Uyarı saptanan virüsün adını ve dosyanın konumunu veya zararlı bulaşmış uygulamayı içerir.



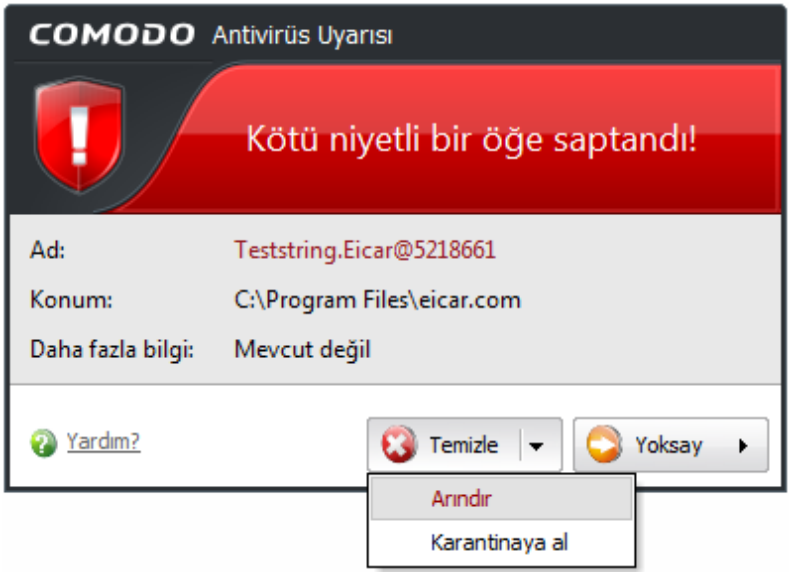
Antivirüs uyarısını cevaplamak için aşağıdaki adımları izleyebilirsiniz.

- **Eğer virüs şüpheli görünüyorsa, dosyası veya uygulamayı daha sonra analiz için Karantinaya Alınmış Öğeler'e taşıyın.**
- **Arındırma mevcutsa saptanan dosyayı arındırın.**
- **Uygulamaya güvenmiyorsanız dosyayı veya uygulamayı sisteminizden silin.**
- **Uygulamaya veya kaynağına güveniyorsanız 'Yoksay' düğmesine tıklayarak uyarı yoksayın.**

Dosyayı veya uygulamayı Karantinaya taşımak için

- **'Temizle' düğmesinin yanındaki açılır liste okuna tıklayarak 'Karantina' düğmesine tıklayın.**

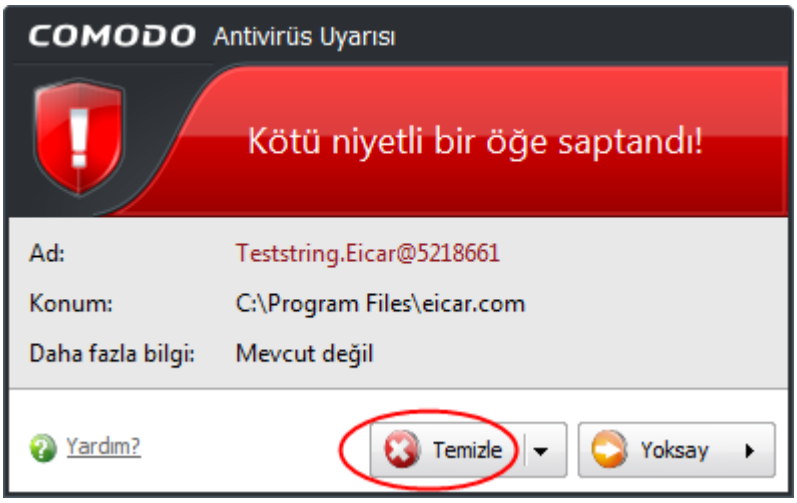
Dosyayı/uygulamayı arındırmak için



- **'Temizle' düğmesinin yanındaki açılır liste okuna tıklayarak 'Arındır' düğmesine tıklayın.**

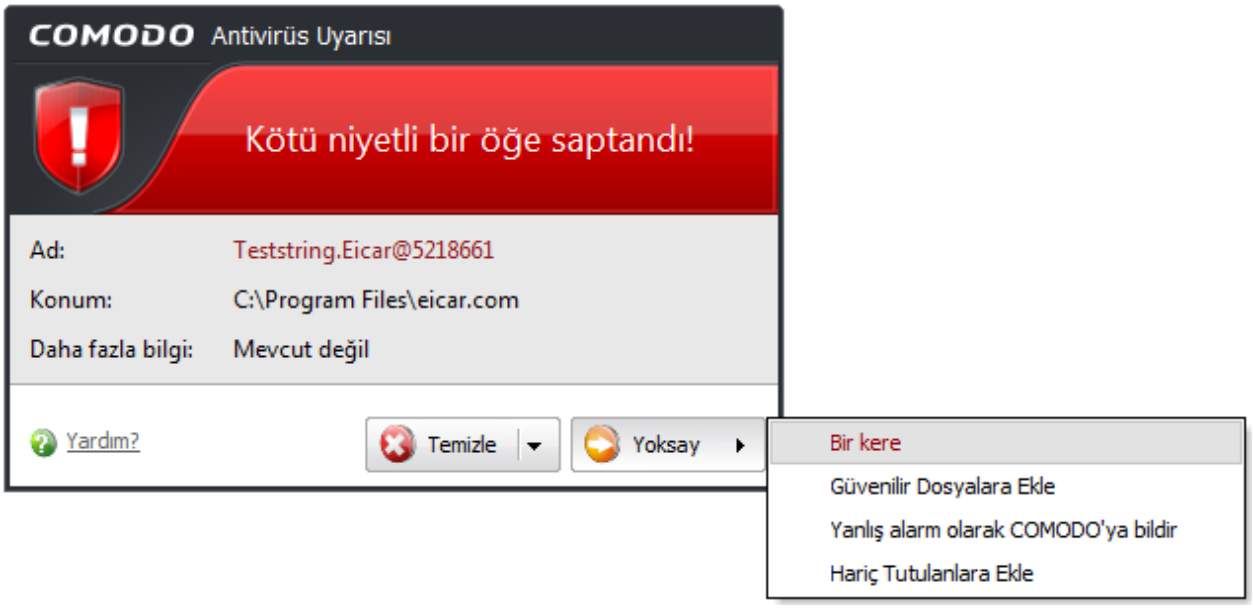
Dosyayı veya uygulamayı kalıcı olarak silmek için

- **'Temizle' düğmesine tıklayın**



Dosyaya/uygulamaya güveniyorsanız uyarı yoksaymak için

- **'Yoksay' düğmesine tıklayın. Yoksayın seçilmesi size dört seçenek sunar.**



- **Bir kere**. Bir kereliğine uyarı yoksayar.
- **Güvenilir Dosyalara ekle**. Dosya Güvenilir Dosyalara taşınır ve bir daha bununla ilgili uyarı çıkmaz.
- **Yanlış Alarm olarak COMODO'ya bildir**. Dosyanın güvenli olduğundan eminseniz dosyayı analiz için COMODO'ya gönderebilirsiniz. Analiz sonucunda dosya güvenilir ise beyaz listeye eklenir.
- **Hariç tutulanlara ekle**. Dosyayı hariç tutulanlara ekler ve bir daha bununla ilgili uyarı almazsınız.

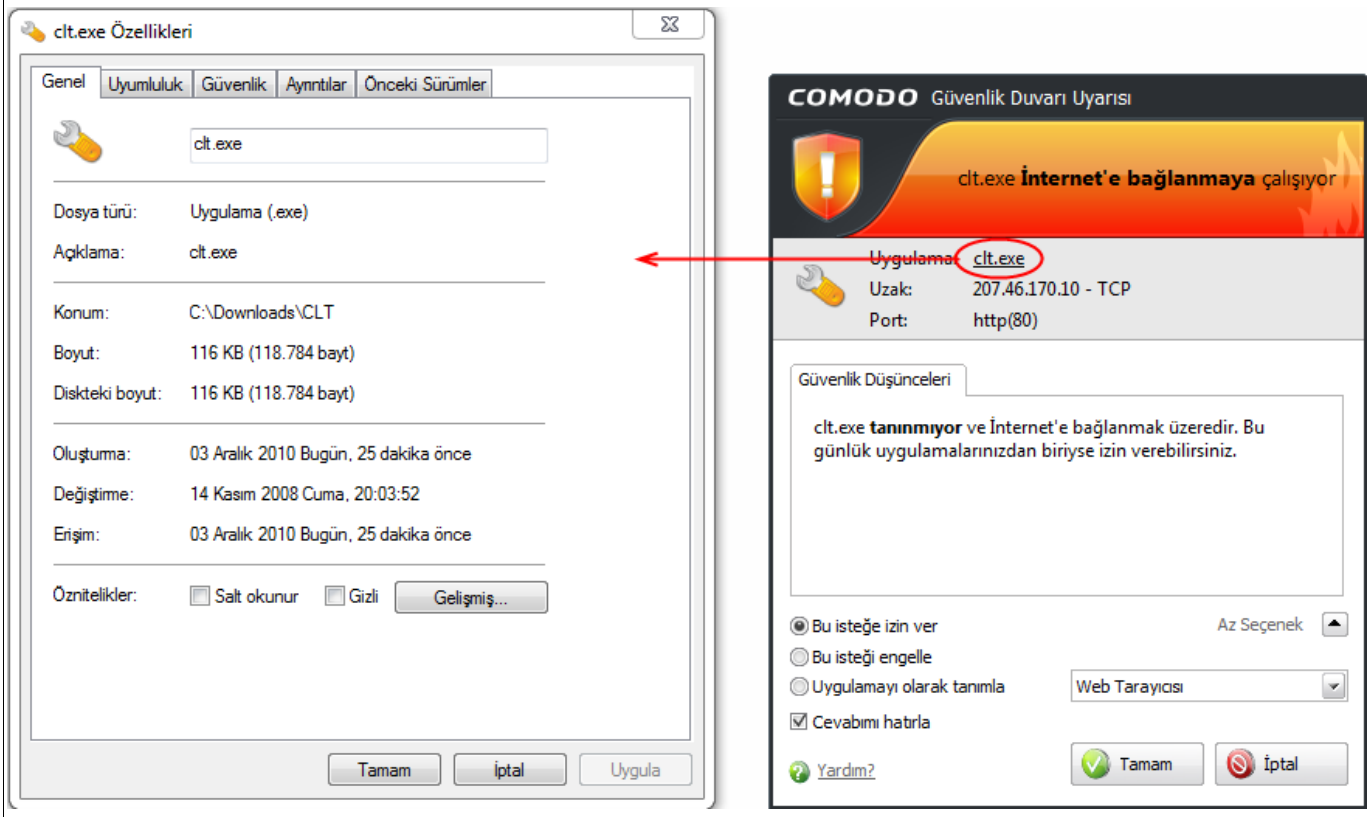
Güvenlik Duvarı Uyarılarının Cevaplanması

Comodo Internet Security ağ bağlantı girişimlerinde Güvenlik Duvarı uyarısı çıkartır. Aşağıdaki adımlar bu uyarılara cevap vermenizde yardımcı olacaktır:

1. Dikkatlicene 'Güvenlik Düşünceleri' bölümünü okuyun. Güvenlik Duvarı binlerce güvenli uygulamayı

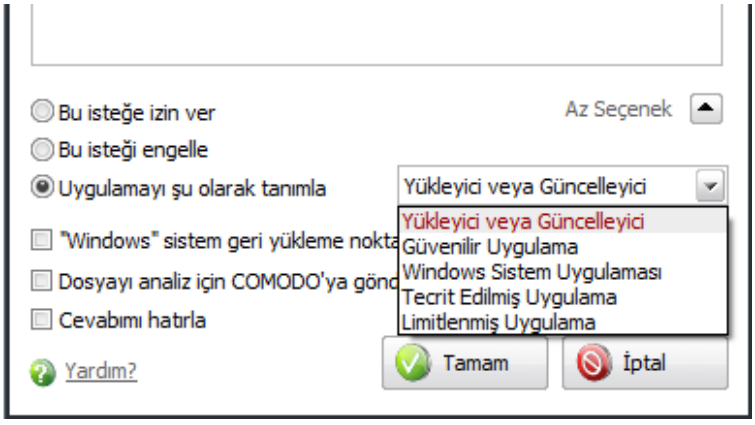
tanıyabilir. Uygulama güvenli olarak biliniyorsa güvenlik düşüncelerinde belirtilir. Benzer olarak, uygulama bilinmiyor veya tanınmıyorsa da belirtilir.

Günlük uygulamalarınızdan biriyse ve internet erişimi vermek istiyorsanız **Bu isteğe izin ver** seçin.



Uygulamayı tanımıyorsanız **Bu isteği engelle** seçin, fakat **Cevabımı hatırla** seçili olmasın.

Tüm durumlarda, uygulama adına tıklayarak karar vermenize yardımcı olabilecek uygulama tercihleri penceresini açabilirsiniz:



2. Günlük uygulamanız olduğundan eminseniz, olabildiğince Bu uygulamayı olarak tanımla seçeneği kullanmaya çalışın. Bu, hedef uygulama için öntanımlı güvenlik duvarı ilkesini kullanır.

Bu uygulamayı olarak tanımla seçeneği görünmüyorsa **Daha Fazla Seçenek** düğmesine tıklayın. **Cevabımı**

hatırla kutusunu işaretleyin.

3. Güvenlik Duvarı uyarısı bir davranışı raporluyorsa, bu davranış güvenlik düşünceleri bölümünde belirtilen kötücül yazılıma uygunsa, bu isteği engellemeli ve bu ayarı kalıcı duruma getirmek için Cevabımı hatırla kutusunu işaretlemelisiniz.

Savunma+ Uyarılarının Cevaplanması

Comodo Internet Security sisteminizde çalışan uygulamaların davranışına göre Savunma+ uyarısı çıkartır. Aşağıdaki adımlar bu uyarılara cevap vermenizde yardımcı olacaktır:

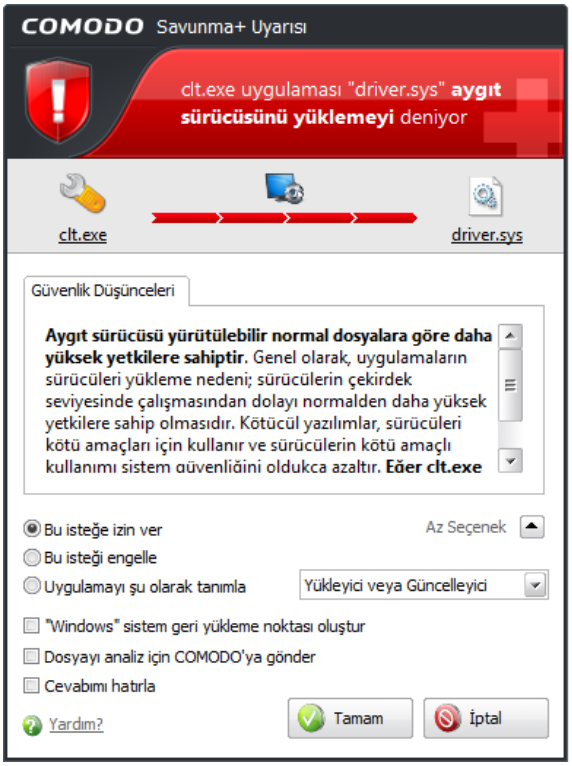
1. Dikkatlicene 'Güvenlik Düşünceleri' bölümünü okuyun. Güvenlik Duvarı binlerce güvenli uygulamayı tanıyabilir. Uygulama güvenli olarak biliniyorsa güvenlik düşüncelerinde belirtilir. Benzer olarak, uygulama bilinmiyor veya tanınmıyorsa da belirtilir.

Günlük uygulamalarınızdan biriyse ve internet erişimi vermek istiyorsanız **Bu isteğe izin ver** seçin.

Uygulamayı tanımıyorsanız **Bu isteği engelle** seçin, fakat **Cevabımı hatırla** seçili olmasın.

2. **Yükleyici veya Güncelleyici** ilkesini bir uygulama kurmuyorsanız kullanmaktan kaçının. Çünkü, uygulamanın 'Kurucu veya Güncelleyici' olarak tanımlanması ona en yüksek ayrıcalıkları atar. Çoğu zaman önceden kurulmuş uygulamalar için bu gerekmemektedir. Eğer 'Yükleyici veya Güncelleyici' seçtiyseniz, **Cevabımı hatırla** seçili olmadan kullanmaya dikkat edin.

3. **Aygıt Sürücüsü Kurulumu** ve **Fiziksel Bellek Erişimi** uyarılarına dikkat edin. Çoğu yasal uygulama bunlara gerek duymaz, bunlar genellikle kötücül yazılım/rootkit davranışlarıdır. Comodo bu istekleri – Bu davranışları yasal bir uygulamanın gerçekleştirdiğinden emin olana dek – engellemenizi önerir.



4. **Korunan Kayıt Defteri** Uyarıları genelde yeni bir uygulama kurarken çıkar. Eğer yeni bir uygulama kurmuyorsanız ve erişim isteğinde bulunan programı tanımıyorsanız 'Korunan Kayıt Defteri Uyarıları' endişeye neden olabilir.

5. **Yükseltilmiş ayrıcalık ile çalıştır**. CIS bilinmeyen bir uygulamanın kurucusunun yönetici veya yükseltilmiş ayrıcalık ile çalıştırılması gerektiği zaman bu tür uyarı verecektir. Bu ayrıcalıklarla çalıştırılan bir kurucu sistemin önemli bölgelerinde değişiklik yapabilir.

•Uygulamaya güveniyorsanız 'İzin Ver' düğmesine tıklayarak kurucuya yükseltilmiş ayrıcalık sağlayabilirsiniz.

- Uygulamanın güvenirliğinden emin değilseniz 'Sandbox' düğmesine basmanızı öneririz.
- Beklenmedik bir uyarı aldıysanız kurulumu 'Engelle' düğmesine basarak iptal etmelisiniz.
- 'Bu dosyanın sağlayıcısına her zaman güven' kutusunu seçtiyseniz CIS bu kurucunun tüm dosyalarını güvenli olarak varsayacaktır ve ileride bu sağlayıcı için bir daha uyarı vermeyecektir.
- Tüm durumlarda lütfen 'Dosyayı analiz için COMODO'ya gönder' kutusunu seçmeyi unutmayın böylece araştırmacılarımız dosyalarda gerekli denetimleri gerçekleştirebilirler.

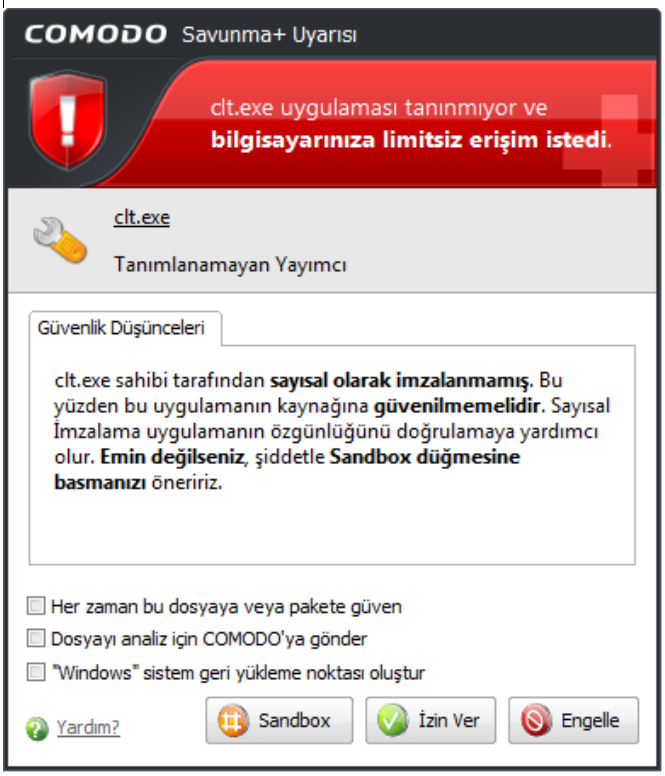
Bu tür bir uyarı göreceksiniz eğer:

- Sandbox etkin ise

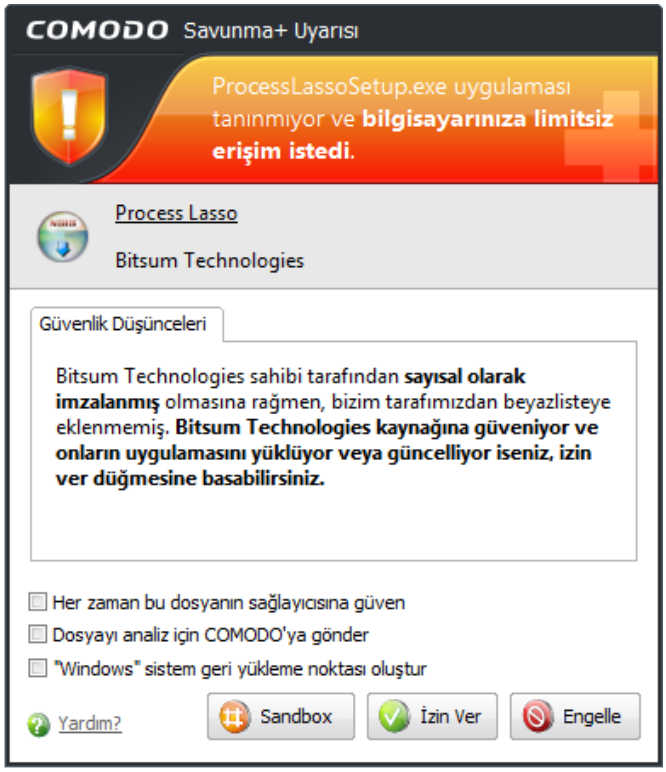
ve

- 'Kurucuları otomatik olarak sapta ve sandbox dışında çalıştır' etkin ise. Bu ayarlar Savunma+ Görevleri > Savunma+ Ayarları > Sandbox Ayarları içinden değiştirilebilir.

İki farklı uyarı vardır – sayısal olarak imzalanmamış ve bilinmeyen kurucular için ve sayısal olarak imzalanmış fakat beyaz listeye eklenmemiş kurucular için.



Tanınmayan ve sayısal olarak imzalanmamış



Tanınmayan ve sayısal olarak imzalanmış fakat henüz beyaz listede değil
(henüz "Güvenilir Yazılım Sağlayıcıları" listesine eklenmemiş)

•Bilinmeyen ve imzalanmamış kurucular sandbox içinde çalıştırılmalı veya engellenmelidir.

•Bilinmeyen fakat imzalanmış kuruculara sağlayıcısına güveniyorsanız izin verilebilir veya uygulamanın davranışını değerlendirmek istiyorsanız sandbox içinde çalıştırabilirsiniz.

•Her iki durumda da 'Dosyaları analiz için COMODO'ya gönder' kutusunu seçebilirsiniz.

Ayrıca bakınız:

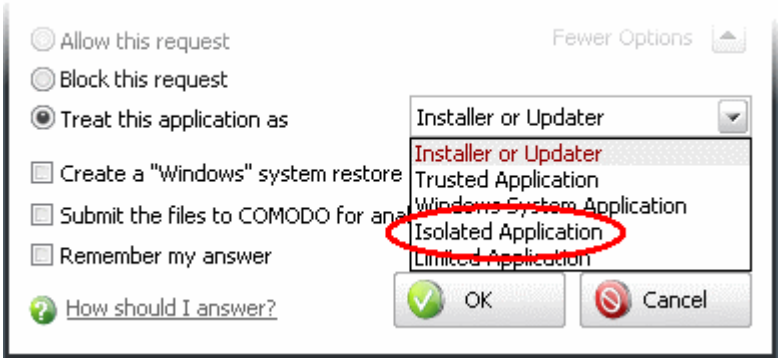
- 'Sandbox Uyarılarının Cevaplanması' - CIS'in kurucu veya güncelleyici olarak tanınmayan uygulamaları nasıl ele aldığını görmek için.
- 'Bilinmeyen Dosyalar: Sandbox ve İşlemlerin Taranması' – CIS'in bazı uygulamaları neden sandbox içine almayı tercih ettiğini anlamak için.
- 'Güvenilir Yazılım Sağlayıcıları' – Sayısal olarak imzalanmış dosyaların açıklaması ve 'Güvenilir Yazılım Sağlayıcıları'.

1. **Korunan Dosya Uyarıları** genellikle doysa indirirken veya kopyalarken veya kurulu uygulamayı güncellerken çıkar.

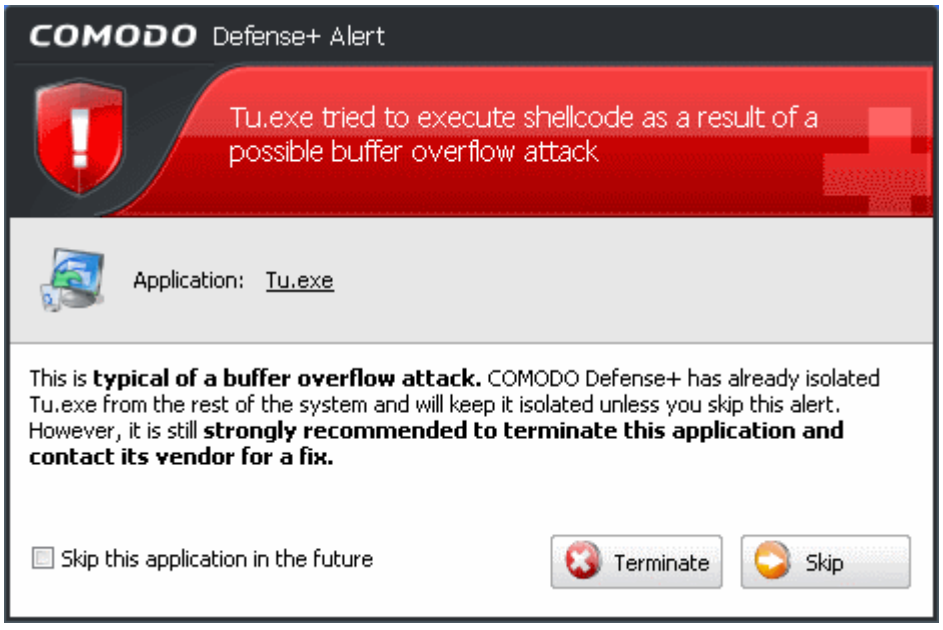
Gereksiz uyarıların kural listenizi doldurmasını önlemek için **Cevabımı hatırla** seçili olmadan uyarılara izin verebilirsiniz.

Tanımadığınız bir uygulama Windows dizininde yürütülebilir dosya oluşturmaya çalışıyorsa buna dikkat edin. Bu dizin kötücül yazılımların favori hedeflerindendir. Yeni bir uygulama kurmuyor veya güncellemiyorsanız, **Cevabımı hatırla** seçili olmadan **Bu isteği engelleyi** seçin.

Uygulama rasgele adla yeni bir dosya oluşturmaya çalışıyorsa örn. "hughbasd.dll" muhtemelen zararlıdır ve kalıcı olarak '**Tecrit Edilmiş Uygulama Olarak Say**' seçilerek engellenmelidir.



2. Tampon taşma Uyarısı uygulama tamponun işleyebileceğinden daha fazla veriyi tampona göndermesiyle meydana gelir. Bu olası bir korsan saldırısı olabilir.



Sonlandıra tıklarsanız uygulamanın çalıştırılması reddedilecektir.

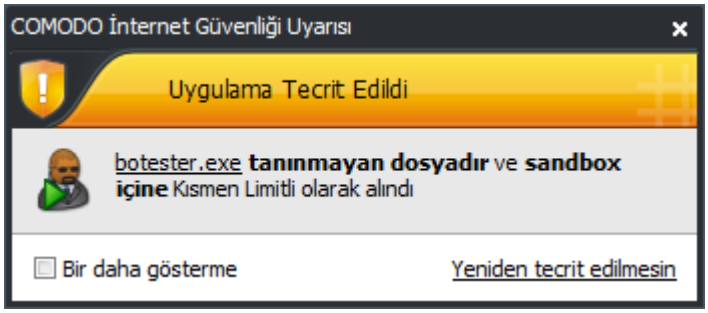
Atlaya tıklarsanız uygulama izlenmeyecektir ve erişime izin verilecektir. Fakat sonraki girişimde uyarı çıkacaktır.

'**Bu uygulamayı ileride atla**' seçerseniz ve **Atla**ya tıklarsanız uygulama kalıcı olarak izlenmeyecektir ve her zaman erişime izin verilecektir. Güvenilir sağlayıcıdan gelen bir uygulamaysa bunu yapın.

3. Savunma+ güvenlik düşünceleri bölümünde kötücül yazılım davranışı bildiriyorsa Cevabımı hatırla seçerek kalıcı olarak Bu isteği engellemelisiniz ve analiz için COMODO'ya göndermelisiniz.
4. Tanınmayan uygulamalar her zaman kötü değildir. Comodo tarafından tanınmayan günlük uygulamalarınıza da izin verebilirsiniz. Bu tür uygulamaları analiz için COMODO'ya gönderebilirsiniz.
5. Savunma+ Temiz BS Kipindeyken muhtemelen çok sayıda uyarı görüyorsunuzdur. 'Tanınmayan Dosyalar' listesindeki dosyaları gözden geçirin ve güvenli olanları listeden kaldırın böylece bu dosyaların CIS tarafından güvenli olarak varsayılmasını sağlayabilirsiniz.
6. Güvenilir Uygulama veya Windows Sistem Uygulaması ilkelerini eposta istemcisi, web tarayıcısı, IM veya P2P uygulamaları için kullanmaktan kaçının. Bu uygulamalar bu tür güçlü erişim haklarına gerek duymazlar.

Sandbox Uyarılarının Cevaplanması

Varsayılan olarak, CIS her ne zaman bilinmeyen bir uygulamayı sandbox içine alırsa uyarı gösterir:



Uyarı tecrit edilen yürütülebilir dosyanın adını gösterir ve otomatik olarak bu dosya Tanınmayan Dosyalara eklenir.

•Uygulama adına tıklayarak Tanınmayan Dosyalar arayüzüne gidebilirsiniz.

•Yeniden tecrit edilmesin bağlantısına tıklayarak uygulamayı Tanınmayan Dosyalar listesinden kaldırarak Güvenilir Dosyalara ekleyerek sandbox dışında çalıştırabilirsiniz. Uygulama güvenliyse bunu seçin.

Ayrıca bakınız:

- 'Yükseltilmiş ayrıcalıklar ile çalıştır' uyarıları.
- 'Bilinmeyen Dosyalar: Sandbox ve İşlemlerin Taranması' - CIS'in bazı uygulamaları neden sandbox içine almayı tercih ettiğini anlamak için.

2 Antivirüs Görevleri - Tanıtım

Antivirüs Görev Merkezi antivirüs bileşenini tüm yönleriyle ve hızlıcana yapılandırmanıza olanak sağlar.

Comodo Antivirüs çoklu koruma teknolojileri sunar, Gerçek zamanlı/Erişimde Tarama, Elle Tarama ve Zamanlanmış Tarama özellikleri de bulunur. Uygulama kullanıcıların özelleştirilmiş tarama profilleri oluşturmasına, tam kapsamlı günlükleme yapmasına, karantinaya almasına ve dosya gönderimi yapabilmelerine de olanak sağlar.

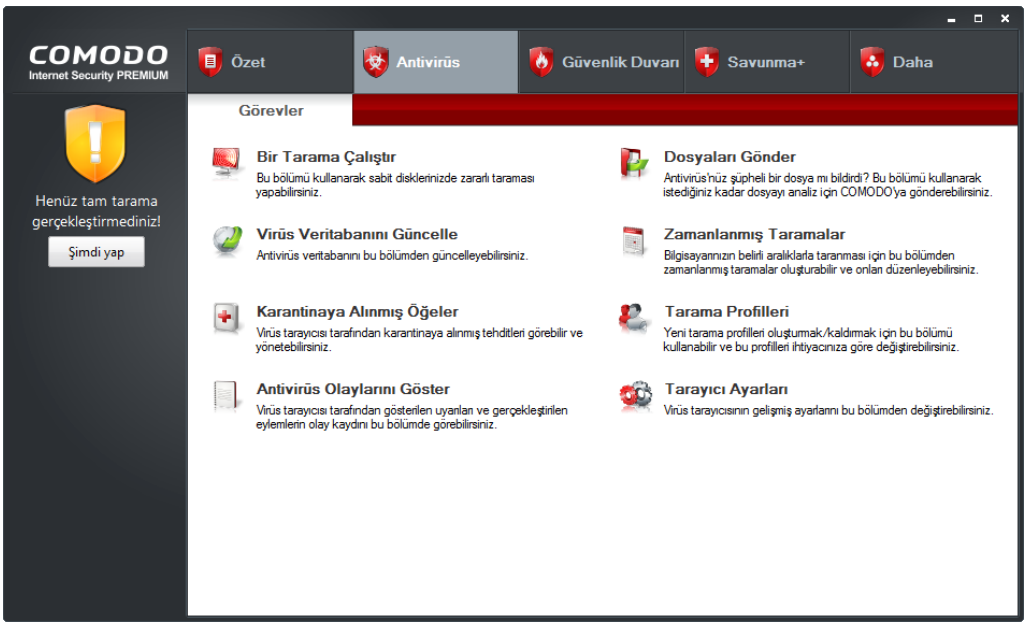
Comodo Antivirüs makinada bulunan tehditleri saptar ve kaldırır. Güvenlik Duvarı ve Savunma+ önleme korumalarının yanında ek bir katmanda koruma sağlar. Sezgisel taraması ile bilinmeyen zararlıları belirler.

En iyi güvenlik seviyesini sürdürmek için Comodo düzenli olarak antivirüs taraması yapmanızı önerir.

Elle Tarama Windows işletim sistemi ile bütünleştirilmiştir. Dosyaya, klasöre veya sürücüye sağ tıklayarak içerik menüsünden '**Comodo Antivirüs ile Tarat**' ile belli nesneleri anında taratabilirsiniz.

Antivirüs görev merkezine gezinti panelindeki Antivirüs sekmesine 

tıklayarak erişilebilir.



Antivirüs yapılandırma alanı tüm özelliklere kolayca erişim sağlar. Bu bölümler hakkında ayrıntılı açıklamaları görmek için aşağıdaki bağlantılara tıklayın.

•Bir Tarama Çalıştır

•Virüs Veritabanını Güncelle

•Karantinaya Alınmış Öğeler

•Antivirüs Olaylarını Göster

2.1 Bir Tarama Çalıştır

Bir sürücüyü veya klasörü olası bir bulaşma için denetlemek istediğinizde **Bir Tarama Çalıştır** ile **Elle Tarama** başlatabilirsiniz.

Elle Tarama seçtiğinizde iki seçeneğiniz vardır:

1. Öntanımlı bir Alanı Tarama; veya
2. Seçtiğiniz bir alanı tarama, Tarama Profili oluşturarak.

- **Belirli nesneleri İçerik Menüsünü kullanarak da taratabilirsiniz.**

Öntanımlı Alanların Taranması

Comodo Antivirüs'te üç tane öntanımlı tarama profili bulunur. Bunlar:

i.**Bilgisayarım** – Tüm sürücüler tamamen taranır.

ii.**Kritik Alanlar** – Program Dosyaları ve WINDOWS klasörü taranır.

iii.**Casus Yazılım Taraması** – Windows Kayıt Defteri ve Sistem dosyaları taranır.

Özel Tarama

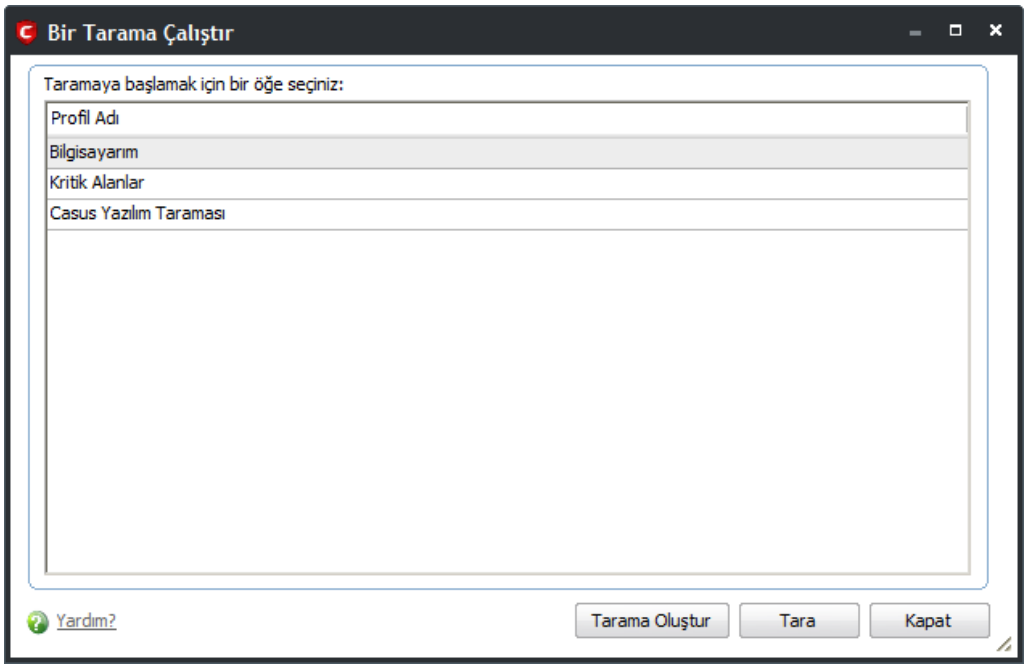
Tarama Profili ayarlayarak özel tarama yapabilirsiniz. Tarama Profilleri hakkında daha fazla bilgi için Antivirüs Görevleri > Tarama Profilleri ne bakın. **Bir Tarama Çalıştır** kullanarak da Taramam Profili oluşturabilirsiniz.

Comodo Antivirüs ayrıca arşiv dosyalarını da tarar (.ZIP, .RAR gibi, elle tarama yapılırken).

Elle tarama başlatmak için

1. Antivirüs Görev Yöneticisinden 'Bir Tarama Başlat' bölümüne tıklayın.

'Bir Tarama Başlat' paneli görünür.



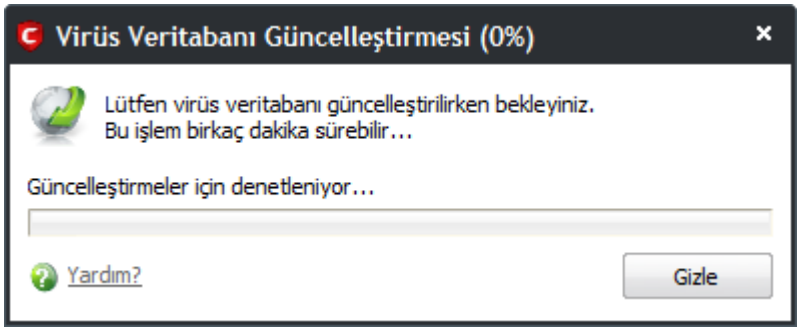
'Bir Tarama Başlat' panelinden

- **Panelde listelenen öğelerden birini taratın**
- **Tarama için yeni bir öğe ekleyerek yeni bir taramam profili oluşturun**
- **Tarama sonucunu metin dosyası olarak kaydedin**
- **Saptanan tehditleri karantinaya taşıyın**
- **Dosyayı/uygulamayı yöntem mevcutsa arındırın**
- **Zararlı bulaşmış dosyaları, klasörleri veya uygulamaları silin**
- **Güvenli olarak saydığınız dosyaları hariç tutun**

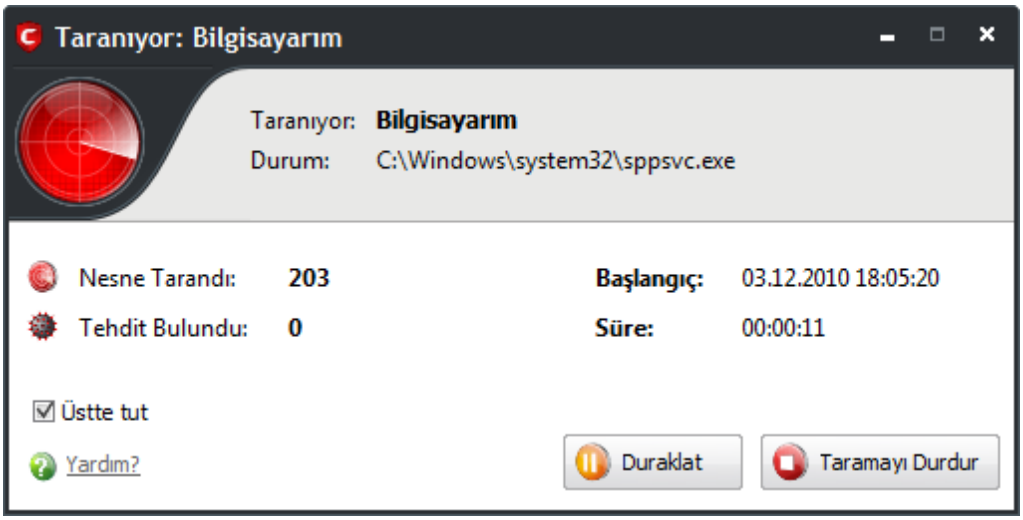
Siteminizi zararlılara karşı taramak için

1. 'Bir Tarama Çalıştır' tıklayın.
2. Tarama Profili'ni seçin ve 'Tara' düğmesine tıklayın.

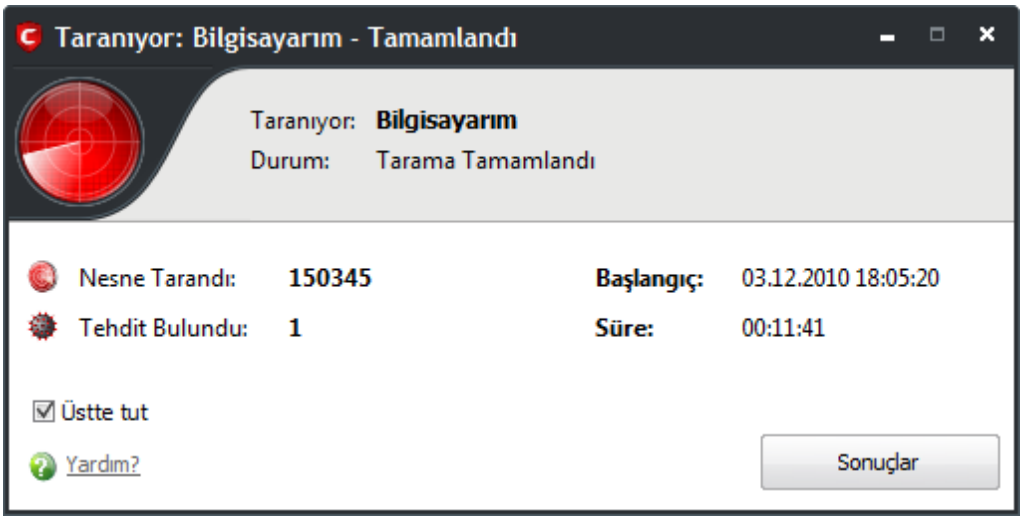
Comodo Antivirüs, AV veritabanı güncelleştirmelerini denetler ve varsa yükler.



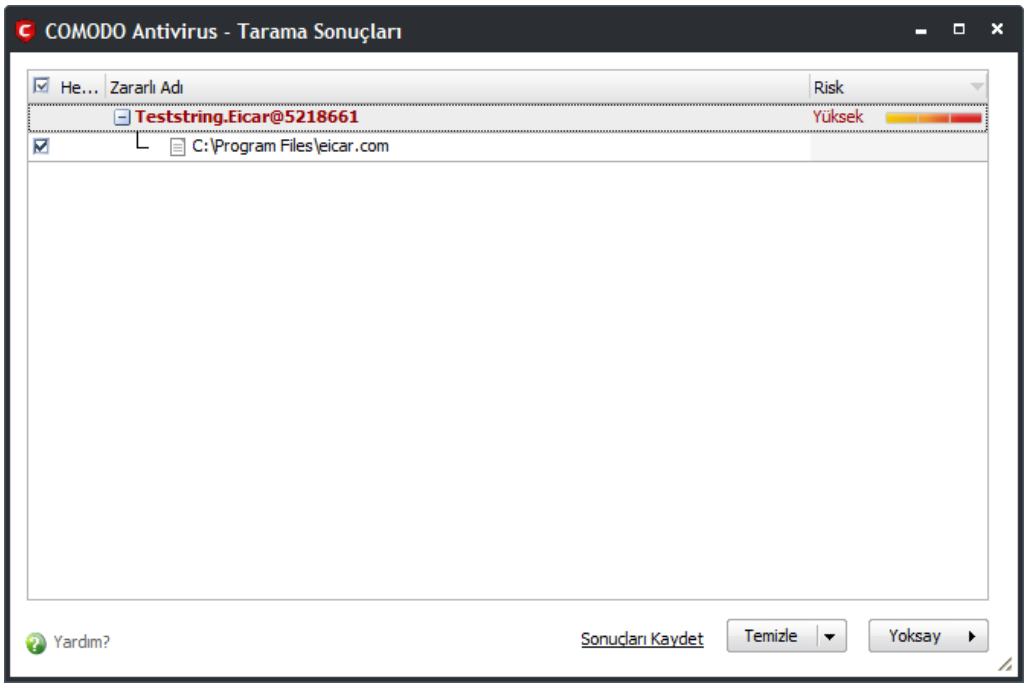
Daha sonra Comodo Antivirüs tarama profiline göre seçili öğeleri taramaya başlar.



Tarama tamamlandıktan sonra 'Tarama Tamamlandı' penceresi görüntülenir.



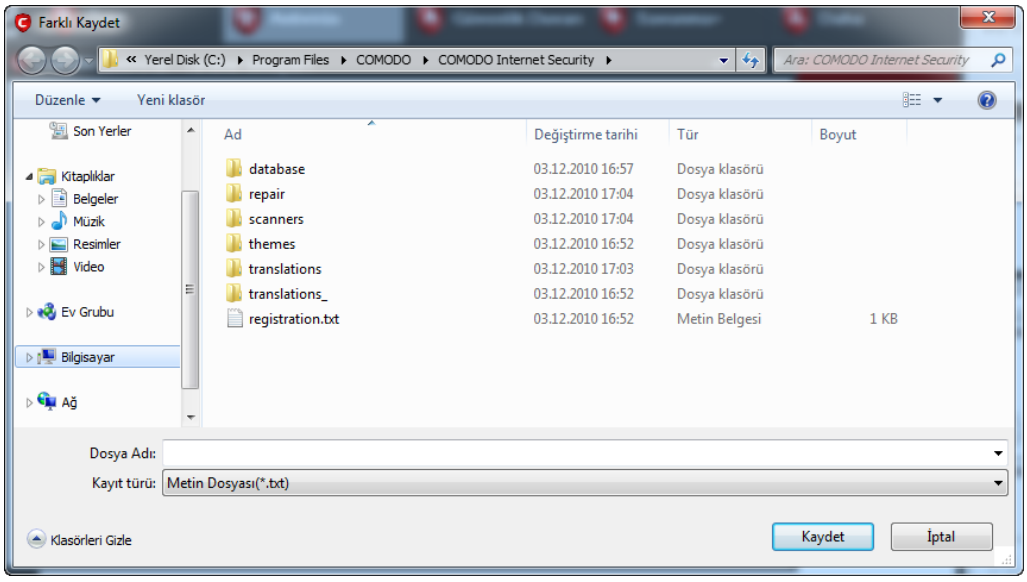
3. Tarama Sonuçları penceresini görüntülemek için 'Sonuçlar' düğmesine tıklayın. Sisteminizde şüpheli dosyalar saptandıysa bunlar tarama sonucu penceresinde görüntülenir.



İpucu: 'Tehdit Adı' sütun başlığına tıklayarak tehditleri alfabetik olarak sıralayabilirsiniz. Benzer olarak 'Risk' sütun başlığına tıklayarak da risk seviyesine göre sıralayabilirsiniz. Tüm girdileri seçmek için 'Tehdit Adı' yanındaki kutuyu işaretleyin.

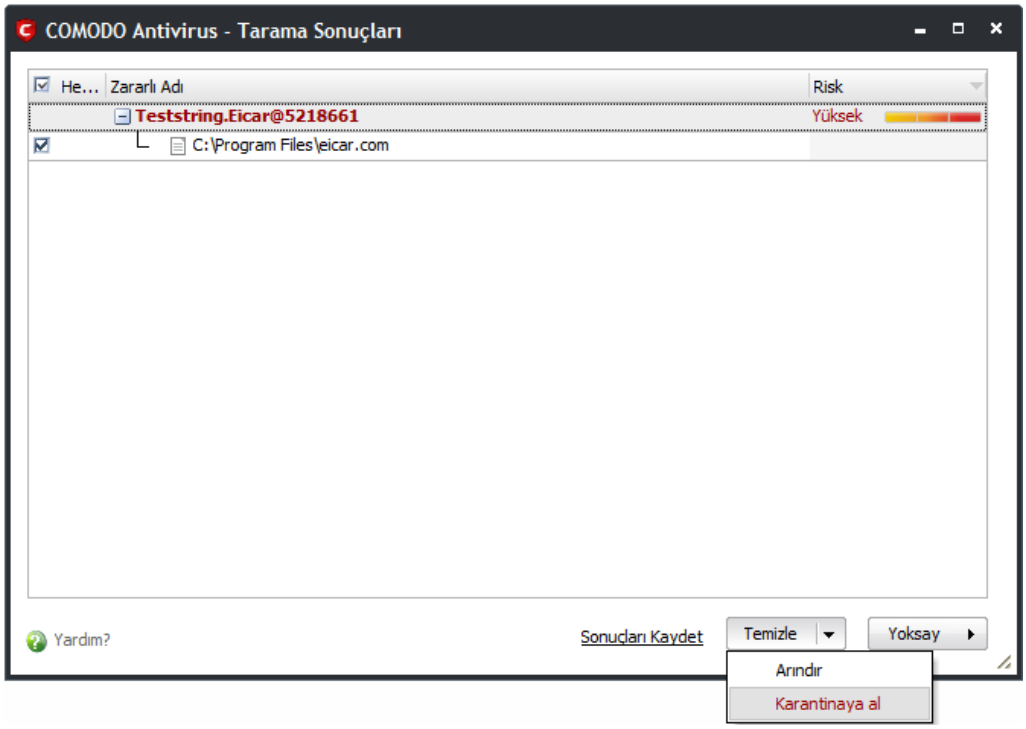
Tarama Sonuçlarını Metin Dosyasına kaydetmek için

1. 'Kaydet' düğmesine tıklayın ve dosyanın kaydedileceği konumu seçin.

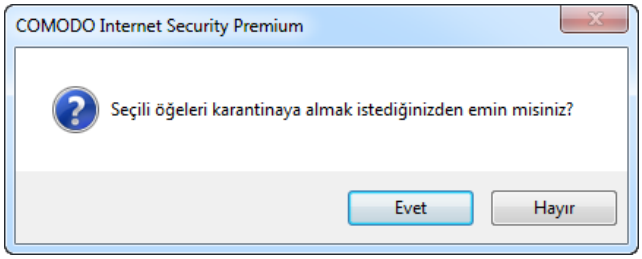


Saptanan dosyaların Karantinaya taşımak için

1.Sonuçlardan uygulamayı seçin, 'Temizle' düğmesinin yanındaki açılır liste düğmesine tıklayın ve 'Karantinaya Al' seçin.



2.Onaylama diyaloğundan 'Evet' düğmesine tıklayın.

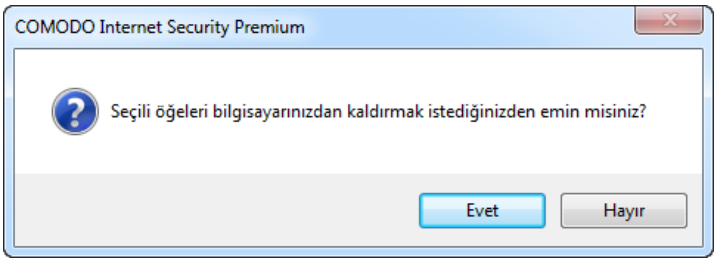


Daha fazla bilgi için Antivirüs Görevleri > Karantinaya Alınmış Öğeler.

Tehditler ile saptanan dosyaları / uygulamaları arındırmak için

1.Sonuçlardan uygulamayı seçin, 'Temizle' düğmesinin yanındaki açılır liste düğmesine tıklayın ve 'Arındır' seçin.

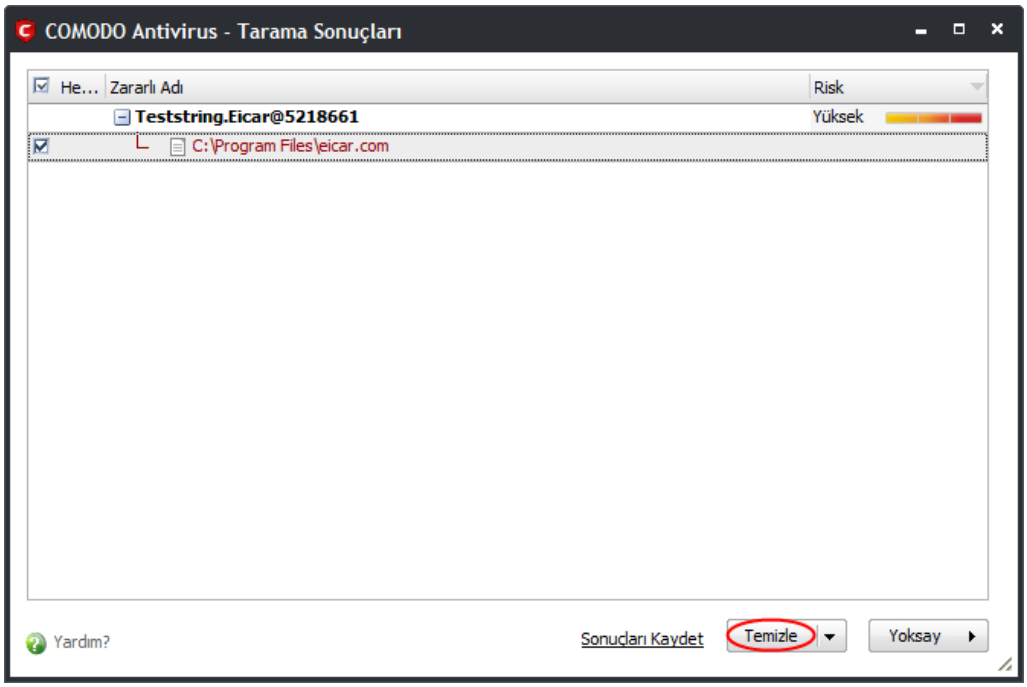
2.Onaylama diyaloğundan ‘Evet’ düğmesine tıklayın.



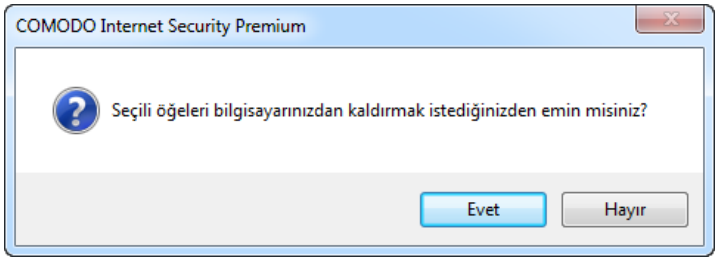
Antivirüs arındırma yöntemi mevcut ise dosyayı arındırır, değilse dosyayı kalıcı olarak sistemden siler.

Tehdit ile saptanan uygulamayı silmek için

1. Sonuçlardan uygulamayı seçin ve ‘Temizle’ düğmesine tıklayın.

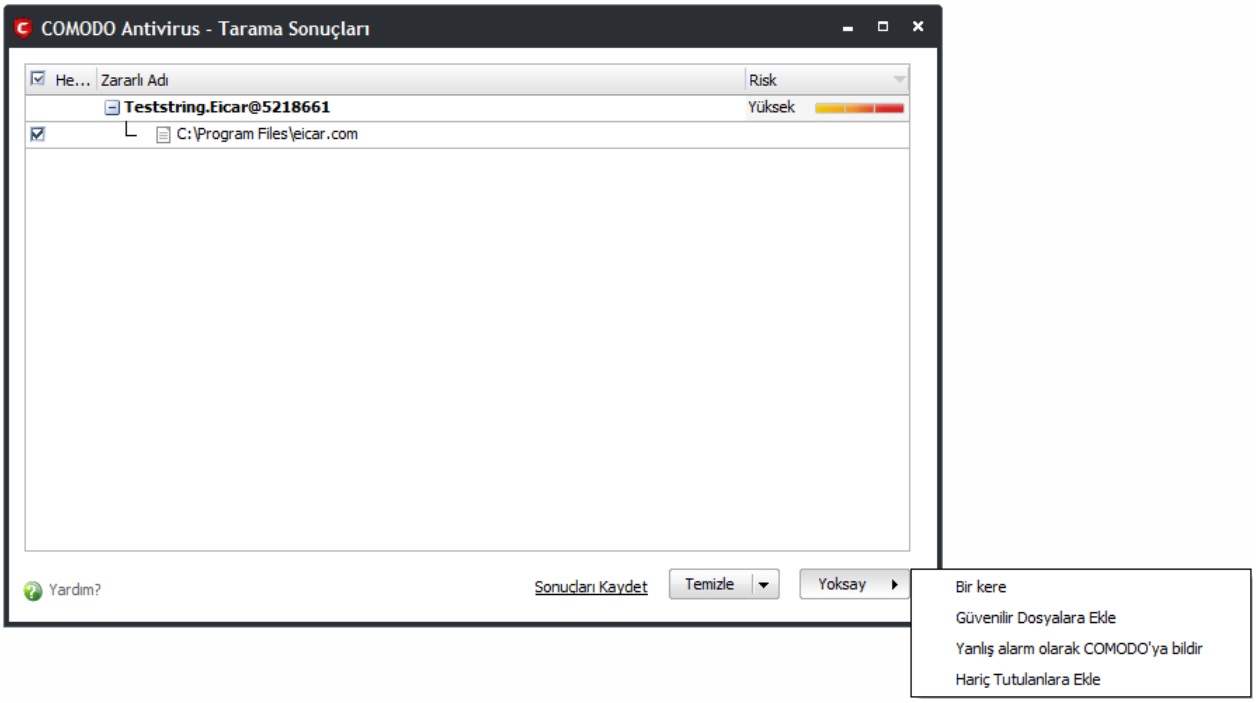


2. Onaylama diyaloğundan 'Evet' düğmesine tıklayın.



Tehdit listesindeki güvenli olarak saydığınız uygulamayı / dosyayı yoksaymak için

•'Yoksay' düğmesine tıklayın



Yoksay altında dört seçenek bulunmaktadır.

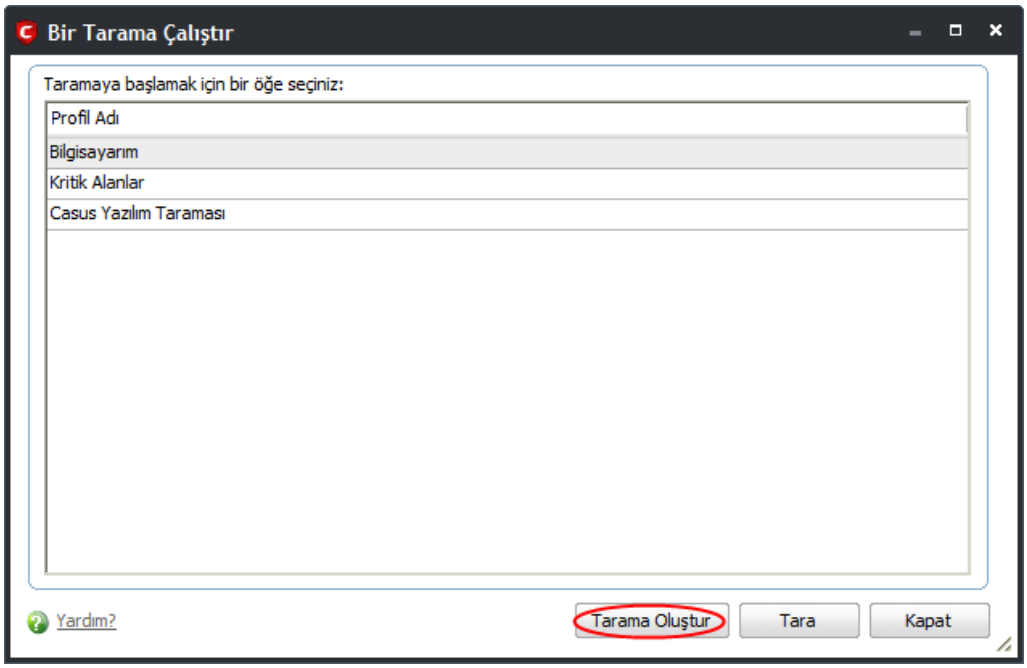
- **Bir kere -** Bir kereliğine yoksayar, aynı uygulama bir daha çağrılırsa uyarı çıkar.
- **Güvenilir Dosyalara Ekle -** Dosya 'Güvenilir Dosyalara' taşınır ve bir daha onunla ilgili uyarı verilmez.
- **Yanlış Alarm olarak COMODO'ya bildir –** Uyarının hatalı olduğunu düşünüyorsanız bunu bildirmek için kullanın. Dosya güvenli ise Comodo beyaz listesine eklenir.
- **Hariç tutulanlara ekle -** Dosya 'Hariç tutulanlara' taşınır ve bir daha onunla ilgili uyarı verilmez.

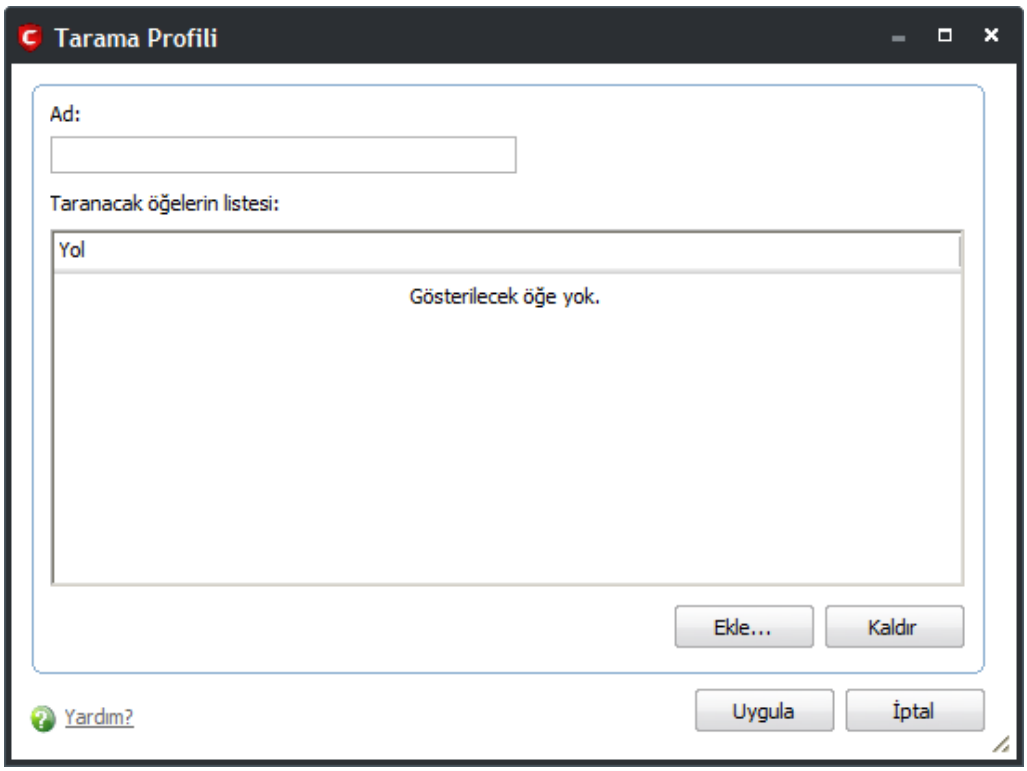
Tarama Profili Oluşturulması

Tarama Profilleri kullanıcı tanımlı bölgelerdir ve ileriki taramalarda yeniden kullanılabilir.

Yeni tarama profili oluşturmak için

1.'Bir Tarama Çalıştır' arayüzünden 'Yeni Tarama Oluştur' düğmesine tıklayın.

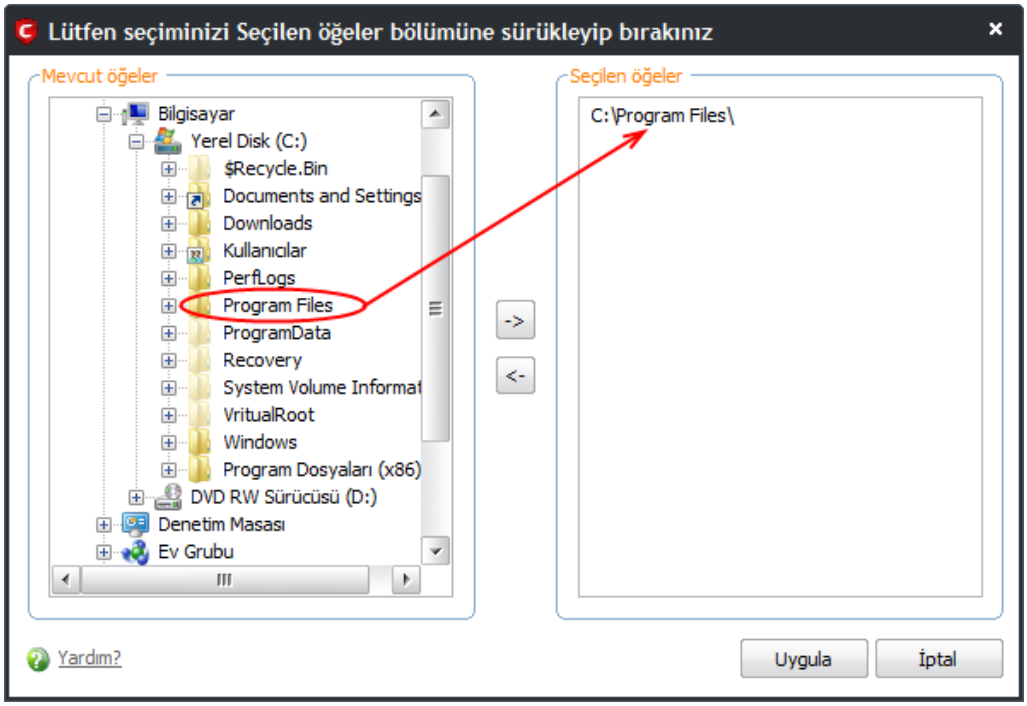




'Tarama Profili' yapılandırması görüntülenecektir.

2.'Ad' bölümüne tarama profili adını girin.

3.'Ekle' düğmesine basın.



Yapılandırma ekranı görünür, taranmasını istediğiniz konumları seçebilirsiniz.

4.Sol sütundan konumları seçerek sağ sütuna sürükleyip bırakarak ekleyebilirsiniz veya okları kullanabilirsiniz.

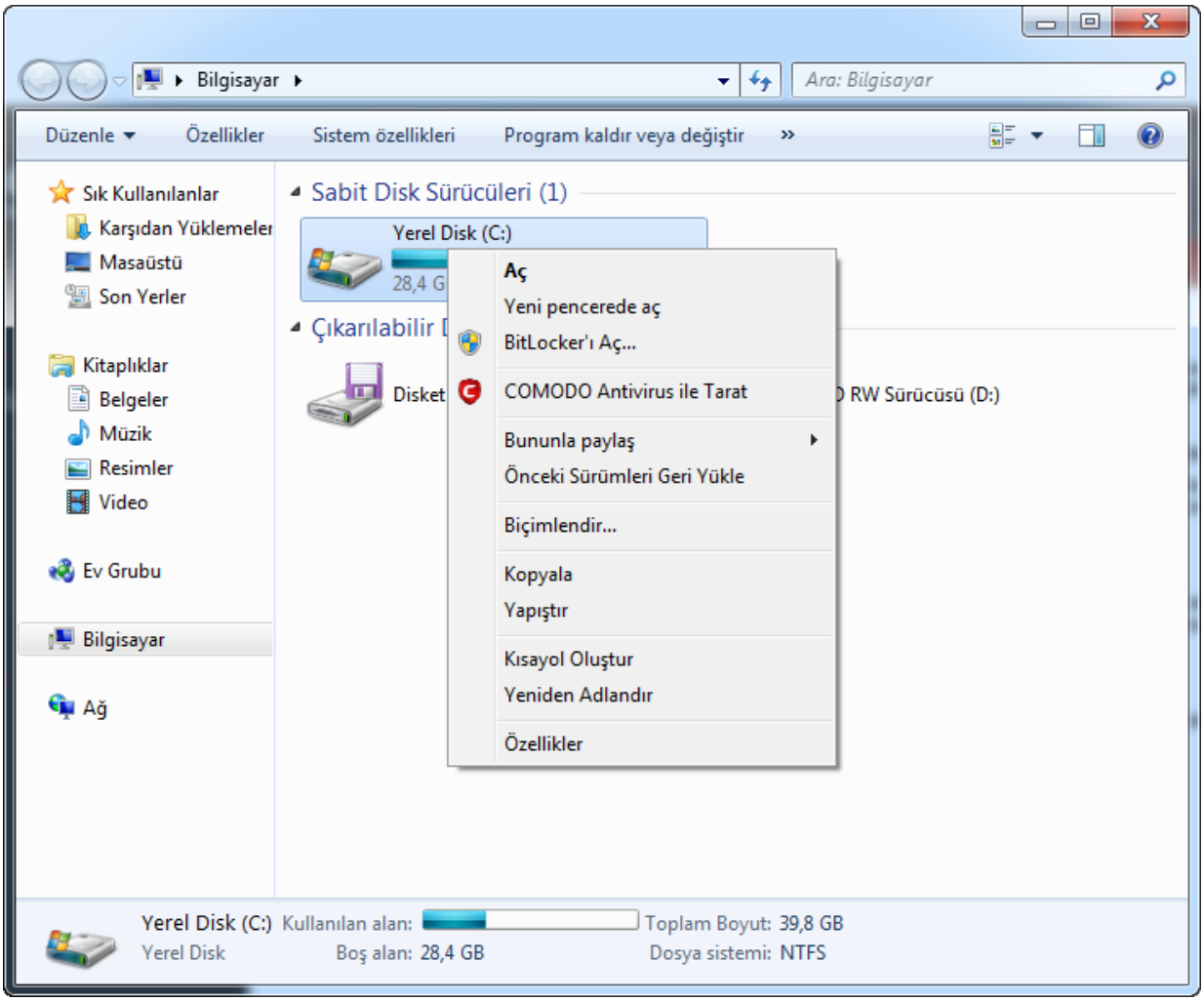
5.'Uygula' düğmesine tıklayın.

6.İşlemi tekrarlayarak daha fazla Tarama Profili oluşturabilirsiniz.

Not: Antivirüs Ekranındaki Tarama Profilleri bölümünü kullanarak da yeni profiller oluşturabilirsiniz.

İçerik Menüsü ile Tarama

Sürücü, dosya veya klasöre sağ tıklayarak 'Comodo Antivirüs ile Tarat' ile seçili nesneleri taratabilirsiniz.



2.2 Virüs Veritabanının Güncellenmesi

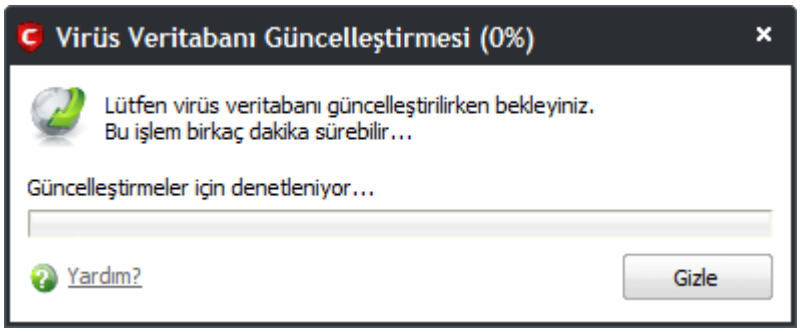
Antivirüs yazılımının geçerliliğini koruyabilmesi için düzenli olarak güncellenmesi gerekmektedir.

Elle virüs Veritabanı denetimi ve daha sonra güncellemelerin yüklenmesi

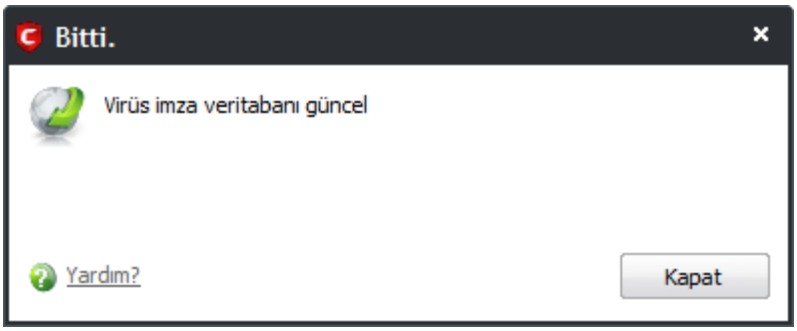
1. Antivirüs ekranından 'Virüs Veritabanını Güncelle' bölümüne tıklayın.

Not: Güncellemeleri yükleyebilmek için internete bağlı olmalısınız.

Güncelleme ilerleyişini gösteren ekran belirir.



Tamamlandığında veritabanınız güncellenmiş olur.



Antivirüs veritabanı uzun süredir güncellenmediyse veya sisteminiz uzun süredir taranmadıysa, zararlı veya muhtemelen zararlı olabilecek dosyalar bulunduğunda Comodo Antivirüs ana ekranında yapılması gereken eylemler ve bunlarla ilgili açıklamalar çıkar.

Otomatik Güncelleştirmeler

Comodo AntiVirüs otomatik olarak güncellemeleri denetler ve yükler. Tarayıcı Ayarlarından Gerçek Zamanlı Tarama ve Zamanlanmış Tarama için otomatik güncelleme ayarlanabilir. Daha fazla bilgi için Gerçek Zamanlı Tarama Ayarları ve Zamanlanmış Tarama Ayarları bölümlerine bakınız.

2.3 Karantinaya Alınmış Öğeler

Karantina şüpheli dosyaları bulaşmaya karşı analiz etmeden önce onları güvenli bir konuma taşıyarak tecrit altına alır. Bu biçimde aktarılan dosyalar şifrelendiği için çalıştırılamaz veya yürütülemezler.

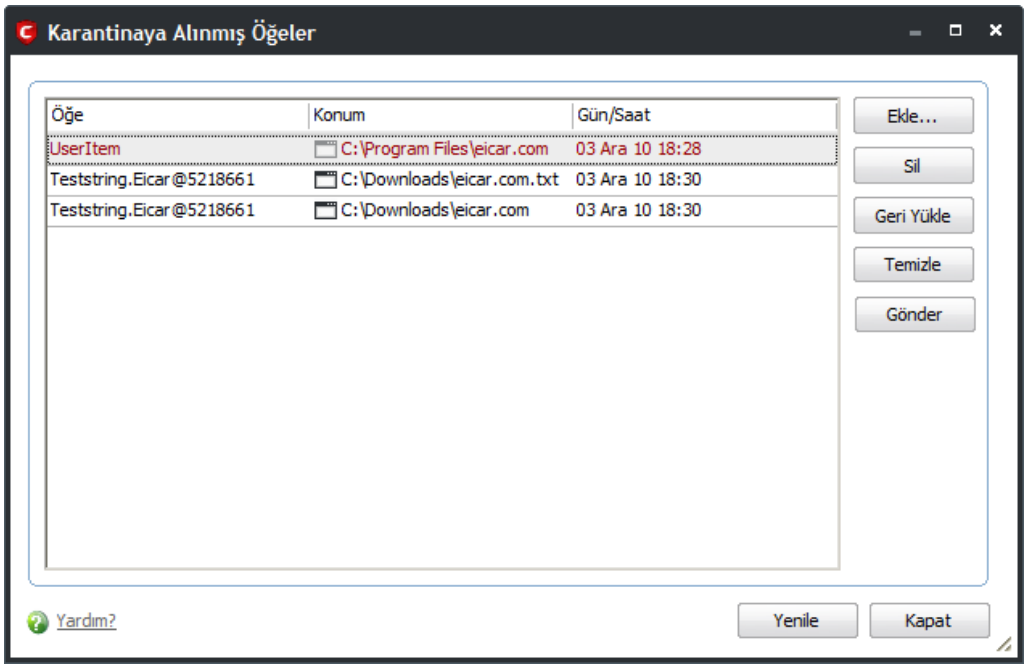
Karantinaya Alınmış Öğeler hakkında daha fazla bilgi için Antivirüs Görevleri > Bir Tarama Çalıştır bölümüne bakınız. Ayrıca:

- Güvenmediğiniz uygulamaları, yürütülebilirleri veya diğer dosyaları elle ekleyebilirsiniz
- Karantinadaki öğeyi sistemden silebilirsiniz
- Karantinadaki öğeyi geri yükleyebilirsiniz

- Karantinadaki tüm öğeleri silebilirsiniz
- Karantinadaki öğeleri analiz için COMODO'ya gönderebilirsiniz

Karantinaya Alınmış Öğelerin Listesini görüntülemek için

- Antivirüs ekranından 'Karantinaya Alınmış Öğeler' bölümüne tıklayın.



Sütun Açıklamaları

- **Öğe -** Olaya neden olan uygulama veya işlem;
- **Konum -** Uygulamanın veya dosyanın bulunduğu konum;
- **Tarih/Saat** - Öğenin karantinaya taşındığı tarih ve saati gösterir.

Dosyaların elle Karantinaya Alınmış Öğelere eklenmesi

Virüs içeren şüpheli dosyanız, klasörünüz veya sürücünüz varsa ve tarayıcı tarafından saptanmadıysa bu seçenek ile onları karantinada tecrit edebilirsiniz.

Elle eklemek için

- **Ekle**'ye tıklayın ve **Aç** diyaloğundan dosyayı seçin.

Karantinadaki bir öğeyi sistemden silmek için

- Öğeyi seçin ve 'Sil' düğmesine tıklayın.

Bu, dosyayı sistemden kalıcı olarak siler.

Karantinadaki bir öğeyi asıl konumuna geri yüklemek için

- Öğeyi seçin ve 'Geri Yükle' düğmesine tıklayın.

Geri yüklenen öğe zararlı içermiyorsa normal olarak çalışmasına devam eder. Fakat zararlı içeriyorsa ve gerçek zamanlı tarama etkinse anında tehdit olarak saptanır veya bir sonraki taramada saptanır.

Karantinadaki tüm öğeleri kalıcı olarak kaldırmak için

- 'Temizle' düğmesine tıklayın.

Bu, tüm öğeleri sistemden kalıcı olarak siler.

Seçili karantina öğesini Comodo'ya analize göndermek için

- Öğeyi seçin ve 'Gönder' düğmesine tıklayın.

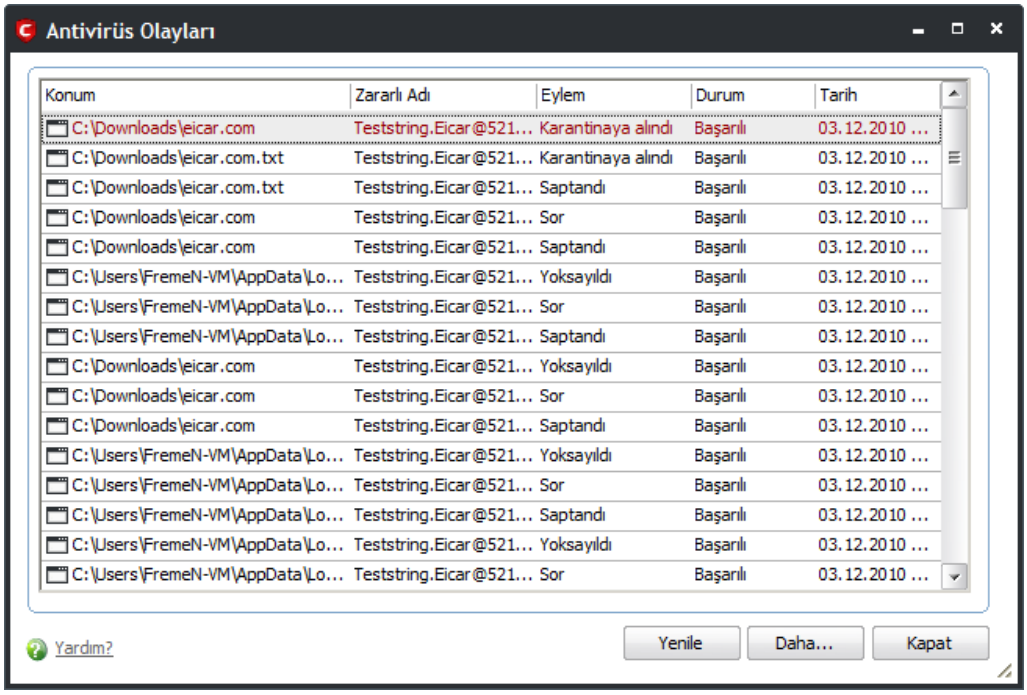
Not: Karantinadaki dosyalar özel bir biçimde saklanır ve bilgisayarınıza tehlike oluşturmaz.

2.4 Antivirüs Olaylarını Göster

Comodo Antivirüs gerçekleştirdiği tüm eylemlerin ayrıntılı raporunu tutar.

Antivirüs Olaylarını görüntülemek için

•Antivirüs ekranından 'Antivirüs Olaylarını Göster' bölümüne tıklayın.



Sütun Açıklamaları

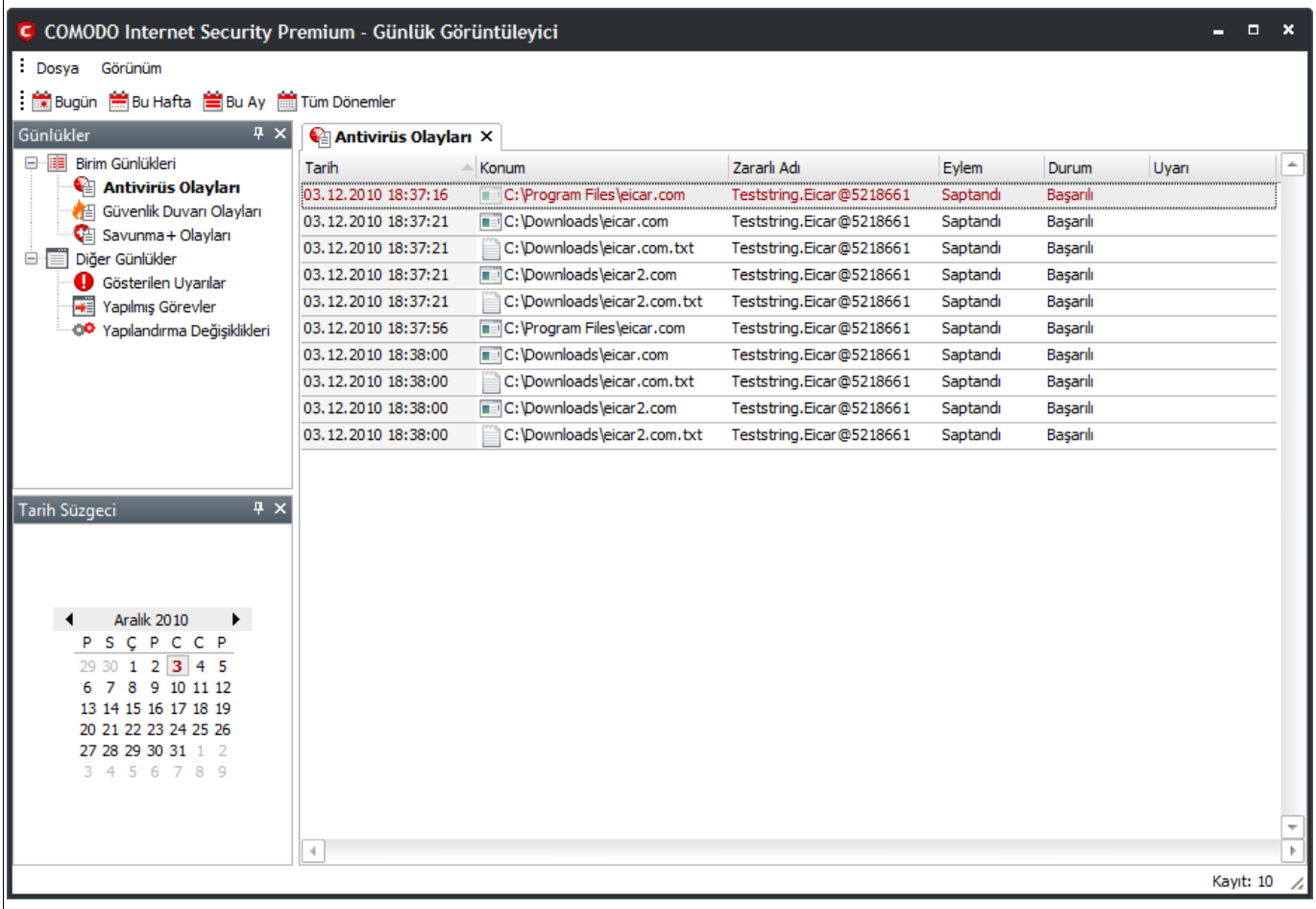
- **Konum – Tehdit içeren uygulamanın bulunduğu konum gösterir.**

- **Zararlı Adı – Saptanan zararlının adı gösterir.**
- **Eylem – Antivirüs tarafından zararlıya uygulanan eylem.**
- **Tarih – Olayın gerçekleştiği tarihini gösterir.**
- **Durum – Gerçekleştirilen eylemin durumunu gösterir. 'Başarılı' veya 'Başarısız' olabilir.**

'Daha' düğmesine tıklayarak CIS Günlük Görüntüleyicisini açabilirsiniz.

Bu pencere iki farklı kategoride günlüklerin tüm geçmişini içerir: Birim Günlükleri ve Diğer Günlükler.

Ayrıca belirli süzgeçler ile raporları kişisel günlük dosyalarına çıkartmanıza da olanak sağlar.



Günlük Görüntüleyici Bileşeni üç bölüme ayrılmıştır. Üst panelde zaman süzgeçleri, sol panelde günlük türü ve sağ panelde seçili ölçütlere uygun olan günlük olayları bulunur.

Birim günlükleri Güvenlik Duvarı, Savunma+, Antivirüs ve Diğer Günlüklerden oluşur. Diğer Günlüklerde aşağıdaki olayları içerir:

- **Gösterilen Uyarılar: CIS tarafından gösterilen uyarıların kayıtları.**
- **Yapılmış Görevler: Çeşitli yapılmış görevleri içerir. (Güncellemeler, tarama sonuçları gibi).**

- **Yapılandırma Değişiklikleri: Yapılandırmada yapılan değişiklikleri gösterir.**

Günlük Dosyalarının Süzülmesi

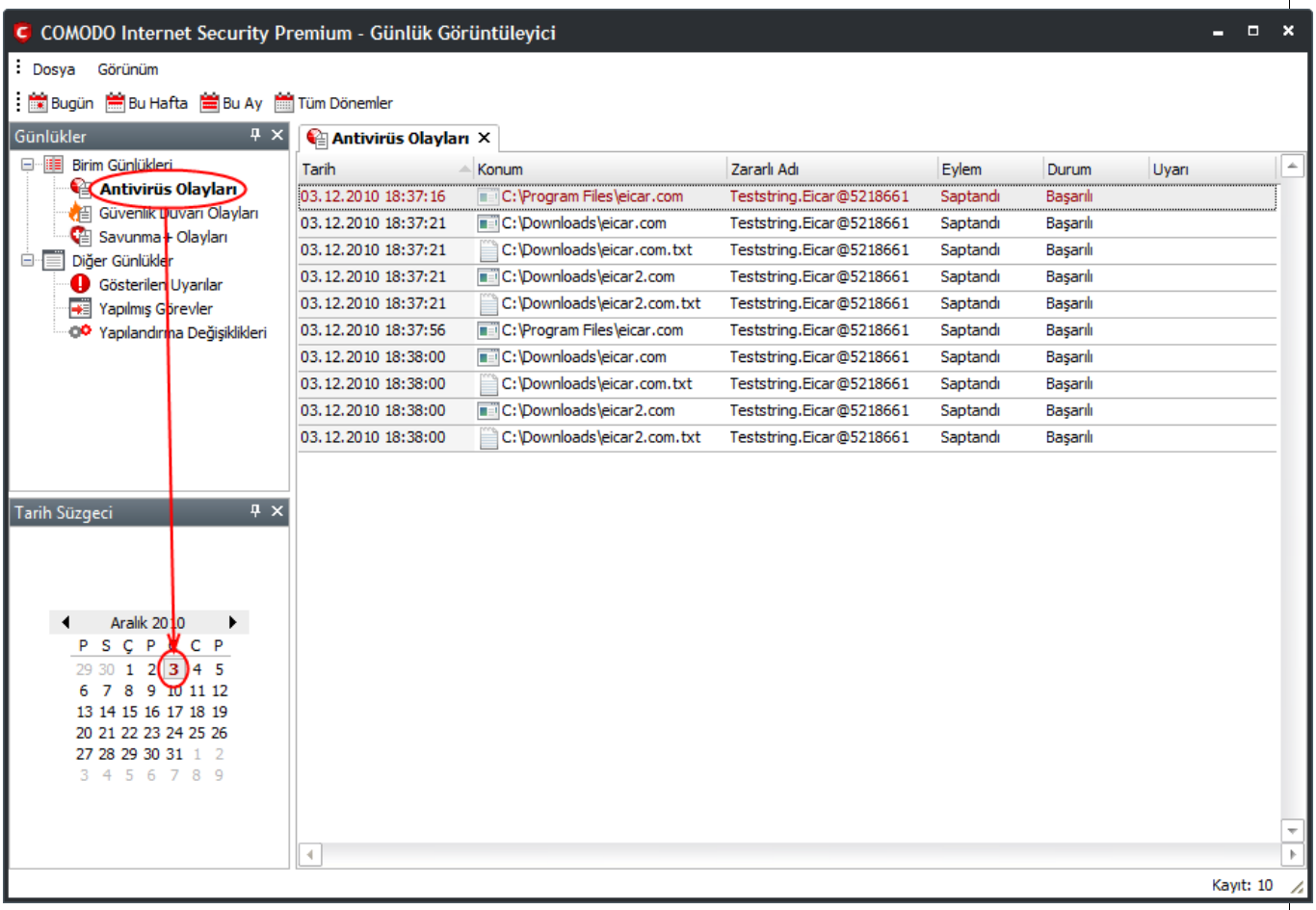
Comodo Internet Security günlük olaylarının belirli süzgeçlere göre gösterilmesine izin verir.

Zaman Süzgeçleri:

Zaman süzgeçleri üst panelde bulunur ve bunlardan biri seçildiğinde sağ panelin görünüşünü değiştirir:

•**Bugün** – Bugün gerçekleşen olayları gösterir.
•**Bu Hafta** – Bu hafta gerçekleşen olayları gösterir.
•**Bu Ay** – Bu ay gerçekleşen olayları gösterir.
•**Tüm Dönemler** – CIS kurulumundan veya son günlük temizlemesinden sonraki tüm olayları gösterir.

Aşağıdaki örnek 'Bugün' zaman dilimini göstermektedir.



Not: Sağ panelin içeriği CIS bileşenlerine göre farklılık gösterebilir.

Kullanıcı Tanımlı Süzgeçler:

Aşağıdaki tablo bulunan süzgeçleri ve onların anlamlarını gösterir:

Bulunan Süzgeçler – Birim Günlükleri		
Antivirüs Süzgeçleri	**Güvenlik Duvarı Süzgeçleri**	**Savunma+ Süzgeçleri**
Tarih – Seçili tarihteki olayları gösterir	**Tarih** - Seçili tarihteki olayları gösterir.	**Tarih** - Seçili tarihteki olayları gösterir.
Konum – Seçili konumdaki olayları gösterir	**Uygulama –** Olaya neden olan uygulamayı gösterir	**Uygulama -** Olaya neden olan uygulamayı gösterir
Zararlı Adı – Zararlı adına uygun olayları gösterir	**Eylem** – Gerçekleştirilen eyleme uygun olayları gösterir	**Eylem** - Gerçekleştirilen eyleme uygun olayları gösterir
Eylem - Gerçekleştirilen eyleme uygun olayları gösterir	**Yön** – Bağlantının yönüne uygun olayları gösterir	**Hedef Adı –** Hedef uygulamaya ilişkin olayları gösterir
Durum - Gerçekleştirilen eylemin durumuna uygun olayları gösterir. 'Başarılı' veya 'Başarısız' olabilir.	**Protokol –** Belli protokole ilişkin olayları gösterir	**Uyarı** – Eylem sütununda 'Soruldu' görünen uyarıların yanında 'İlişkili Uyarı' adında bir bağlantı görünür. Bu bağlantı sizi 'Gösterilen Uyarılar' olay günlüğüne götürür
Uyarı - Eylem sütununda 'Soruldu' görünen uyarıların yanında 'İlişkili Uyarı' adında bir bağlantı görünür. Bu bağlantı sizi 'Gösterilen Uyarılar' olay günlüğüne götürür	**Kaynak IP adresi** - Belli IP adresinden gerçekleştirilen bağlantılara ilişkin olayları gösterir	
	Kaynak Portu - Belli porttan yapılan bağlantılara ilişkin olayları gösterir	
	Hedef IP adresi Belli IP adresinden gerçekleştirilen bağlantılara ilişkin olayları gösterir	

Bulunan Süzgeçler – Birim Günlükleri		
	Hedef Portu - Belli porttan yapılan bağlantılara ilişkin olayları gösterir	
	Uyarı - Eylem sütununda 'Soruldu' görünen uyarıların yanında 'İlişkili Uyarı' adında bir bağlantı görünür. Bu bağlantı sizi 'Gösterilen Uyarılar' olay günlüğüne götürür	

Özel Süzgeçlerin Oluşturulması

Özel Süzgeçler Gelişmiş Süzgeç arayüzü kullanılarak oluşturulabilir. Gelişmiş Süzgeç arayüzü günlük görüntüleyiciye sağ tıklayarak içerik menüsünden açılabilir.

- **'Gelişmiş Süzgeç' alanını açmak için Görünüm > Gelişmiş Süzgeç seçeneğine tıklayın.**

Veya

- **Olay panelinde sağ tıklayın ve 'Gelişmiş Süzgeç' seçin.**

'Gelişmiş Süzgeç' paneli üstte açılır.

Gelişmiş rapor süzgeç görünümü seçili bileşene göre farklılık gösterir.

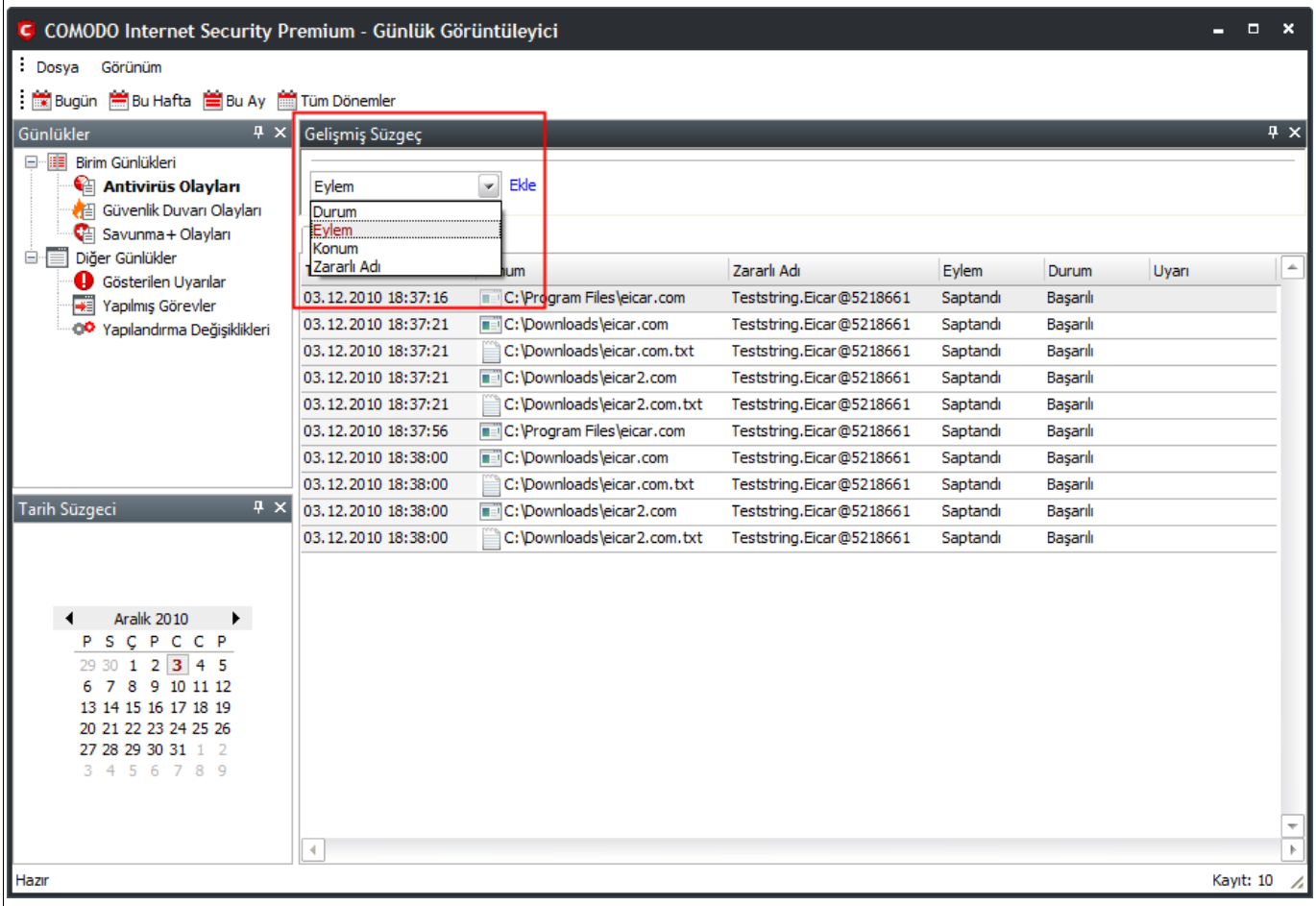
Antivirüs Olayları – Gelişmiş Süzgeçler

Antivirüs olayları için Gelişmiş Süzgeçlerin yapılandırılması

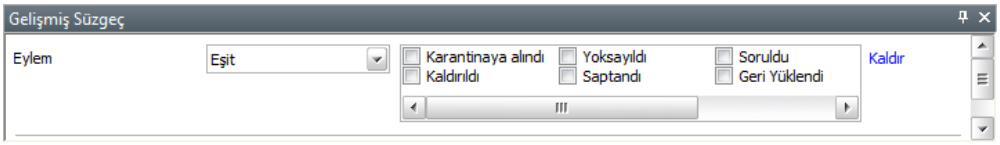
1. 'Görünüm > Gelişmiş Süzgeç' seçin.
2. 'Birim Günlükleri' altından 'Antivirüs Olayları' seçin.

Ekleyebileceğiniz 4 süzgeç kategorisi ve her bir kategori altında farklı parametreler bulunmaktadır.

3. 'Ekle' düğmesini kullanarak süzgeçler ekleyebilirsiniz.



Aşağıdakiler 'Ekle' açılır menüsünde bulunmaktadır:



i.**Eylem**: Seçilebilen süzgeçler açılır alanda görünür.

a) 'Eşit' veya 'Eşit Değil' seçeneklerinden birini seçin. 'Eşit Değil' seçeneği seçimi tersine çevirir.

b) Aramayı geliştirmek için değişkenlerin kutularını işaretleyebilirsiniz. Bulunan değişkenler şunlardır:

•Karantinaya Alındı: Karantina olaylarını gösterir
•Kaldırıldı: Silinen öğe olaylarını gösterir
•Yoksayıldı: Yoksayılan öğe olaylarını gösterir
•Saptandı: Zararlı saptanma olaylarını gösterir
•Soruldu: Kullanıcıya sorulan uyarı olaylarını gösterir
•Geri Yüklendi: Karantinaya alınıp daha sonra geri yüklenmiş uygulamaların olaylarını gösterir.

Örneğin, 'Karantinaya Alındı' ile birlikte 'Eşit Değil' kutusunu seçerseniz yalnızca 'Karantinaya Alındı' eylemi *dışındakileri* görürsünüz.

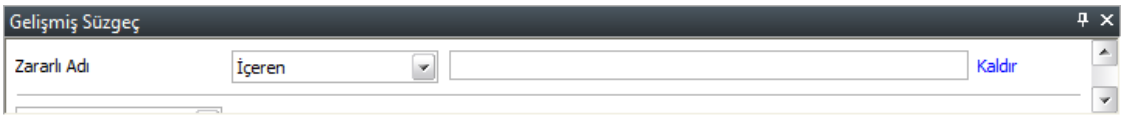
ii.**Konum**: 'Konum' seçeneğinin seçilmesi açılır alan ve metin giriş alanı gösterir.

a) 'İçeren' veya 'İçermeyen' seçeneklerinden birini seçin.
b) Süzgece eklenmesi gereken metni girin.

Süzülen girdiler doğrudan altta görünür.

Örneğin, 'İçeren' seçip metin alanına 'unclassifiedMalware' girdiyseniz bu kelimeyi *içeren* tüm olaylar doğrudan altta görüntülenecektir. Eğer 'İçermeyen' seçip metin alanına 'System' girdiyseniz altta bu kelimeyi *içermeyen* olaylar görüntülenecektir.

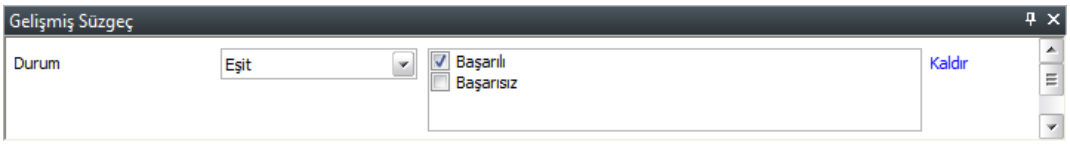
i. **Zararlı Adı**: 'Zararlı Adı' seçeneğinin seçilmesi açılır alan ve metin giriş alanı gösterir.



a) 'İçeren' veya 'İçermeyen' seçeneklerinden birini seçin.
b) Süzgece eklenmesi gereken metni girin.

Süzülen girdiler doğrudan altta görünür.

Örnek olarak 'Konum' bölümündeki örneğe bakınız.



i. **Durum**: 'Durum' seçeneği açılır listeden seçilince bulunan süzgeçler açılır alanda görünür.

a) 'Eşit' veya 'Eşit Değil' seçeneklerinden birini seçin. 'Eşit Değil' seçeneği seçimi tersine çevirir.
b) Aramayı geliştirmek için değişkenlerin kutularını işaretleyebilirsiniz. Bulunan değişkenler şunlardır:
   - Başarılı: Başarılı olarak gerçekleştirilen olayları gösterir
   - Başarısız: Başarılı olarak gerçekleştirilemeyen olayları gösterir

Süzülen girdiler doğrudan altta görünür.

Örnek olarak 'Eylem bölümündeki örneğe bakınız.

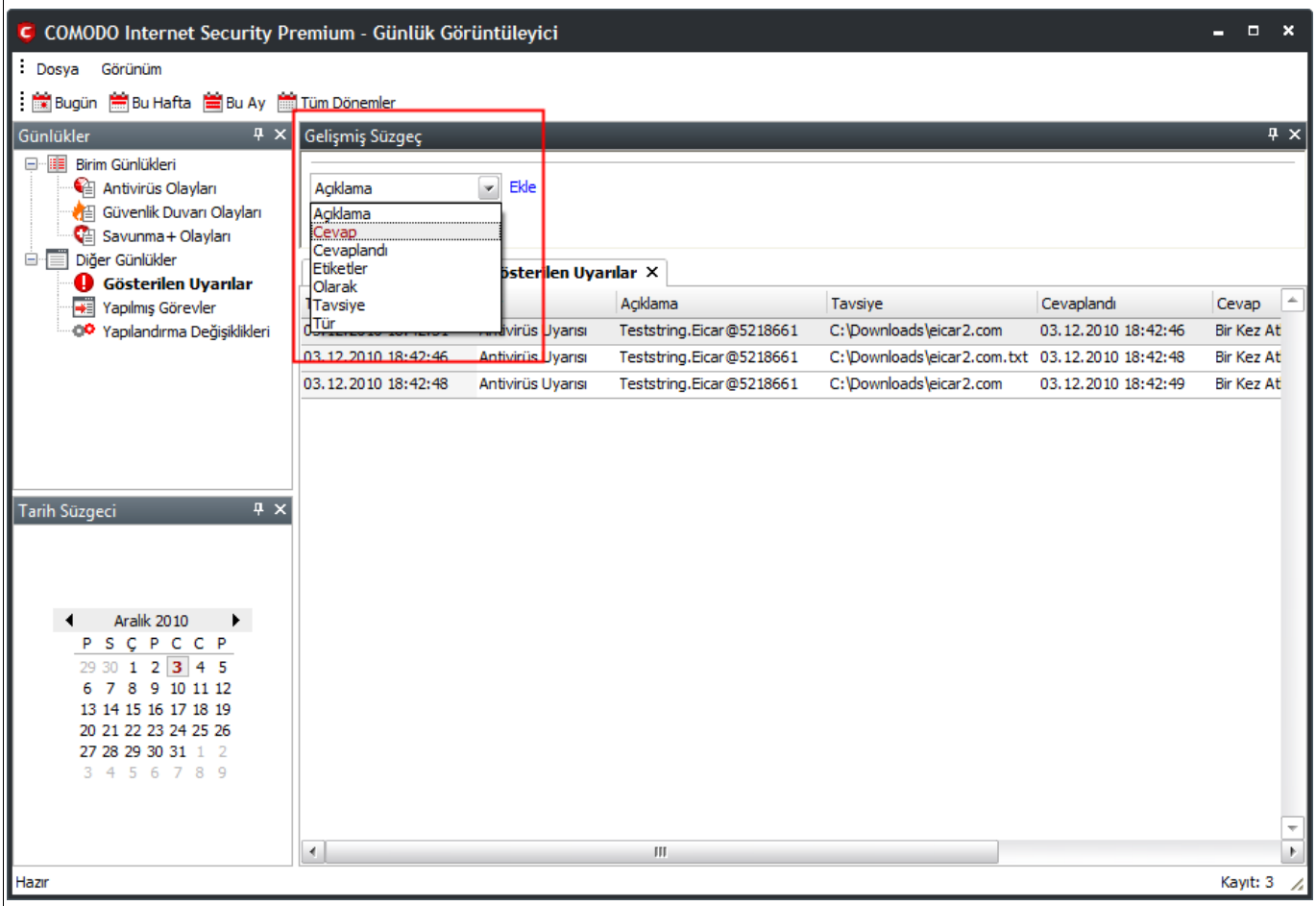
Not: 'Gelişmiş Süzgeç' bölümünde birden fazla süzgeç eklenebilir. Eklenmiş bir süzgeci 'Kaldır' düğmesine tıklayarak kaldırabilirsiniz.

Diğer Günlükler – Gelişmiş Süzgeçler

Gösterilen Uyarılar, Yapılmış Görevler ve Yapılandırma Değişiklikleri için Gelişmiş Süzgeçler işlevi tüm CIS bileşenleri için aynıdır.

Gösterilen Uyarılar için Gelişmiş Süzgeçlerin Yapılandırılması

1. 'Görünüm > Gelişmiş Süzgeçler' seçin.
2. 'Diğer Günlükler' altında 'Gösterilen Uyarıları' seçin.
3. Süzmek istediğiniz kategoriyi seçip 'Ekle' düğmesine tıklayın.

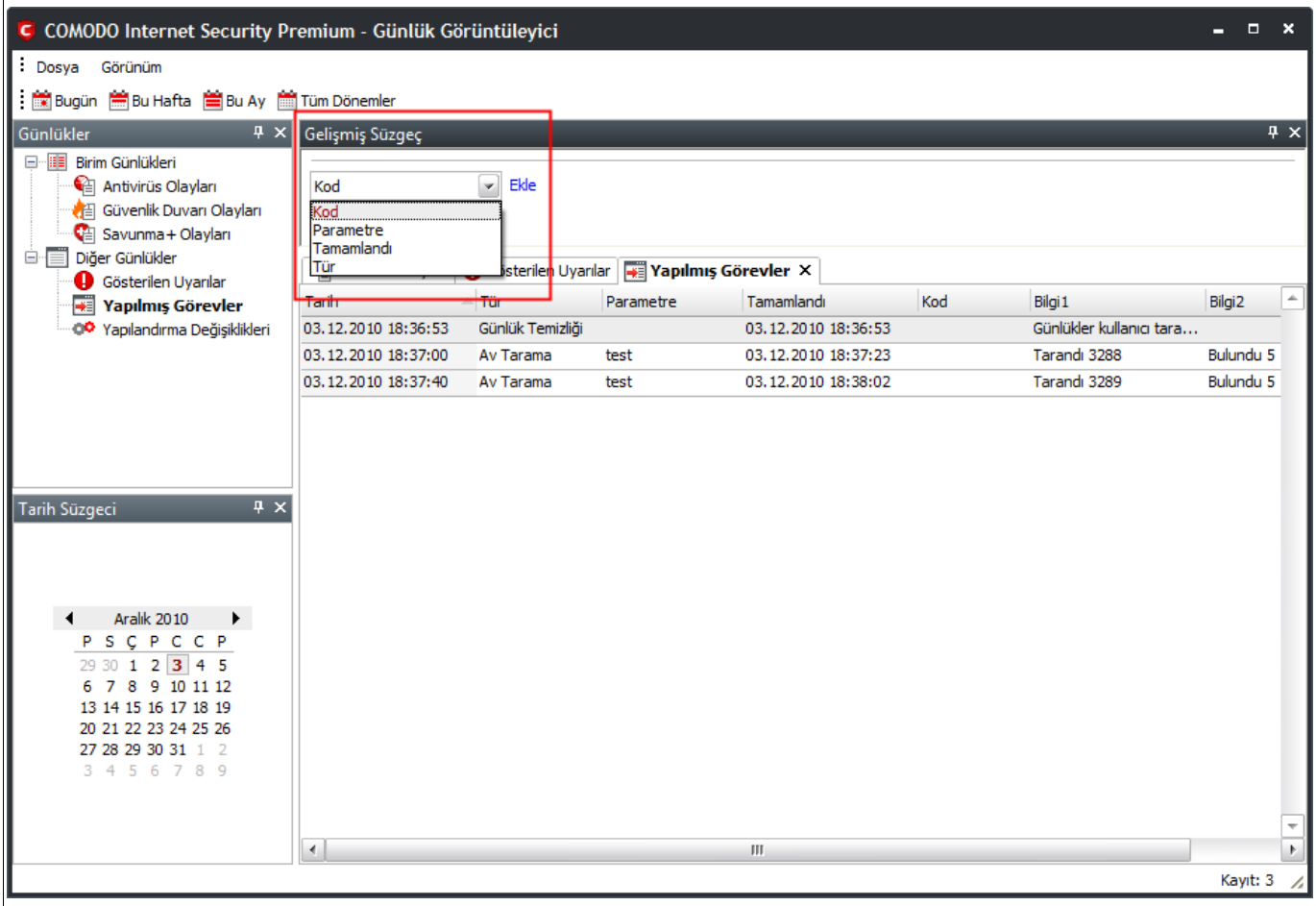


Aşağıdaki tablo 'Gösterilen Uyarılar' için çeşitli süzgeç kategorilerini ve parametrelerini listeler.

Bulunan Süzgeçler – Diğer Günlükler – Gösterilen Uyarılar	
Süzgeç Seçeneği	**Açıklama**
Tür	Uyarının türünü gösterir
Açıklama	Olayın adını gösterir
Tavsiye	Olay için kullanıcıya sunulan tavsiyeyi içerir
Cevaplandı	Uyarının cevağlandığı tarih ve saati içerir
Etiketler	Belirlenen etiketlere göre süzer.
Cevap	Kullanıcı tarafından uyarıya verilen cevap
Olarak	Olay türüne göre ilke türünü gösterir

Yapılmış Görevler için Gelişmiş Süzgeçlerin Yapılandırılması

1. 'Görünüm > Gelişmiş Süzgeçler' seçin.
2. 'Diğer Günlükler' altında 'Yapılmış Görevler' seçin.
3. Süzmek istediğiniz kategoriyi seçip 'Ekle' düğmesine tıklayın.

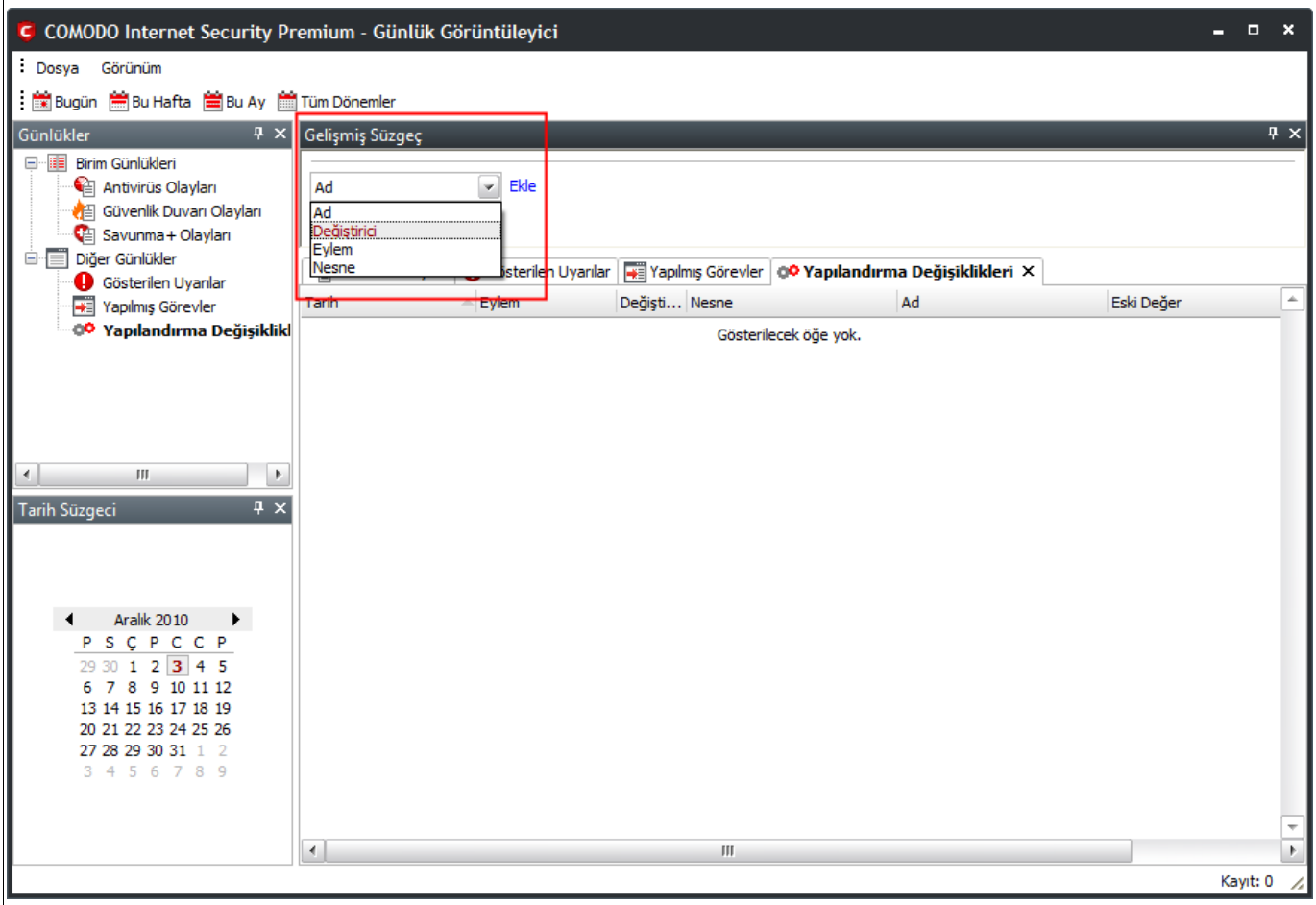


Aşağıdaki tablo 'Yapılmış Görevler' için çeşitli süzgeç kategorilerini ve parametrelerini listeler.

Bulunan Süzgeçler – Diğer Günlükler – Yapılmış Görevler	
Süzgeç Seçeneği	**Açıklama**
Tür	Görev türünü gösterir.
Parametre	Tarama profilinin adını gösterir. Bu sütun yalnızca 'Tür' sütununda 'Av Taraması' görünüyorsa dolu olur.
Tamamlandı	Görevin gerçekleştiği tarihi ve saati gösterir.
Kod	Görev başarılı olarak gerçekleştirilemediyse kod değerini gösterir veya standart değer olarak veritabanı güncel ise: 0x00000001 görünür

Yapılandırma Değişiklikleri için Gelişmiş Süzgeçlerin Yapılandırılması

1. ‘Görünüm > Gelişmiş Süzgeçler’ seçin
2. ‘Diğer Günlükler’ altında ‘Yapılmış Görevler’ seçin



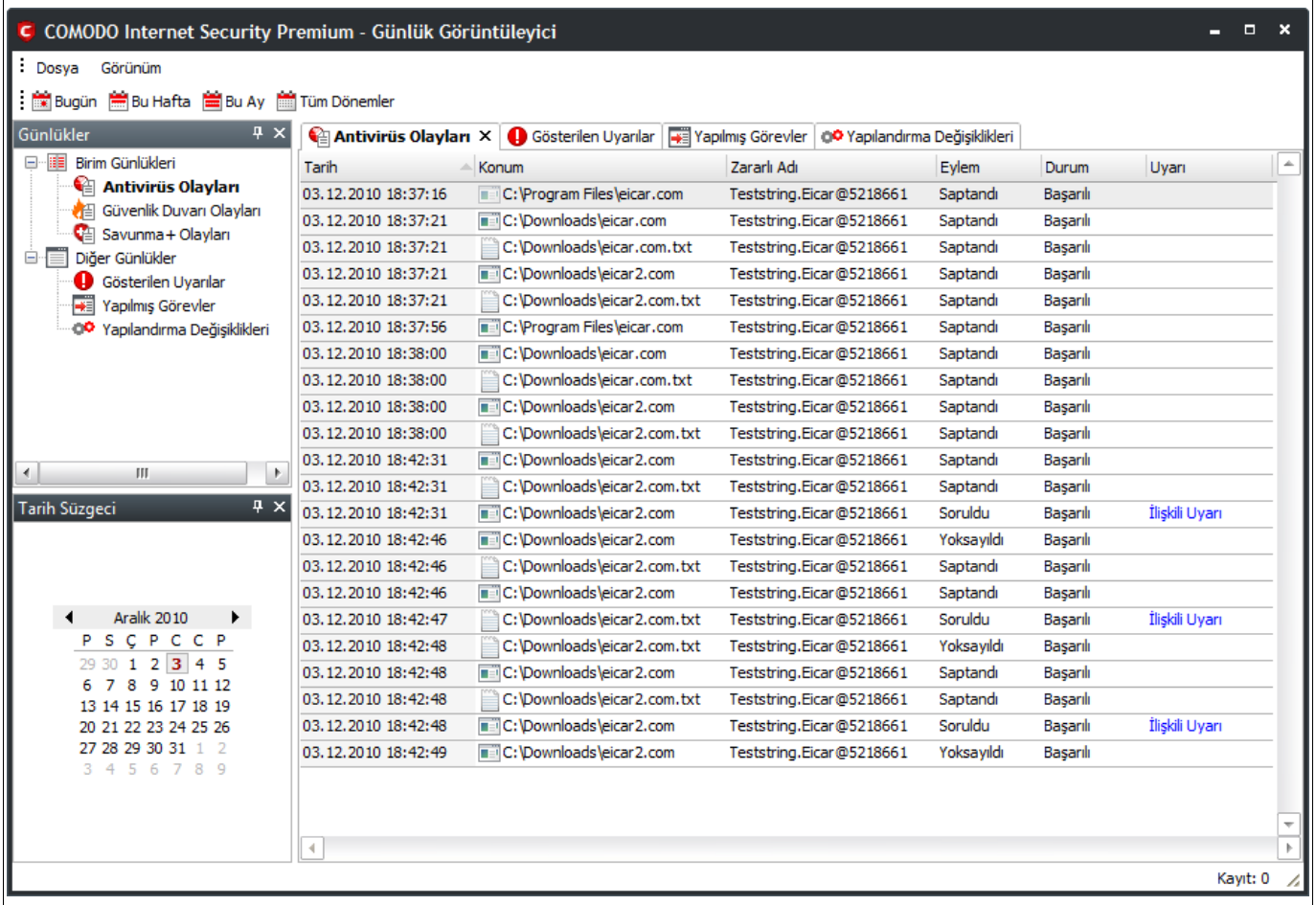
3. Süzmek istediğiniz kategoriyi seçip ‘Ekle’ düğmesine tıklayın.

Aşağıdaki tablo ‘Yapılandırma Değişiklikleri’ için çeşitli süzgeç kategorilerini ve parametrelerini listeler.

Bulunan Süzgeçler – Diğer Günlükler – Yapılandırma Değişiklikleri	
Süzgeç Seçeneği	**Açıklama**
Eylem	Cevaba göre olayları gösterir
Değiştirici	Kullanıcı veya CIS bileşenleri tarafından yapılan değişikliklere göre olayları gösterir.

Bulunan Süzgeçler – Diğer Günlükler – Yapılandırma Değişiklikleri	
Nesne	Yapılandırma değişikliğinin yerine geçen nesneleri gösterir.
Ad	Yapılandırma girdisinin adını gösterir

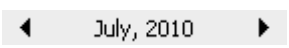
Tarih Süzgeci



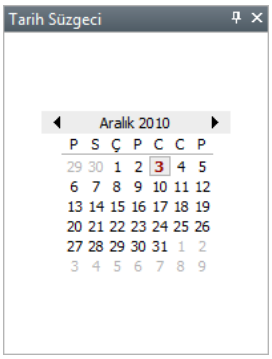
Tarih Süzgeci sol alt panelden ayarlanabilir.

Belirli günlerdeki olayları görmek için

1.Oklara tıklayarak yılı ve ayı ayarlayın.

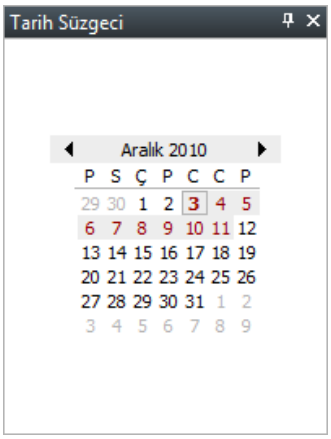


2.Şimdi, güne tıklayın.



Gün aralığındaki olayları görüntülemek için

1.Oklara tıklayarak yılı ve ayı ayarlayın.



2.Başlangıç gününü seçin ve daha sonra üst karakter tuşuna basılı tutarak bitiş gününü seçin. Böylece gün aralığı seçilmiş olacaktır.

Tarih Süzgecini kapatmak için

- **'X' sembolüne tıklayarak kapatabilirsiniz.**

Veya

•'Görünüm' menüsünden 'Tarih Süzgeci' seçeneği kullanılarak da kapatılabilir.

Günlüklerin HTML dosyasına Çıkartılması

Günlük dosyalarının çıkartılması arşivleme ve sorun giderme açısından kullanışlıdır. İki yolla dosyaya çıkartma yapılabilir. İçerik menüsü veya 'Dosya' menüsü kullanılarak çıkartılabilir.

i. Dosya Menüsü

1. Çıkartılmasını istediğiniz olayları seçin.
2. Dosya menüsünden 'Çıkart' düğmesine tıklayın.
3. Dosyanın kaydedileceği konumu seçin ve kaydedin.

ii. **İçerik Menüsü**

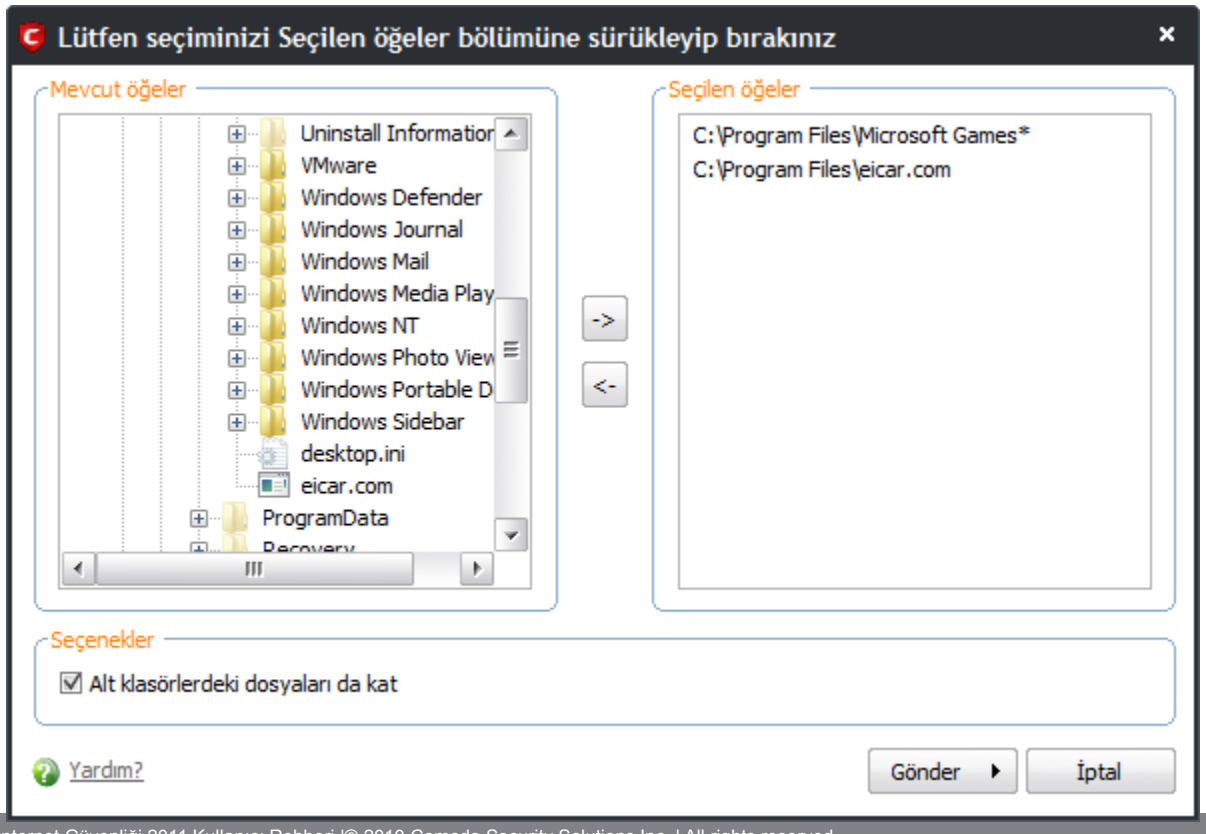
1.Günlük penceresinde sağ tıklayarak görüntülenen olayları HTML dosyasına çıkartın.

Günlük penceresinde sağ tıklayarak görüntülenen olayları HTML dosyasına çıkartabilirsiniz.

2.5 Dosyaların analiz için Comodo'ya Gönderilmesi

Comodo beyaz listesinde olmayan ve bilinmeyen dosyalar analiz için Comodo'ya gönderilebilir. Dosyalar ayrıca Tanınmayan Dosyalar arayüzündeki 'Gönder' düğmesi kullanılarak da gönderilebilir.

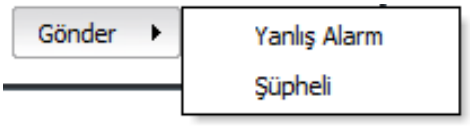
Şüpheli veya yanlış alarm olduğunu düşündüğünüz dosyaları analiz için gönderebilirsiniz. Bunlar duruma göre beyaz veya kara listeye eklenecektir.



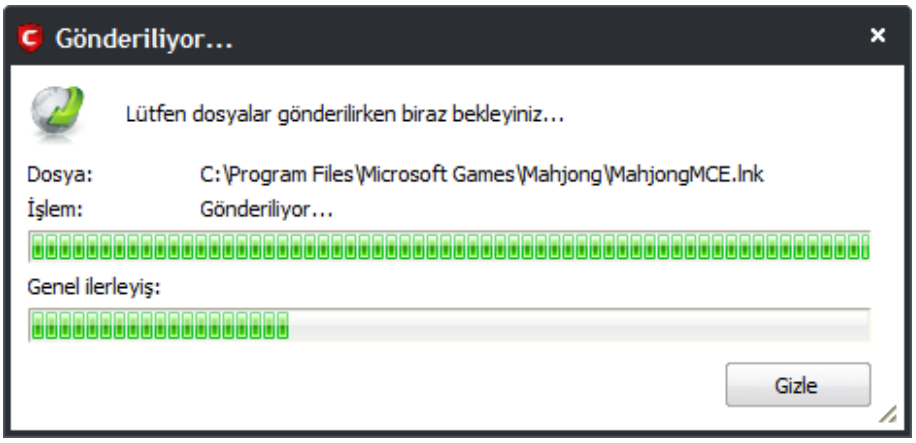
Dosyaları Comodo'ya göndermek için

1. Antivirüs ekranından 'Dosyaları Gönder' bağlantısına tıklayarak gönderebilirsiniz. Tarayıcı penceresi açılır.

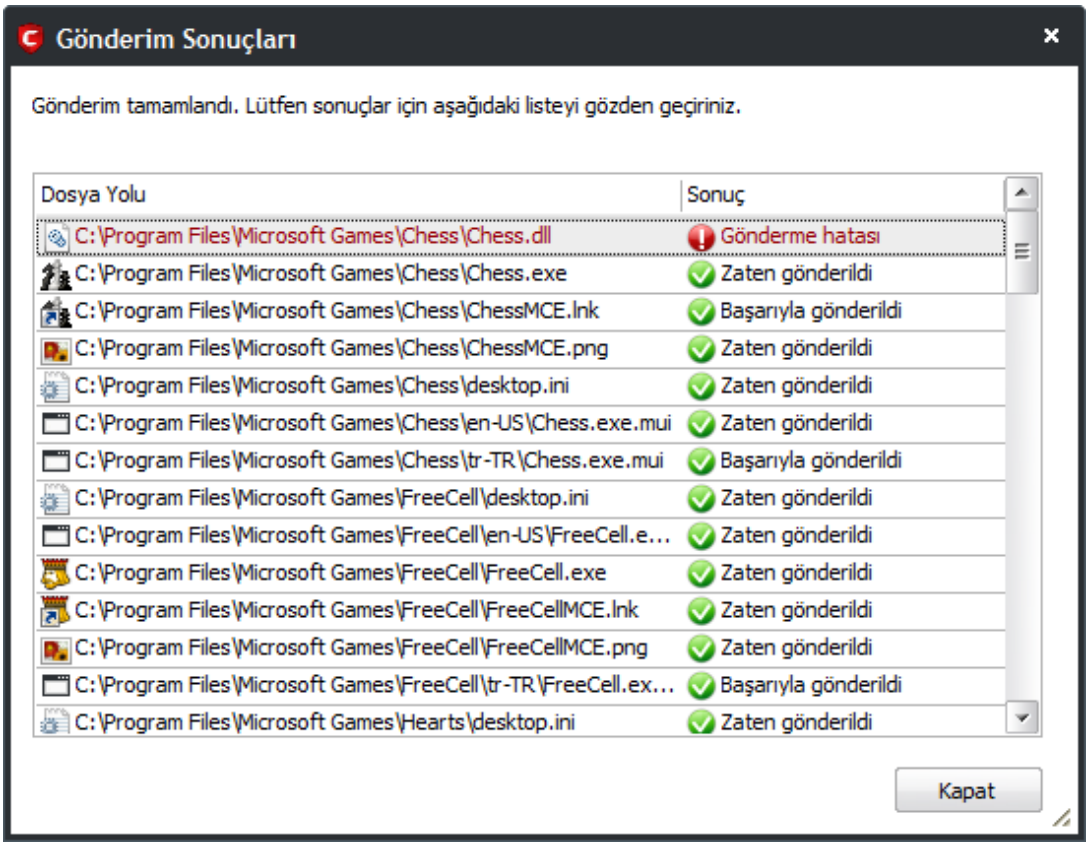
2. Göndermek istediğiniz dosyaları seçin.
3. 'Gönder' düğmesine tıklayın ve seçin:
   - 'Yanlış Alarm' güvenli olarak sayılması için veya
   - 'Şüpheli' zararlı olarak sayılması için.



İlerleyiş çubuğu dosya gönderiminin ilerleyişini gösterir.



Bir dosya ilk defa yollanırken Comodo çevrimiçi inceleme hizmeti dosyanın daha önce gönderilip gönderilmediğini denetleyecektir. Sonuç ekranı aşağıdaki gibidir:



•'Başarıyla Gönderildi' – Dosya imzası denetleme sırasında bekleyen dosyalar listesinde bulunamadı dolayısıyla araştırma merkezine sizin makinanızdan gönderildi.

- 'Zaten gönderilmiş' – Dosya başka bir kullanıcı tarafından daha önce gönderilmiş.

Comodo gönderilen tüm dosyaları analiz edecektir. Gönderilenler güvenilir bulunursa beyaz listeye, şüpheli bulunursa kara listeye eklenecektir.

2.6 Zamanlanmış Taramalar

Comodo Antivirüs'ün zamanlayıcısı ile tercihinize göre taramalarınızı zamanlayabilirsiniz. Böylece seçtiğiniz profile göre sistemi veya diski veya klasörü otomatik olarak taratabilirsiniz.

Sayısız zamanlayıcı oluşturabilir ve bunlara istediğiniz profilleri atayabilirsiniz.

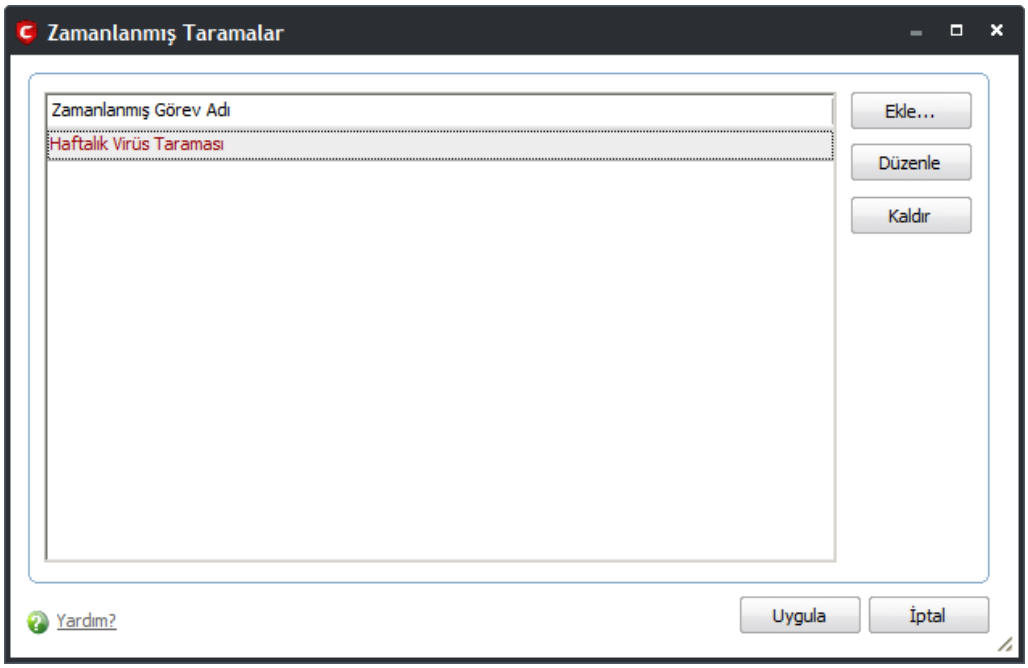
'Zamanlanmış Taramalar' panelinden, şunları yapabilirsiniz

- **Zamanlanmış tarama oluşturabilir**
- **Ön zamanlanmış taramayı düzenleyebilir ve**
- **Ön zamanlanmış taramayı iptal edebilirsiniz**

Zamanlanmış Taramaların saptama ayarlarını Tarayıcı Ayarları altında Zamanlanmış Taramalar sekmesinden ayarlayabilirsiniz.

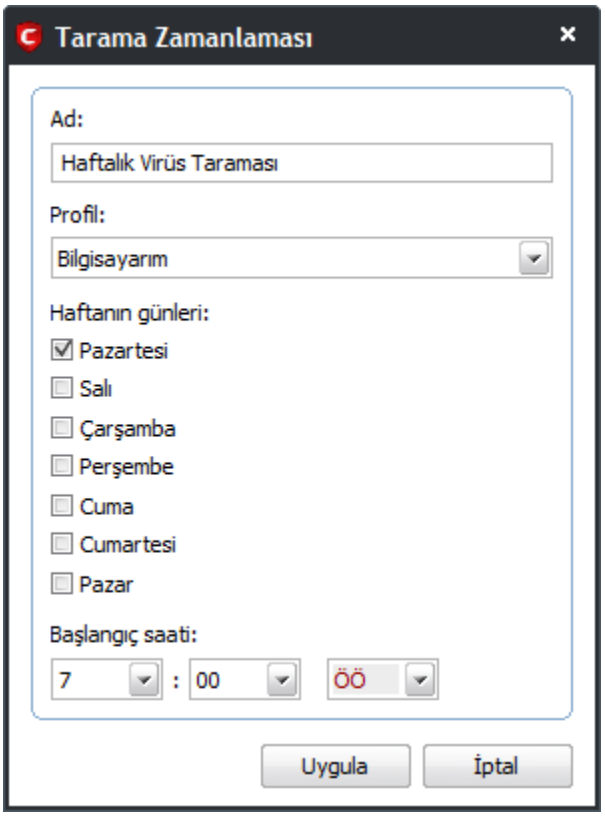
Zamanlanmış Tarama ayarlamak için

1. Antivirüs ekranından Zamanlanmış Taramalara tıklayın.



Varsayılan zamanlama 'Haftalık Virüs Taraması' görünür. Bu zamanlama her Pazar saat 12:00'da bilgisayarı tarayacak şekilde ayarlanmıştır. 'Düzenle' düğmesini kullanarak bu zamanlamayı düzenleyebilirsiniz.

2. 'Ekle' düğmesine tıklayın. 'Tarama Zamanlaması' paneli açılır.



3. 'Ad' kutusuna zamanlama için bir ad giriniz.
4. 'Profil' kutusundan bulunan bir profili seçin. (Daha fazla bilgi için Antivirüs Görevleri > Tarama Profilleri bölümüne bakın)
5. 'Haftanın Günleri' bölümünden istediğiniz günleri işaretleyin.
6. 'Başlangıç Saati' bölümünden zamanlama için başlangıç saati belirleyin.
7. 'Uygula' düğmesine tıklayın.

Diğer profilleri kullanarak işlemi tekrarlayın.

Zamanlanmış Taramayı düzenlemek için

1. Listeden zamanlamayı seçin.
2. 'Zamanlanmış Taramalar' panelinden 'Düzenle' düğmesine tıklayın.
3. Gerekli alanları düzenleyin.
4. 'Uygula' düğmesine tıklayın.

Ön zamanlanmış taramayı iptal etmek için

1. İptal etmek istediğiniz taramayı 'Zamanlanmış Taramalar' panelinden seçin.
2. 'Kaldır' düğmesine tıklayın.

2.7 Tarama Profilleri

Tarama Profilleri seçili konumların taranmasına izin verir.

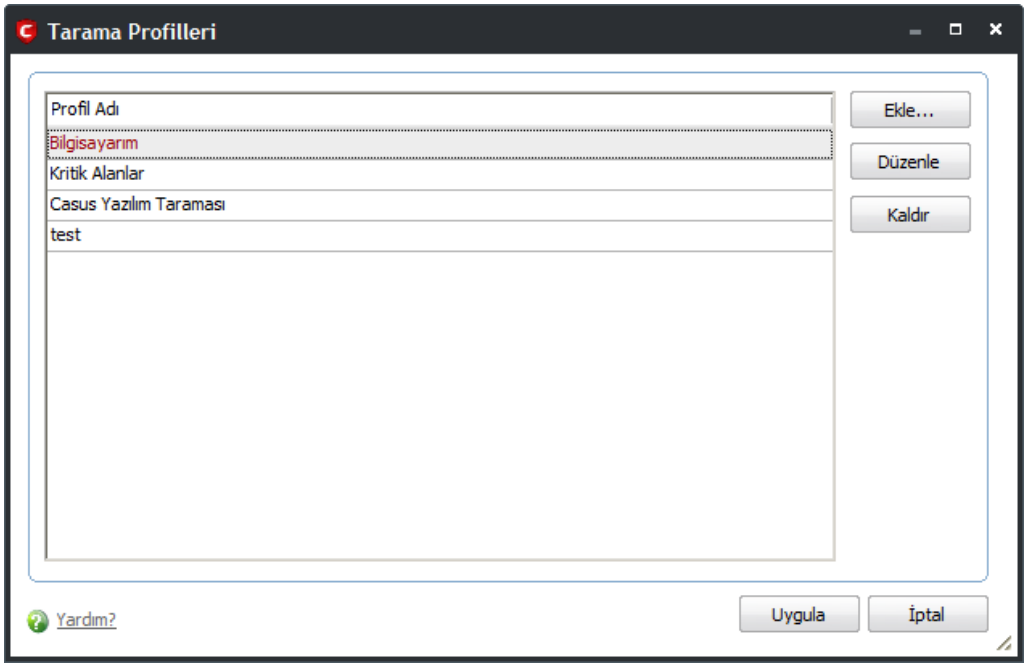
Tarama Profillerini kullanarak yalnızca taranmasını istediğiniz konumları seçerek zamandan tarasarruf edebilirsiniz.

- **Yeni tarama profilleri 'Bir Tarama Çalıştır' bölümünden 'Yeni Tarama Oluştur' veya 'Tarama Profillerinden' 'Ekle' düğmesi kullanılarak oluşturulabilir.**

Tarama Profilleri tarama konumları ile ilgilidir, tarama parametreleri ile değil. Tüm tarama profilleri 'Tarayıcı Ayarları' altındaki yapılandırılmış ayarları kullanır.

Tarama Profilleri arayüzüne erişmek için

- Antivirüs ekranından 'Tarama Profilleri' bölümüne tıklayın.



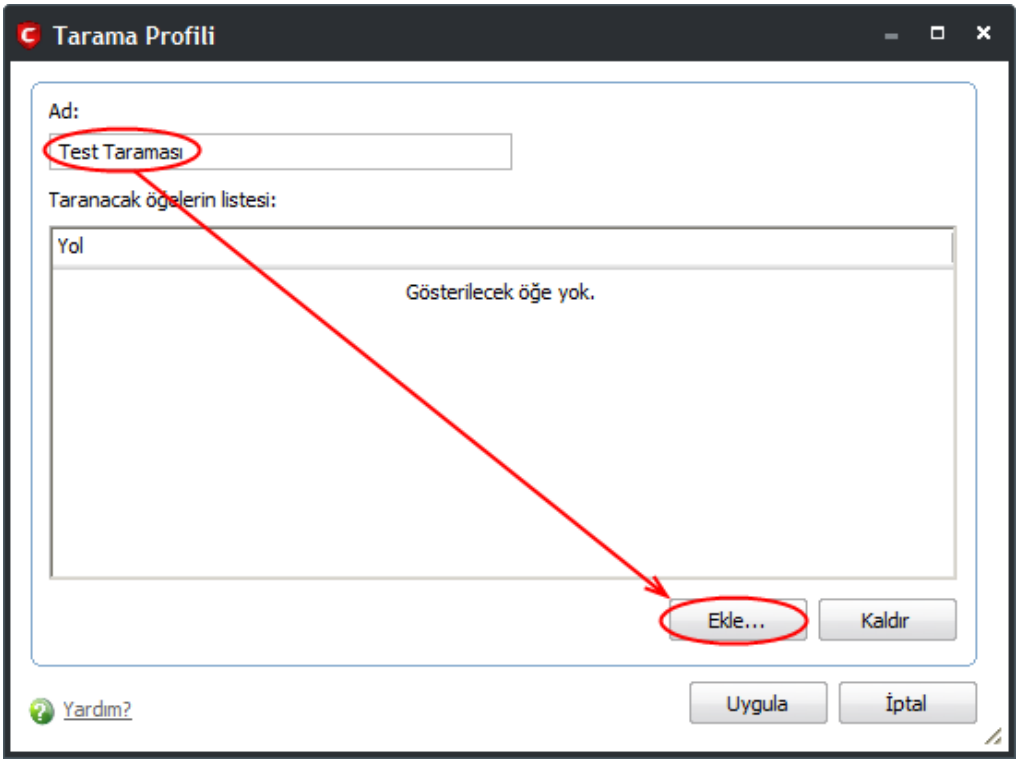
Comodo Antivirüs üç tane varsayılan Tarama Profili içerir. 'Bilgisayarım' , 'Kritik Alanlar' ve 'Casus Yazılım Taraması'. Bu üç profile öntanımlıdır ve düzenlenemez/kaldırılamaz.

- **Bilgisayarım – Tüm sürücüler taranır.**
- **Kritik Alanlar – "Windows", "Program Dosyaları" ve "Document and Settings" klasörleri taranır.**
- **Casus Yazılım Taraması – Windows Kayıt Defteri taranır**

Tarama Profili seçeneklerinden yeni tarama oluşturmak için

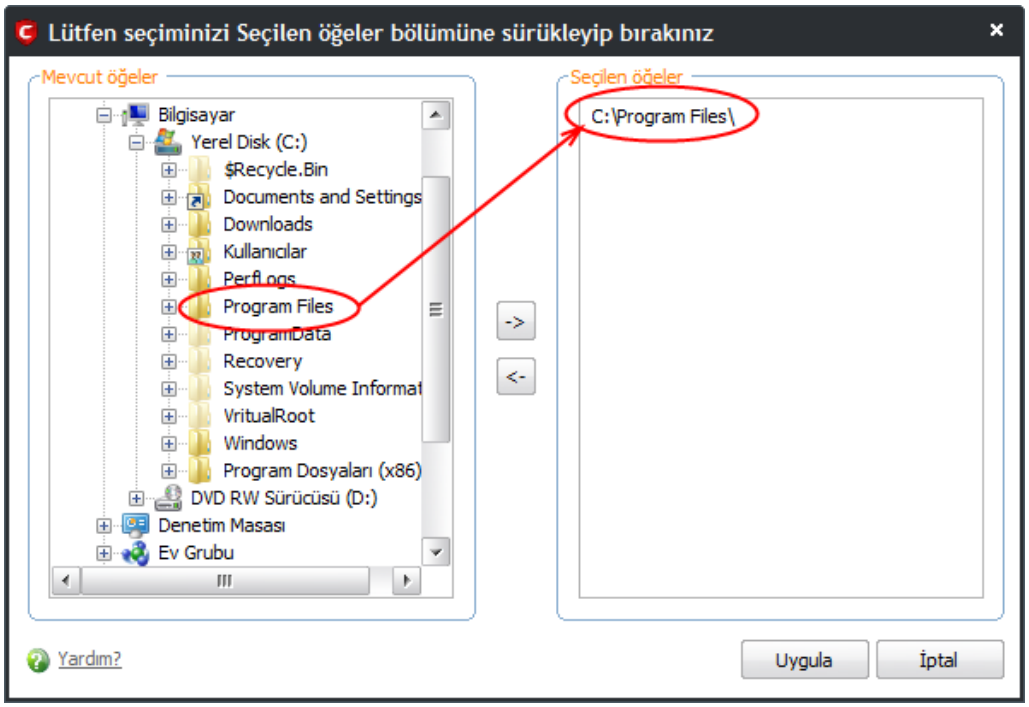
1. Antivirüs ekranından 'Tarama Profilleri' bölümüne tıklayın.
2. 'Ekle' düğmesine tıklayın. 'Tarama Profilleri' diyaloğu görünür.

3. ‘Ad’ kutusuna tarama profili adını girin ve ‘Ekle’ düğmesine tıklayın.



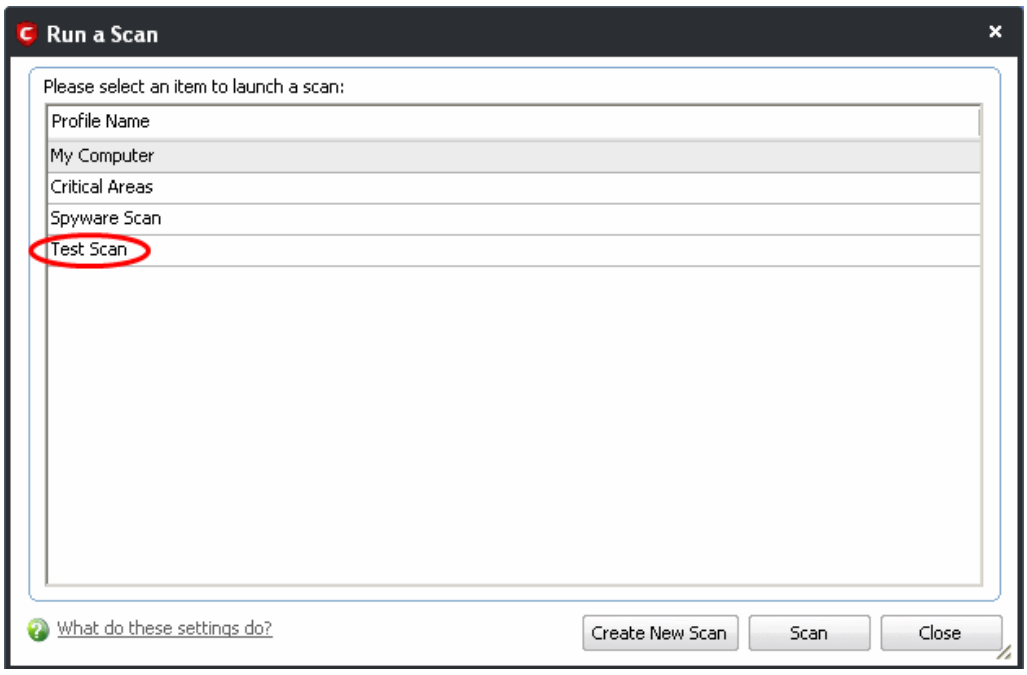
Yapılandırma ekranı açılır ve taranacak konumları seçmenizi ister. Sol sütun taranabilir tüm öğeleri gösterir.

4. Sol sütundan taranacak konumları seçin.
5. Sürükle ve bırak ile taranmasını istediğiniz öğeleri sağ sütuna taşıyın. (Seçimi geri döndürmek için öğeyi seçip sol oka tıklayın)

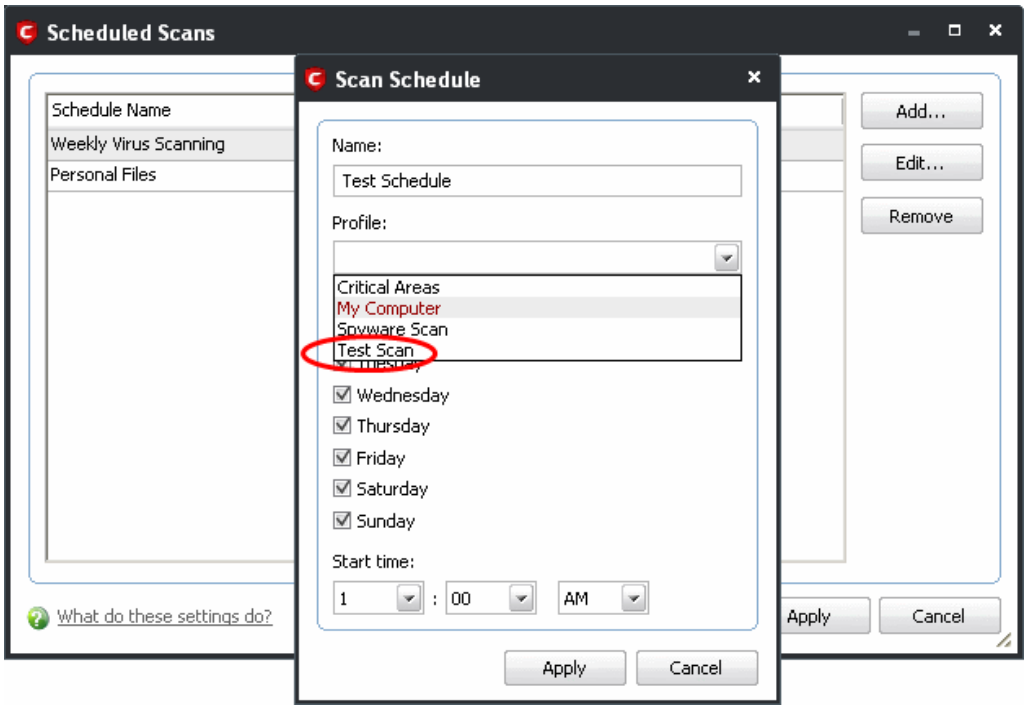


6. ‘Uygula’ düğmesine tıklayın.
7. Daha fazla Tarama Profili oluşturmak için işlemi tekrarlayın.
8. Tarama Profilleri ekranından ‘Uygula’ düğmesine tıklayarak profili geçerli duruma getirin.

Oluşturduğunuz profil ‘Bir Tarama Çalıştır’ panelinde görünecektir…



...ayrıca zamanlanmış taramalar profil seçimi açılır listesinde de yer alacaktır.



- **Tarama Profilini düzenlemek için 'Düzenle' düğmesine tıklayın.**
- **Tarama Profilini kaldırmak için 'Kaldır' düğmesine.**

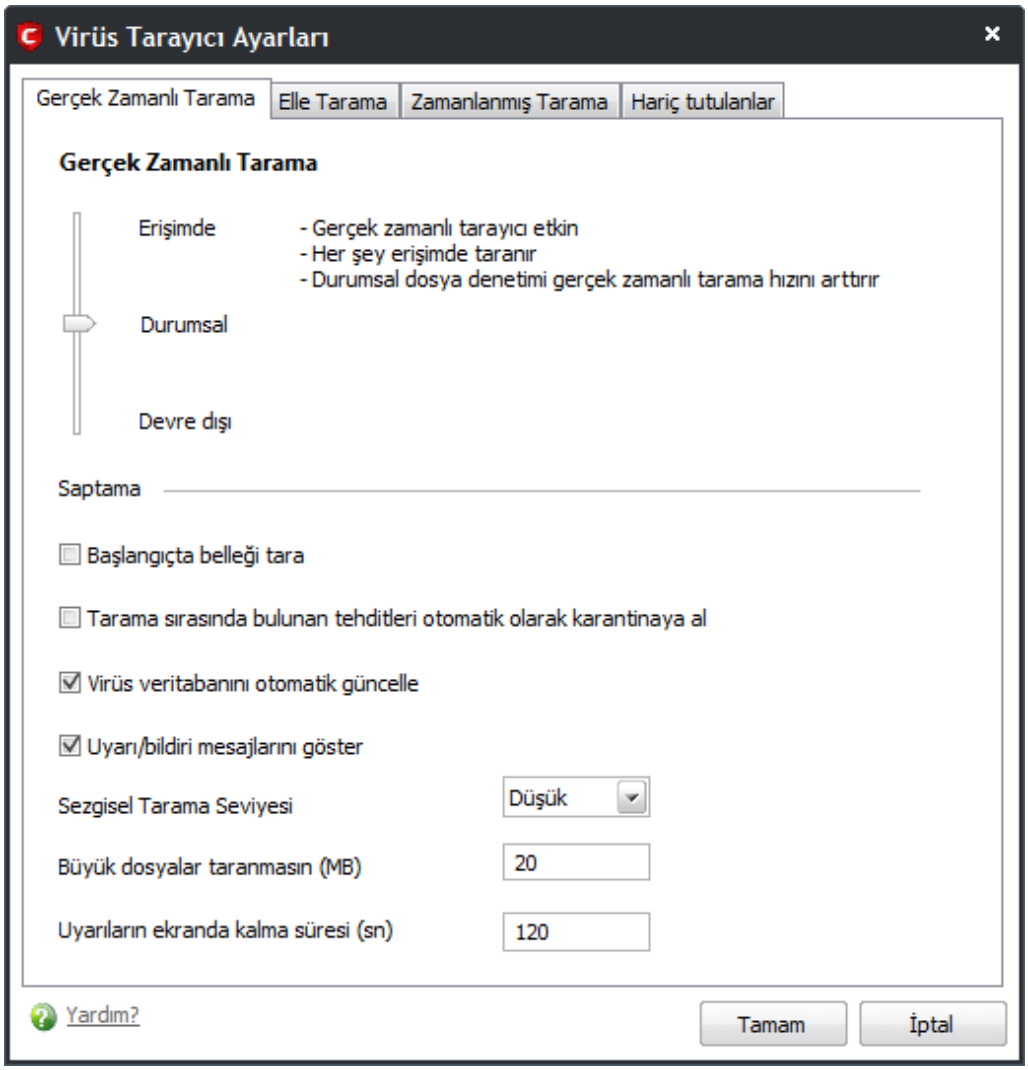
2.8 Tarayıcı Ayarları

Ayarlar yapılandırma paneli çeşitli tarayıcı ayarlarını yapmanıza izin verir.

- **Tarama türü için yapılmış ayarlamalar ileride yapılacak o tür taramaların tümüne uygulanır.**
- **'Hariç tutulanlar' listesindeki öğeler tüm taramalarda tarama dışı tutulur.**

Virüs Tarayıcı Ayarları panelini açmak için

- **Antivirüs ekranından 'Tarayıcı Ayarları' bölümüne girin.**



Bu panel kullanılarak yapılandırılabilecek seçenekler

- **Gerçek Zamanlı Tarama – Gerçek zamanlı tarama (Erişimde tarama) parametrelerini ayarlamak için;**
- **Elle Tarama – Elle tarama parametrelerini ayarlamak için (Bir Tarama Çalıştır);**
- **Zamanlanmış Tarama – Zamanlanmış tarama parametrelerini ayarlamak için;**
- **Hariç tutulanlar – Yoksayılan tehditleri ve hariç tutulanlar parametrelerini görmek için.**

2.8.1 Gerçek Zamanlı Tarama

Gerçek Zamanlı Tarama ('Erişimde' tarama olarak da bilinir) sürekli olarak oluşturulan , açılan veya erişilen dosyaları tarar.

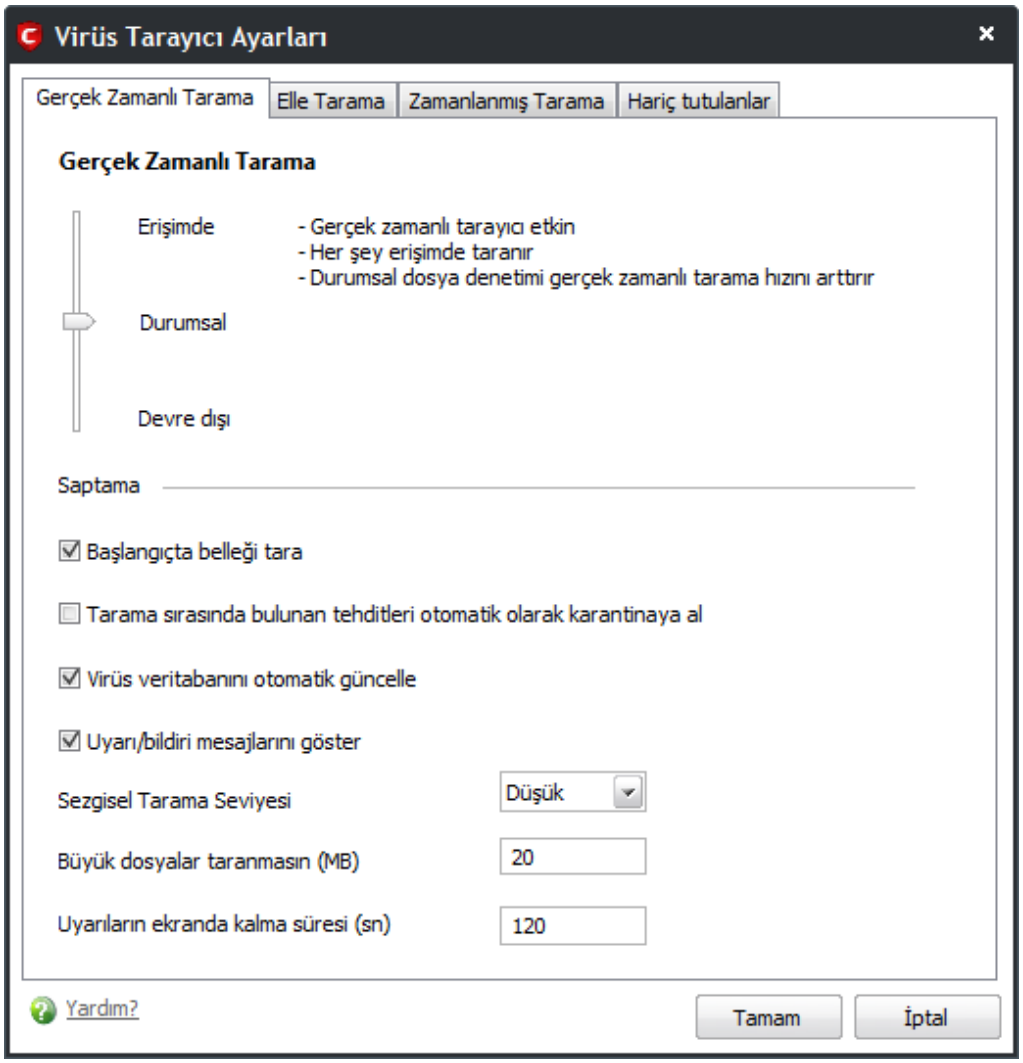
Gerçek Zamanlı Tarama ayrıca sistem belleğini de açılışta tarar. Yıkıcı anormallikler oluşturan programlar veya

dosyalar açarsanız virüs tarayıcısı anında engeller ve uyarı verir – tehditlere karşı gerçek zamanlı koruma sağlar.

Gerçek Zamanlı Tarama için '**Devre Dışı**', '**Durumsal**' ve '**Erişimde**' olarak üç ayar bulunur.

Gerçek Zamanlı Tarama seviyesini ayarlamak için

- **'Tarayıcı Ayarları' panelinden 'Gerçek Zamanlı Tarama' sekmesine tıklayın.**
- **Tarama kaydırıcısını gereken seviyeye çekin. Bulunan seçenekler Devre Dışı (önerilmez), Durumsal (varsayılan) ve Erişimde'dir. Burada seçtiğiniz ayar ayrıca Özet ekranında da görüntülenir.**



- **Erişimde – En yüksek seviyede koruma sağlar. Açılan tüm dosyalar çalışmadan önce taranır ve tehditler yürütülmeden önce saptanır.**
- **Durumsal – CIS içinde bulunan Durumsal Dosya Denetimi (tm) adındaki özelliği ile erişimde taramanın sistem performansını üzerindeki etkilerini en aza indirir. 'Durumsal' seçilmesi ile CIS yalnızca son güncellemeden bu yana taranmamış dosyaları tarar – tarama hızını ve verimliliğini arttırır.**
- **Devre Dışı – Gerçek zamanlı tarama devre dışıdır. Antivirüs herhangi bir tarama gerçekleştirmez ve tehditler saptanamaz.**

Saptama Ayarları

- **Başlangıçta belleği tara – Sistem başlangıcında sistem belleği taranır.**
- **Tarama sırasında bulunan tehditleri otomatik olarak karantinaya al – Zararlı içeren dosyalar tarama sırasında karantinaya taşınır. Karantinadan bu dosyaları geri yükleyebilir veya kaldırabilirsiniz.**
- **Taramadan önce virüs veritabanını güncelle – Tarama başlamadan önce virüs veritabanı güncellemesi yapılır.**
- **Uyarı/bildiri mesajlarını göster – Ekranın sağ alt köşesinde görüntülenen uyarı/bildirim mesajlarını etkinleştirir. Bu uyarılar kullanıcının uyarıya neden olan dosyayı belirlemesine yardımcı olur. Uyarılan devre dışı bırakılması tarama işlemini etkilemez ve Antivirüs arka planda tehditleri belirlemeye devam eder. Antivirüs uyarıları hakkında daha fazla bilgi için buraya tıklayın.**
- **Sezgisel Tarama Seviyesi - Comodo AntiVirüs bilinmeyen zararlıları saptamak için çeşitli sezgisel tarama teknikleri kullanır. 'Sezgisel' tarama, dosya kodunun incelenerek tipik zararlı kodu içerip içermediğine bakılmasıdır. Sezgisel tarama dosya imzalarına bakmak yerine dosyanın zararlı davranışları veya özellikleri içerip içermediğine bakar.**

Bu sayede tarama motoru şüpheli betikleri ve programları virüs veritabanında bulunmasalar bile saptayabilir.

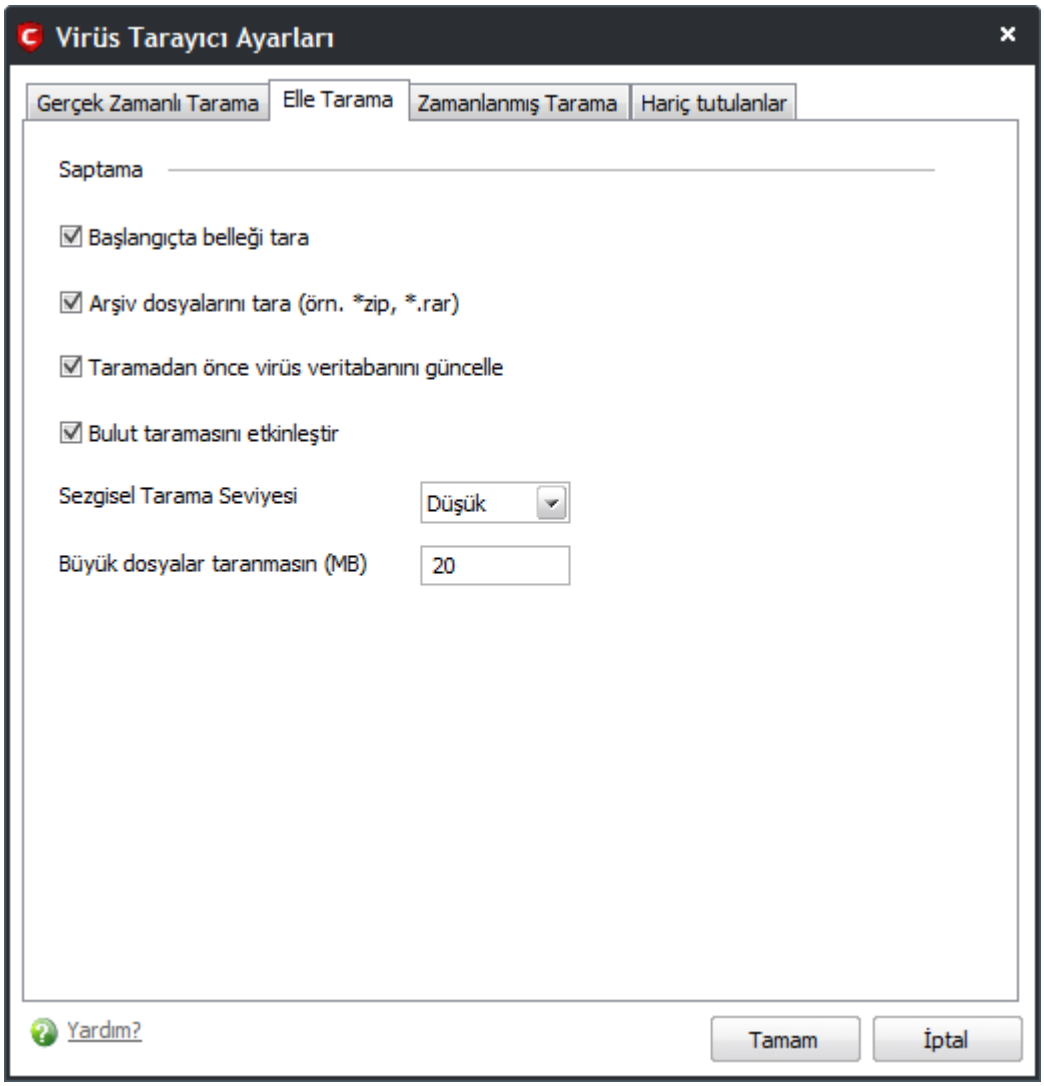
Sezgisel koruma 4 seviyeye ayarlanabilir:

- **Kapalı** – Sezgisel tarama devre dışıdır ve geleneksel veritabanı yöntemi kullanılarak zararlılar taranır.
- **Düşük** – Düşük hassaslık ve düşük sayıda yanlış alarm.
- **Orta** – Orta hassaslık ve orta sayıda yanlış alarm.
- **Yüksek** – Yüksek hassaslık ve yüksek sayıda yanlış alarm.

- **Büyük dosyalar taranmasın – Bu kutuya girilen değerden (MB olarak) büyük boyuttaki dosyalar otomatik olarak taranmayacaktır. Bu dosyaları taramak için Bir Tarama Çalıştır seçeneğini kullanabilirsiniz.**
- **Uyarıların ekranda kalma süresi – Uyarıların ekranda kalacağı süreyi saniye olarak ayarlayabilirsiniz.**
- **Ayarların geçerli olabilmesi için 'Tamam' düğmesine tıklayın.**

2.8.2 Elle Tarama

Elle Tarama ayarları Bir Tarama Çalıştır (Elle Tarama) özelliklerini ve parametrelerini ayarlamanıza izin verir.



- **Başlangıçta belleği tara – Sistem başlangıcında sistem belleği taranır.**
- **Arşiv dosyalarını tara - .ZIP ve .RAR gibi arşiv dosyaları taranır ve içlerinde zararlı bulunursa uyarı verilir. RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ ve CAB arşivleri de dahildir.**
- **Taramadan önce virüs veritabanını güncelle – Tarama başlamadan önce virüs veritabanı güncellemesi yapılır.**
- **Bulut taramasını etkinleştir -** Comodo'nun çevrimiçi veritabanına bağlanılarak dosyalar denetlenir.
- **Sezgisel Tarama Seviyesi - Comodo AntiVirüs bilinmeyen zararlıları saptamak için çeşitli sezgisel tarama teknikleri kullanır. 'Sezgisel' tarama, dosya kodunun incelenerek tipik zararlı kodu içerip içermediğine bakılmasıdır. Sezgisel tarama dosya imzalarına bakmak yerine dosyanın zararlı davranışları veya özellikleri içerip içermediğine bakar.**

Bu sayede tarama motoru şüpheli betikleri ve programları virüs veritabanında bulunmasalar bile saptayabilir.

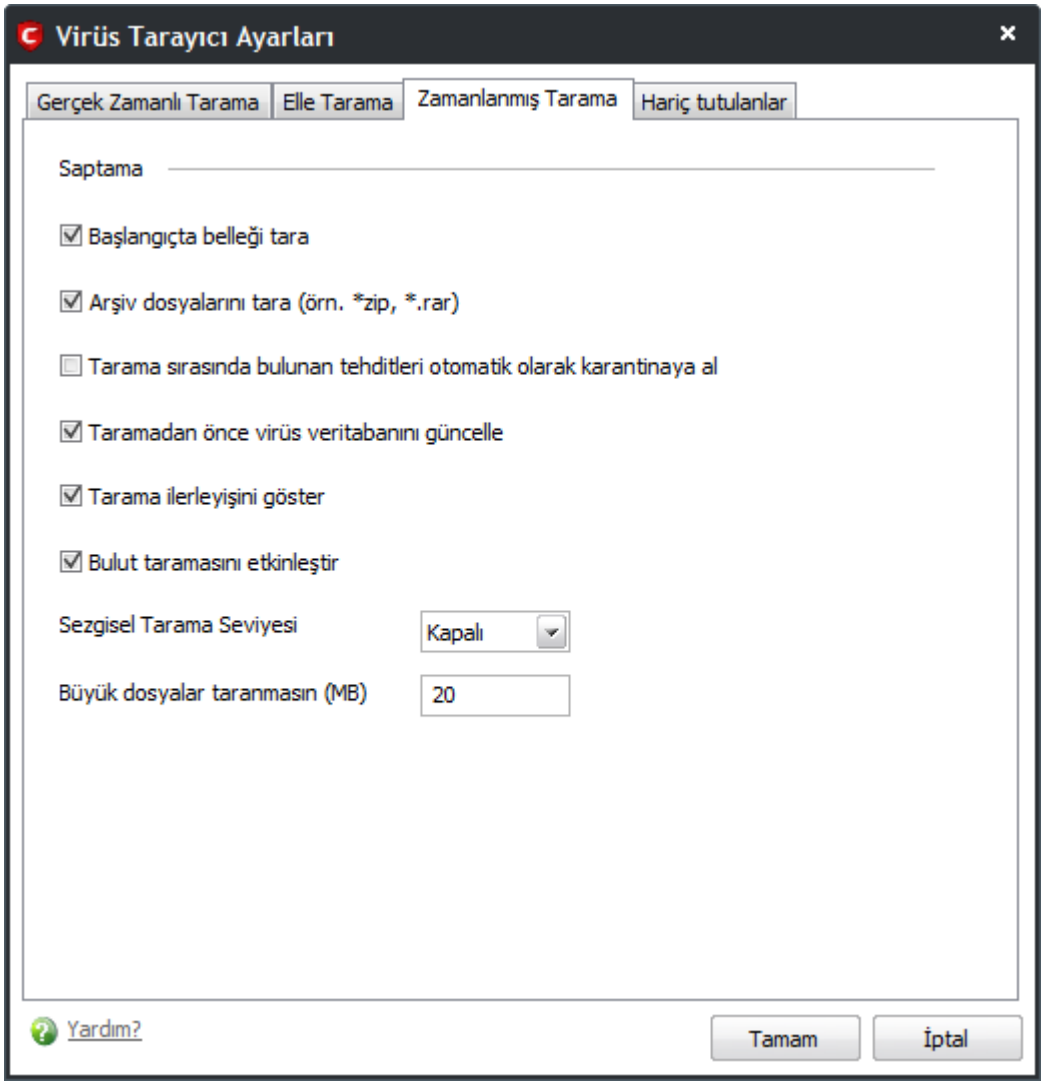
Sezgisel koruma 4 seviyeye ayarlanabilir:

- **Kapalı** – Sezgisel tarama devre dışıdır ve geleneksel veritabanı yöntemi kullanılarak zararlılar taranır.
- **Düşük** – Düşük hassaslık ve düşük sayıda yanlış alarm.
- **Orta** – Orta hassaslık ve orta sayıda yanlış alarm.
- **Yüksek** – Yüksek hassaslık ve yüksek sayıda yanlış alarm.
- **Büyük dosyalar taranmasın** – Bu kutuya girilen değerden (MB olarak) büyük boyuttaki dosyalar otomatik olarak taranmayacaktır. Bu dosyaları taramak için Bir Tarama Çalıştır seçeneğini kullanabilirsiniz.

- Ayarların geçerli olabilmesi için **'Tamam'** düğmesine tıklayın.

2.8.3 Zamanlanmış Tarama

Zamanlanmış Tarama ayar paneli taramalarınızı tercihlerinize göre özelleştirmenize izin verir.



Taramalarınızı belirlediğiniz zamanlarda çalıştırabilir ve belirli konumları taramak için tarama profillerini

kullanabilirsiniz.

Saptama ayarları aşağıdaki gibidir:

- **Başlangıçta belleği tara – Sistem başlangıcında sistem belleği taranır.**
- **Arşiv dosyalarını tara - .ZIP ve .RAR gibi arşiv dosyaları taranır ve içlerinde zararlı bulunursa uyarı verilir. RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ ve CAB arşivleri de dahildir.**
- **Tarama sırasında bulunan tehditleri otomatik olarak karantinaya al – Zararlı içeren dosyalar tarama sırasında karantinaya taşınır. Karantinadan bu dosyaları geri yükleyebilir veya kaldırabilirsiniz.**
- **Taramadan önce virüs veritabanını güncelle – Tarama başlamadan önce virüs veritabanı güncellemesi yapılır.**
- **Tarama ilerleyişini göster – Tarama başladığında tarama ilerleyişini gösteren pencere açılır.**
- **Bulut taramasını etkinleştir -** Comodo'nun çevrimiçi veritabanına bağlanılarak dosyalar denetlenir.
- **Sezgisel Tarama Seviyesi - Comodo AntiVirüs bilinmeyen zararlıları saptamak için çeşitli sezgisel tarama teknikleri kullanır. 'Sezgisel' tarama, dosya kodunun incelenerek tipik zararlı kodu içerip içermediğine bakılmasıdır. Sezgisel tarama dosya imzalarına bakmak yerine dosyanın zararlı davranışları veya özellikleri içerip içermediğine bakar.**

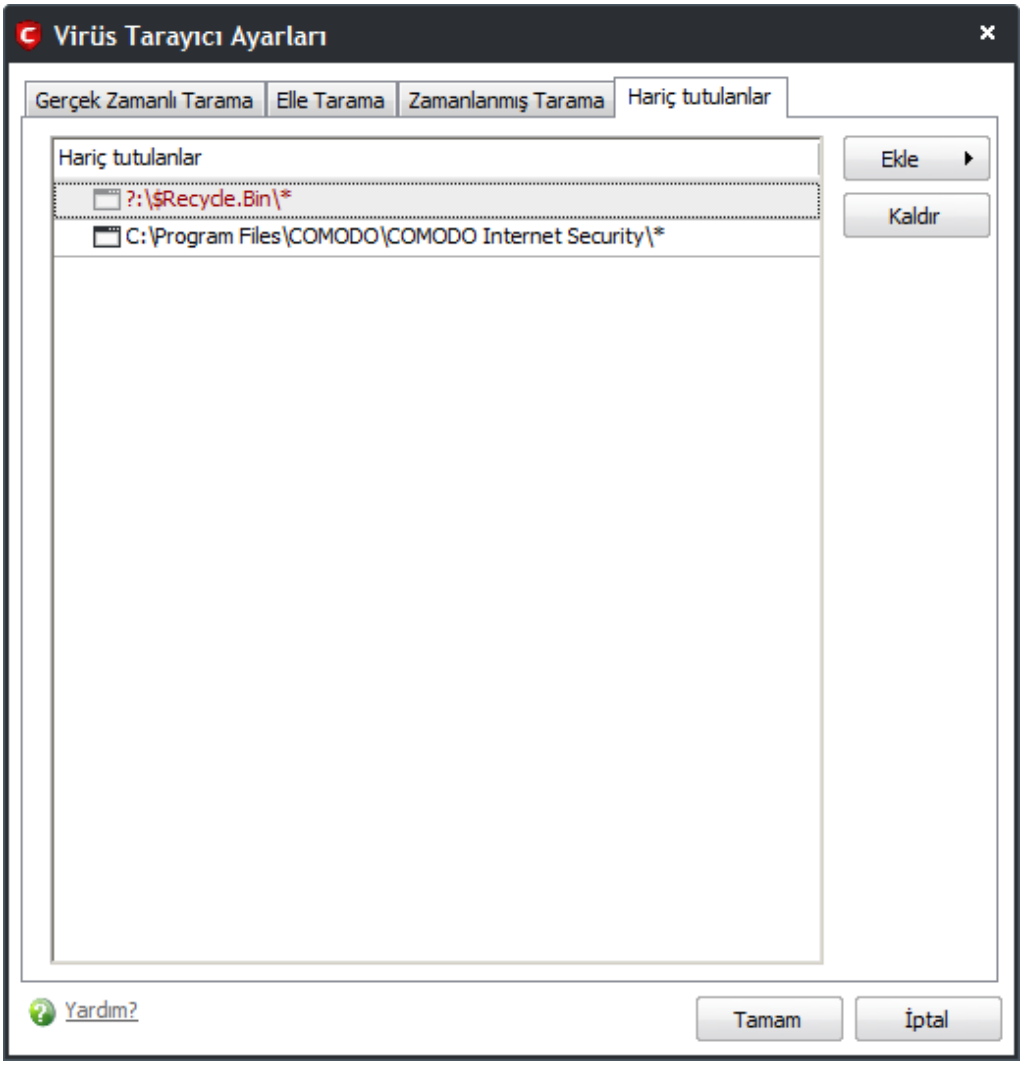
Bu sayede tarama motoru şüpheli betikleri ve programları virüs veritabanında bulunmasalar bile saptayabilir.

Sezgisel koruma 4 seviyeye ayarlanabilir:

- **Kapalı** – Sezgisel tarama devre dışıdır ve geleneksel veritabanı yöntemi kullanılarak zararlılar taranır.
- **Düşük** – Düşük hassaslık ve düşük sayıda yanlış alarm.
- **Orta** – Orta hassaslık ve orta sayıda yanlış alarm.
  - **Yüksek** – Yüksek hassaslık ve yüksek sayıda yanlış alarm.
  - **Büyük dosyalar taranmasın** – Bu kutuya girilen değerden (MB olarak) büyük boyuttaki dosyalar otomatik olarak taranmayacaktır. Bu dosyaları taramak için Bir Tarama Çalıştır seçeneğini kullanabilirsiniz.

- Ayarların geçerli olabilmesi için **'Tamam'** düğmesine tıklayın**.**

2.8.4 Hariç Tutulanlar



Tarama Sonuçlarından **Yoksay** ile yoksayılan uygulamalar/dosyalar veya antivirüs uyarısı ile hariç tutulanlara eklenen dosyaları gösterir.

Listedeki tüm öğeler ileride yapılacak tüm taramaların dışında tutulur.

Ayrıca elle de bu listeye ekleme yapabilirsiniz.

Dosyaları/uygulamaları güvenli olarak varsayarak tarama dışında tutmak için

1. 'Ekle' düğmesine tıklayın.

   Güvenmek istediğiniz dosyaları seçmek için 2 yöntem bulunmaktadır – **'Dosyalara Göz At…'** ve **'Çalışan İşlemlere Göz At'**.

   - **Dosyalara Göz At… -** Hariç tutmak istediğiniz dosyaları açılan pencereden seçerek kolayca ekleyebilirsiniz.
   - **'Çalışan İşlemlere Göz At –** Çalışan işlemler listesinden seçerek ekleme yapabilirsiniz.

Yukarıdaki yöntemleri kullanarak seçtiğiniz uygulama konumuyla birlikte listede görünür.

2.Ayarların geçerli olabilmesi için 'Tamam' düğmesine tıklayın.

3 Güvenlik Duvarı Görevleri - Tanıtım

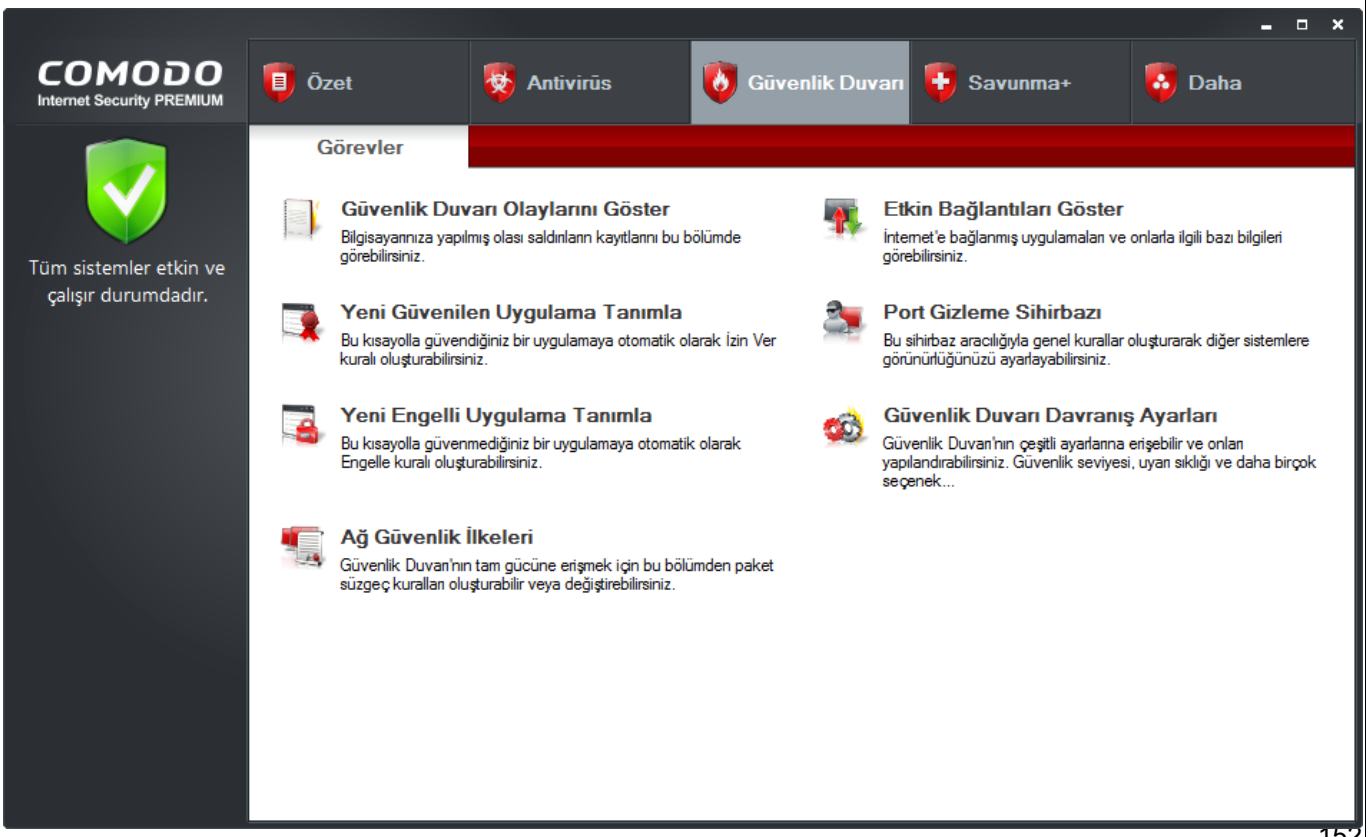
Comodo Güvenlik Duvarı gelen ve giden tehditlere karşı yüksek seviyede koruma sağlar, portlarınızı diğer bilgisayarlardan gizler, zararlı yazılımların bilgi sızdırmasını önler.

Güvenlik Duvarına gezinti menüsündeki 

bağlantısı kullanılarak erişilebilir.

Yapılandırma alanı tüm özelliklere kolay erişim sağlar ve kurallar oluşturmanıza izin verir. Ayrıntılı bilgi için aşağıdaki bağlantılara tıklayın.

- **Güvenlik Duvarı Olaylarını Göster**
- **Yeni Güvenilen Uygulama Tanımla**
- **Yeni Engelli Uygulama Tanımla**
- **Ağ Güvenlik İlkeleri**
- **Etkin Bağlantıları Göster**
- **Port Gizleme Sihirbazı**
- **Güvenlik Duvarı Davranış Ayarları**

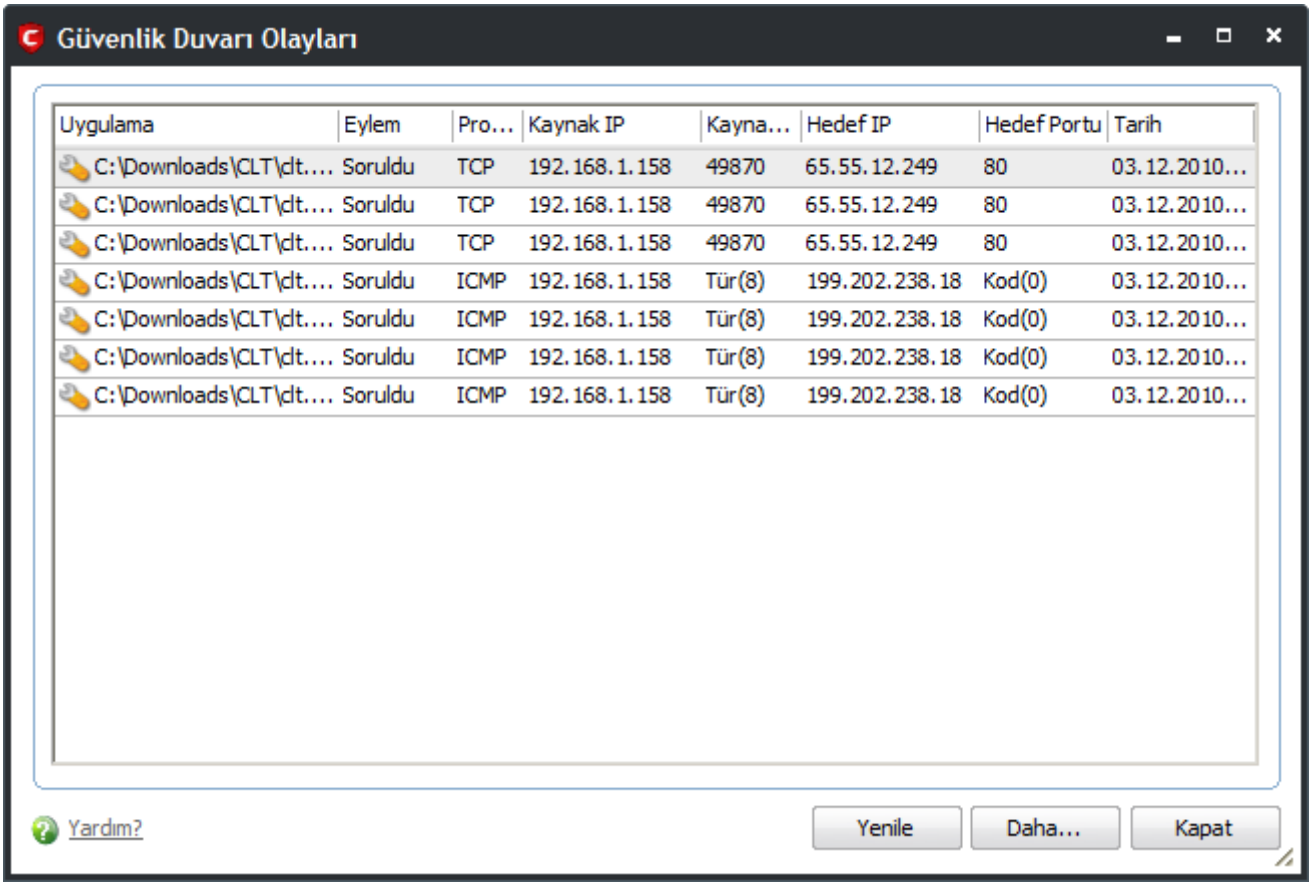


3.1 Güvenlik Duvarı Olaylarını Göster

'Güvenlik Duvarı Olaylarını Göster' güvenlik duvarı tarafından oluşturulan raporları içerir.

Güvenlik Duvarı olaylarını görüntülemek için

- Güvenlik Duvarı ekranından 'Güvenlik Duvarı Olaylarını Göster' bağlantısına tıklayın.



Sütun Açıklamaları

1. **Uygulama** – Olayı tetikleyen uygulama;
2. **Eylem** – Bağlantı isteğine nasıl tepki verildiğini gösterir.
3. **Protokol** – Bağlantının hangi iletişim kuralı kullanılarak yapıldığını gösterir. Genelde TCP veya UDP dir.
4. **Kaynak IP** – Bağlantı girişiminde bulunan makinanın IP adresidir. Giden bağlantılar için sizin bilgisayarınızın IP adresini gösterir.
5. **Kaynak Port** – Bağlantının hangi porttan yapıldığını gösterir.

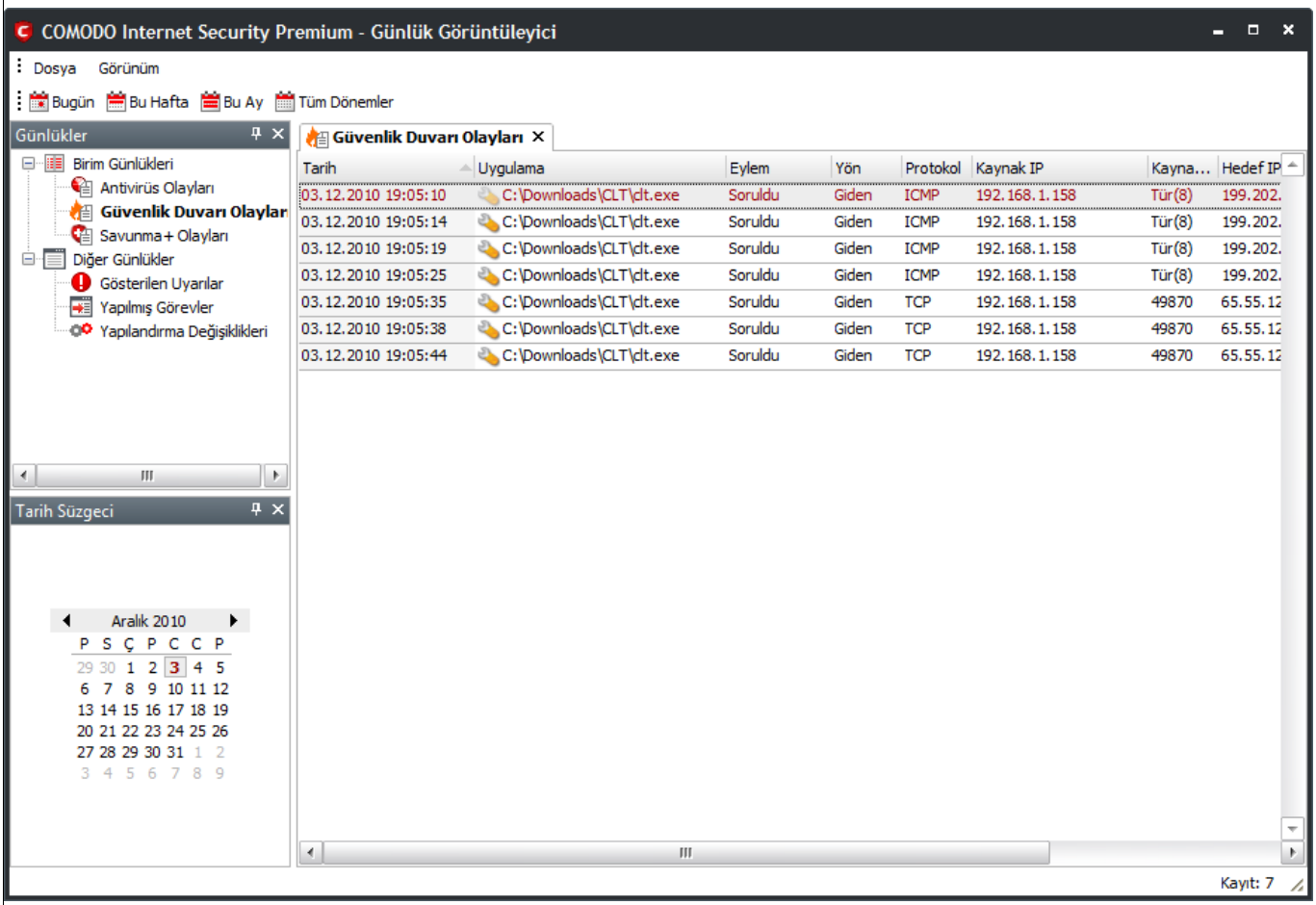
6. **Hedef IP** - Bağlantı girişiminin yapıldığı makinanın IP adresidir. Gelen bağlantılar için sizin bilgisayarınızın IP adresini gösterir.
7. **Hedef Port** - Bağlantının hangi porta yapıldığını gösterir.
8. **Tarih/Saat** – Bağlantı girişiminin yapıldığı tarih ve saati gösterir.

- **Listeyi güncellemek için** 'Yenile' **düğmesine tıklayın.**
- **CIS Günlük Görüntüleyiciyi açmak için** 'Daha ...' **düğmesine tıklayın. Daha fazla bilgi için aşağıya bakın.**

Günlük Görüntüleyici Bileşen

Tüm tutulmuş günlüklerin geçmişini iki kategoride tutar: Birim Günlükleri ve Diğer Günlükler.

Ayrıca belirli süzgeçler ile raporları kişisel günlük dosyalarına çıkartmanıza da olanak sağlar.



Günlük Görüntüleyici Bileşeni üç bölüme ayrılmıştır. Üst panelde zaman süzgeçleri, sol panelde günlük türü ve sağ panelde seçili ölçütlere uygun olan günlük olayları bulunur.

Birim günlükleri Güvenlik Duvarı, Savunma+, Antivirüs ve Diğer Günlüklerden oluşur. Diğer Günlüklerde aşağıdaki olayları içerir:

- **Gösterilen Uyarılar: CIS tarafından gösterilen uyarıların kayıtları.**

- **Yapılmış Görevler: Çeşitli yapılmış görevleri içerir. (Güncellemeler, tarama sonuçları gibi).**
- **Yapılandırma Değişiklikleri: Yapılandırmada yapılan değişiklikleri gösterir**

Günlük Dosyalarının Süzülmesi

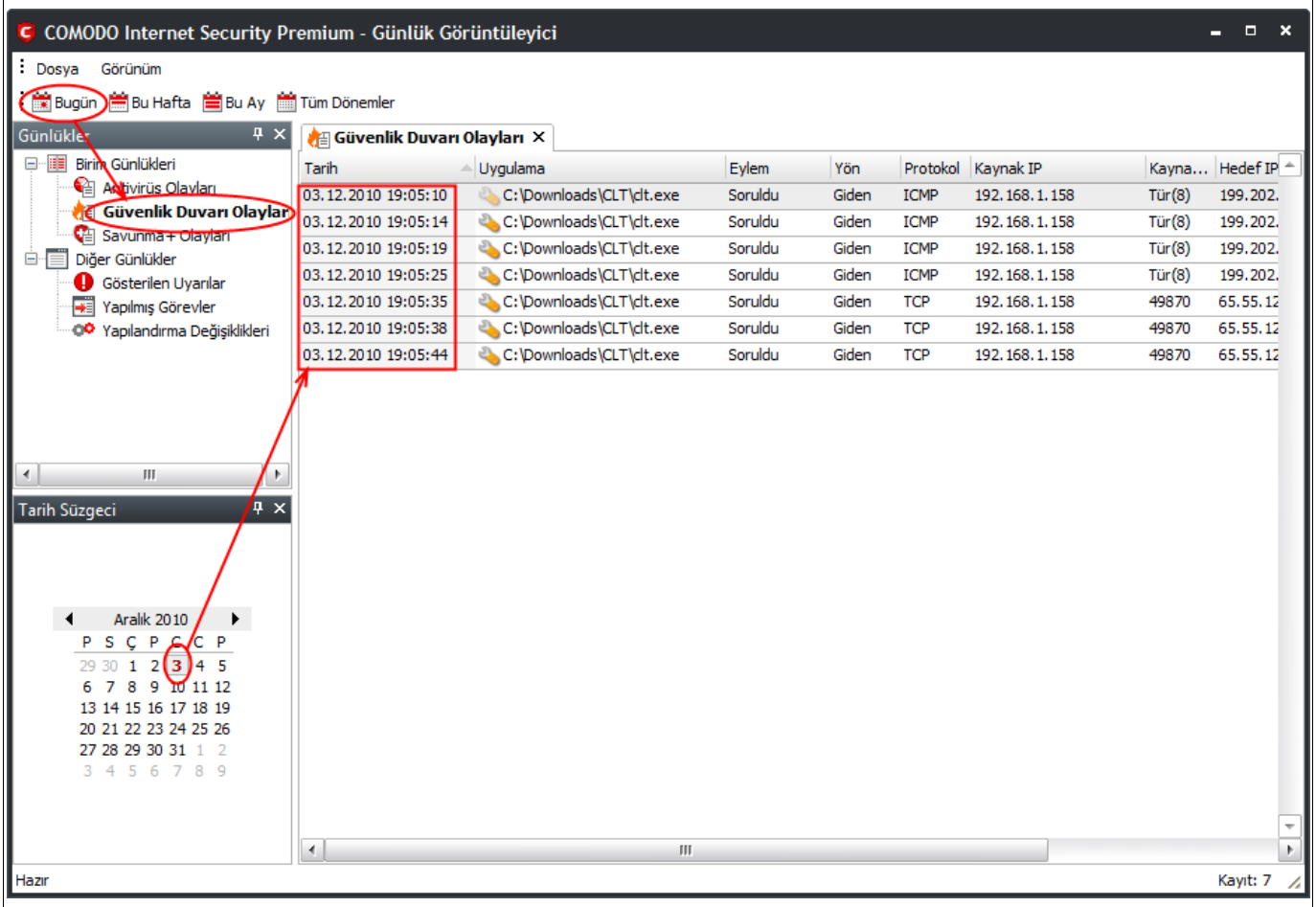
Comodo Internet Security günlük olaylarının belirli süzgeçlere göre gösterilmesine izin verir.

Zaman Süzgeçleri:

Zaman süzgeçleri üst panelde bulunur ve bunlardan biri seçildiğinde sağ panelin görünüşünü değiştirir:

•**Bugün** – Bugün gerçekleşen olayları gösterir.
•**Bu Hafta** – Bu hafta gerçekleşen olayları gösterir.
•**Bu Ay** – Bu ay gerçekleşen olayları gösterir.
•**Tüm Dönemler** – CIS kurulumundan veya son günlük temizlemesinden sonraki tüm olayları gösterir.

Aşağıdaki örnek 'Bugün' zaman dilimini göstermektedir.



Not: Sağ panelin içeriği CIS bileşenlerine göre farklılık gösterebilir.

Kullanıcı Tanımlı Süzgeçler:

Aşağıdaki tablo bulunan süzgeçleri ve onların anlamlarını gösterir:

Bulunan Süzgeçler – Birim Günlükleri		
Antivirüs Süzgeçleri	**Güvenlik Duvarı Süzgeçleri**	**Savunma+ Süzgeçleri**
Tarih – Seçili tarihteki olayları gösterir	**Tarih** - Seçili tarihteki olayları gösterir.	**Tarih** - Seçili tarihteki olayları gösterir.
Konum – Seçili konumdaki olayları gösterir	**Uygulama –** Olaya neden olan uygulamayı gösterir	**Uygulama -** Olaya neden olan uygulamayı gösterir
Zararlı Adı – Zararlı adına uygun olayları gösterir	**Eylem** – Gerçekleştirilen eyleme uygun olayları gösterir	**Eylem** - Gerçekleştirilen eyleme uygun olayları gösterir
Eylem - Gerçekleştirilen eyleme uygun olayları gösterir	**Yön** – Bağlantının yönüne uygun olayları gösterir	**Hedef Adı –** Hedef uygulamaya ilişkin olayları gösterir
Durum - Gerçekleştirilen eylemin durumuna uygun olayları gösterir. 'Başarılı' veya 'Başarısız' olabilir.	**Protokol –** Belli protokole ilişkin olayları gösterir	**Uyarı** – Eylem sütununda 'Soruldu' görünen uyarıların yanında 'İlişkili Uyarı' adında bir bağlantı görünür. Bu bağlantı sizi 'Gösterilen Uyarılar' olay günlüğüne götürür
Uyarı - Eylem sütununda 'Soruldu' görünen uyarıların yanında 'İlişkili Uyarı' adında bir bağlantı görünür. Bu bağlantı sizi 'Gösterilen Uyarılar' olay günlüğüne götürür	**Kaynak IP adresi** - Belli IP adresinden gerçekleştirilen bağlantılara ilişkin olayları gösterir	
	Kaynak Portu - Belli porttan yapılan bağlantılara ilişkin olayları gösterir	
	Hedef IP adresi Belli IP adresinden gerçekleştirilen	

Bulunan Süzgeçler – Birim Günlükleri		
	bağlantılara ilişkin olayları gösterir	
	Hedef Portu - Belli porttan yapılan bağlantılara ilişkin olayları gösterir	
	Uyarı - Eylem sütununda 'Soruldu' görünen uyarıların yanında 'İlişkili Uyarı' adında bir bağlantı görünür. Bu bağlantı sizi 'Gösterilen Uyarılar' olay günlüğüne götürür	

Özel Süzgeçlerin Oluşturulması

Özel Süzgeçler Gelişmiş Süzgeç arayüzü kullanılarak oluşturulabilir. Gelişmiş Süzgeç arayüzü günlük görüntüleyiciye sağ tıklayarak içerik menüsünden açılabilir.

- **'Gelişmiş Süzgeç' alanını açmak için Görünüm > Gelişmiş Süzgeç seçeneğine tıklayın.**

Veya

- **Olay panelinde sağ tıklayın ve 'Gelişmiş Süzgeç' seçin.**

'Gelişmiş Süzgeç' paneli üstte açılır.

Gelişmiş rapor süzgeç görünümü seçili bileşene göre farklılık gösterir.

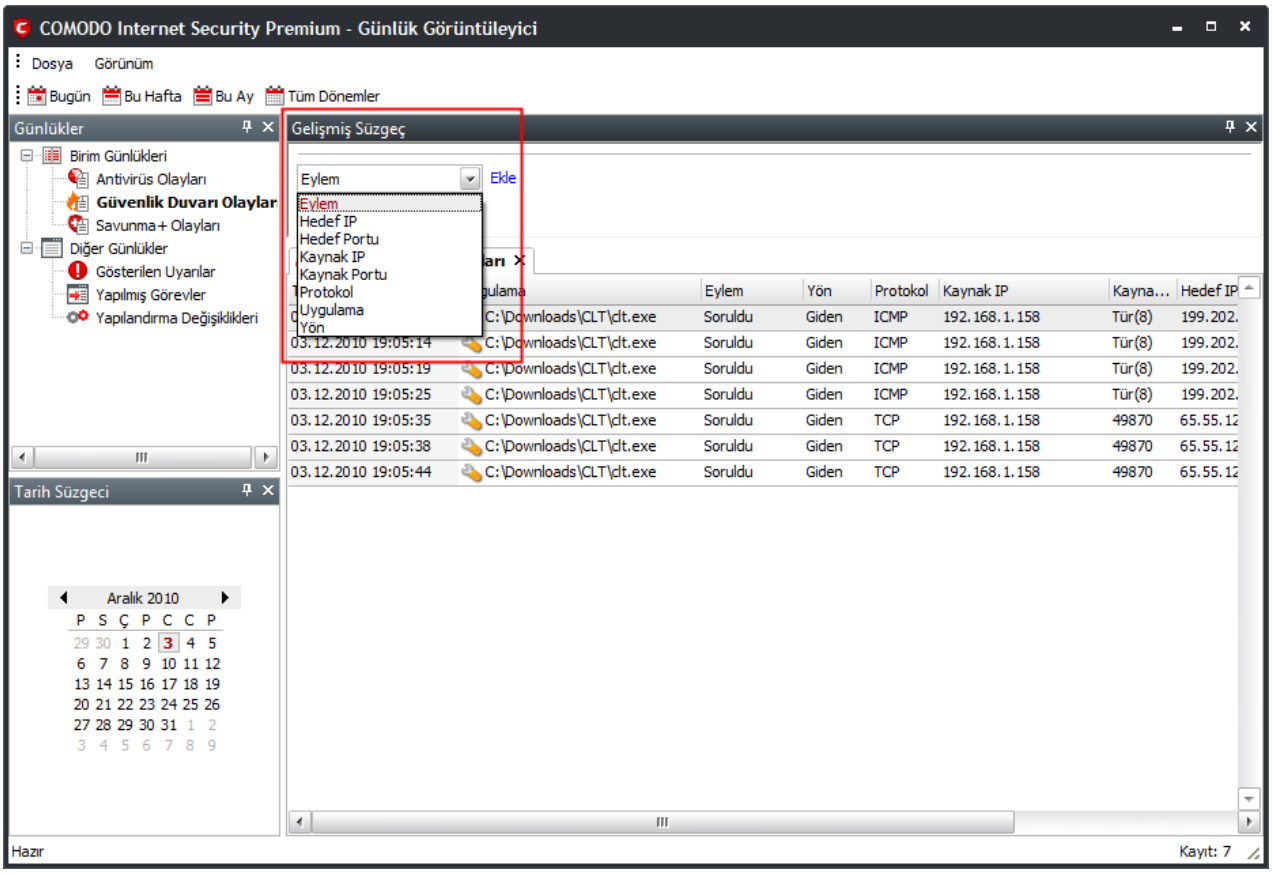
Güvenlik Duvarı Olayları – Gelişmiş Süzgeçler

Güvenlik Duvarı olayları için Gelişmiş Süzgeçlerin yapılandırılması

1. 'Görünüm > Gelişmiş Süzgeç' seçin.
2. 'Birim Günlükleri' altından 'Güvenlik Duvarı Olayları' seçin.

Ekleyebileceğiniz 4 süzgeç kategorisi ve her bir kategori altında farklı parametreler bulunmaktadır.

3. 'Ekle' düğmesini kullanarak süzgeçler ekleyebilirsiniz.



Aşağıdakiler 'Ekle' açılır menüsünde bulunmaktadır:

i. **Eylem**: Açılır liste ve bulunan seçilebilir eylem süzgeçlerini gösterir.

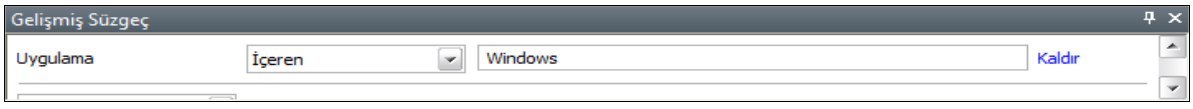
a) Açılır listeden 'Eşit' veya 'Eşit Değil' seçin. 'Eşit Değil' seçeneği seçimi tersine çevirir.

b) Aramayı geliştirmek için değişkenlerin kutularını işaretleyebilirsiniz. Bulunan değişkenler şunlardır:

- Engellendi: Engellenen olayların listesini görüntüler
- İzin Verildi: İzin verilen olayların listesini görüntüler
- Soruldu: Kullanıcıya sorulan olayların listesini görüntüler
- Bastırıldı: Bastırılan olayların listesini görüntüler

Süzülen girdiler doğrudan altta görünür.

i. **Uygulama**: Açılır liste ve metin alanı görünür.

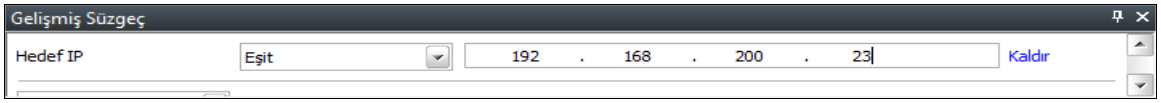


a) Açılır listeden 'İçeriyor' veya 'İçermiyor' seçeneğini seçin.

b) Süzülmesi gereken metini girin.

Süzülen girdiler doğrudan altta görünür.

i. **Hedef IP**: Açılır liste ve metin alanı görünür.

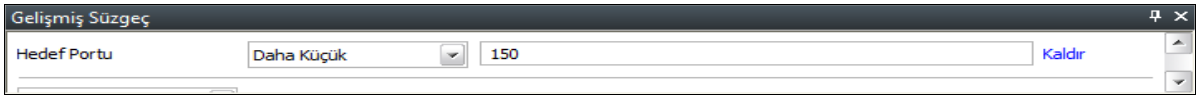


a) Açılır listeden 'Eşit' veya 'Eşit Değil' seçin. 'Eşit Değil' seçeneği seçimi tersine çevirir.

b) Süzülmesi gereken hedef IP adresini girin.

Süzülen girdiler doğrudan altta görünür.

i. **Hedef Port**: Açılır liste ve metin alanı görünür.



a) Aşağıdaki seçeneklerden birini açılır listeden seçin.

- Eşit
- Büyük
- Büyük veya Eşit
- Küçük
- Küçük veya Eşit
- Eşit Değil

a) Hedef portu metin alanına girin.

Süzülen girdiler doğrudan altta görünür.

i. **Yön**: Açılır liste ve bulunan seçilebilir yön süzgeçlerini gösterir.

a) Açılır listeden 'Eşit' veya 'Eşit Değil' seçin. 'Eşit Değil' seçeneği seçimi tersine çevirir.

b) Aramayı geliştirmek için değişkenlerin kutularını işaretleyebilirsiniz. Bulunan değişkenler şunlardır:

- Gelen: Sisteme gelen olayların listesini görüntüler
- Giden: Sistemden giden olayların listesini görüntüler

Süzülen girdiler doğrudan altta görünür.

i. **Protocol**: Açılır liste ve bulunan seçilebilir protokol süzgeçlerini gösterir.

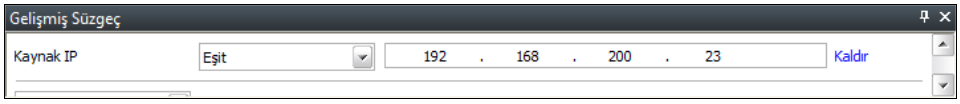
a) Açılır listeden 'Eşit' veya 'Eşit Değil' seçin. 'Eşit Değil' seçeneği seçimi tersine çevirir.

b) Aramayı geliştirmek için değişkenlerin kutularını işaretleyebilirsiniz. Bulunan değişkenler şunlardır:

- TCP
- UDP
- ICMP
- IPV4
- IGMP
- GGP
- PUP
- IDP
- ND

Süzülen girdiler doğrudan altta görünür.

i. **Kaynak IP**: Açılır liste ve bulunan seçilebilir süzgeçleri gösterir.

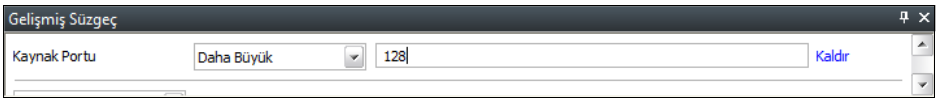


a) Açılır listeden 'Eşit' veya 'Eşit Değil' seçin. 'Eşit Değil' seçeneği seçimi tersine çe.

b) Süzülmesi gereken sistemin IP adresini girin.

Süzülen girdiler doğrudan altta görünür.

i. **Kaynak Port**: Açılır liste ve bulunan seçilebilir süzgeçleri gösterir.



a) Aşağıdaki seçeneklerden birini açılır listeden seçin.

- Eşit
- Büyük
- Büyük veya Eşit
- Küçük
- Küçük veya Eşit
- Eşit Değil

a) Kaynak portunu metin alanına girin.

Süzülen girdiler doğrudan altta görünür.

Not: 'Gelişmiş Süzgeç' bölümünde birden fazla süzgeç eklenebilir. Eklenmiş bir süzgeci 'Kaldır' düğmesine tıklayarak kaldırabilirsiniz.

Diğer Günlükler – Gelişmiş Süzgeçler

Ayrıntılı bilgi için Antivirüs Görevleri > Antivirüs Olaylarını Göster > Günlük Görüntüleyici > Özel Süzgeçlerin Oluşturulması > Diğer Günlükler – Gelişmiş Süzgeçler bölümüne bakın.

Tarih Süzgeci

Tarih süzgeci işlevi hakkında daha fazla bilgi için buraya tıklayın.

Günlüklerin HTML dosyasına Çıkartılması

Günlük dosyalarının çıkartılması arşivleme ve sorun giderme açısından kullanışlıdır. İki yolla dosyaya çıkartma yapılabilir. İçerik menüsü kullanılarak veya 'Dosya' menüsü içinden..

i. **Dosya Menüsü**

1. Çıkartılmasını istediğiniz olayları seçin.
2. Dosya menüsünden 'Çıkart' düğmesine tıklayın.
3. Dosyanın kaydedileceği konumu seçin ve kaydedin.

i. **İçerik Menüsü**

1. Günlük penceresinde sağ tıklayarak görüntülenen olayları HTML dosyasına çıkartın.

Günlük penceresinde sağ tıklayarak görüntülenen olayları HTML dosyasına çıkartabilirsiniz.

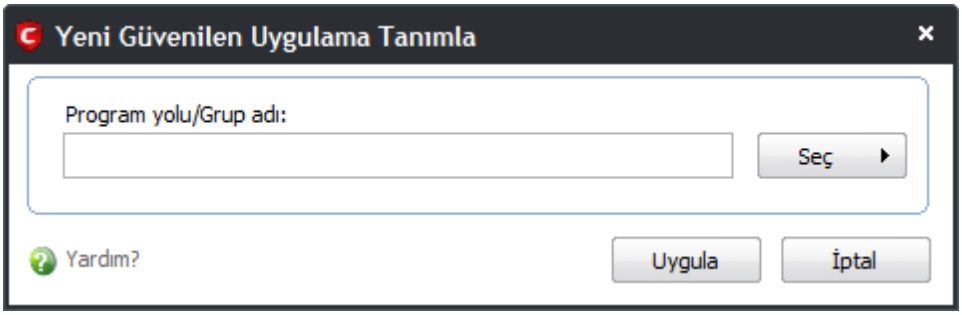
3.2 Yeni Güvenilen Uygulama Tanımla

Bu kısayol ile bir uygulamaya kolaylıkla 'İzin Ver' kuralı oluşturabilirsiniz.

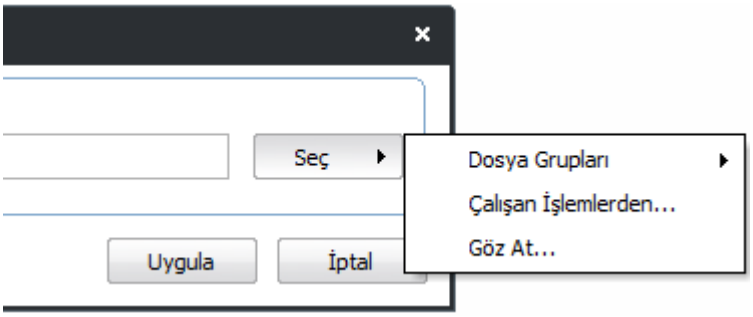
Tecrübeli kullanıcılar 'Ağ Güvenlik İlkeleri' bölümünü kullanarak kuralları düzenleyebilirler.

Yeni güvenilen uygulama tanımlamak için

1. Güvenlik Duvarı görevleri bölümünde ' Yeni Güvenilen Uygulama Tanımla ' bağlantısına tıklayın.
2. Güvenmek istediğiniz uygulamayı seçmenizi isteyen diyalog görünecektir.



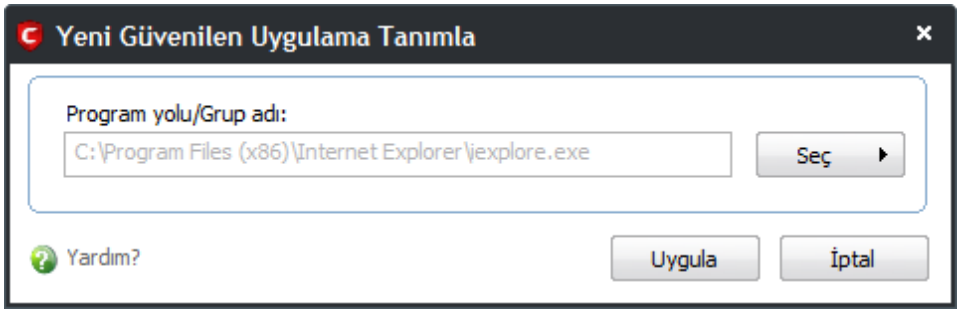
3. 'Seç' düğmesine tıklayın.



4. 3 yöntem ile güvenmek istediğiniz uygulamayı seçebilirsiniz - 'Dosya grupları'; 'Çalışan İşlemlerden' ve 'Göz At...'.
   - **Dosya Grupları** – Öntanımlı dosya gruplarından seçim yapabilirsiniz.
   - **Çalışan İşlemler** – Çalışan işlemler listesinden seçim yapabilirsiniz.
   - **Göz At... –** Uygula seç penceresinden istediğiniz uygulamayı bularak seçebilirsiniz.

Yukarıdaki yöntemlerden birini kullanarak seçim yaptıktan sonra uygulama konumuyla birlikte görünür:

5. Seçiminizi onaylamak için 'Uygula' düğmesine tıklayın.



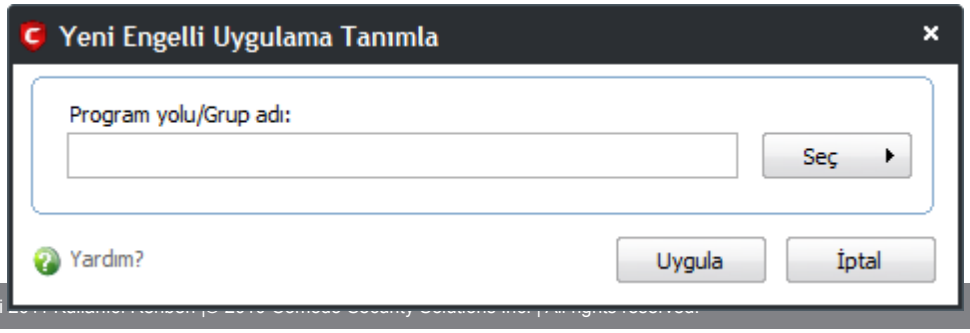
3.3 Yeni Engelli Uygulama Tanımla

Bu kısayol ile internete erişmesini istemediğiniz uygulamalar için 'Engelle' kuralı oluşturarak onları kolaylıkla engelleyebilirsiniz.

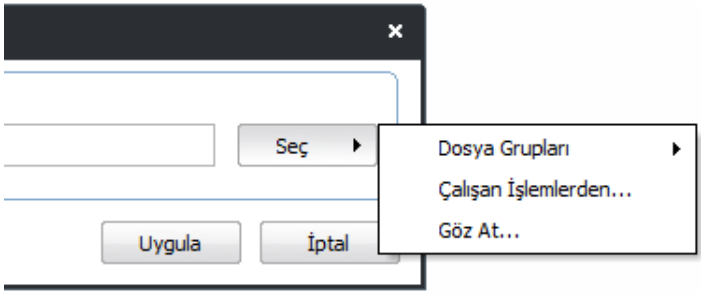
Tecrübeli kullanıcılar 'Ağ Güvenlik İlkeleri' bölümünü kullanarak kuralları değiştirebilir veya kaldırabilir.

Yeni engelli uygulama tanımlamak için

1. Güvenlik Duvarı görevleri bölümünde ' Yeni Engelli Uygulama Tanımla ' bağlantısına tıklayın.
2. Engellemek istediğiniz uygulamayı seçmenizi isteyen diyalog görünecektir.



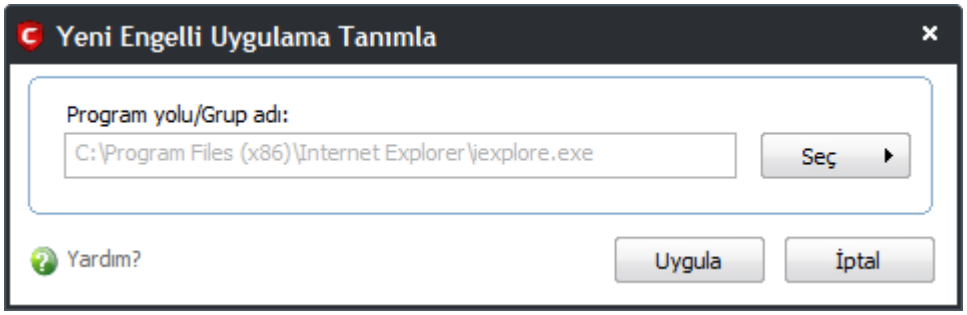
3. ‘Seç’ düğmesine tıklayın:



4. 3 yöntem ile güvenmek istediğiniz uygulamayı seçebilirsiniz - 'Dosya grupları'; 'Çalışan İşlemlerden' ve 'Göz At...'.

   - **Dosya Grupları** – Öntanımlı dosya gruplarından seçim yapabilirsiniz.
   - **Çalışan İşlemler** – Çalışan işlemler listesinden seçim yapabilirsiniz.
   - **Göz At... –** Uygula seç penceresinden istediğiniz uygulamayı bularak seçebilirsiniz.

1. Yukarıdaki yöntemlerden birini kullanarak seçim yaptıktan sonra uygulama konumuyla birlikte görünür:



2. Seçiminizi onaylamak için 'Uygula' düğmesine tıklayın.

3.4 Ağ Güvenlik İlkeleri

Ağ Güvenlik İlkeleri arayüzü tecrübeli kullanıcıların uygulamalar için veya genel olarak ilkeler oluşturmasına veya ilkeleri değiştirmesine izin verir.

Bir bağlantıya izin verilip verilmemesi için uygulama kurallarına ve genel kurallara bakılır.

- **Giden bağlantılar için, ilk olarak uygulama kurallarına bakılır.**
- **Gelen bağlantılar için, ilk olarak genel kurallara bakılır.**

Ağ Güvenlik İlkeleri arayüzünden ayrıca Ağ Bölgeleri ve Port Setleri de tanımlanabilir.

Arayüz altı ayrı ana bölüme ayrılmıştır - **Uygulama Kuralları**, **Genel Kurallar**, **Öntanımlı Güvenlik İlkeleri**, **Ağ Bölgeleri**, **Engellenmiş Ağ Bölgeler** ve **Port Setleri**.

Uygulama Kuralları sekmesi kullanıcıların uygulamaların ağ ve internet erişim kurallarını görüntülemesine,

yönetmesine ve tanımlamasına izin verir.

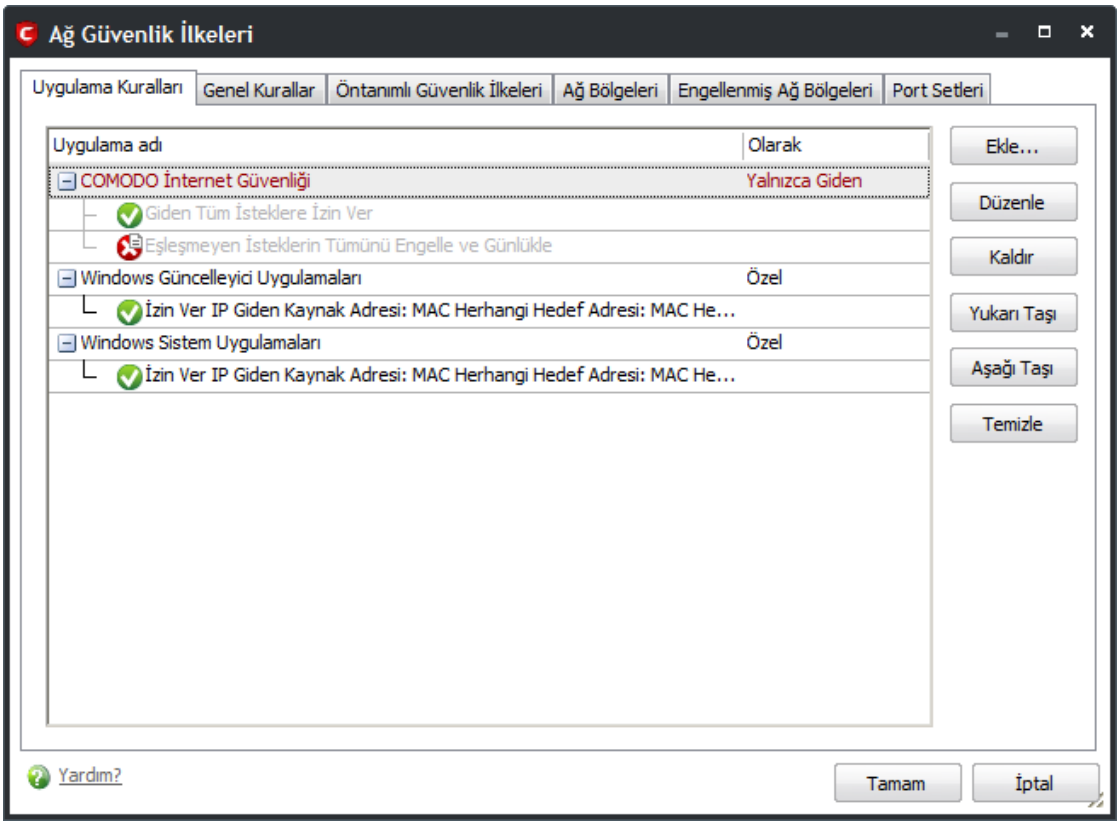
Genel Kurallar sekmesi kullanıcıların uygulamalardan bağımsız ağ ve internet erişim kurallarını görüntülemesine, yönetmesine ve tanımlamasına izin verir.

Öntanımlı Güvenlik İlkeleri sekmesi kullanıcıların önceden tanımlanmış güvenlik ilkelerini görüntülemesine ve daha sonra kullanım için yeni öntanımlı ilkeler oluşturmasına izin verir.

Ağ Bölgeleri sekmesi kullanıcıların erişim ayrıcalığı tanımlamak için ağ bölgeleri oluşturmasına izin verir.

Engellenmiş Ağ Bölgeleri sekmesi kullanıcıların erişimi engellemek için ağ bölgeleri eklemesine izin verir.

Port Setleri sekmesi kullanıcıların uygulamalarda veya genel kurallarda kullanmak üzere port setleri oluşturmasına izin verir.



- **Ayrıca bakınız Genel Gezinti.**
- **Ayrıca bakınız 'Uygulama Kuralları'.**
- **Ayrıca bakınız 'Genel Kurallar'.**
- **Ayrıca bakınız Öntanımlı Güvenlik İlkeleri.**
- **Ayrıca bakınız Ağ Bölgeleri.**
- **Ayrıca bakınız Engellenmiş Ağ Bölgeleri.**
- **Ayrıca bakınız Port Setleri.**

3.4.1 Genel Gezinti

- **Ekle... – Uygulama Kuralları sekmesindeyken Listeye yeni Uygulama eklemeye ve daha sonra onun için ilke oluşturmaya, Genel Kurallar sekmesindeyken ise Ağ Denetim Kuralları arayüzünü kullanarak genel kurallar oluşturmaya veya düzenlemenize izin verir.**
- **Düzenle... – Kullanıcının seçili kuralları veya uygulama ilkelerini değiştirmesine izin verir. Ayrıca bakınız İlkelerin ve Kuralların Tanıtımı, Ağ İlkelerinin Oluşturulması ve Düzenlenmesi ve Ağ Denetim Kurallarının Anlaşılması**
- **Kaldır... – Seçili ilkeyi veya kuralı siler**
- **Yukarı Taşı – Seçili öğeyi öncelik listesinde bir üst satıra taşır. Sürükle/Bırak yönetimini kullanarak da önceliklendirmede değişiklik yapabilirsiniz.**
- **Aşağı Taşı - Seçili öğeyi öncelik listesinde bir alt satıra taşır. Sürükle/Bırak yönetimini kullanarak da önceliklendirmede değişiklik yapabilirsiniz.**
- **Temizle – Listede bulunan öğelerin konumunu denetler ve belirtilen konumda bulunmayan öğelerle ilişkili kural ve ilkeleri listeden kaldırmak için kullanıcı onayı ister.**

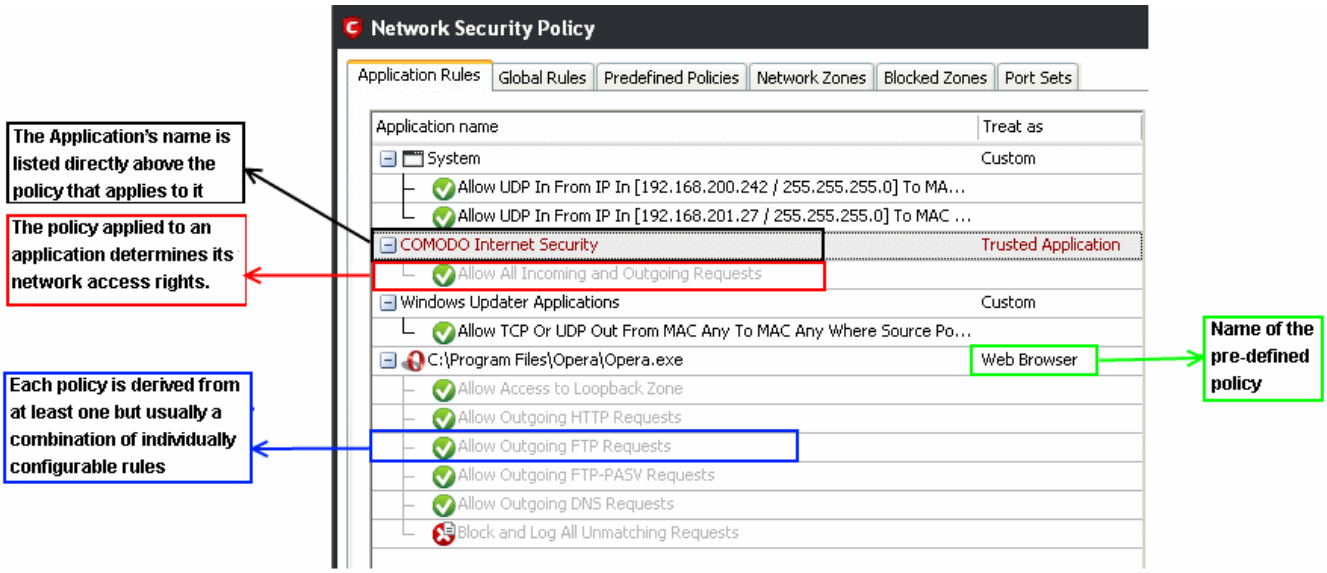
Sürükle/Bırak yönetimini kullanarak da önceliklendirmede değişiklik yapabilirsiniz.

3.4.2 Uygulama Kuralları

- **Ayrıca bakınız İlkelerin ve Kuralların Tanıtımı**
- **Ayrıca bakınız Uygulama Ağ Erişimi Denetimi arayüzü**
- **Ayrıca bakınız Ağ İlkelerinin Oluşturulması ve Değiştirilmesi**
- **Ayrıca bakınız Ağ Denetim Kurallarının Anlaşılması**
- **Ayrıca bakınız Ağ Denetim Kuralı Eklenmesi ve Düzenlenmesi**

İlkelerin ve Kuralların Tanıtımı

Ne zaman bir uygulama internet veya ağ erişimi için istekte bulunursa, Comodo Güvenlik Duvarı o uygulama için atanmış ilkelere göre isteğe izin verir veya engeller.



Bir uygulama için güvenlik duvarı ilkesini değiştirmek istiyorsanız:

- **'Ağ İlkesi Oluşturmak veya Değiştirmek' için uygulama adına çift tıklayın**
- **'Ağ İlkesi Oluşturmak veya Değiştirmek' için listeden uygulamayı seçin, sağ tıklayın ve 'Düzenle' seçin**
- **'Ağ İlkesi Oluşturmak veya Değiştirmek' için listeden uygulamayı seçin ve arayüzden 'Düzenle' düğmesine tıklayın**

İlke içindeki özel kuralları değiştirmek istiyorsanız:

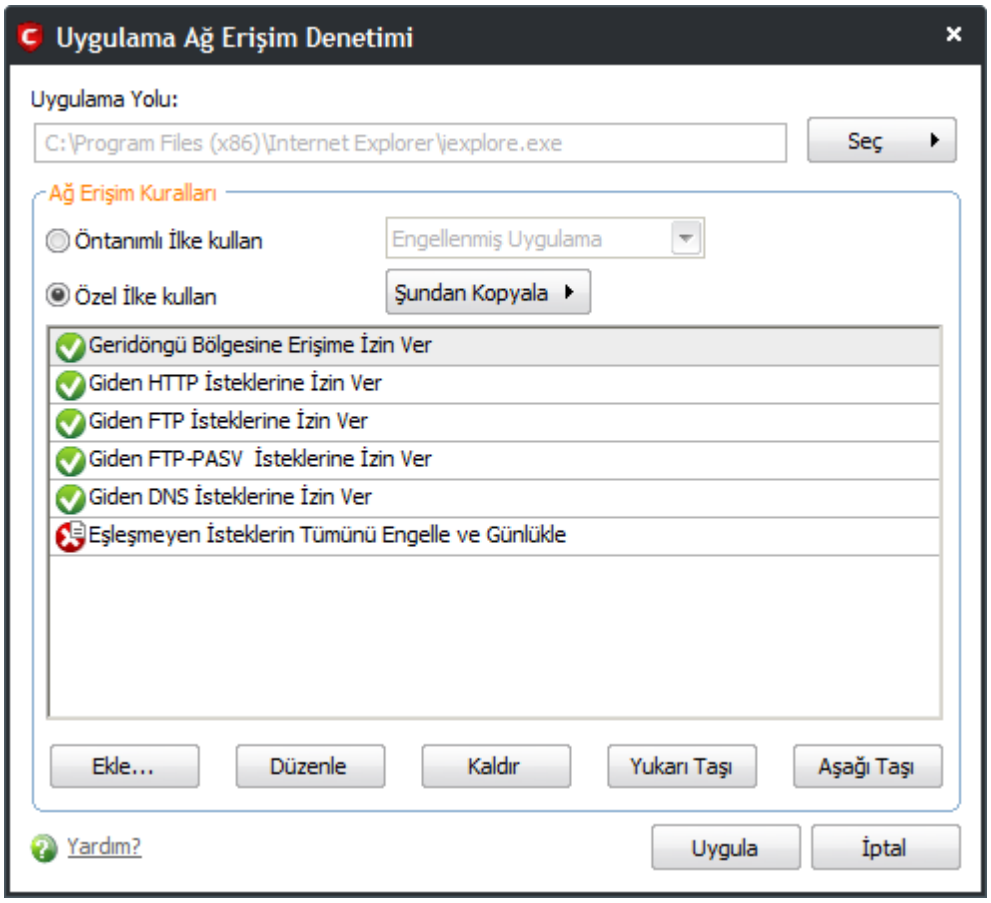
- **'Ağ İlkesi Oluşturmak ve Düzenlemek' için belli kurala çift tıklayın**
- **'Ağ İlkesi Oluşturmak ve Düzenlemek' için listeden kuralı seçin, sağ tıklayın ve 'Düzenle' seçin**
- **'Ağ İlkesi Oluşturmak ve Düzenlemek' için listeden uygulamayı seçin ve arayüzden 'Düzenle' düğmesine tıklayın**

Sürükle/Bırak yönetimini kullanarak da önceliklendirmede değişiklik yapabilirsiniz.

İlkeler sistemde bulunan her bir uygulama için ayrı ayrı oluşturabilir fakat bu işlem çok zaman alacaktır. Bu yüzden uygulamalar için genel kapsamlı öntanımlı ilkeler bulunmaktadır. Gereksinimlerinize göre bu ilkeleri uygulamalara atayabilir ve isteğinize göre Öntanımlı İlkeleri değiştirebilirsiniz.

Uygulama Ağ Erişimi Denetimi arayüzü

Bu arayüz kullanılarak kurallar ekleyebilir/düzenleyebilir/kaldırabilirsiniz. Ağ Denetim Kuralı Eklenmesi ve Düzenlenmesi kullanılarak oluşturulan kurallar bu listede görüntülenir.



Comodo Güvenlik Duvarı kuralları paket başına uygular ve süzülen paket türüne uyan ilk kuralı uygular. (Daha fazla bilgi için Ağ Denetim Kurallarının Anlaşılması bölümüne bakın). Pakete uyan birden fazla kural varsa listenin en üstündeki kural uygulanır.

Sürükle/Bırak yönetimini kullanarak da önceliklendirmede değişiklik yapabilirsiniz. Ağ ilkelerini oluşturmaya başlamak için ilk önce 'İlkelerin ve Kuralların Tanıtımı' bölümünü okuyun daha sonra 'Ağ Denetim İlkelerinin Oluşturulması ve Değiştirilmesi' bölümüne bakın.

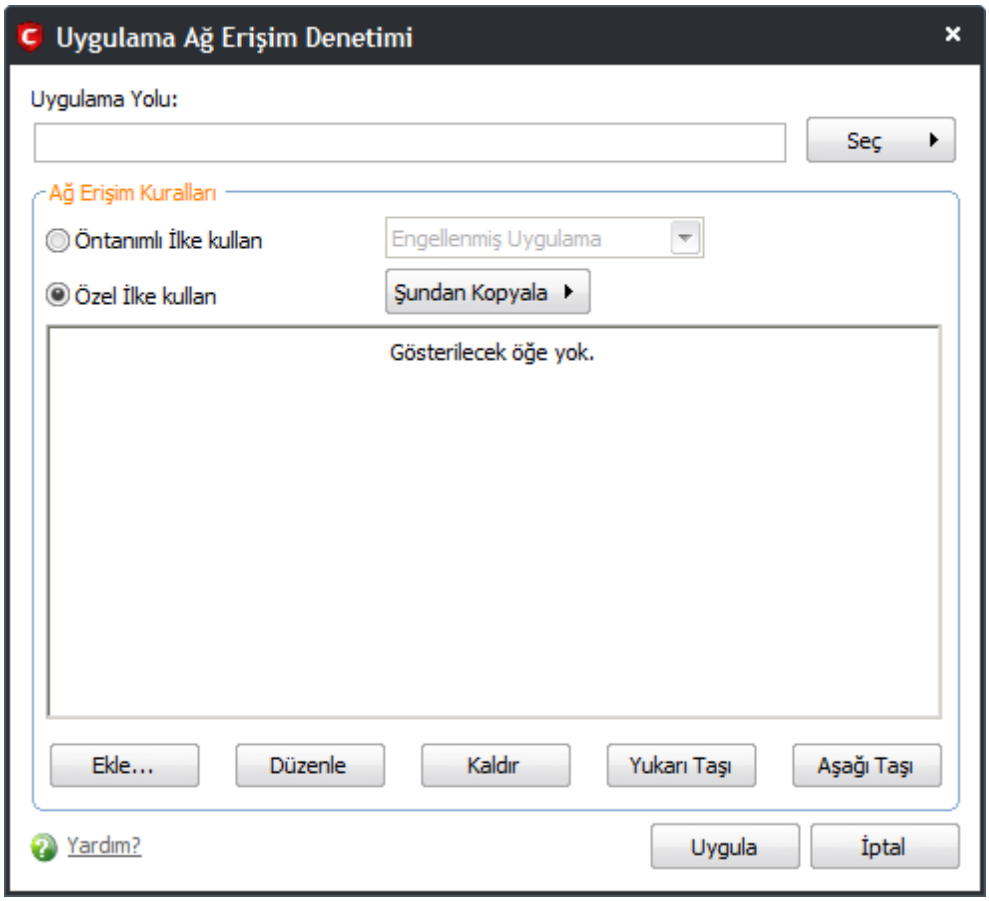
Ağ İlkelerinin Oluşturulması ve Değiştirilmesi

Uygulamanın ağ ilkesini tanımlamaya başlamak için iki temel adımı uygulamanız geremektedir.

1. İlkenin uygulanmasını istediğiniz uygulamayı seçin.
2. Bu uygulamanın ilkesindeki kuralları yapılandırın.

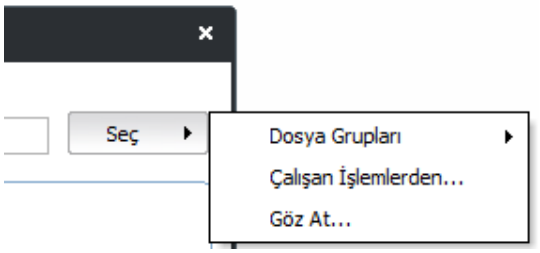
1. İlkenin uygulanmasını istediğiniz uygulamayı seçin

Yeni bir uygulamaya (ör. listede bulunmayan) ilke tanımlamak istiyorsanız 'Ekle…' düğmesin tıklayın. Aşağıdaki arayüz açılacaktır:



Bu yeni bir uygulama olduğu için 'Uygulama Yolu' alanı boştur.

'Seç' düğmesine tıklayın.

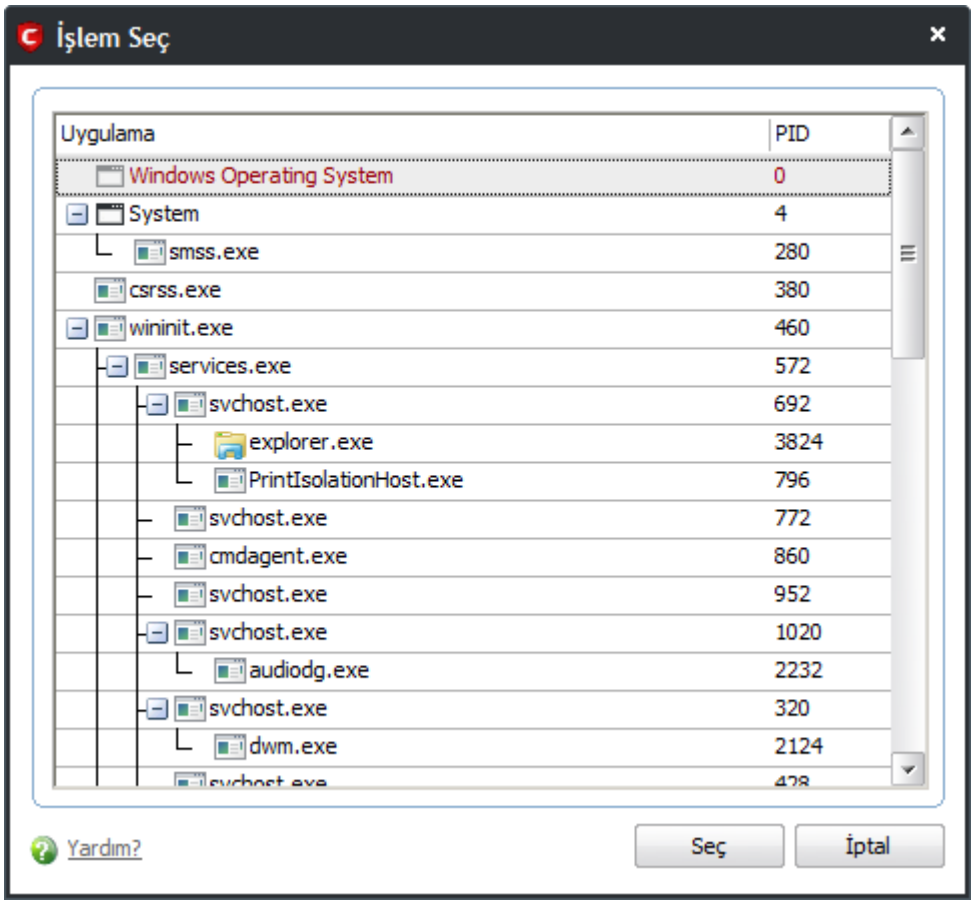


Şu 3 yöntemi kullanarak uygulama seçebilirsiniz - Dosya Grupları; Çalışan İşlemler ve Göz At...

i.**Dosya Grupları** – Öntanımlı dosya gruplarından seçim yapabilirsiniz

Dosyalar ve Dosya Gruplaması için Korunan Dosyalar ve Klasörler ve Engellenmiş Dosyalar bölümlerine bakın.

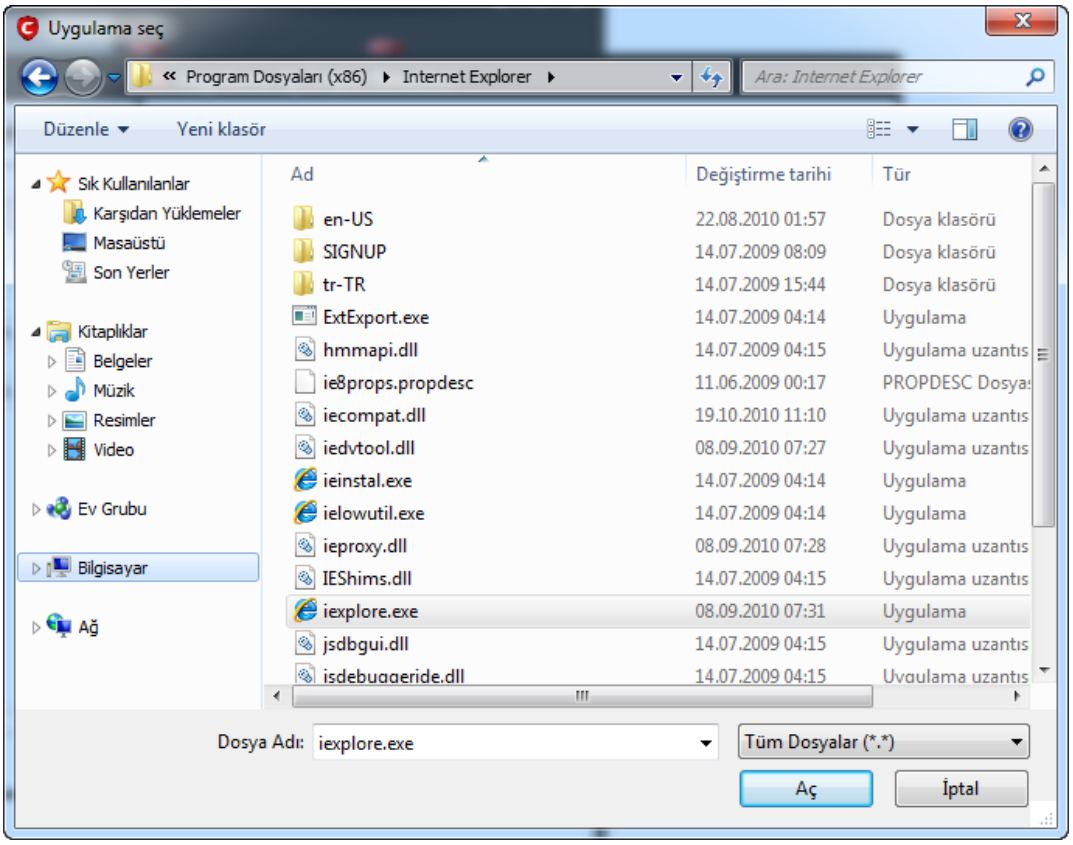
ii.**Çalışan İşlemler** – Çalışan işlemler listesinden seçim yapabilirsiniz.



Seçiminizi onaylamak için ‘Seç’ düğmesine tıklayın.

Not: Daha ayrıntılı ve güçlü bir araç olan Savunma+ Görevleri altında 'Etkin İşlemler Listesini Göster' bulunmaktadır.

iii.**Göz At... –** Uygula seç penceresinden istediğiniz uygulamayı bularak seçebilirsiniz. Aşağıdaki örnekte Opera web tarayıcısı gösterilmiştir.



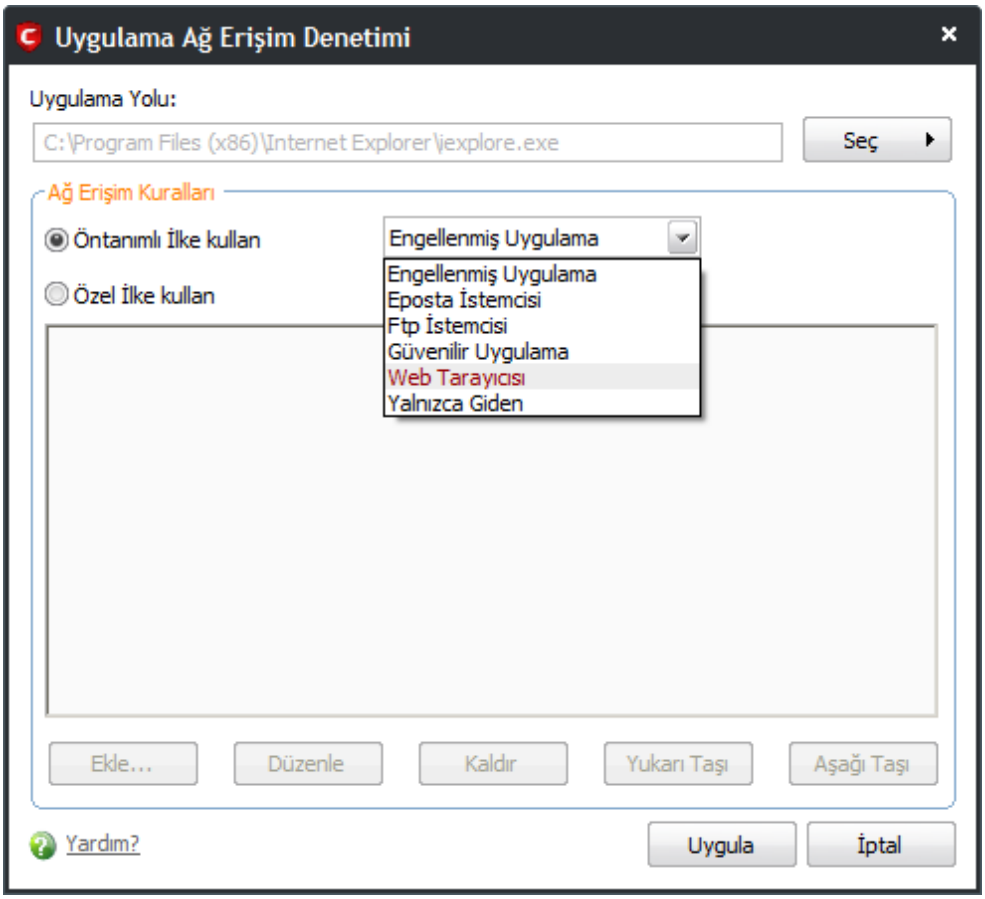
Seçimden sonraki adım uygulama kurallarının yapılandırılmasıdır.

(2) Uygulamanın ilkesindeki kuralların yapılandırılması

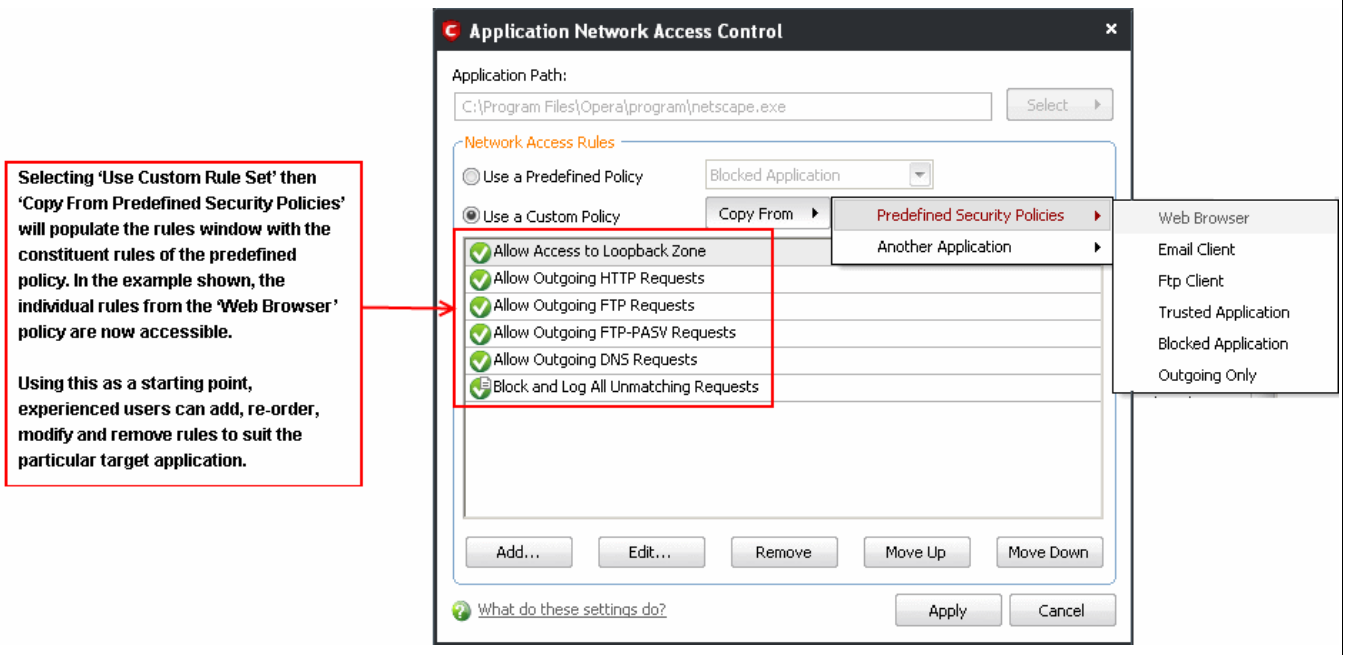
Bir uygulamaya ilke oluşturmak için iki genel seçeneğiniz vardır - Öntanımlı İlke Kullanmak veya Özel İlke Kullanmak.

•**Öntanımlı İlke Kullanmak –** Bu seçenek ile hızlıcana hedef uygulama için ilke oluşturabilirsiniz. Açılır listeden öntanımlı ilkeyi seçin. Seçtiğiniz öntanımlı ilke arayüzde **Olarak** sütununda görünür.

Not: Öntanımlı ilke **doğrudan** arayüz kullanılarak düzenlenemez, düzenlemek için Öntanımlı İlkeler arayüzünü kullanın. Daha esnek ilkeler oluşturmak istiyorsanız Özel İlke seçeneğini kullanın.



•**Özel İlke Kullanmak** – Deneyimli kullanıcılar için tasarlanmıştır, **Özel İlke** seçeneği ilkeler üzerinde tam denetim sağlar.



Tamamen yeni ilke oluşturabilir veya öntanımlı ilkeleri başlangıç noktası olarak kullanabilirsiniz:

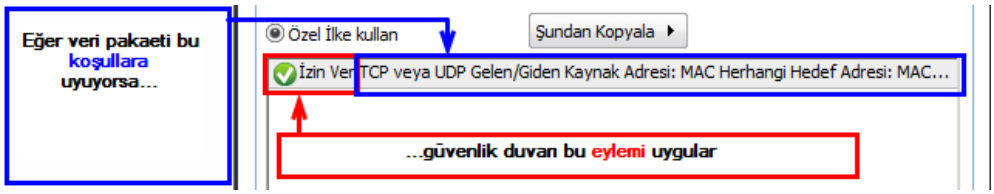
- **Ağ denetim kuralı eklemek için 'Ekle…' düğmesine tıklayın. Ayrıca bakınız 'Ağ Denetim Kuralı Eklenmesi ve Düzenlenmesi'.**
- **'Şuradan Kopyala' düğmesini kullanarak Öntanımlı Güvenlik Duvarı İlkesinin kurallarını kopyalayabilirsiniz**
- **'Şuradan Kopyala' düğmesini kullanarak başka bir uygulamanın ilkesini diğer bir uygulamaya kopyalayabilirsiniz.**

Genel İpuçları:

- **Birden fazla uygulamaya aynı kuralları atamak yerine Öntanımlı Güvenlik Duvarı İlkesi oluşturarak tüm uygulamalara atayabilirsiniz. (veya bulunan bir ilkeyi gereksinimlerinize göredüzenleyin).**
- **Bir veya iki uygulama için 'Özel İlke Kullan' seçeneği ile ayrı ayrı ilkeler oluşturabilirsiniz.**

Ağ Denetim Kurallarının Anlaşılması

Comodo Güvenlik Duvarı gelen ve giden her bir paketi **koşullara** (özniteliklerini) göre inceler, daha sonra koşullara uyan paketleri eylem durumuna göre izin verir veya engeller. Bağlantıya uyan bir ağ denetim kuralı bulunmuyorsa otomatik olarak bu bağlantı engellenir.



Ağ Denetim Kuralı Eklenmesi ve Düzenlenmesi bölümünde görünen* **Koşullar** (öznitelikler) seçilen protokole göre değişiklik gösterebilir.

'TCP' , 'UDP' veya 'TCP ve 'UDP' seçtiyseniz: Eylem | Protokol | Yön | Kaynak Adresi | Hedef Adresi | Kaynak Portu | Hedef Portu

'ICMP' seçtiyseniz: Eylem | Protokol | Yön | Kaynak Adresi | Hedef Adresi | ICMP Ayrıntıları

'IP' seçtiyseniz: Eylem | Protokol | Yön | Kaynak Adresi | Hedef Adresi | IP Ayrıntıları

Eylem: Güvenlik duvarının kural koşulları sağlandığı zaman gerçekleştirdiği eylem. Kural '**İzin Ver**', '**Engelle**' veya '**Sor**' olarak görünür.**

Protokol: Bağlantıda kullanılan protokol belirtir. Kural '**TCP**', '**UDP**', '**TCP veya UDP**', '**ICMP**' veya '**IP**' olarak görünür.

Yön: Bağlantının yönünü belirtir. Kural **'Gelen', 'Giden' veya 'Gelen/Giden'** olarak görünür.

Kaynak Adresi: Bağlantının çıktığı kaynak adresini belirtir. Kural '**Kaynak Adresi**' sonrasında: **IP , IP aralığında , IP Maskesi, Ağ Bölgesi, Sunucu Adı** veya **Mac Adresi** olarak görünür.

Hedef Adresi: Bağlantının girdiği hedef adresini belirtir. Kural '**Hedef Adresi**' sonrasında: **IP , IP aralığında ,**

IP Maskesi, Ağ Bölgesi, Sunucu Adı veya **Mac Adresi** olarak görünür.

Kaynak Port: Bağlantının çıktığı kaynak portu belirtir. Kural '**Kaynak Port**' sonrasında: '**Herhangi**', '**Port #**', '**Port aralığı**' veya '**Port Seti**' olarak görünür.

Hedef Port: Bağlantının girdiği hedef portu belirtir. Kural '**Hedef Port**' sonrasında: '**Herhangi**', '**Port #**', '**Port aralığı**' veya '**Port Seti**' olarak görünür.

ICMP Ayrıntıları: ICMP mesaj türünü ve kodunu belirtir. Ayrıca bakınız Ağ Denetim Kuralı Eklenmesi ve Düzenlenmesi.

IP Ayrıntıları: IP protokolünü belirtir. Ayrıca bakınız Ağ Denetim Kuralı Eklenmesi ve Düzenlenmesi.

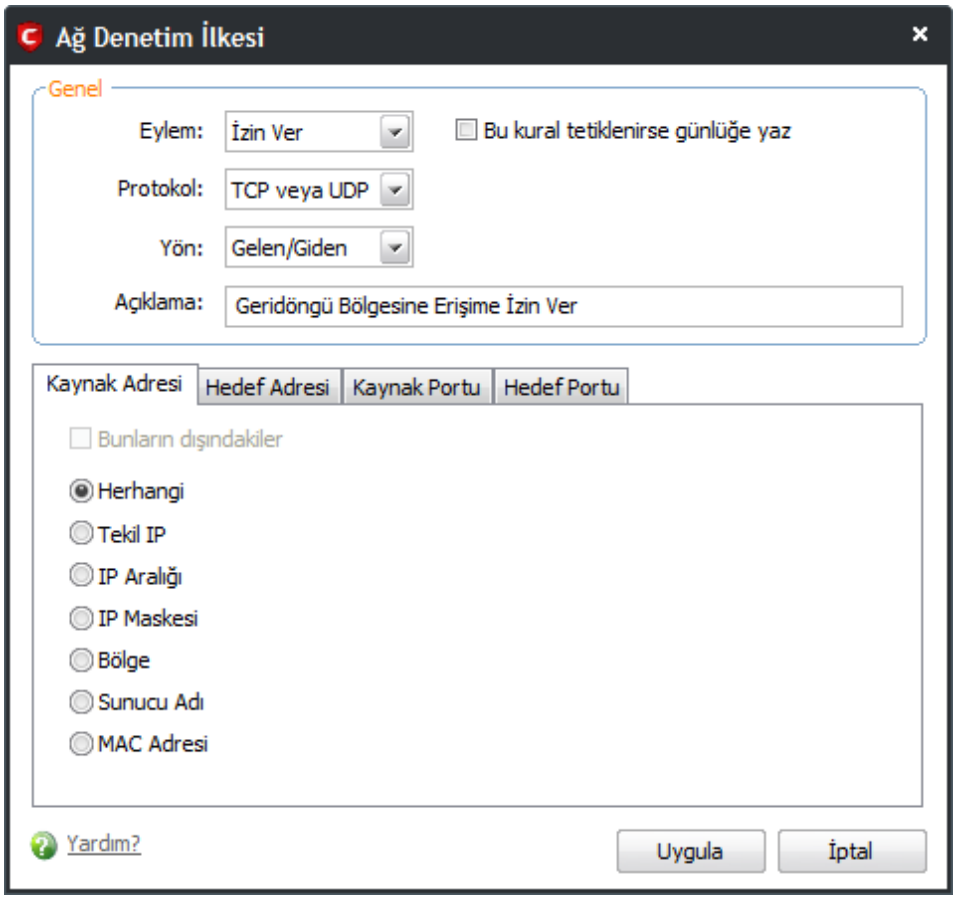
Kural bir kere uygulandıktan sonra seçili uygulamanın tüm trafiği izlemeye alınır ve koşullara göre eylem gerçekleştirilir. Uygulama Kuralları ve Genel Kurallar arasındaki etkileşimi anlayabilmek için 'Genel Kurallar' bölümüne bakınız.

* *Kural oluştururken özel bir açıklama girildiği zaman tam parametre yerine bu özel açıklama görünecektir. Ayrıca bakınız 'Ağ Denetim Kuralı Eklenmesi ve Düzenlenmesi'.*

** *'Bu kural tetiklenirse günlüğe yaz' seçilirse eylem ile birlikte sonek olarak "ve Günlükle" de görüntülenecektir. (örn. Engelle ve Günlükle)*

Ağ Denetim Kuralı Eklenmesi ve Düzenlenmesi

Ağ Denetim Kuralları arayüzü kural eylemlerini ve koşullarını yapılandırmak için kullanılabilir. Deneyimli bir kullanıcı değilseniz veya bu bölümdeki ayarlar hakkında bilginiz yoksa öncelikle şu bölümlere göz atmanızı öneririz: 'Ağ Denetim Kurallarının Anlaşılması', 'Kuralların ve İlkelerin Tanıtımı' ve 'Ağ İlkelerinin Oluşturulması ve Değiştirilmesi'.



Genel Ayarlar

Eylem: Güvenlik duvarının kural koşulları sağlandığı zaman gerçekleştirdiği eylem. Bulunan seçenekler '**İzin Ver**', '**Engelle**' veya '**Sor**'.

Protokol: Bağlantıda kullanılan protokol belirtir. Bulunan seçenekler '**TCP**', '**UDP**', '**TCP veya UDP**', '**ICMP**' veya '**IP**'.

Not: Bu bölümdeki seçiminize göre arayüzün alt yarısındaki sekmeler değişiklik gösterecektir.

Yön: Bağlantının yönünü belirtir. Bulunan seçenekler **'Gelen', 'Giden' veya 'Gelen/Giden'**.

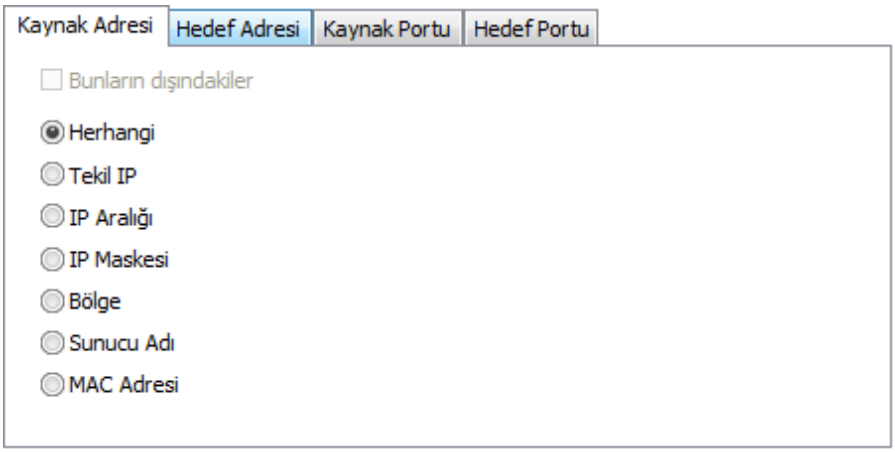
Bu kural tetiklenirse günlüğe yaz: Bu seçenek işaretliyse kurala uyan bir koşul gerçekleştiği zaman bu olay günlükte ilgili bölüme yazılacaktır. Güvenlik Duvarı Olay Görüntüleyicisi

Açıklama: Kurallar için kullanıcı dostu açıklamalar girmenize izin verir. ('Giden HTTP isteklerine İzin Ver'). Girilen açıklama Uygulama Kuralları ve Uygulama Ağ Erişimi Denetimi arayüzünde tam eylem/koşul açıklaması yerine görüntülenir.

Protokol

i. TCP', 'UPD' veya 'TCP veya UDP'

Protokol olarak 'TCP', 'UPD' veya 'TCP veya UDP' seçnerseniz IP adresi ve port tanımlamalısınız.



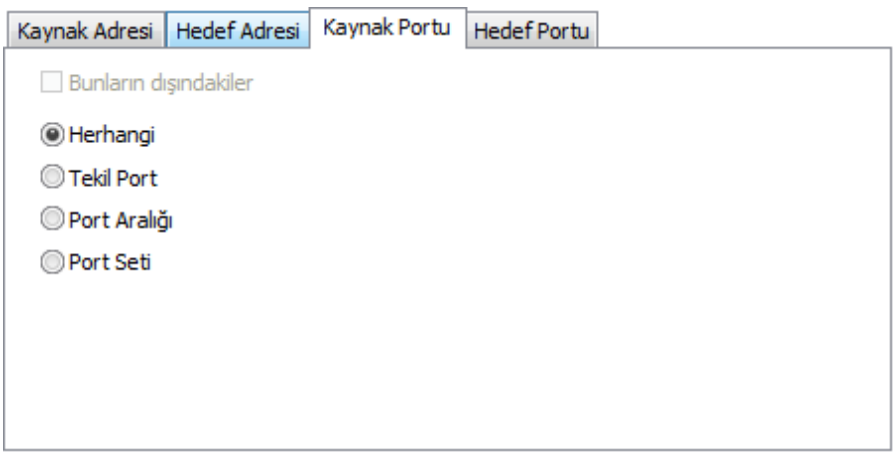
Kaynak Adresi ve Hedef Adresi:

1. Herhangi seçeneğini işaretleyerek her bir IP adresini seçebilirsiniz. Bu seçenek 0.0.0.0- 255.255.255.255 aralığındaki tüm bağlantılara izin verir.
2. Tekil IP işaretleyerek tek bir IP adresi girebilirsiniz. Örn. 192.168.200.113.
3. IP Aralığı seçeneğini işaretleyerek IP aralığı belirleyebilirsiniz. Örneğin özel ağınızın IP aralığını başlangıç ve bitiş kutularına girerek.
4. IP Maskesi seçeneğini işaretleyerek IP maskesi girebilirsiniz. IP ağları alt ağ diye adlandırılan küçük ağlara ayrılabilir.
5. Bölge seçeneğini işaretleyerek ağ bölgesi seçebilirsiniz. Ayrıca bakınız 'Ağ Bölgeleri'.
6. Sunucu Adı seçeneğini işaretleyerek IP'yi gösteren bir sunucu adı girebilirsiniz.
7. MAC Adresi seçeneğini işaretleyerek MAC Adresi girebilirsiniz.

    - Bunların dışındakiler: Seçimin dışında kalanları kapsar.

Kaynak Port ve Hedef Port:

Metin kutusuna kaynak ve hedef portları girin.



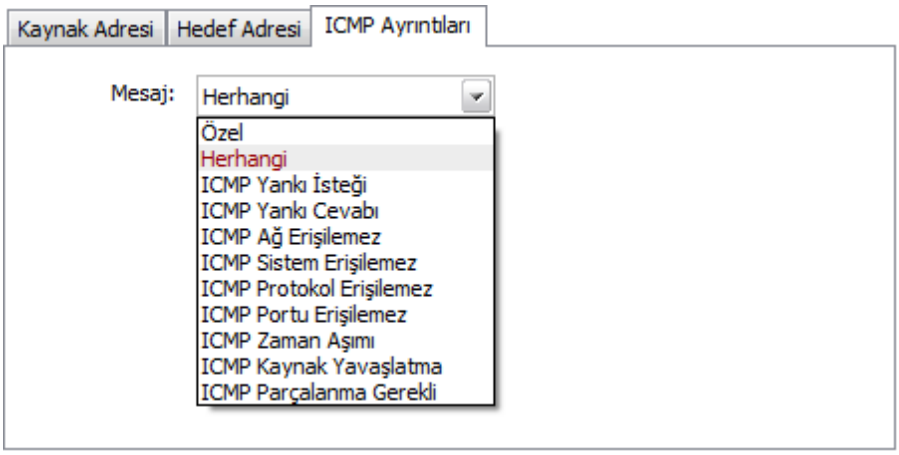
1. Herhangi seçeneğini işaretleyerek her bir portu seçebilirsiniz. 0-65535.
2. Tekil Port seçeneğini işaretleyerek tek bir port seçebilirsiniz.
3. Port Aralığı seçeneğini işaretleyerek port aralığı seçebilirsiniz.
4. Port Setleri seçeneğini işaretleyerek port setlerinden birini seçebilirsiniz. Ayrıca bakınız 'Port Setleri'.

i. **ICMP**

Genel Ayarlar bölümünden protokol olarak ICMP seçtiğiniz zaman 'ICMP Ayrıntıları' sekmesiyle birlikte Hedef Adresi sekmesi görünür. Son iki sekme yukarıda anlatıldığı gibi ayarlanır. Kaynak ve hedef port sekmeleri görünmez.

ii. **ICMP Ayrıntıları**

ICMP (Internet Control Message Protocol/ İnternet Denetim İleti Kuralı) paketleri ağ durumlarıyla ilgili bilgileri içerir. Genellikle ping ve izleme amacıyla kullanılır.



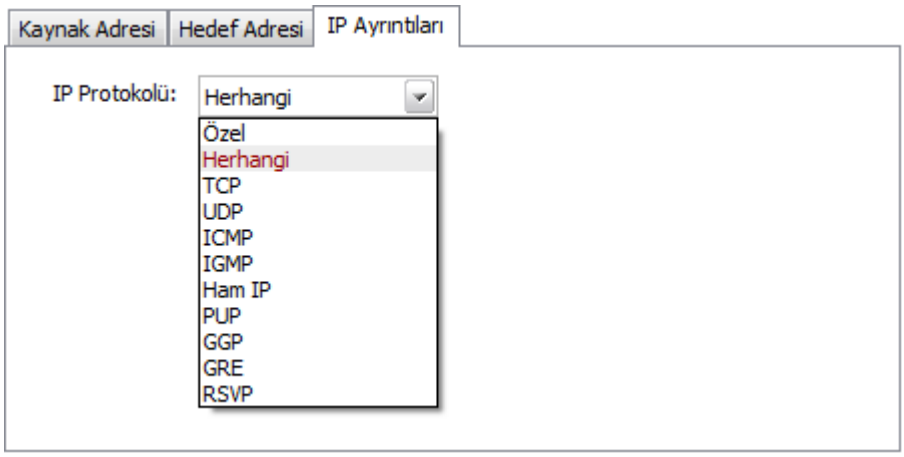
1. Kaynak/ hedef IP adresini girin.
2. ICMP Mesajını belirleyin, Tür ve Kod olarak.
   Menüden belli ICMP mesajlarını seçtiğinizde onların tür ve kodları ayarlanır. 'Özel' seçerek türü ve kodu kendiniz girebilirsiniz.

IP

Genel Ayarlar bölümünden IP seçtiğinizde 'IP Ayrıntıları' sekmesiyle birlikte Kaynak Adresi ve Hedef Adresi sekmeleri görünür. Son iki sekme yukarıda anlatıldığı gibi ayarlanır. Kaynak ve hedef port sekmeleri görünmez.

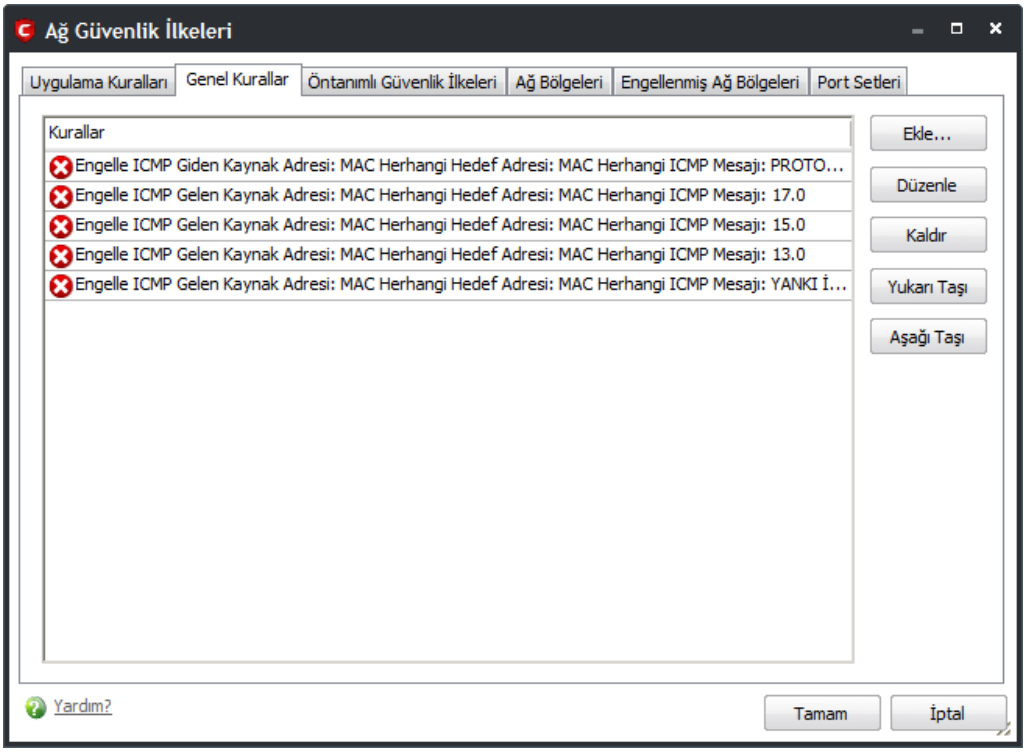
i. **IP Ayrıntıları**

IP protokolünün türünü listeden seçin.



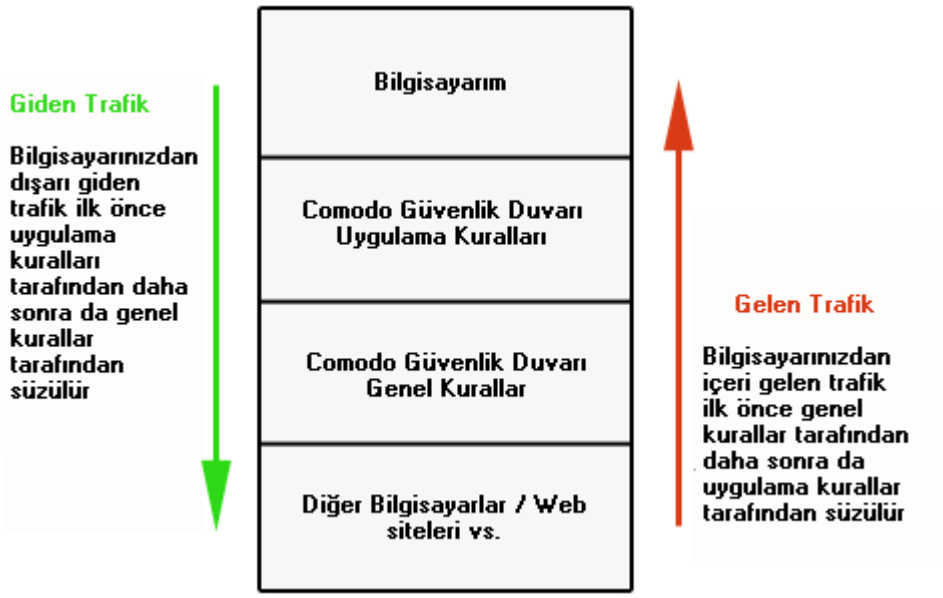
3.4.3 Genel Kurallar

Uygulama kurallarının aksine Genel Kurallar tüm bağlantılara uygulanır.



Comodo Güvenlik Duvarı her bir paketi Uygulama ve Genel kurallara göre inceler.

- Giden bağlantılar için ilk önce uygulama kurallarına daha sonra genel kurallara bakılır.
- Gelen bağlantılar için ilk önce genel kurallara daha sonra uygulama kurallarına bakılır.



Bu nedenle giden trafik sistemden çıkabilmek için her iki kuralı da 'geçemelidir'. Aynı durum gelen bağlantılarda da geçerlidir.

Genel Kurallar daha çok TCP ve UDP dışındaki protokolleri süzmek içindir.

Genel Kurallar uygulama kuralları gibi yapılandırılabilir. Genel kural eklemek için 'Ekle…', düzenlemek için 'Düzenle…' düğmesine tıklayın.

Ayrıca bakınız Uygulama Ağ Erişimi Denetim arayüzü.

Ayrıca bakınız Ağ Denetim Kurallarının Anlaşılması.

Ayrıca bakınız Ağ Denetim Kuralı Eklenmesi ve Düzenlenmesi.

3.4.4 Öntanımlı İlkeler

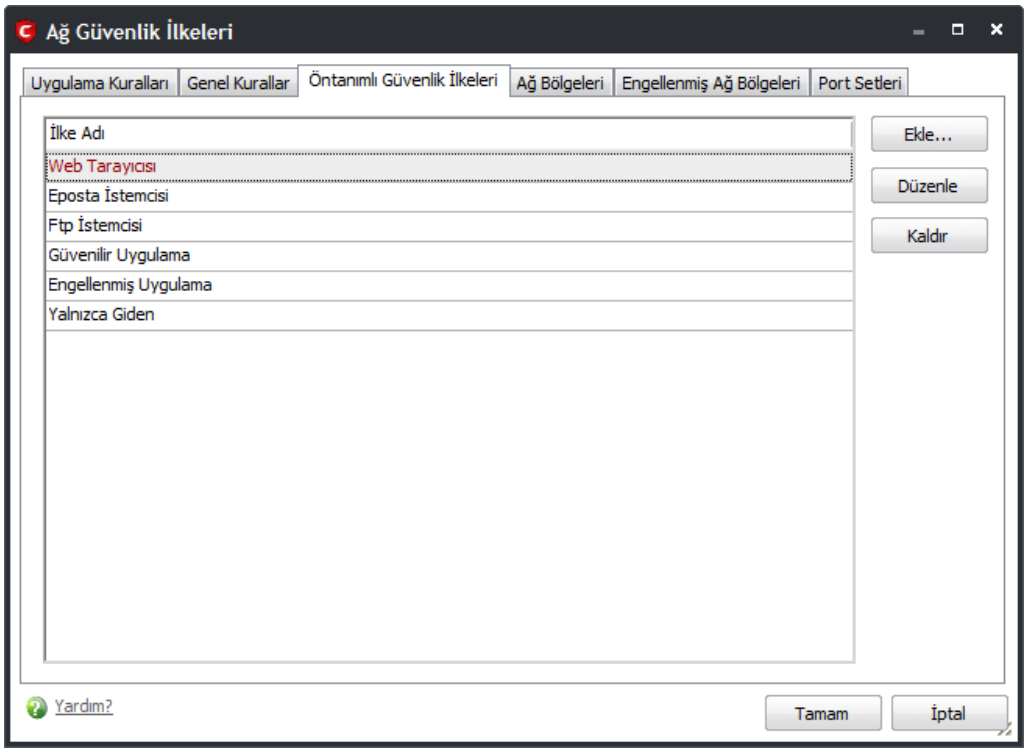
Yeniden kullanılabilir öntanımlı güvenlik ilkeleri oluşturabilirsiniz.

Not: Bu bölüm deneyimli kullanıcılar içindir. Ayrıntılı bilgi için Ağ Güvenlik İlkeleri bölümüne bakın.

İlkeler sistemde bulunan her bir uygulama için ayrı ayrı oluşturabilir fakat bu işlem çok zaman alacaktır. Bu yüzden uygulamalar için genel kapsamlı öntanımlı ilkeler bulunmaktadır Gereksinimlerinize göre bu ilkeleri uygulamalara atayabilir ve isteğinize göre bunları değiştirebilirsiniz.

Öntanımlı İlkeler arayüzüne erişmek için

1. Güvenlik Duvarı Görevleri > Ağ Güvenlik İlkeleri arayüzünden ‘Öntanımlı İlkeler' sekmesine gidin.



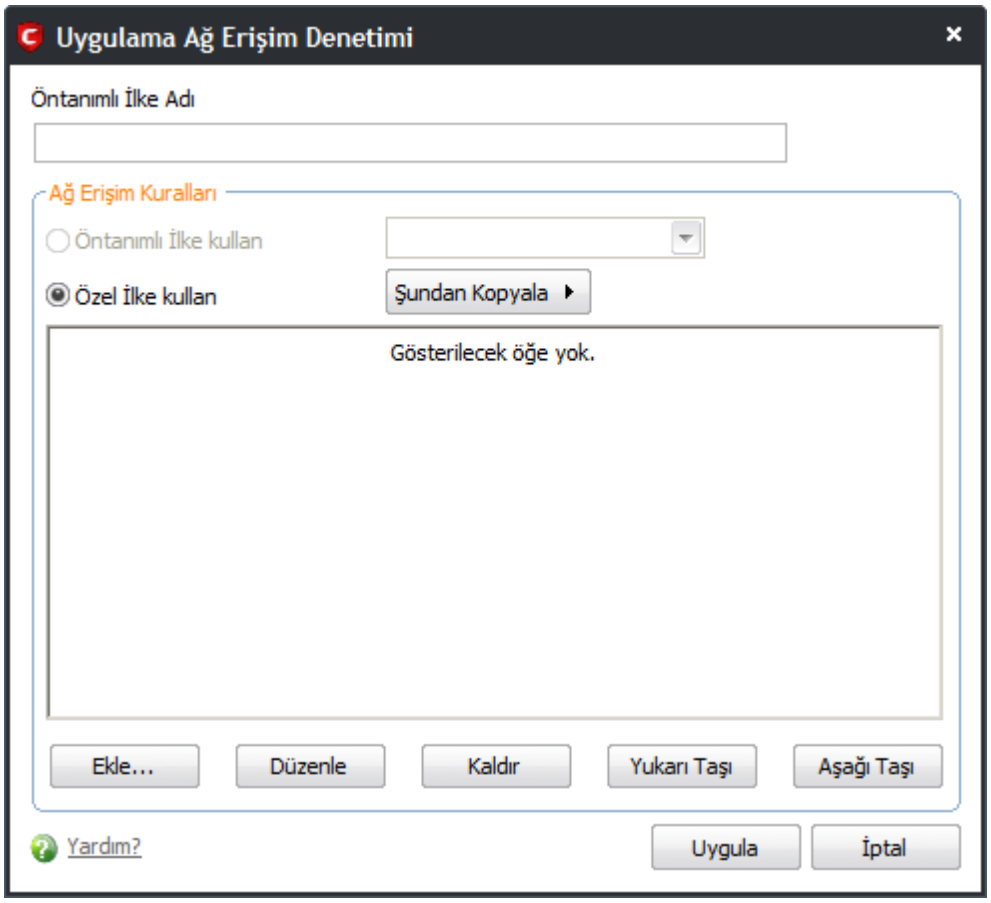
Bulunan öntanımlı ilkeyi görüntülemek veya düzenlemek için

- Listeden ilke adına çift tıklayın
- Listeden ilke adını seçin, sağ tıklayın ve ‘Düzenle’ seçin
- Listeden ilke adını seçin ve sağdan ‘Düzenle’ düğmesine tıklayın

Bu noktadan sonraki ayrıntılı işlemlere buradan Bakabilirsiniz.

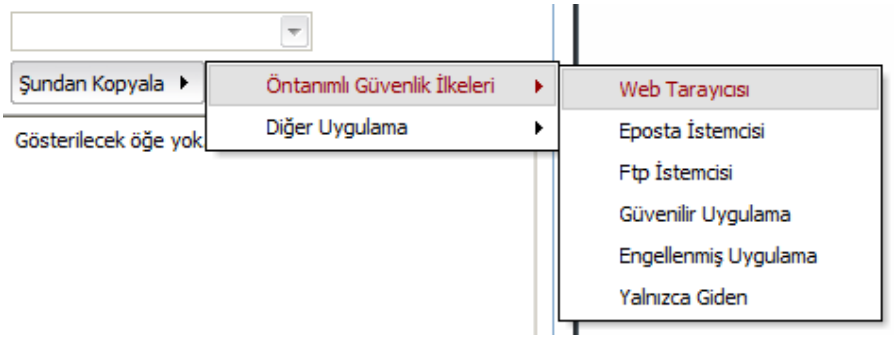
Yeni bir öntanımlı ilke eklemek için

•‘Ekle…’ düğmesine tıklayın. Bu aşağıda görünen ekranı açacaktır.



•Bu yeni bir öntanımlı ilke olduğu için ad girmeniz gerekecektir. Daha sonra bu ilke için özel kurallar ekleyip yapılandırmalısınız. Ayrıca bakınız 'Ağ Denetim Kuralı Eklenmesi ve Düzenlenmesi'.

Oluşturduktan sonra bu ilke 'Öntanımlı İlkeler' menüsünden seçilebilir.



3.4.5 Ağ Bölgeleri

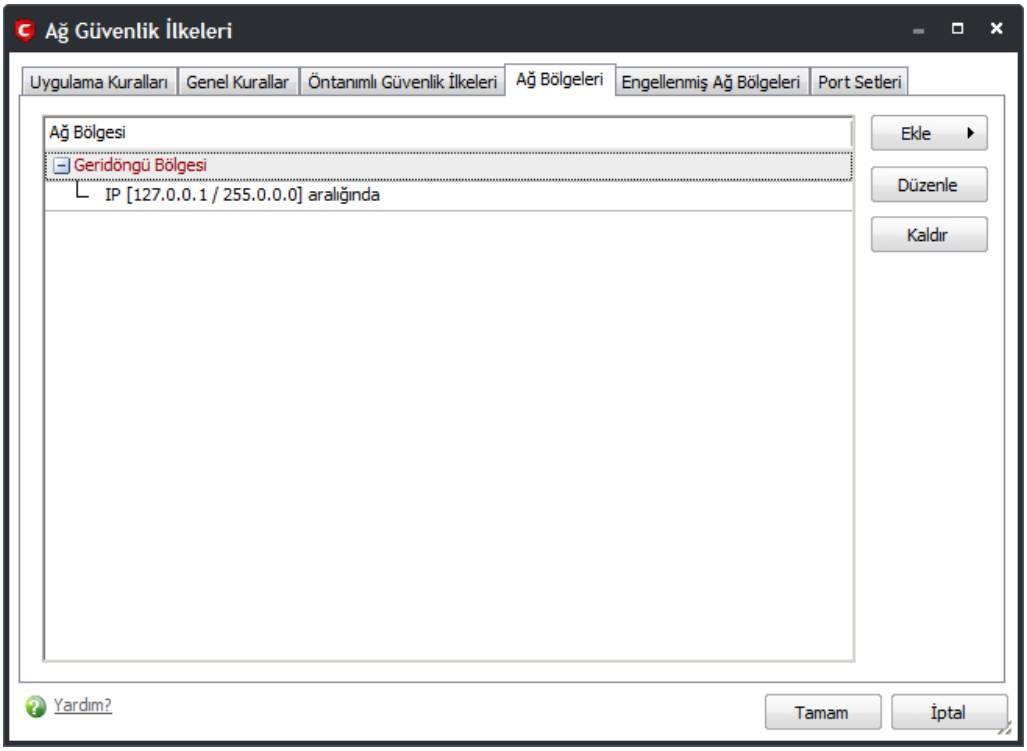
Comodo Güvenlik Duvarı 'Ağ Bölgeleri' oluşturarak bunlara özel erişim ayrıcalıkları belirlemenize izin verir. Bir 'Ağ Bölgesi' yalnız bir makinadan veya binlerce makinayı içeren bir ağdan oluşabilir.

Not: Kablolu veya kablosuz olarak birbirine bağlı bilgisayarlardan oluşan ağ bir bilgisayar ağıdır. Ağ içinde

kullanıcıların aygıtları ve bilgilerini diğer ağ içindeki kullancılar ile paylaşmasını sağlar. Ağda erişime izin vermeniz, erişimini kısıtlamanız veya engellemeniz gereken bilgisayarlar da bulunabilir.

Ağ Bölgelerine erişmek için

•Güvenlik Duvarı Görevleri > Ağ Güvenlik İlkeleri arayüzünden 'Ağ Bölgeleri' sekmesine gidin.



Not 1: Bu bölüme bölge eklenmesi o bölgeye erişim ayrıcalıkları tanımlamaz. Bu bölüme eklenen bölgeler daha sonra güvenlik duvarının diğer alanlarında kullanılarak bu bölgelere erişim ayrıcalığı tanımlanabilir.

Not 2: 'Port Gizleme Sihirbazı' arayüzü kullanılarak bir ağ bölgesi 'Güvenilir' olarak tanımlanabilir. (Örneğin bir ev bilgisayarı veya ağı)

Not 3: 'Engellenmiş Bölgeler' arayüzü kullanılarak bir ağ bölgesi 'Engellenmiş' olarak tanımlanabilir. (Örneğin bilinen bir casus yazılım sitesi)

Not 4: Bir uygulama, Uygulama Kuralı tanımlanırken bir ağ bölgesine erişim ayrıcalığı atanabilir. Benzer olarak, özel bir Genel Kural bir ağ bölgesine atanabilir.

Not 5: Varsayılan olarak Comodo Güvenlik Duvarı yeni ağları otomatik olarak saptar (Yerel Ağ, Kablosuz vb. gibi). Bu seçenek Daha > Tercihler bölümünden değiştirilebilir.

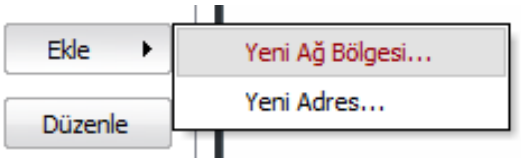
Bir Ağ Bölgesi eklemek için

1. Bölge için bir ad girin.

2. Bu bölgeye dahil edilecek adresleri seçin.

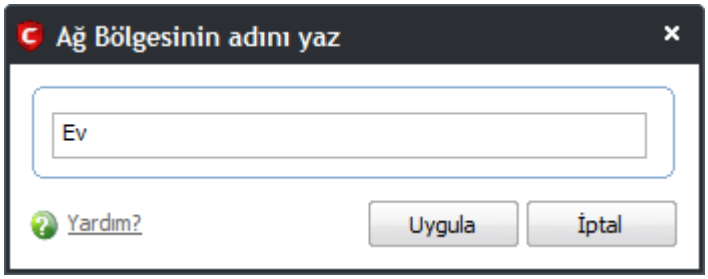
Bölgeye ad tanımlanması

1. ‘Ekle…’ düğmesine tıklayın ve ‘Yeni Ağ Bölgesi…’ seçin.



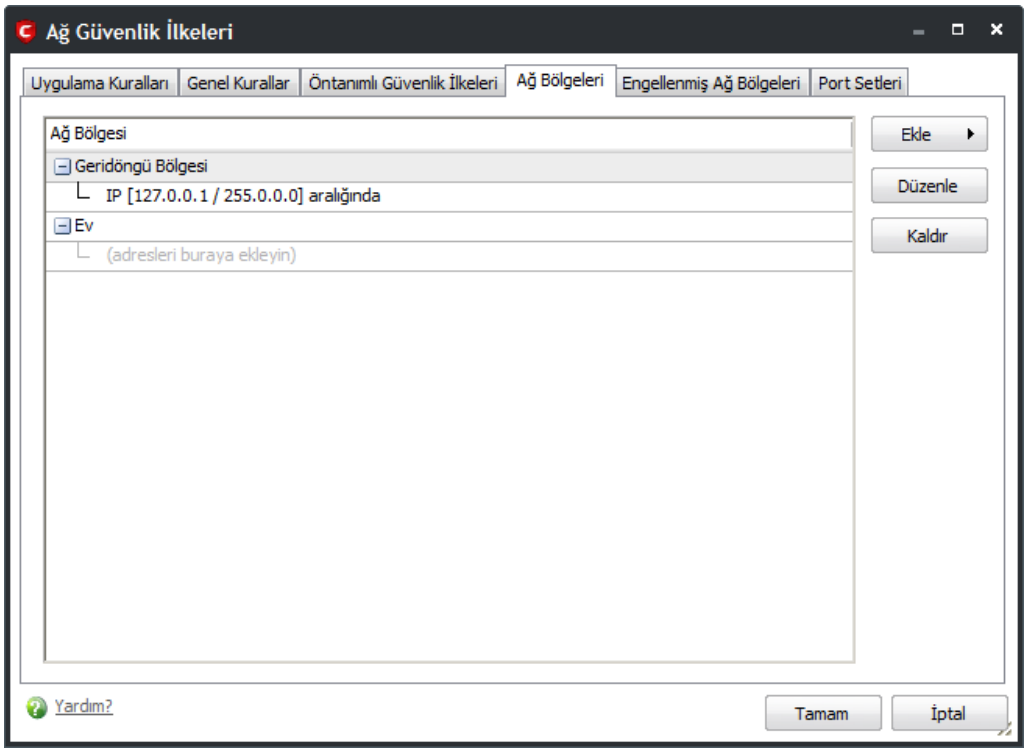
Ağ bölgesi için ad girilmesini soran bir diyalog görünecektir..

2. Oluşturduğunuz ağı açıklayan bir ad seçin.



3. Adı onaylamak için ‘Uygula’ düğmesine tıklayın.

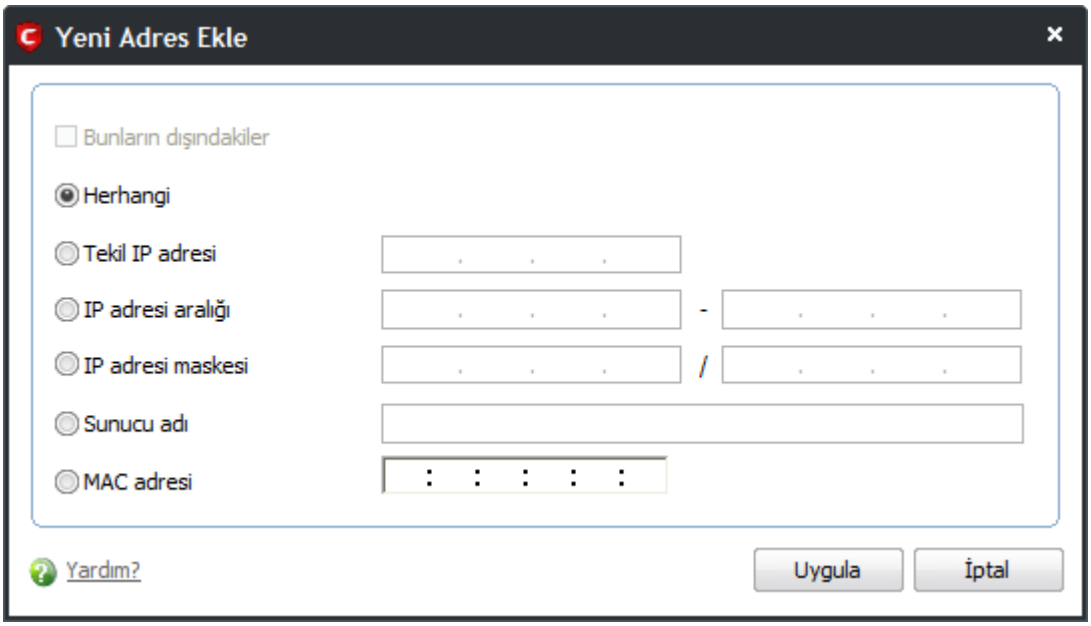
Bu, ağ bölgesini listeye ekler.



Bu bölgeye dahil edilecek adresleri seçmek için

1. Ağ adını seçin, sağ tıklayın ve menüden ‘Ekle…’ seçin.

Açılan diyalogdan seçiminizi yapın ve ona göre doldurun.

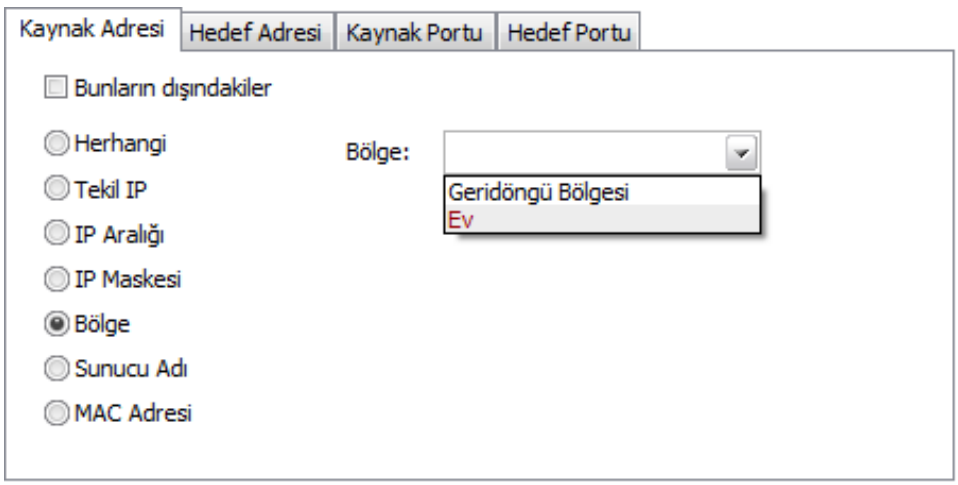


2. Seçiminizi onaylamak için ‘Uygula’ düğmesine tıklayın.
3. ‘Ağ Bölgeleri’ arayüzünden ‘Tamam’ düğmesine tıklayın.

Yeni bölge atadığınız adresle birlikte listede yer alacaktır.

Ağ bölgesi oluşturulduğunda:

- Ağ ilkesi oluşturulurken veya değiştirilirken ‘Bölge’ menüsünden hızlıcana seçilebilir



- 'Ağ Bölgeleri' arayüzünden hızlıcana seçilebilir ve güvenilir bölge olarak atanabilir
- 'Engellenmiş Bölgeler' arayüzünden hızlıcana seçilebilir ve engellenmiş bölge olarak atanabilir

Bulunan Ağ Bölgelerinin adını düzenlemek için

1. Listeden ağ adını seçin (örn. Ev Ağı).
2. 'Düzenle…' seçerek adlandırma diyaloğunu açın.

Bulunan Ağ Bölgesine daha fazla adres eklemek için

- Ağ adına sağ tıklayın ve 'Ekle…' tıklayın veya,
- Ağ adını seçip sağdan 'Ekle…' düğmesine tıklayın ve 'Yeni Adres Ekle…' seçin.

Bölgede bulunan adresi değiştirmek için

- Adrese sağ tıklayın (bölge adına değil) 'Düzenle…' seçin veya
- Adresi seçin (bölge adını değil) ve sağdan 'Düzenle…' düğmesine tıklayın.

3.4.6 Engellenmiş Ağ Bölgeleri

Ağ içinde kullanıcıların aygıtları ve bilgilerini diğer ağ içindeki kullancılar ile paylaşmasını sağlar. Ağda erişime izin vermeniz, erişimini kısıtlamanız veya engellemeniz gereken bilgisayarlar da bulunabilir.

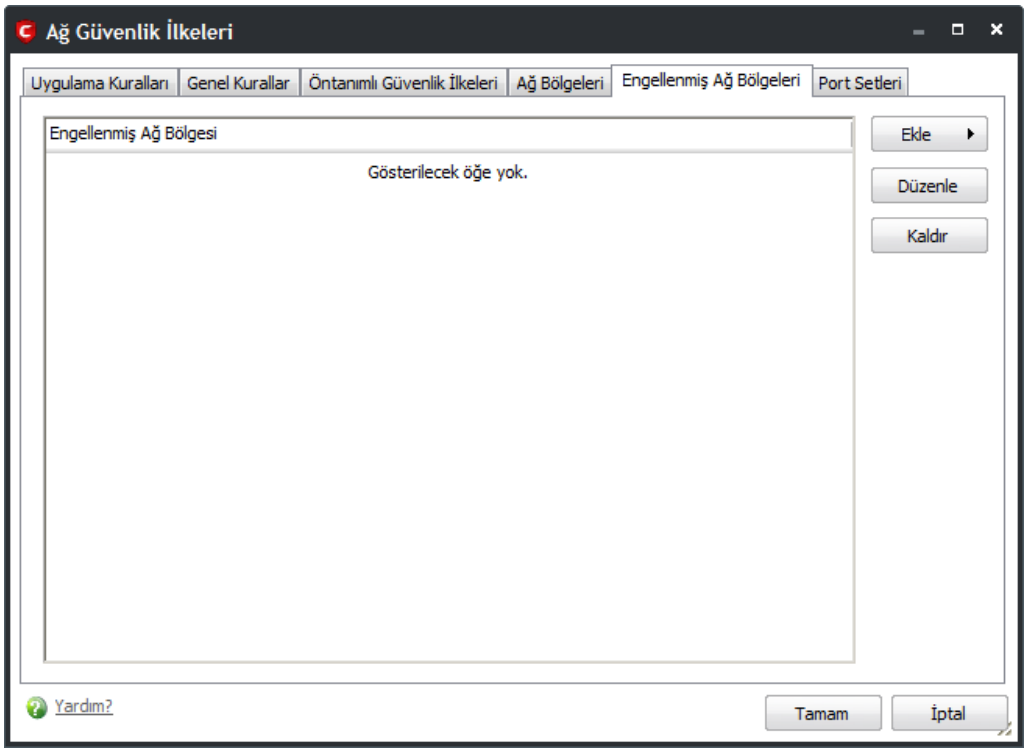
Not: Yeni ve deneyimsiz kullanıcılara bu arayüzü kullanarak bir bölgeyi engellemeden önce 'Ağ Bölgeleri', 'Port Gizleme Sihirbazı' ve 'Ağ Güvenlik İlkeleri' bölümlerini okumalarını öneririz.

'Engellenmiş Ağ Bölgeleri' alanı şunlara izin verir:

- **Önceden bulunan bir ağ bölgesini engellenmiş olarak tanımlayarak o bölgeye erişimi engeller**
- **Elle yeni bir ağ bölgesi tanımlayarak o bölgeye erişimi engeller**

Engellenmiş Ağ Bölgeleri arayüzüne erişmek için

•Güvenlik Duvarı Görevleri > Ağ Güvenlik İlkeleri arayüzünden 'Engellenmiş Ağ Bölgeleri' sekmesine gidin.



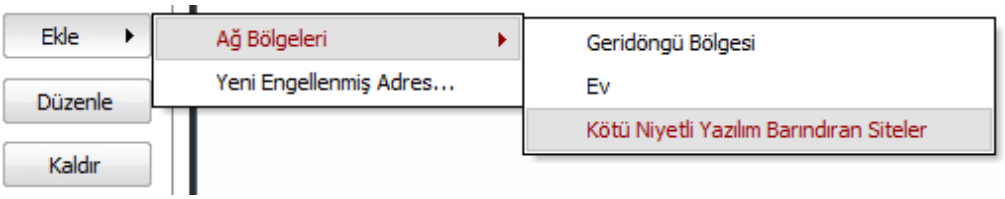
Not 1: Bölgeyi engellemeden önce o bölgeyi oluşturmalısınız. Bunun iki yolu vardır;

1. 'Ağ Bölgeleri' arayüzünü kullanarak engellemek istediğiniz ağ bölgesi tanımlayın.
2. Arayüzden 'Yeni Engellenmiş Adres' seçerek

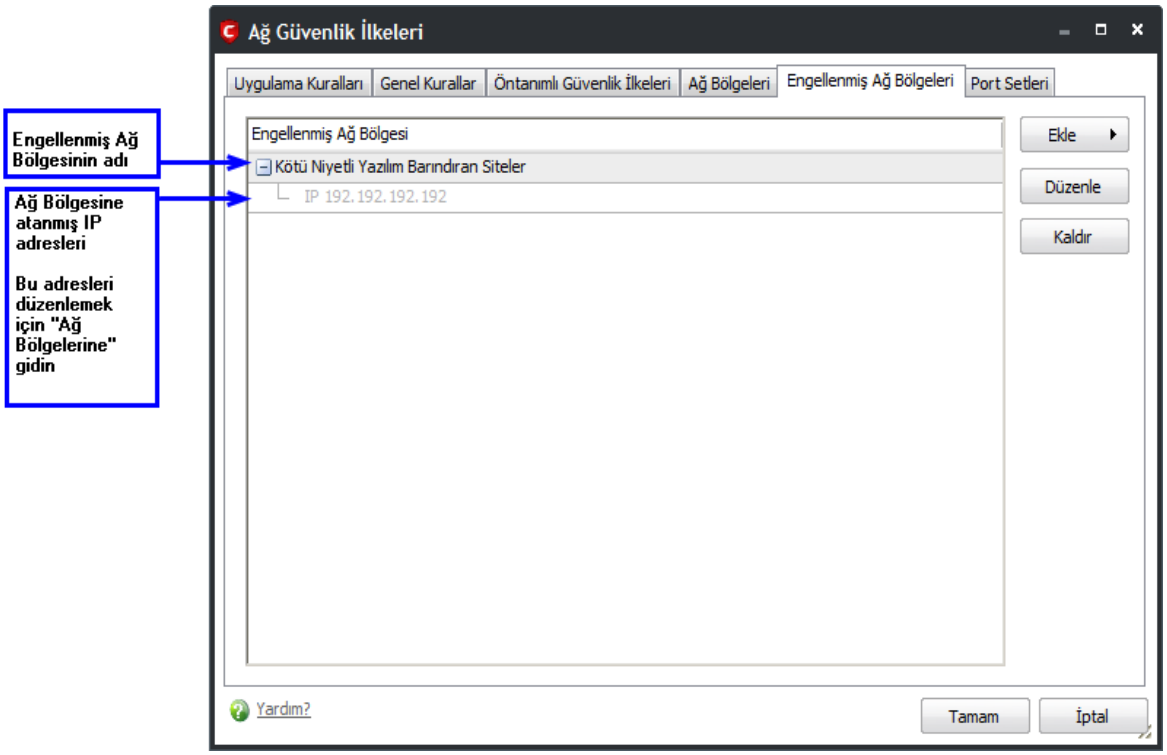
Not 2: Bu arayüzü kullanarak bulunan ağ bölgeleri üzerinde değişiklik yapmazsınız. Bulunan bölge üzerinde değişiklik yapmak için 'Ağ Bölgelerim' arayüzünü kullanın.

Önceden bulunan bir ağ bölgesini engellenmiş olarak tanımlayarak o bölgeye erişimi engellemek için

1. 'Ekle' düğmesine tıklayın ve engellemek istediğiniz 'Ağ Bölgesini' seçin.



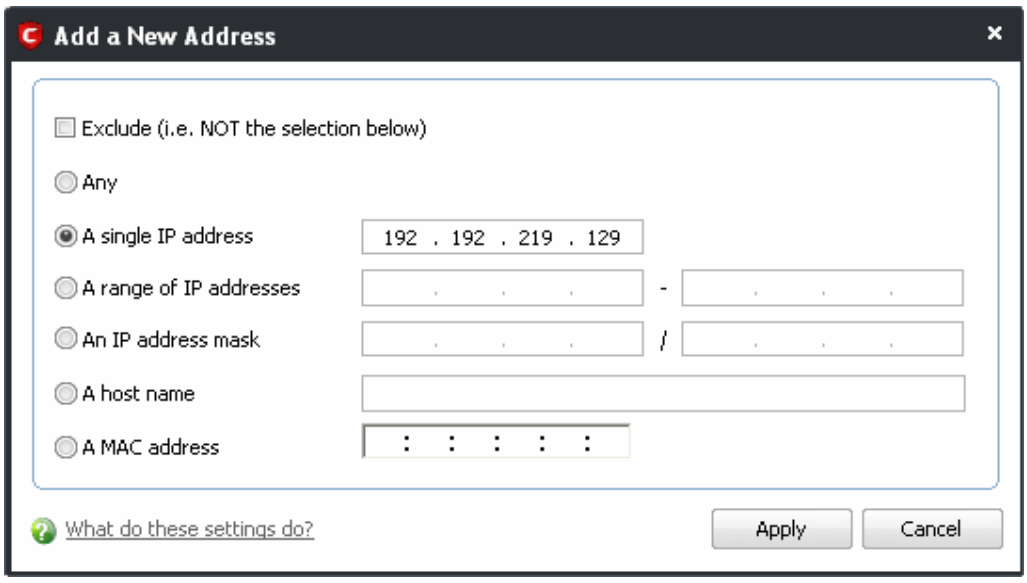
Seçilen bölge listede görünür.



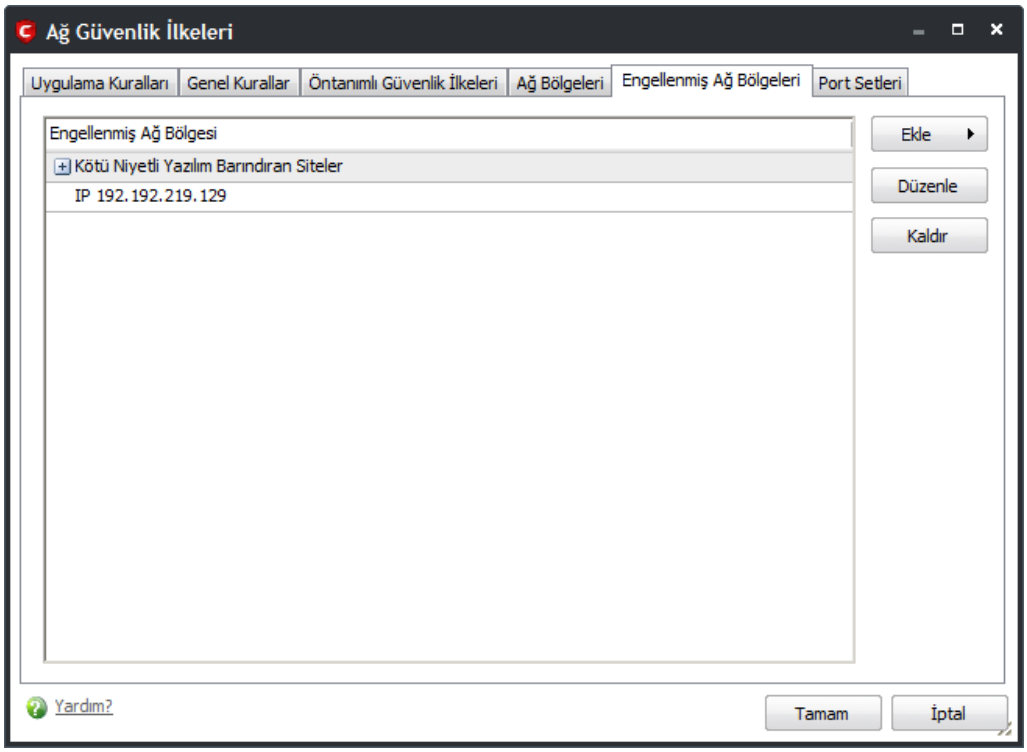
2. Seçiminizi onaylamak için ‘Uygula’ düğmesine tıklayın. Bu bölgeye erişim tamamen engellenecektir.

Elle yeni bir ağ bölgesi tanımlayarak o bölgeye erişimi engellemek için

1. ‘Ekle’ düğmesine tıklayın ve ‘Yeni Engellenmiş Adres’ seçin. Açılan diyalogdan seçiminizi yapın ve ona göre doldurun.



Seçiminizi onaylamak için ‘Uygula’ düğmesine tıkladıktan sonra engellediğiniz adresler listede görünür. Bu adresleri istediğiniz zaman ‘Düzenle’ düğmesine tıklayarak düzenleyebilirsiniz.



1. Seçiminizi onaylamak için 'Uygula' düğmesine tıklayın. Bu bölgeye erişim tamamen engellenecektir.

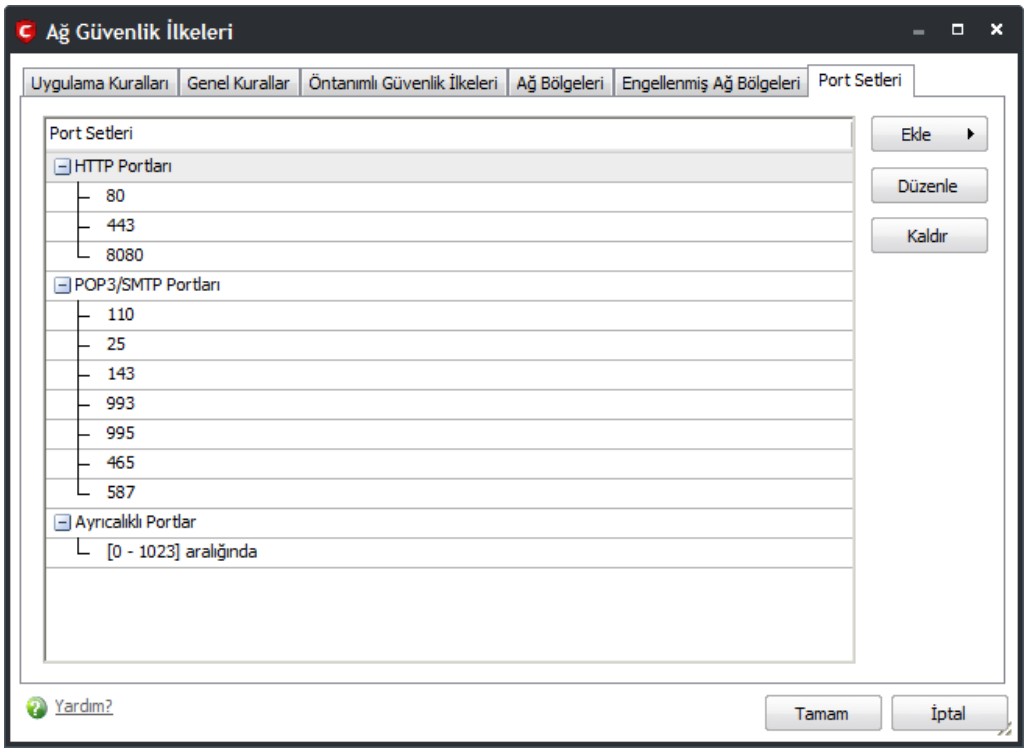
Özel Not: Engellenmiş ağ bölgesi oluşturmak ilgili bölge için 'tümünü engelle' genel kuralını uygular. Buna rağmen, 'Güvenilir Bölge' oluşturmanın aksine, bu kural Ağ Güvenlik İlkeleri'nin Genel Kurallar sekmesinde görüntülenmez veya bu sekmeden düzenlenemez.

3.4.7 Port Setleri

Port Setleri yeniden ve çoklu olarak Uygulama Kuralları ve Genel Kurallar bölümlerinde kullanım için yararlıdır.

'Port Setleri' arayüzüne erişmek için

1. Güvenlik Duvarı Görevleri > Ağ Güvenlik İlkeleri arayüzünden 'Port Setleri' sekmesine gidin.



Comodo Internet Security ile birlikte varsayılan olarak gelen port setleri:

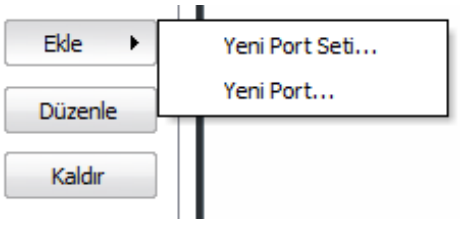
- **HTTP Portları**: 80 ve 443. HTTP trafiğinin gerçekleştiği varsayılan portlar.
- **POP3/SMTP Portları**: 110, 25, 143, 995, 465. Posta istemcileri tarafından genellikle kullanılan portlar. POP3, SMTP ve IMAP protokolleri.
- **Ayrıcalıklı Portlar:** 0-1024**.**

Yeni port seti eklemek için

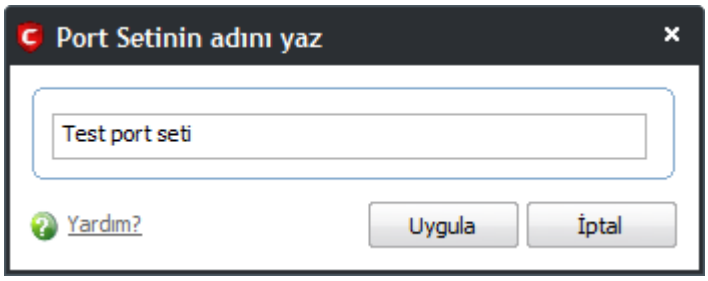
1. Set için ad girin.
2. Bu sete katmak istediğiniz portları seçin.

Set için ad tanımlamak

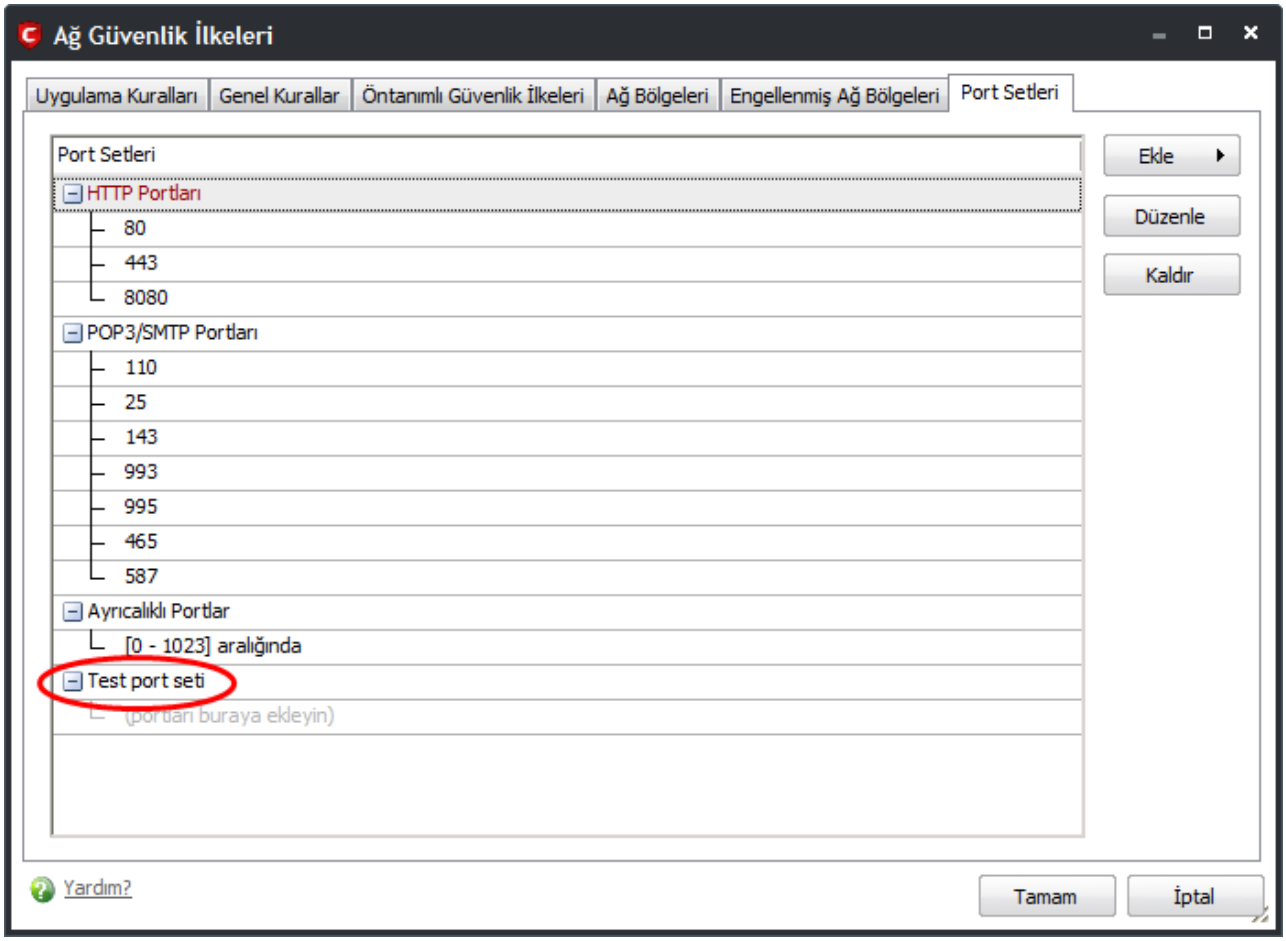
1. 'Ekle' düğmesine tıklayıp menüden 'Yeni Port Ekle…' seçin.



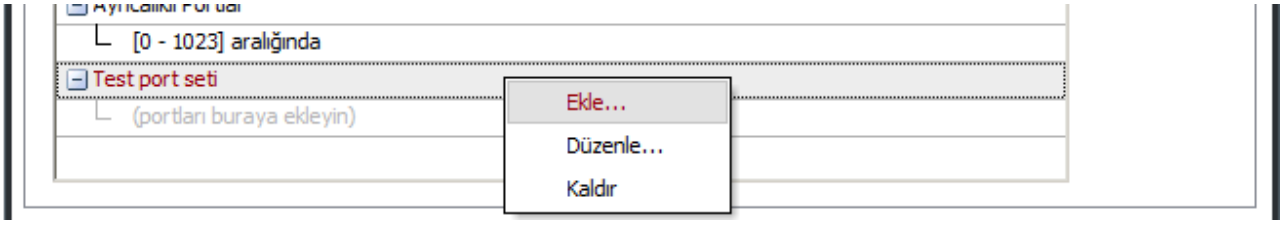
2. Set için ad girin. Aşağıdaki örnekte port setimiz için test port set seçtik.



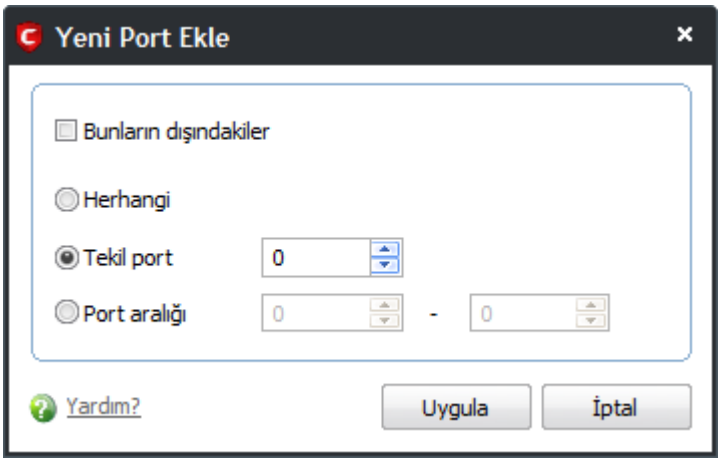
3. ‘Uygula’ düğmesine tıklayın. Yeni port seti listede görünür:



4. Port setine sağ tıklayarak bu sete eklemek istediğiniz portları menüden ‘Ekle’ seçerek ekleyiniz.



Bu port seçimi diyaloğunu açar.



5. Portları seçin:
    - **Herhangi**, tüm portları seçer;
    - **Tekil port** ve yanındaki kutuya port girerek;
    - **Port aralığı** ve başlangıç ve bitiş portlarını girerek.
1. 'Uygula' düğmesine tıklayın.
2. 'Port Setleri' arayüzünden 'Tamam' düğmesine tıklayın.

Daha fazla port eklemek istiyorsanız dördüncü adımı yineleyin.

Bulunan port set adını düzenlemek için

- Listeden port adını seçin ve 'Düzenle…' düğmesine tıklayarak port adlandırma penceresini açın.

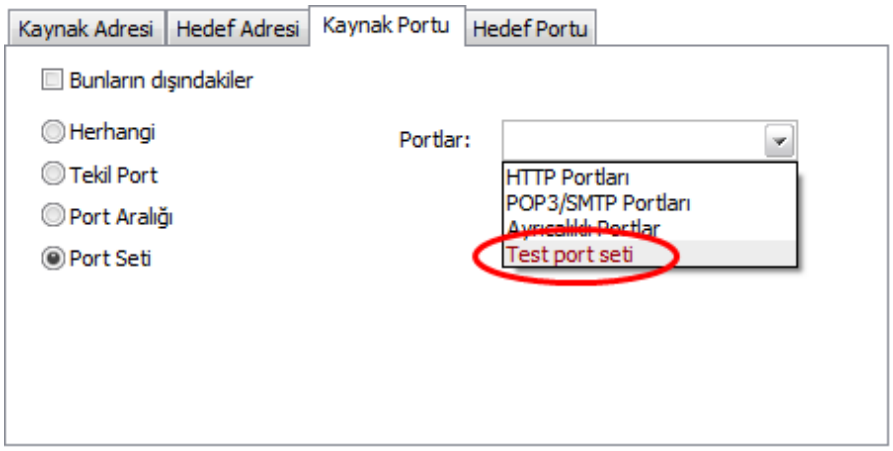
Bulunan port setine port eklemek için

- Port adına sağ tıklayın ve 'Ekle…' seçin veya port adını seçin ve sağdan 'Ekle…' düğmesine tıklayın açılır menüden 'Yeni Port…' seçin.

Bulunan port setindeki port numaralarını değiştirmek için

- Port numarasını (port adını değil) seçin ve 'Düzenle…' düğmesine tıklayın VEYA port numarasına (port adına değil) sağ tıklayın ve açılır menüden 'Düzenle…' seçin.

Ağ denetim kuralı tanımlarken veya değiştirirken, bu arayüzde listelenen port setlerini hem kaynak hem hedef port sekmelerinde kullanabilirsiniz.



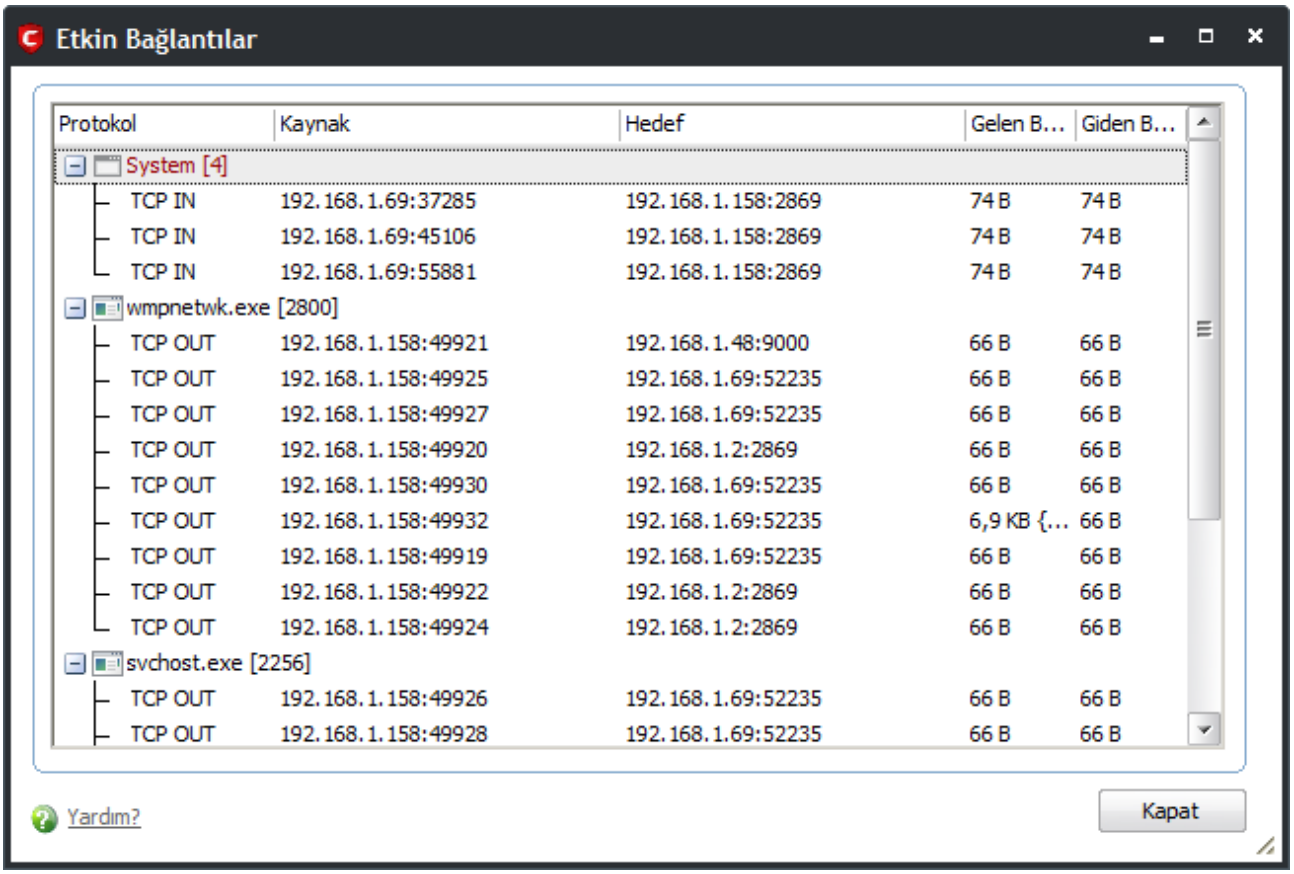
3.5 Etkin Bağlantıları Göster

Etkin Bağlantılar arayüzü tüm etkin uygulama bağlantılarının özetini gösterir.

Bu liste gerçek zamanlı olarak güncellenir.

Etkin bağlantılara erişmek için

1. Güvenlik Duvarı Görevlerinden Etkin Bağlantıları Göster bölümüne girin.

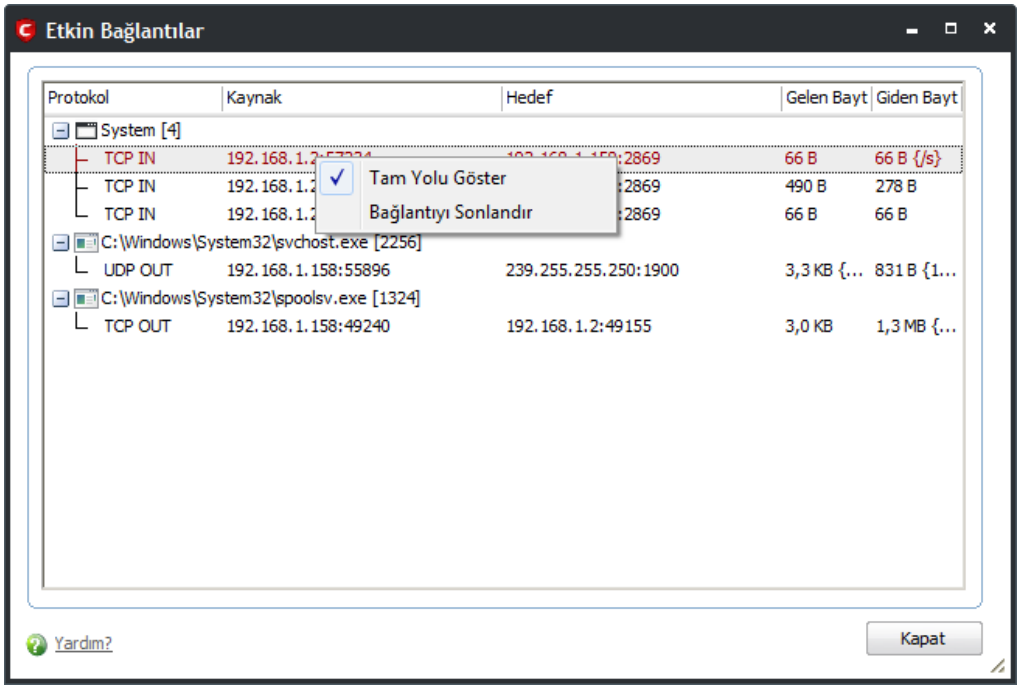


Sütun Açıklamaları

- **Protokol – Bağlantıyı gerçekleştiren uygulamayı, kullandığı protokolü ve trafiğin yönünü gösterir.**
- **Kaynak (IP : Port) – Uygulamanın hangi IP ve port üzerinden bağlantı kurduğunu gösterir. Uygulama bağlantı bekleme durumundaysa 'Dinleniyor' olarak tanımlanır.**
- **Hedef (IP : Port) - Uygulamanın hangi IP ve porta bağlandığını gösterir. Kaynak 'Dinleniyor' olarak tanımlanmışsa bu sütun boştur.**
- **Gelen Bayt – Bağlantıya izin verildiğinden beri toplam gelen veriyi gösterir.**
- **Giden Bayt - Bağlantıya izin verildiğinden beri toplam giden veriyi gösterir.**

İçerik Menüsü

1. İçerik menüsünü görüntülemek için öğelere sağ tıklayın.



2. Tam yolu görüntülemek için 'Tam Yolu Göster' seçin.
3. Uygulamaya ait bağlantıyı sonlandırmak için 'Bağlantıyı Sonlandır' seçin.

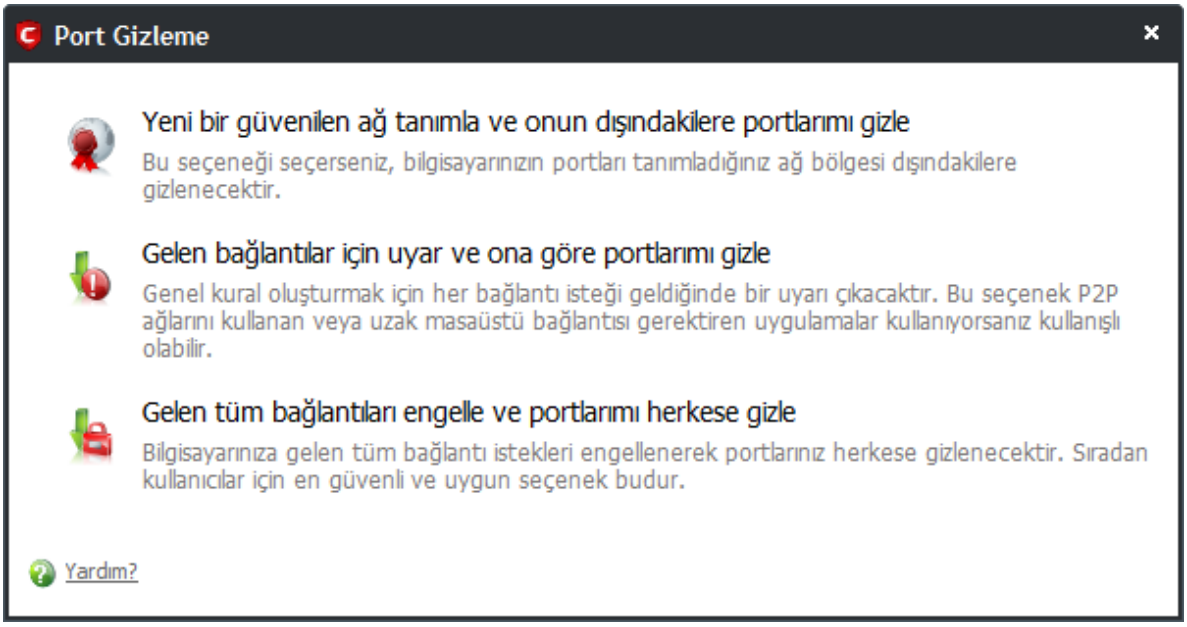
3.6 Port Gizleme Sihirbazı

Port Gizleme bir güvenlik özelliğidir, fırsatçı port taramalarına cevap vermeyerek internete bağlı olan bilgisayarı gizler.

Genel Not: Kötü niyetli kişiler port taraması ile sisteminizdeki açık portlara göre saldırı düzenleyebilirler.

Portun gizlenmesi o portu taramalardan gizler. Bu portun 'kapalı' olma durumundan farklıdır. Kapalı olan port, bağlantı isteğine HAYIR cevabı gönderir; böylece saldırgan karşıda bir bilgisayar olduğunu anlar. Bu özellik bilgisayarınız için yüksek seviyede güvenlik sağlar. Saldırgan portlarınızı göremez ise bilgisayarın kapalı olduğunu farzeder ve başka hedefe yönelir. Bu özellik ile dış tehditlerden gizlenirken sorunsuzcana internete bağlanabilir ve bilgi transferi yapabilirsiniz. Comodo Güvenlik Duvarı tarafından sunulan gizleme seçenekleri:

1. Güvenlik Duvarı Görevlerindeki 'Port Gizleme Sihirbazı' bölümüne tıklayın.
2. Seçebileceğiniz üç seçenek vardır:
   - Yeni güvenilir ağ tanımla
   - Gelen bağlantılarda uyar
   - Gelen tüm bağlantıları engelle



Ayrıntılı bilgi için istediğiniz seçeneğe tıklayın:

- Yeni bir güvenilen ağ tanımla ve onun dışındakilere portlarımı gizle
- Gelen bağlantılar için uyar ve ona göre portlarımı gizle
- Gelen tüm bağlantıları engelle ve portlarımı herkese gizle

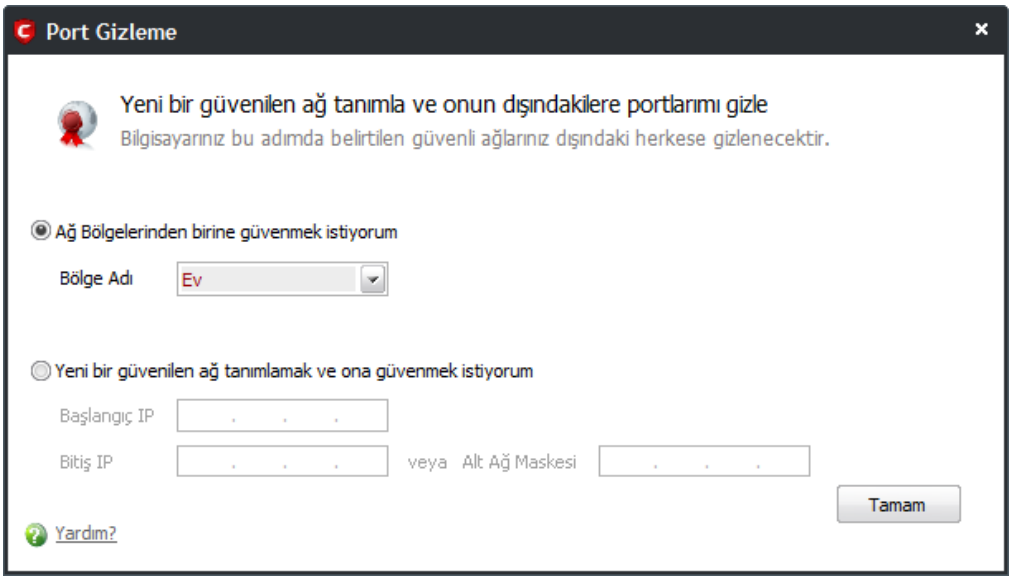
Yeni bir Güvenilen Ağ Tanımla ve Onun Dışındakilere Portlarımı Gizle

Bilgisayarınızın portları tanımladığınız ağ bölgesi DIŞINDAKİLERE gizlenecektir.

Sihirbaza başlamak için

1. 'Yeni bir güvenilen ağ tanımla ve onun dışındakilere portlarımı gizle' bağlantısına tıklayın.

Yeni güvenilir bölge girmenizi isteyen bir diyalog görünür:

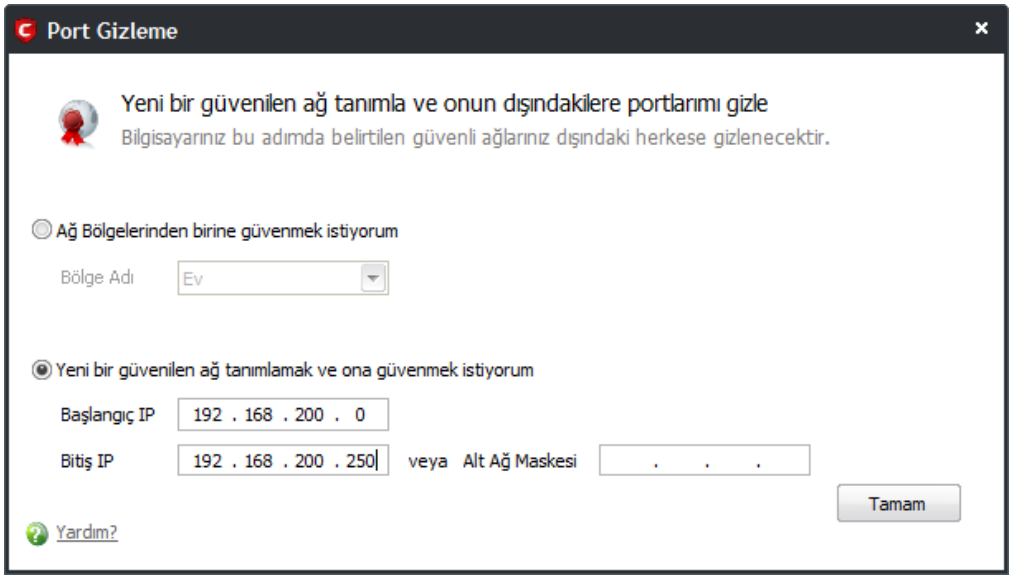


2. Yapılandırılmış ağ bölgeniz varsa üstteki seçenekte kalsın ve açılır menüden ‘Bölge Adını’ seçin ve ‘Tamam’ düğmesine tıklayın.

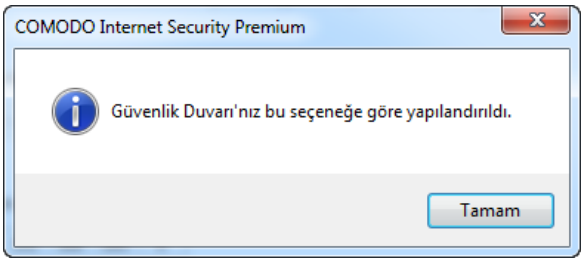
Henüz bir ağ bölgesi tanımlamadıysanız Ağ Güvenlik İlkeleri altındaki 'Ağ Bölgeleri' bölümünü kullanarak veya bu diyaloğun alt seçeneğinin yardımıyla elle yeni güvenilen ağ bölgesi ekleyebilirsiniz.

Bu diyalogdan elle güvenilen ağ bölgesi tanımlamak için

1. 'Yeni bir güvenilen ağ tanımlamak ve ona güvenmek istiyorum' seçin.

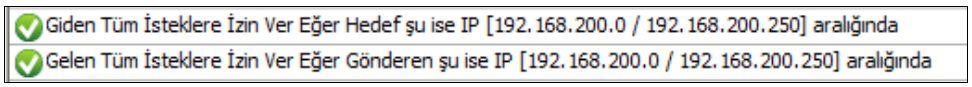


2. Bilgisayarınızın görünür olmasını istediğiniz IP aralığını girin (veya Alt Ağ Maskesi belirtin)
3. Yeni Bölge kuralını oluşturmak için ‘Tamam’ düğmesine tıklayın.



Daha fazla bölge eklemek istiyorsanız bu adımları yineleyin.

'Yeni bir güvenilen ağ tanımla ve onun dışındakilere portlarımı gizle' seçeneği 'Genel Kurallar' arayüzüne aşağıdaki kuralları ekler:



Yukarıda açıklanan kuralın parametreleri:

İzin Ver | IP | Giden | Kaynak Adresi: Herhangi | Hedef Adresi: <BÖLGE> | Protokol: Herhangi

İzin Ver | IP | Gelen | Kaynak Adresi: <BÖLGE> | Hedef Adresi: Herhangi | Protokol: Herhangi

Daha fazla bilgi için lütfen buraya tıklayın.

Gelen bağlantılar için uyar ve ona göre portlarımı gizle

Gelen bağlantılar için kullanıcı cevabı istenir. P2P veya uzak masaüstü uygulamalarını kullananlar için kullanışlı olabilir. Bu seçenek aşağıdaki kuralı 'Genel Kurallar' arayüzüne ekler:

Engelle | ICMP | Gelen | Kaynak Adresi: Herhangi | Hedef Adresi: Herhangi | ICMP Mesajı: YANKI İSTEĞİ

Daha fazla bilgi için lütfen buraya tıklayın.

Gelen tüm bağlantıları engelle ve portlarımı herkese gizle

Bilgisayarınıza gelen tüm bağlantı istekleri engellenerek portlarınız herkese gizlenir. Gelen bağlantılar engellendiği zaman uyarı gösterilmez, fakat bu olay güvenlik duvarı günlüğüne girilir. Bu seçenek aşağıdaki kuralı 'Genel Kurallar' arayüzüne ekler:

Engelle ve Günlükle | IP | Gelen | Kaynak Adresi: Herhangi | Hedef Adresi: Herhangi | Protokol: Herhangi

Daha fazla bilgi için lütfen buraya tıklayın.

3.7 Güvenlik Duvarı Davranış Ayarları

Güvenlik Duvarı Davranış Ayarları güvenlik ve uyarı sıklıklarını ayarlamanıza izin verir. Bu diyaloğa 'Güvenlik Duvarı Görevleri' bölümünden veya daha hızlı olarak Özet Ekranı güvenlik seviyesi (güvenli kip) bağlantısına tıklayarak girebilirsiniz.

Bu ayarlar aşağıdaki sekmeler kullanılarak yapılabilir.

- **Genel Ayarlar sekmesi**
- **Uyarı Ayarları sekmesi**
- **Gelişmiş Ayarlar sekmesi**

3.7.1 Genel Ayarlar

Güvenlik Duvarı Seviyesini değiştirebilirsiniz.

Seçenekler:

•Tümünü Engelle

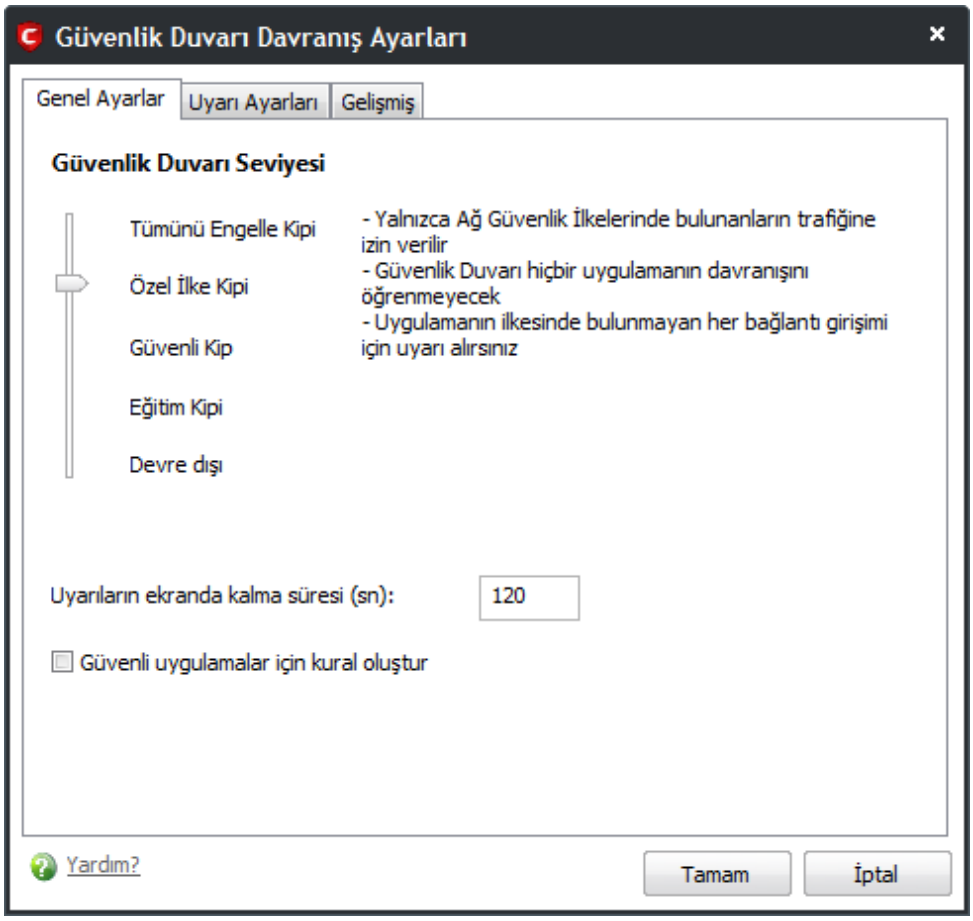
•Özel İlke

•Güvenli Kip (varsayılan)

•Eğitim

•Devre Dışı

Burada yapılan seçim özet ekranında görünür.



- **Tümünü Engelle Kipi:** Kullanıcı yapılandırmasına ve kurallara bakılmaksızın tüm gelen ve giden ağ trafiği engellenir. Güvenlik Duvarı otomatik olarak kural oluşturmaz ve uygulamaların davranışını öğrenmez.
- **Özel İlke Kipi:** Kullanıcının tanımladığı kurallara göre trafik denetlenir. Kurallarda yer almayan uygulamaların (Comodo Beyaz Listesinde bulunsa bile) istekleri için uyarı gösterilir.
- **Güvenli Kip:** Comodo tarafından 'Güvenli' olarak imzalanmış uygulamalara otomatik olarak izin verilir. Güvenli uygulamalar için kural oluştur seçiliyse ek olarak bu uygulamalar için otomatik olarak izin ver kuralı oluşturulur. Diğer uygulamaların bağlantı istekleri için uyarı alırsınız.

  'Güvenli Kip' çoğu kullanıcı için en uygun güvenlik seviyesidir. Yüksek seviyede güvenlik sağlarken bir yandan da kolay yönetilebilirdir.
- **Eğitim Kipi :** Tüm uygulamaların davranışı güvenlik seviyesi değiştirilene kadar uyarı verilmeden öğrenilir.

İpucu: Çevrimiçi bir oyunu ilk defa oynarken bu ayarı geçici olarak kullanabilirsiniz. Bu şekilde oyun sırasında uyarı almaz ve otomatik olarak oyun için kural oluşturulur. Daha sonra önceki güvenlik seviyenize dönebilirsiniz.

- **Devre Dışı:** Güvenlik Duvarını devre dışı bırakır. Tüm bağlantı isteklerine izin verilir.

Uyarıların ekranda kalma süresi (sn)
Uyarıların ne kadar süre görüntülenmesi gerektiğini ayarlayabilirsiniz. Varsayılan değer 120 sn'dir.

Güvenli uygulamalar için kural oluştur

Comodo Güvenlik Duvarı şu durumlarda uygulamalara güvenir:

- **Uygulama/dosya Savunma+ Görevleri altındaki Güvenilir Dosyalarda bulunuyorsa;**
- **Savunma+ Görevleri altındaki Güvenilir Yazılım Sağlayıcıları listesinden bir sağlayıcı tarafından imzalanmış ise;**
- **Comodo Beyaz Listesinde yer alıyorsa.**

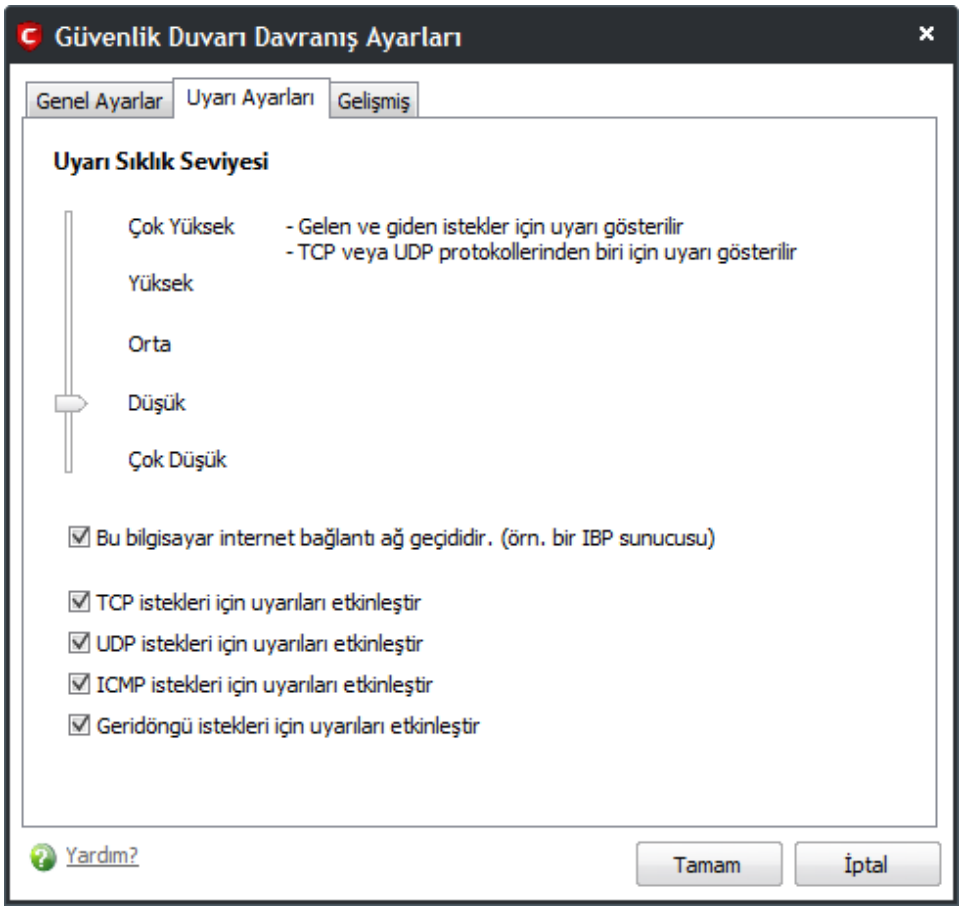
Varsayılan olarak CIS otomatik olarak kural oluşturmaz böylece yapılandırma gereksiz yere büyümemiş olur.

Bu seçenek etkinleştirilse CIS otomatik olarak 'izin ver' kuralı oluşturmaya başlar. Bu kurallar Ağ Güvenlik İlkeleri > Uygulama Kuralları arayüzünde listelenir. Deneyimli kullanıcılar bunları isteklerine ve gereksinimlerine göre değiştirebilirler.

3.7.2 Uyarı Ayarları

Bu bölümdeki kaydırıcıyı kullanarak uyarı sayısı arttırıp azaltılabilir. Bu ayar yapılandırdığınız kurallar tarafından sağlanan (örneğin, 'Ağ Güvenlik İlkeleri' içindeki) güvenliği etkilemez. Çoğu kullanıcı için varsayılan 'Düşük' ayarı en iyi seviyedir – sizi uyarılara boğmadan bağlantı isteklerinde bildirim yapılır.

Uyarı Sıklığı ayarı güvenli olarak tanımlanmamış uygulamalar ve IP adresleri içindir.



- **Çok Yüksek**: Her bir IP adresi, port, protokol (UDP ve TCP için) ve bağlantı yönü (Gelen/Giden) için uyarı gösterilir. Çok yüksek sayıda uyarıya neden olur.
- **Yüksek**: Her bir port, protokol (UDP ve TCP için) ve bağlantı yönü (Gelen/Giden) için uyarı gösterilir. Yüksek sayıda uyarıya neden olur.
- **Orta**: Her bir protokol (UDP ve TCP için) ve bağlantı yönü (Gelen/Giden) için uyarı gösterilir. Orta sayıda uyarıya neden olur.
- **Düşük**: Protokol (UDP veya TCP için) ve bağlantı yönü (Gelen/Giden) için uyarı gösterilir. Düşük sayıda uyarıya neden olur. Comodo tarafından önerilen seviyedir.
- **Çok Düşük**: Güvenlik Duvarı yalnızca bir tane bağlantı uyarısı gösterir.

İşaret kutuları

Bu bilgisayar internet bağlantı ağ geçididir (ICS sunucusu gibi) – İnternet Bağlantı Paylaşımı Sunucusu bir bilgisayardır ve ağdaki diğer bilgisayarlar bu bilgisayar üzerinden bağlantı kurarlar.

- Ağınızda ICS kullanarak bağlanan bilgisayarlar yoksa bu kutuyu işaretlemeyin.
- Ağınızda ICS kullanarak bağlanan bilgisayarlar varsa bu kutuyu işaretleyin.

Not: Bilgisayarınız ICS ise ve bu kutuyu işaretlememişseniz güvenlik duvarı uyarılarında artış olacaktır. Bu

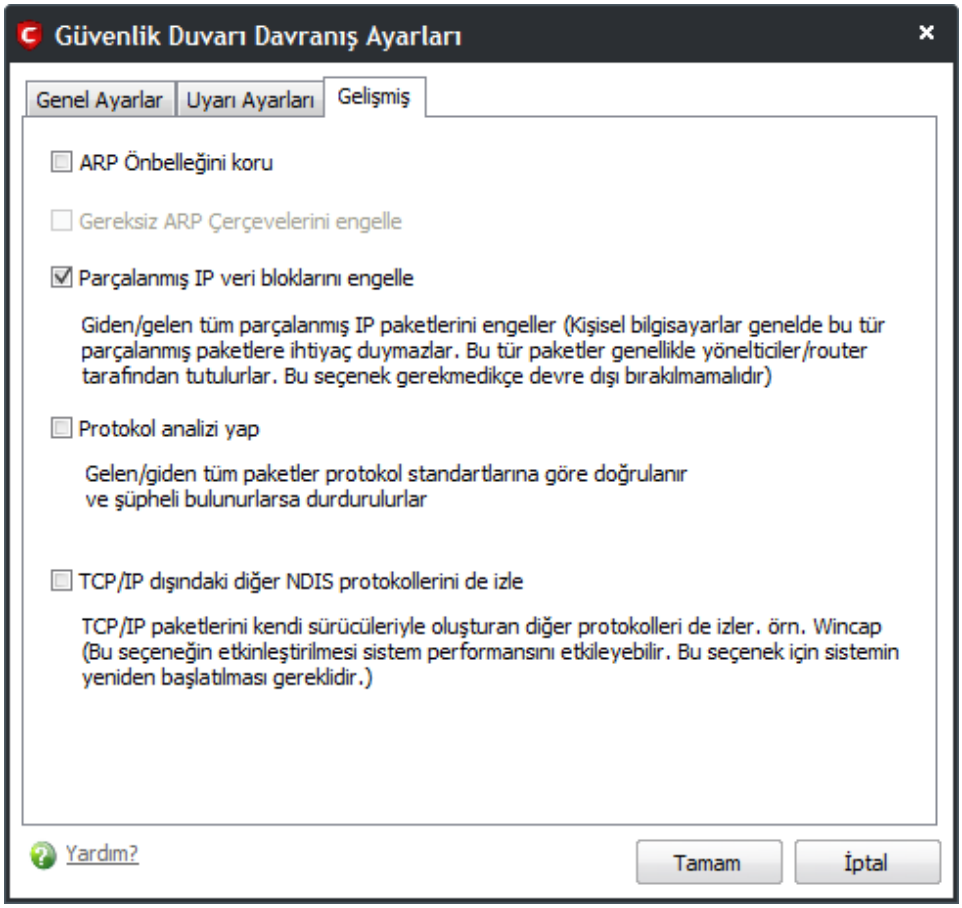
seçeneğin işaretlenmesi güvenliğinizi azaltmaz aksine uyarıları azaltmanıza yardımcı olur.

S: "Evimde birden fazla internete bağlı bilgisayarım var. Bu kutuyu işaretlemeli miyim?'

C: Çoğu durumda hayır. Evde 'yönlendirici (router) aracılığıyla veya kablosuz olarak' internete bağlı birden fazla bilgisayar bulunması burada bahsedilen ICS ile 'paylaşımdan' farklıdır. Yalnızca bilgisayar ICS olarak atanmışsa bu kutuyu işaretleyin.

TCP istekleri için uyarıları etkinleştir / UDP istekleri için uyarıları etkinleştir / ICMP istekleri için uyarıları etkinleştir / Geridöngü istekleri için uyarıları etkinleştir – Kaydırıcıyla birlikte bu işaretleme kutuları uyarılarını görmek istediğiniz protokollere göre ayarlamanıza izin verir.

3.7.3 Gelişmiş Ayarlar



Comodo Güvenlik Duvarı bilgisayarınızı korumanıza yardımcı olacak gelişmiş özellikler içerir.

- **ARP Önbelleğini Koru - ARP (Address Resolution Protocol) bağlantıları durumsal olarak denetlenir. Bu yanıltıcı ARP isteklerini engeller ve bilgisayarınızı ARP önbellek zehirlenmelerine karşı korur.**

ARP Önbelleği (veya ARP Tablosu) IP adreslerinin hangi MAC adreslerine karşılık geldiğini bilgisayarınızda saklar. Durumsal inceleme bulunan oturumları en düşük protokol seviyesinde karılaştırarak şüpheli durumları saptar.

Not – Ağdaki her cihaz iki adrese sahiptir: MAC (Media Access Control) adresi ve IP (Internet Protocol) adresi.

MAC adresi cihaz içindeki gömülü fiziksel adrestir ve takıldığı sisteme göre değişiklik göstermez. Diğer yandan IP adresi ağdan ağa ve DHCP sunucusunun atamasına göre farklılık gösterebilir. Ana makinadan hedef ağ kartına veri paketlerini düzgün gönderebilmek için MAC ve IP adres ikilisi kaydedilir. Adres Çözümleme Protokolü bu işlemi IP -> MAC ve MAC -> IP eşlemesi yaparak gerçekleştirir. ARP önbelleği eşlenen bu IP ve MAC adreslerinin kaydıdır.

- **Gereksiz ARP çerçevelerini engelle – Gereksiz ARP çerçevesi ağdaki makinalara yay olarak istenmediği halde yollanan ARP cevabıdır. ARP cevabı yayınlandığı zaman diğer tüm makinaların ARP isteklerine karşılık gönderilmiş olsun veya olmasın yerel ARP önbelleklerini güncellemeleri gerekmektedir. Gereksiz ARP çerçeveleri ağda değişen bir makine olduğu zaman makinanızın ARP önbelleğini güncellediği için önemlidir (örneğin, ağdaki bir makinanın ağ kartı değiştirildiği zaman yayın yapılarak bu değişikliği ağdaki sistemlere bildirir böylece veriler doğru şekilde yönlendirilebilir). Bu seçenek ile ARP önbelleğinizi şüpheli güncellemelerden koruyabilirsiniz.**
- **Parçalanmış IP veri bloklarını engelle – İki bilgisayar arasında bağlantı kurulduğu zaman bu makinalar MTU (Maximum Transmission Unit) boyutu üzerinden anlaşmalıdır. IP veri bloğu parçalanması veriler anlaşılan MTU değerinden daha düşük MTU değeri kullanan yönlendirici üzerinden geçerken oluşur ve veriler parçalanarak daha küçük parçalar halinde gönderilir. Parçalanmış IP paketleri DOS saldırısına benzer tehdit oluşturabilir. Üstelik parçalanmış paketler aktarım hızını yavaşlatabilir.**

Bu seçenek varsayılan olarak seçilidir.

- **Protokol analizi yap – Protokol analizi DOS saldırılarında kullanılan sahte paketleri belirlemek içindir. Bu seçenek işaretlendiği zaman Comodo Güvenlik Duvarı tüm paketleri protokol standartlarına göre inceler ve duruma göre bu paketleri engeller.**
- **TCP/IP dışındaki diğer NDIS protokollerini de izle** – Bu seçenek ile Comodo Güvenlik Duvarı'nın TCP/IP dışındaki diğer protokol sürücülerine ait olan paketleri de yakalamasını sağlayabilirsiniz. Truva atları paket aktarımı için kendi protokol sürücülerini kullanabilir. Bu seçenek ile bu tür girişimleri yakalayabilirsiniz. Varsayılan olarak işaretli değildir çünkü: sistem performansını düşürebilir ve bazı protokol sürücüleriyle uyumsuz olabilir.

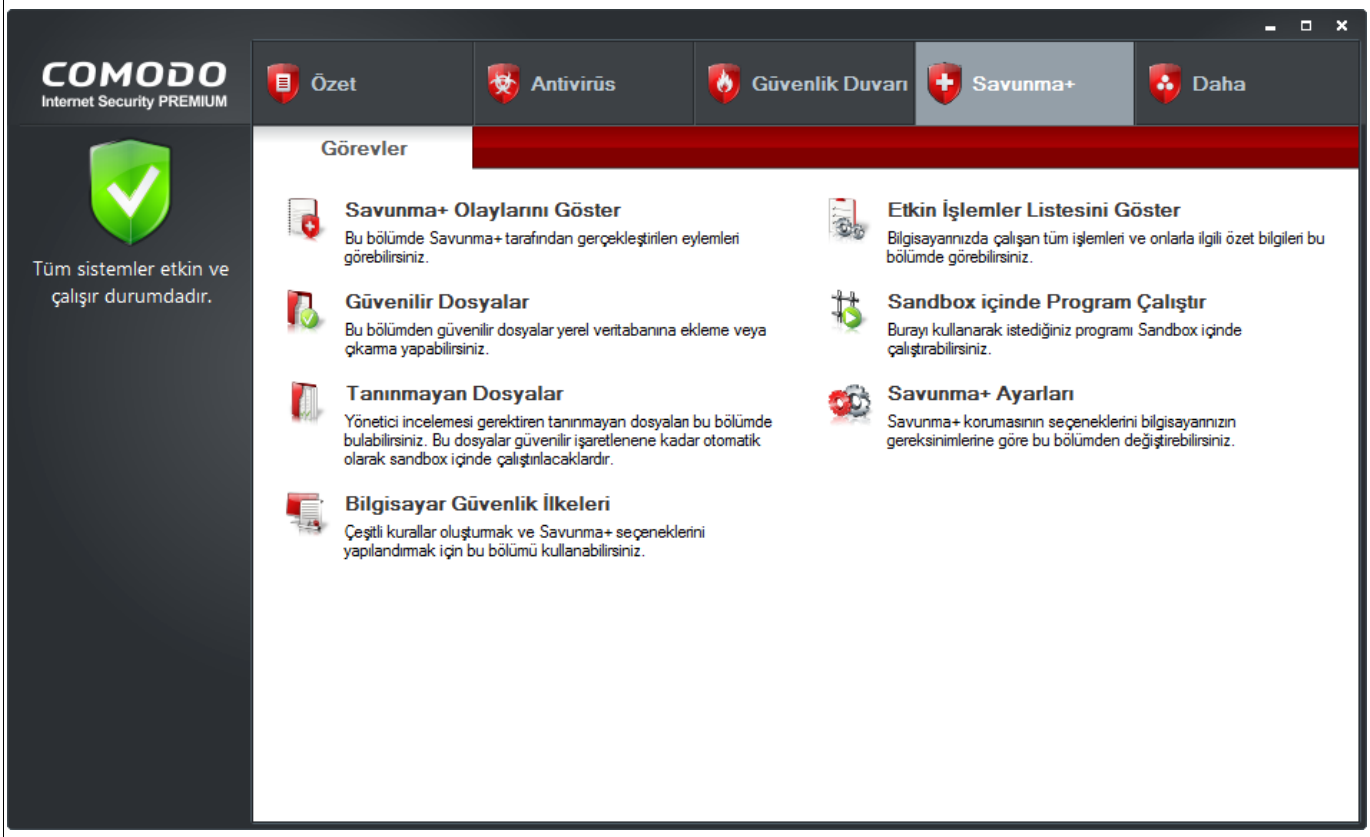
4 Savunma+ Görevleri - Tanıtım

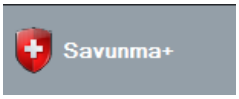
Savunma+ bilgisayarınızdaki tüm yürütülebilir dosyaları sürekli olarak izler. Savunma+ açıkken, HER defasında bilinmeyen uygulama yürütülebiliri (.exe, .dll, .sys, .bat vb.) çalıştırılırken kullanıcı uyarılır. Çalıştırılmasına izin verilen yürütülebilirler yalnızca sizin izin verdiklerinizdir.

Savunma+ ayrıca veri hırsızlığına, bilgisayar çökmelerine ve sisteme zarar verebilecek çoğu tampon taşırmalarına karşı korur. Ayrıntılı bilgi için Yürütme Denetimi Ayarları.

Savunma+ büyük ölçüde yapılandırılabilir güvenlik kuralları arayüzü sunar ve rootkit, işlemlerarası bellek enjeksiyonu, tuş kaydediciler ve daha bir çok saldırıyı önler. Virüslerin, Truva atlarının ve Casus yazılımların sisteminize kurulmasını engeller ve işletim sisteminin önemli bölümlerinde ve kayıt defteri girdilerinde yapılacak izinsiz değişiklikleri önler.

Savunma+ Sandbox işlevi şüpheli ve bilinmeyen dosyaları sistemden tecrit edilmiş ortamda çalıştırarak sistemi bunların etkilerinden korur.



Savunma+ bölümüne gezinti panelinden Savunma+ sekmesine  tıklayarak erişebilirsiniz.

Savunma+ ana yapılandırma alanı tüm özelliklere kolaycana erişmenizi ve bunları bulunan alt bölümler ve kısayollar yardımıyla ayarlamanızı sağlar. Bu bölümler hakkında ayrıntılı bilgi için aşağıdaki bağlantılara tıklayın.

- **Savunma+ Olaylarını Göster**
- **Güvenilir Dosyalar**
- **Tanınmayan Dosyalar**
- **Bilgisayar Güvenlik İlkeleri**
- **Etkin İşlemler Listesini Göster**
- **Sandbox için Program çalıştır**

•Savunma+ Ayarları

4.1 Sandbox - Giriş

Comodo Internet Security'nin yeni sandbox işlevi bilinmeyen ve güvenilmeyen uygulamalar için tecrit edilmiş ortam oluşturur. Uygulamanın sandbox içinde çalıştırılıyor olması onun sistemdeki diğer işlemler, programlar ve 'gerçek' sisteminizdeki veriler üzerinde kalıcı değişiklikler yapamayacağı anlamına gelir. Comodo'nun diğer bileşenlerini (Güvenlik Duvarı, Savunma+ ve Antivirüs) güçlendirmek için sandbox bileşeni doğrudan güvenlik mimarisine eklenmiştir. Sandbox içindeki uygulamalar dikkatlice seçilmiş ayrıcalıklarla çalıştırılır ve gerçek sistem yerine verileri sanallaştırılmış dosya sistemine ve kayıt defterine yazarlar. Bu şekilde sisteme bir zarar gelmeden bilinmeyen uygulamaların çalışmasına izin verilir.

Bilinmeyen uygulama sandbox içine alındığı zaman CIS otomatik olarak dosyayı Comodo Bulut Tarayıcısına davranış analizi için yollar. Dosya zararsız bulunursa Comodo'nun genel beyaz listesine eklenir ve bir sonraki güncellemede bu tüm kullanıcılara gönderilir. Dosya beyaz listeye eklendikten sonra bir daha otomatik olarak sandbox içinde çalıştırılmayacaktır. Diğer taraftan, dosya zararlı bulunursa Comodo'nun kara listesine eklenecektir ve sonraki güncellemede silinecektir. Buradaki fayda dosya bu süreç içinde bir hasar veremeyecektir.

'Güvenlik olarak sandbox' uygulamak CIS 4'ün güvenliğini attırmıştır, uyarı sayısını azaltmıştır ve kullanımını kolaylaştırmıştır.

4.1.1 Bilinmeyen Dosyalar: Sandbox içine Alma ve Tarama Süreci

- **Bir yürütülebilir ilk çalıştırıldığı zaman CIS tarafından aşağıdaki güvenlik incelemelerinden geçer:**
  - Antivirüs taraması
  - Savunma+ Sezgisel denetimi
  - Tampon Taşma denetimi
- **Yukarıdaki inceleme sonunda dosya zararlı olarak saptanırsa kullanıcıya uyarı verilir ve dosya karantinaya alınır veya silinir**
- **Bir uygulama CIS tarafından aşağıdaki yollarlar kullanılarak 'güvenli' olarak tanınır (böylece sandbox içine alınmaz ve bulut içinde taranmaz):**
  - Çünkü Comodo yerel beyaz listesindedir
  - Çünkü kullanıcı uygulamayı yerel 'Güvenilir Dosyalar' listesine eklemiştir.
  - Kullanıcı tarafından kurucuya yükseltilmiş ayrıcalık verilmiştir (CIS otomatik olarak yönetici yetkisi gerektiren uygulamaları belirler ve kullanıcıya bu kurucuya güvenilip güvenilmeyeceğini sorar. Kullanıcı bu kurucuyu güvenli olarak onaylarsa CIS otomatik olarak bu kurucu tarafından yüklenen dosyaları güvenli olarak işaretler)
  - Ek olarak, Savunma+ güvenlik ilkesinde Kurucu/Güncelleyici olarak tanımlanmış ise sandbox içine alınmaz ve bulut içinde taranmaz (Ayrıca daha ayrıntılı bilgi için Bilgisayar Güvenlik İlkeleri bölümüne bakınız)

- **Bulut Taraması Bölüm 1**
  Yukarıdaki incelemelerden geçen dosyalar ve işlemler henüz 'güvenli' (beyaz listelenmiş) olarak tanınmamış dosyalar 'Tanınmayan' dosyalardır. Dosyanın güvenli olup olmadığını kanıtlamak için CIS ilk önce Comodo'nun Dosya İnceleme Sunucularındaki (FLS) son imza veritabana danışacaktır:
  - Tanınmayan işlemin veya dosyanın sayısal imzası oluşturulur.
  - Bu imzalar FLS'ye gönderilip son imza veritabanında olup olmadığına bakılır.
    - •İlk olarak, bu imzaların kara listede olup olmadığına bakılır
    - •Kara listede yer alıyorsa zararlıdır
    - •Sonuç CCS'nin yerel kurulumuna geri gönderilir
  - •İmza kara listede bulunmuyorsa en son beyaz listeye bakılır
    - •İmza beyaz listede bulunuyorsa güvenlidir
    - •Sonuç CCS'nin yerel kurulumuna geri gönderilir
    - •Yerel beyaz liste güncellenir
  - •FLS yukarıda ayrıntılı olarak anlatılanları hemen denetler.

- **•Sandbox ve Bulut Taraması Bölüm 2**
  İmza kara ve beyaz listelerde bulunmuyorsa 'tanınmayan' olarak kalır. CIS eş zamanlı olarak iki farklı fakat birbirini tamamlayıcı eylem uygular -

  (1) Tanınmayan dosya sandbox içinde çalıştırılacaktır ve

  (2) Comodo'nun Bulut Taramasına dosyanın zararlı olup olmadığını inceletecektir.

  - **•Tanınmayan dosyalar ve uygulamalar yerel olarak sandbox içine alınacaktır ve kullanıcı bilgilendirilecektir.**
  - **•Otomatik olarak sandbox içinde çalıştırılan uygulamalar 'Kısmen Kısıtlı' sınırlamalar ile çalıştırılır. Ayrıntı*: CIS farklı sınırlamalar sunar. Kısmen Kısıtlı, Kısıtlı, Limitli, Güvenilmeyen ('Kısmen Kısıtlı' varsayılan ayardır). Sandbox sınırlama seviyeleri Windows'un sağlayabileceği hakları arttırıp azaltarak uygulanır. Örneğin, 'Limitli' ayarı işletim sisteminin bazı sınırlamalarını uygular ve yönetici olmayan hesaptakine benzer bazı haklar tanır. Bu sınırlamalar Savunma+ sınırlamalarıyla daha da güçlendirilir.***
  - **•Otomatik olarak sandbox içine alınan uygulamalar arayüzden görüntülenmez ve değiştirilemez. Otomatik olarak sandbox içine alınan uygulamalar yalnızca CIS tarafından 'güvenli' olarak tanınırsa kaldırılabilir (yukarıdaki koşullara bakın).**
  - •Tanınmayan dosyalar eş zamanlı olarak Comodo'nun Anında Kötücül Yazılım İnceleme sunucularına gönderilerek ek denetimlerden geçirilir:
    - •İlk olarak dosyalar sunucuda Antivirüs taramasından geçirilir.

•Taramada kötü niyetli olarak saptanırsa zararlı olarak işaretlenir. Bu sonuç geri gönderilerek yerel ve genel kara liste güncellenir.

•Taramada kötü niyetli bulunmazsa sonraki inceleme aşamasına geçilir – davranış izlemesi.

•Davranış inceleme sistemi bulut tabanlı bir hizmettir ve dosyaların kötü niyetli olup olmadığını anlamada yardımcı olur. Sisteme gönderilen yürütülebilir dosyalar sanal ortamda çalıştırılarak denetlenir. Örneğin, çalıştırdığı işlemler, dosya ve kayıt defteri değişiklikleri, ağ etkinliği kaydedilir.

• Bu davranışlar kötü niyrtli bulunursa dosya imzası kara listeye eklenir.

•Bu davranışlar kötü niyetli bulunmazsa beyaz listeye eklenir.

•Her iki durumda da, sonuçlar kısa süre içerisinde CIS kurulumunuza geri gönderilir. Yürütülebilir temiz ise çalıştırılmasına izin verilir (uygulama bir sonraki çalışmasında sandbox içine alınmaz). Kötü niyetli ise karantinaya alınır veya silinir.

•Bu sonuç ayrıca genel beyaz ve siyah listeleri de günceller böylece tüm CIS kullanıcıları bundan faydalanır.

Sandbox – Diğer notlar

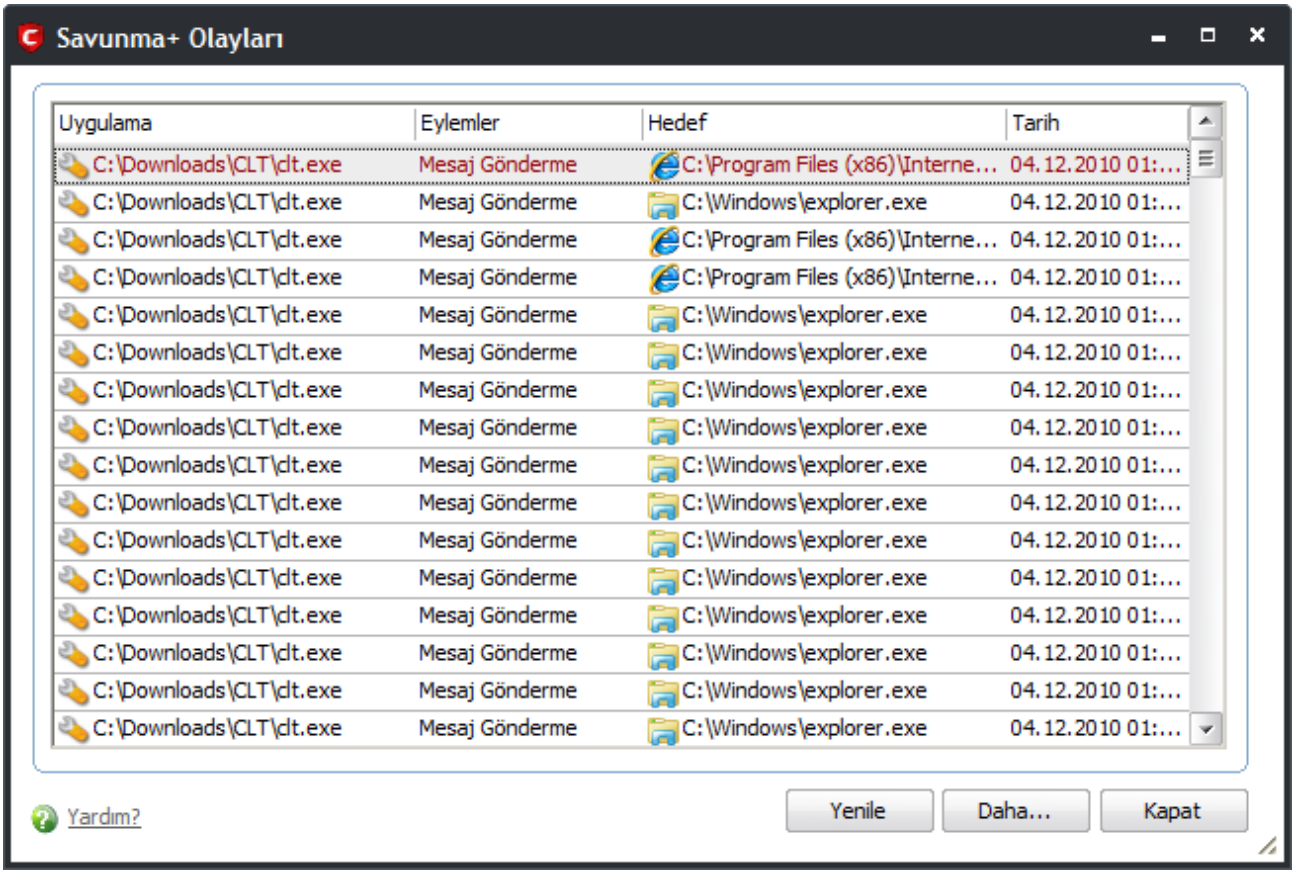
- Uygulamalar otomatik olarak sandbox içine CIS tarafından veya Her zaman Sandbox özelliği kullanılarak alınabilir.
- **Sandbox içinde çalışan bir uygulamanın çalıştırdığı diğer uygulamalarda ne olursa olsun sandbox içinde çalıştırılır.**
- **Kullanıcı uygulamayı sandbox içinde çalışmaya ayarlarsa bu uygulamanın yürüttüğü uygulamalarda sandbox içinde çalıştırılır.**
- **Sandbox sınırlama seviyelerinin yanı sıra Savunma+ aşağıdaki kısıtlamaları da uygular. Sandbox içine alınan uygulama şunları yapamaz:**
  - Sandbox dışındaki uygulamaların belleğine erişemez
  - Korunan COM arabirimlerine erişemez
  - Tuş kaydedemez veya ekran yakalayamaz
  - Windows kancaları yapamaz
  - Korunan kayıt defteri anahtarlarını değiştiremez (sanallaştırma devre dışı ise)
  - Korunan dosyaları ve klasörleri değiştiremez (sanallaştırma devre dışı ise).

Sandbox hakkında daha fazla bilgi için aşağıdaki bölümlere bakın:

- **Her zaman Sandbox**
- **Sandbox içinde Program Çalıştır**
- **Sandbox Ayarları**

4.2 Savunma+ Olaylarını Göster

Savunma+ bileşeninin Bilgisayar Güvenlik İlkeri bölümündeki kurallara göre uyguladığı eylemlerin raporlarını gösterir.



Sütun Açıklamaları

•Uygulama – Olaya neden olan uygulama.

•Etiketler – Dosya tarafından tetiklenen eylem.

•Hedef – Hedef dosyanın konumunu gösterir.

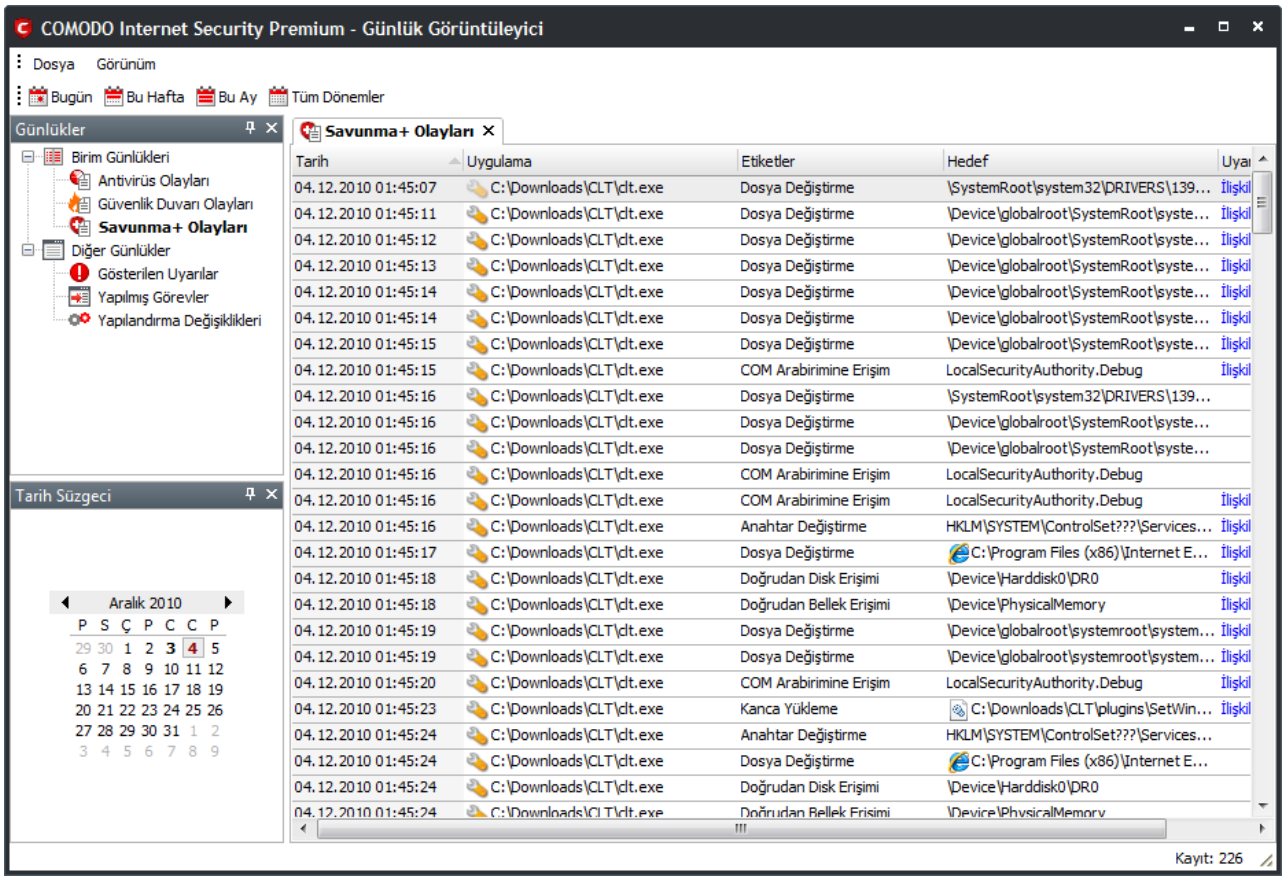
•Tarih/Saat – Erişim girişiminin gerçekleştiği tarih ve saati gösterir.

- **Listeyi güncellemek için Yenile düğmesine tıklayın.**
- **Comodo Internet Security Günlük Görüntüleyicisini açmak için 'Daha…' düğmesine tıklayın.**

Günlük Görüntüleyici Bileşeni

Tüm tutulmuş günlüklerin geçmişini iki kategoride tutar: Birim Günlükleri ve Diğer Günlükler.

Ayrıca belirli süzgeçler ile raporları kişisel günlük dosyalarına çıkartmanıza da olanak sağlar.



Günlük Görüntüleyici Bileşeni üç bölüme ayrılmıştır. Üst panelde zaman süzgeçleri, sol panelde günlük türü ve sağ panelde seçili ölçütlere uygun olan günlük olayları bulunur.

Günlük Dosyalarının Süzülmesi

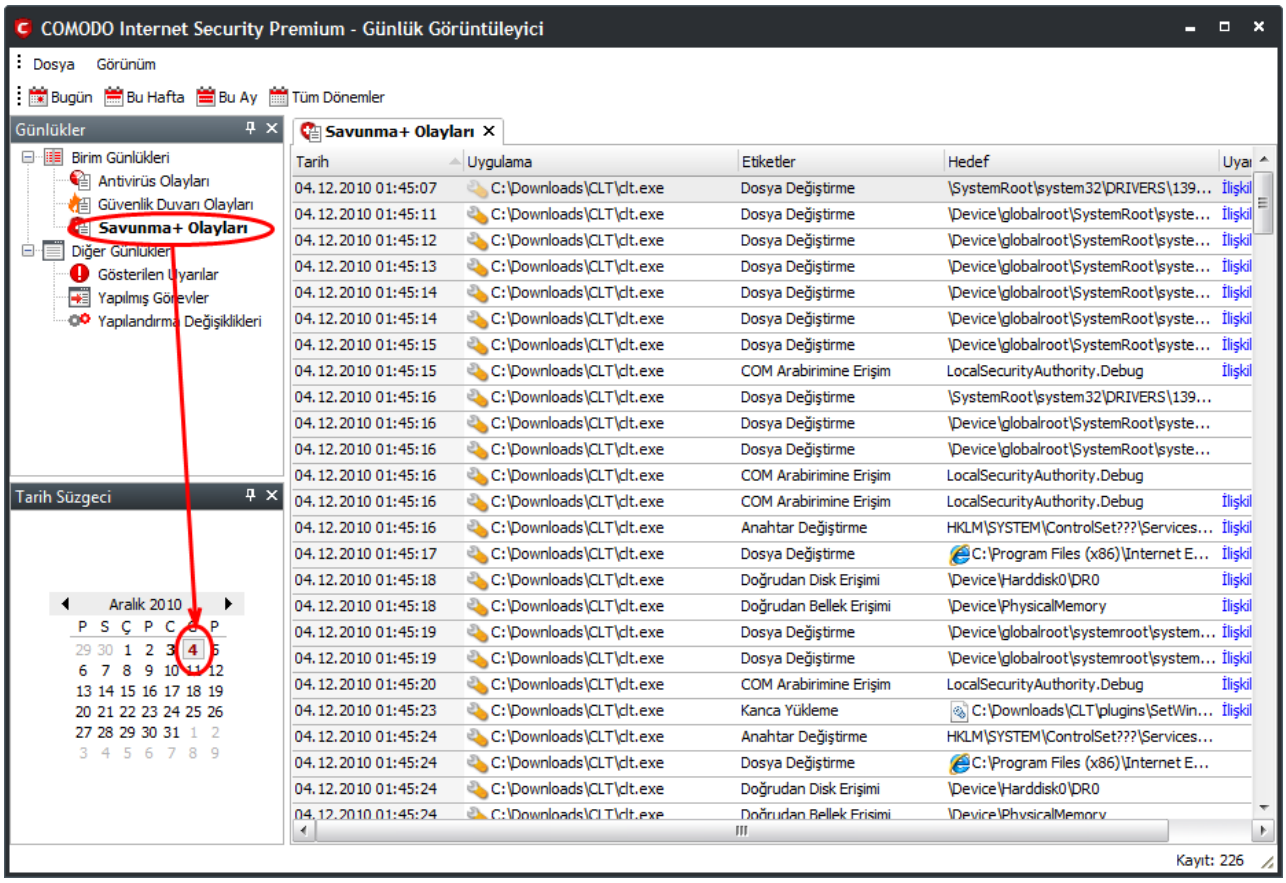
Comodo Internet Security günlük olaylarının belirli süzgeçlere göre gösterilmesine izin verir.

Zaman Süzgeçleri:

Zaman süzgeçleri üst panelde bulunur ve bunlardan biri seçildiğinde sağ panelin görünüşünü değiştirir:

- **Bugün** – Bugün gerçekleşen olayları gösterir.
- **Bu Hafta** – Bu hafta gerçekleşen olayları gösterir.
- **Bu Ay** – Bu ay gerçekleşen olayları gösterir.

Tüm Dönemler – CIS kurulumundan veya son günlük temizlemesinden sonraki tüm olayları gösterir.



Not: Sağ panelin içeriği CIS bileşenlerine göre farklılık gösterebilir.

Kullanıcı Tanımlı Süzgeçler:

Aşağıdaki tablo bulunan süzgeçleri ve onların anlamlarını gösterir:

Bulunan Süzgeçler – Birim Günlükleri		
Antivirüs Süzgeçleri	**Güvenlik Duvarı Süzgeçleri**	**Savunma+ Süzgeçleri**
Tarih – Seçili tarihteki olayları gösterir	**Tarih** - Seçili tarihteki olayları gösterir.	**Tarih** - Seçili tarihteki olayları gösterir.
Konum – Seçili konumdaki olayları gösterir	**Uygulama –** Olaya neden olan uygulamayı gösterir	**Uygulama -** Olaya neden olan uygulamayı gösterir
Zararlı Adı – Zararlı adına uygun olayları gösterir	**Eylem** – Gerçekleştirilen eyleme uygun olayları gösterir	**Eylem** - Gerçekleştirilen eyleme uygun olayları gösterir

Bulunan Süzgeçler – Birim Günlükleri		
Eylem - Gerçekleştirilen eyleme uygun olayları gösterir	**Yön** – Bağlantının yönüne uygun olayları gösterir	**Hedef Adı –** Hedef uygulamaya ilişkin olayları gösterir
Durum - Gerçekleştirilen eylemin durumuna uygun olayları gösterir. 'Başarılı' veya 'Başarısız' olabilir.	**Protokol –** Belli protokole ilişkin olayları gösterir	**Uyarı** – Eylem sütununda 'Soruldu' görünen uyarıların yanında 'İlişkili Uyarı' adında bir bağlantı görünür. Bu bağlantı sizi 'Gösterilen Uyarılar' olay günlüğüne götürür
Uyarı - Eylem sütununda 'Soruldu' görünen uyarıların yanında 'İlişkili Uyarı' adında bir bağlantı görünür. Bu bağlantı sizi 'Gösterilen Uyarılar' olay günlüğüne götürür	**Kaynak IP adresi** - Belli IP adresinden gerçekleştirilen bağlantılara ilişkin olayları gösterir	
	Kaynak Portu - Belli porttan yapılan bağlantılara ilişkin olayları gösterir	
	Hedef IP adresi Belli IP adresinden gerçekleştirilen bağlantılara ilişkin olayları gösterir	
	Hedef Portu - Belli porttan yapılan bağlantılara ilişkin olayları gösterir	
	Uyarı - Eylem sütununda 'Soruldu' görünen uyarıların yanında 'İlişkili Uyarı' adında bir bağlantı görünür. Bu bağlantı sizi 'Gösterilen Uyarılar' olay günlüğüne götürür	

Özel Süzgeçlerin Oluşturulması

Özel Süzgeçler Gelişmiş Süzgeç arayüzü kullanılarak oluşturulabilir. Gelişmiş Süzgeç arayüzü günlük görüntüleyiciye sağ tıklayarak içerik menüsünden açılabilir.

- **'Gelişmiş Süzgeç' alanını açmak için Görünüm > Gelişmiş Süzgeç seçeneğine tıklayın.**

Veya

- **Olay panelinde sağ tıklayın ve 'Gelişmiş Süzgeç' seçin.**

'Gelişmiş Süzgeç' paneli üstte açılır.

Gelişmiş rapor süzgeç görünümü seçili bileşene göre farklılık gösterir.

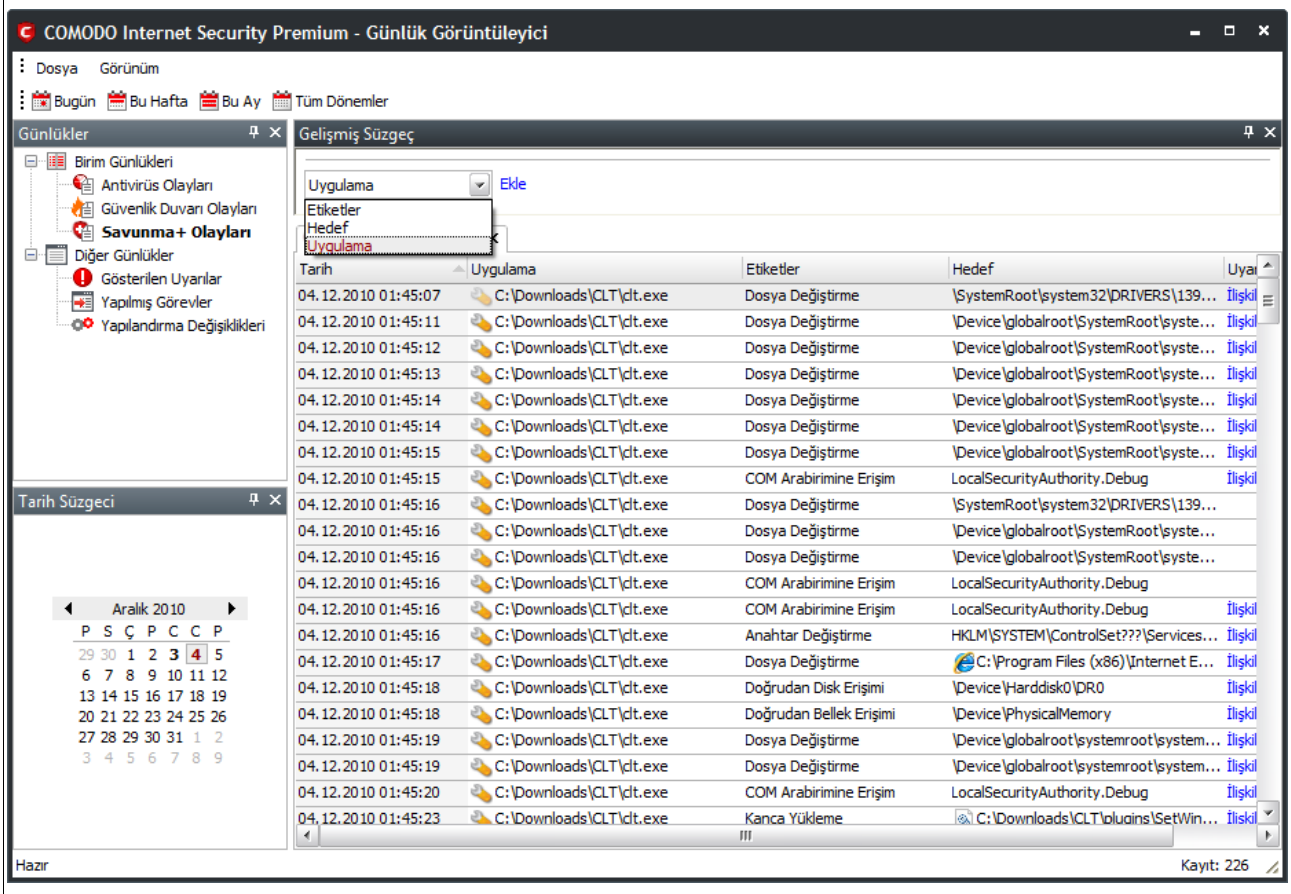
Savunma+ Olayları - Gelişmiş Süzgeçler

Savunma+ olayları için Gelişmiş Süzgeçlerin yapılandırılması

1. 'Görünüm > Gelişmiş Süzgeç' seçin
2. 'Birim Günlükleri' altından 'Savunma+ Olayları' seçin

Ekleyebileceğiniz 3 süzgeç kategorisi ve her bir kategori altında farklı parametreler bulunmaktadır.

3. 'Ekle' düğmesini kullanarak süzgeçler ekleyebilirsiniz.



Aşağıdakiler 'Ekle' açılır menüsünde bulunmaktadır:

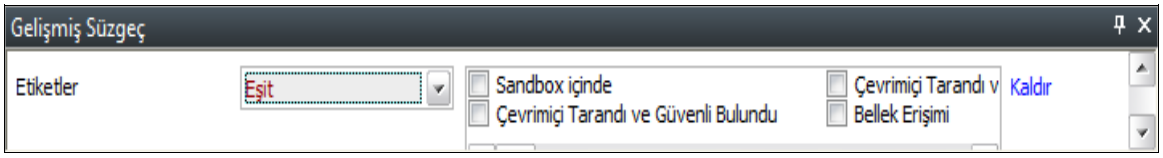
i. **Uygulama**: Açılır liste ve metin alanı görünür.

a) Açılır listeden 'İçeriyor' veya 'İçermiyor' seçeneğini seçin.

b) Süzülmesi gereken metini gir.

Süzülen girdiler doğrudan altta görünür.

i. **Etiketler**: Açılır liste ve bulunan seçilebilir etiket süzgeçlerini gösterir.



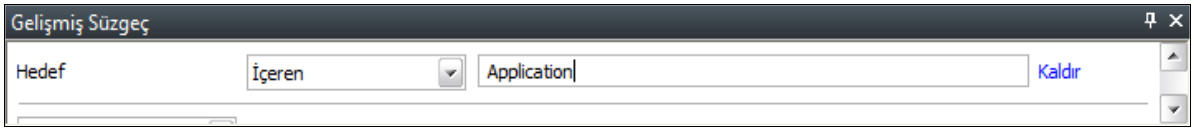
a) Açılır listeden 'Eşit' veya 'Eşit Değil' seçin. ‘Eşit Değil’ seçeneği seçimi tersine çevirir.

b) Aramayı geliştirmek için değişkenlerin kutularını işaretleyebilirsiniz. Bulunan değişkenler şunlardır:

- Sandbox içinde
- Çevrimiçi Tarandı ve Güvenli Bulundu
- Çevrimiçi Tarandı ve Kötü Amaçlı Bulundu
- Bellek Erişimi
- İşlem Oluşturma
- İşlem Sonlandırma
- Anahtar Değiştirme
- Dosya Değiştirme
- Doğrudan Bellek Erişimi
- Doğrudan Disk Erişimi
- Direct Keyboard Access
- Doğrudan Klavye Erişimi
- Sürücü Yükleme
- Mesaj Gönderme
- Kanca Yükleme
- COM Arabirimine Erişim
- Görüntü Yürütmesi
- DNS/RPC İstemcisi Erişimi
- Savunma+ Kipi Değiştirme
- Kabuk kodu Enjeksiyonu
- Dosya Engelleme
- Şüpheli
- Kanca
- Uyarı Bastırıldı

Süzülen girdiler doğrudan altta görünür.

i. **Hedef**: Açılır liste ve metin alanı görünür.



a) Açılır listeden 'İçeriyor' veya 'İçermiyor' seçeneğini seçin.

b) Süzülmesi gereken metini girin.

Süzülen girdiler doğrudan altta görünür.

Not: 'Gelişmiş Süzgeç' bölümünde birden fazla süzgeç eklenebilir. Eklenmiş bir süzgeci 'Kaldır' düğmesine tıklayarak kaldırabilirsiniz.

Diğer Günlükler – Gelişmiş Süzgeçler

Ayrıntılı bilgi için Antivirüs Görevleri > Antivirüs Olaylarını Göster > Günlük Görüntüleyici > Özel Süzgeçlerin Oluşturulması > Diğer Günlükler – Gelişmiş Süzgeçler bölümüne bakın.

Tarih Süzgeci

Tarih süzgeci işlevi hakkında daha fazla bilgi için buraya tıklayın.

Günlüklerin HTML dosyasına Çıkartılması

Günlük dosyalarının çıkartılması arşivleme ve sorun giderme açısından kullanışlıdır. İki yolla dosyaya çıkartma yapılabilir. İçerik menüsü veya 'Dosya' menüsü kullanılarak çıkartılabilir.

i. **Dosya Menüsü**

1. Çıkartılmasını istediğiniz olayları seçin.
2. Dosya menüsünden 'Çıkart' düğmesine tıklayın.
3. Dosyanın kaydedileceği konumu seçin ve kaydedin.

- **Güvenlik Duvarı Olayları** – Panelin sağ tarafında görüntülenen Güvenlik Duvarı olaylarını çıkartır.
- **Savunma+ Olayları** - Panelin sağ tarafında görüntülenen Savunma+ olaylarını çıkartır..
- **Antivirüs Olayları** - Panelin sağ tarafında görüntülenen Antivirüs olaylarını çıkartır..

1. Dosyanın kaydedileceği konumu seçin ve 'Kaydet' düğmesine tıklayarak kaydedin.

i. **İçerik Menüsü**

1. Günlük penceresinde sağ tıklayarak görüntülenen olayları HTML dosyasına çıkartın.

Günlük penceresinde sağ tıklayarak görüntülenen olayları HTML dosyasına çıkartabilirsiniz.

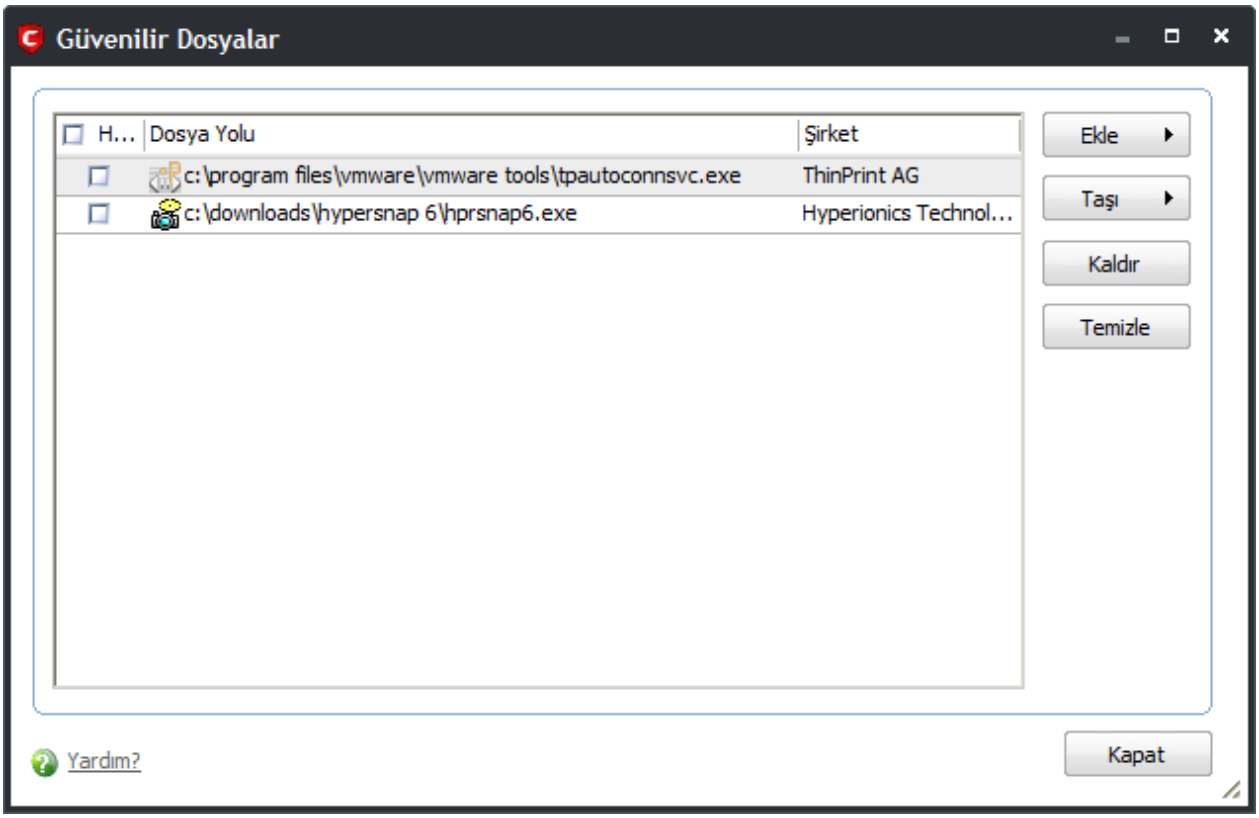
4.3 Güvenilir Dosyalar

Savunma+ Comodo'nun güveni listesine ek olarak kişisel güvenli listenizi oluşrumanıza da olanak sağlar.

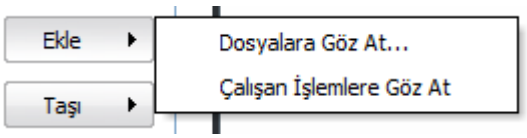
Güvenilir Dosyalar listesine eklenenler otomatik olarak Savunma+ tarafından güvenilir olarak sayılır. Yürütülebilir bir dosya Savunma+ güvenli listesi tarafından bilinmiyorsa bu yürütülebilir ve tüm etkin bileşenleri çalıştıklarında

Savunma+ uyarısı verir. Tabii ki, uyarıdan ‘Güvenilir Uygulama olarak say’ seçeneğini seçebilirsiniz fakat bunun daha uygun yolu dosyaların tümünün bulunduğu klasörü ‘Güvenilir Dosyalar’ listesine eklemektir.

'Tanınmayan Dosyalar' bölümünden ‘Taşı’ düğmesini kullanarak istediğiniz dosyaları güvenilir dosyalara

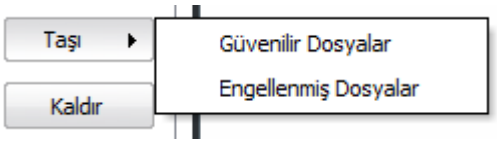


aktarabilirsiniz.



Dosyaları veya işlemleri bu bölüme elle eklemek için ‘Ekle’ düğmesine tıklayın:

‘Taşı’ düğmesini kullanarak bu listedeki dosyaları diğer listelere (Tanınmayan Dosyalara veya Engellenmiş Dosyalara) aktarabilirsiniz:



Güvenilir Dosyalar listesinden bir girdi kaldırmak için

•‘Kaldır’ düğmesini kullanarak dosyayı bu listeden kaldırabilirsiniz.

Geçersiz girdileri kaldırmak için (bilgisayardan kaldırdığınız veya bilgisayarda bulunmayan programlar/dosyalar)

•'Temizle' düğmesine tıklatın.

4.4 Tanınmayan Dosyalar

Comodo güvenlik denetimlerinde güvenli olarak tanımlanamayan dosyalar 'Tanınmayan Dosyalar' bölümüne eklenir ve incelenmesi için Comodo sunucularına gönderilir. Değiştirilmiş yürütülebilrilerler de bu bölüme taşınırlar.

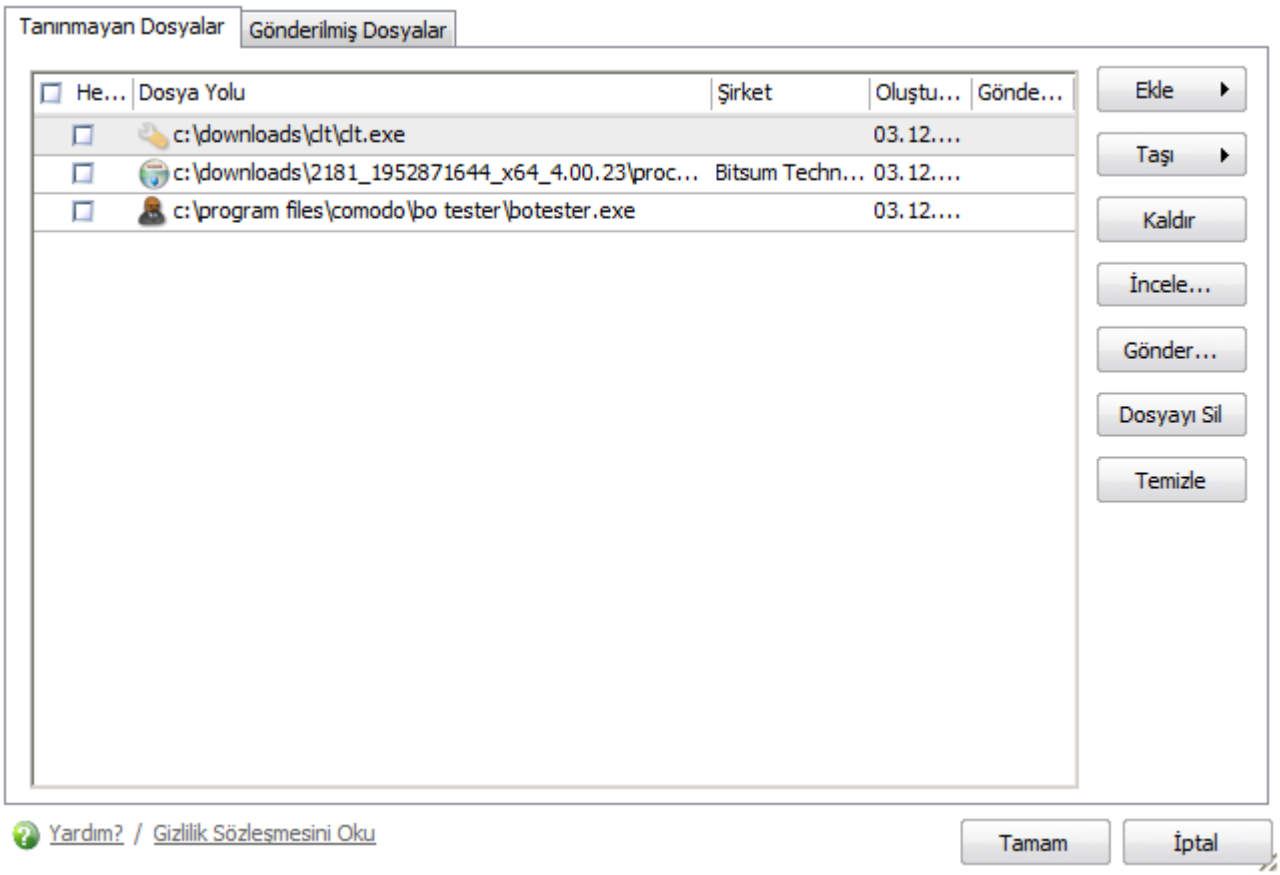
'Tanınmayan Dosyalar' bölümü özellikle Savunma+ 'Temiz BS' kipindeyken önemlidir. Temiz BS kipinde, 'Tanınmayan Dosyalar' temiz olarak sayılmaz. Daha fazla bilgi için Savunma+ Ayarları bölümündeki 'Temiz BS Kipi'.

'Tanınmayan Dosyalar' bölümü kullanıcıya şu olanakları sağlar:

- **Dosyaları 'Taşı' düğmesini kullanarak güvenli ise 'Güvenilir Dosyalar', şüpheli ise 'Engellenmiş Dosyalar' bölümlerine taşıyabilirsiniz.**
- **'İncele...' özelliği ile Comodo ana güvenli listesinden dosya imzasına bakabilirsiniz.**
- **'Gönder' düğmesi ile dosyaları analiz için Comodo sunucularına göndererek dosya gönderim işlemini başlatabilirsiniz.**
- **Dosyaları elle, incelenmek üzere Comodo sunucularına gönderilmesi için gönderim listesine ekleyebilirsiniz.**
- **'Temizle' düğmesi ile listedeki geçersiz girdileri kaldırabilirsiniz.**
- **'Dosyayı Sil' düğmesi ile dosyayı sistemden silebilirsiniz.**

Tanınmayan Dosyalar arayüzüne erişmek için

•Savunma+ Görevleri > Tanınmayan Dosyalar.



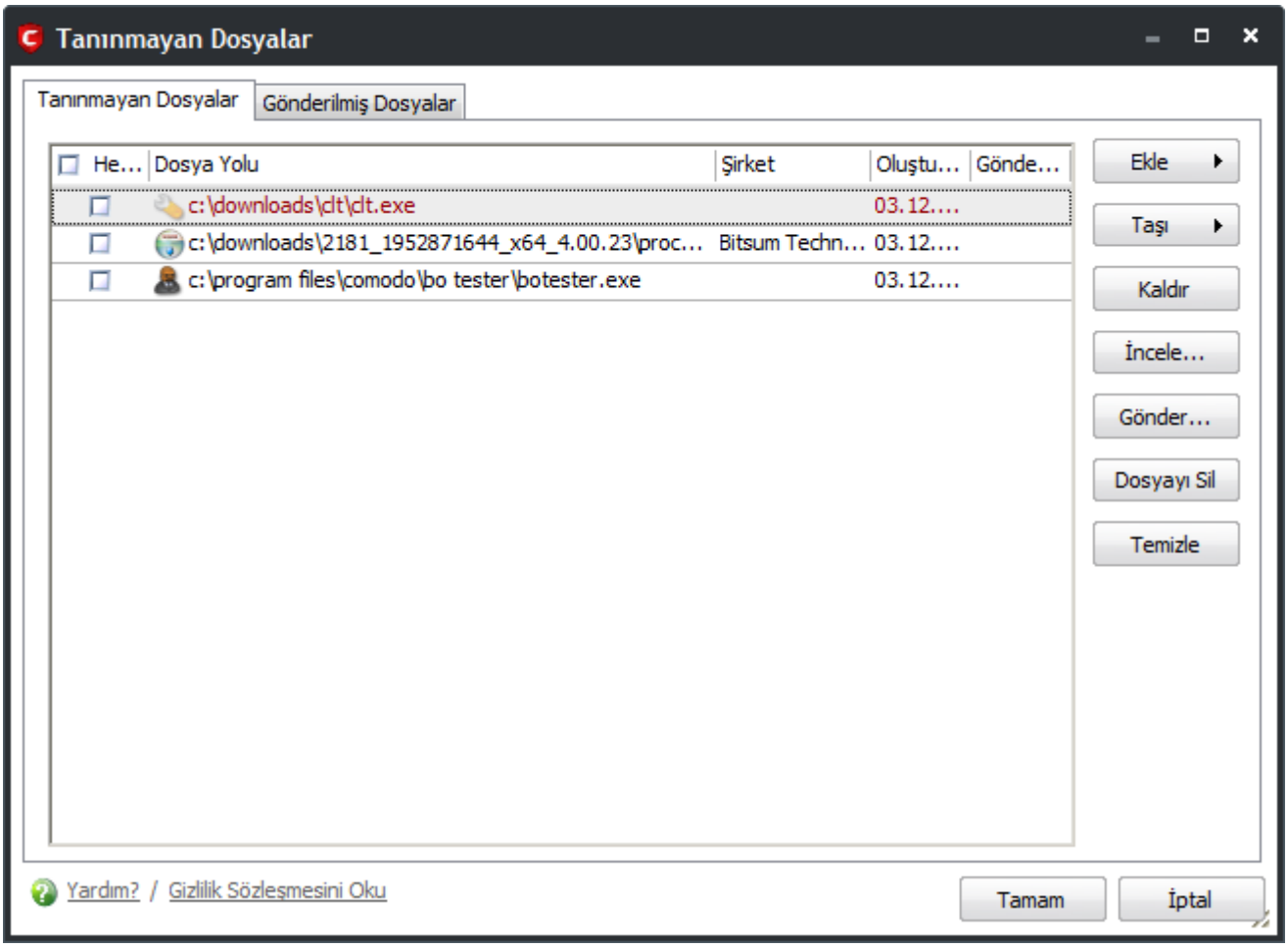
Bu bölüm iki sekmeden oluşur:

•Tanınmayan Dosyalar – Savunma+ tarafından şüpheli olarak belirlenen dosyaların listesi ve elle eklenen dosyalar.

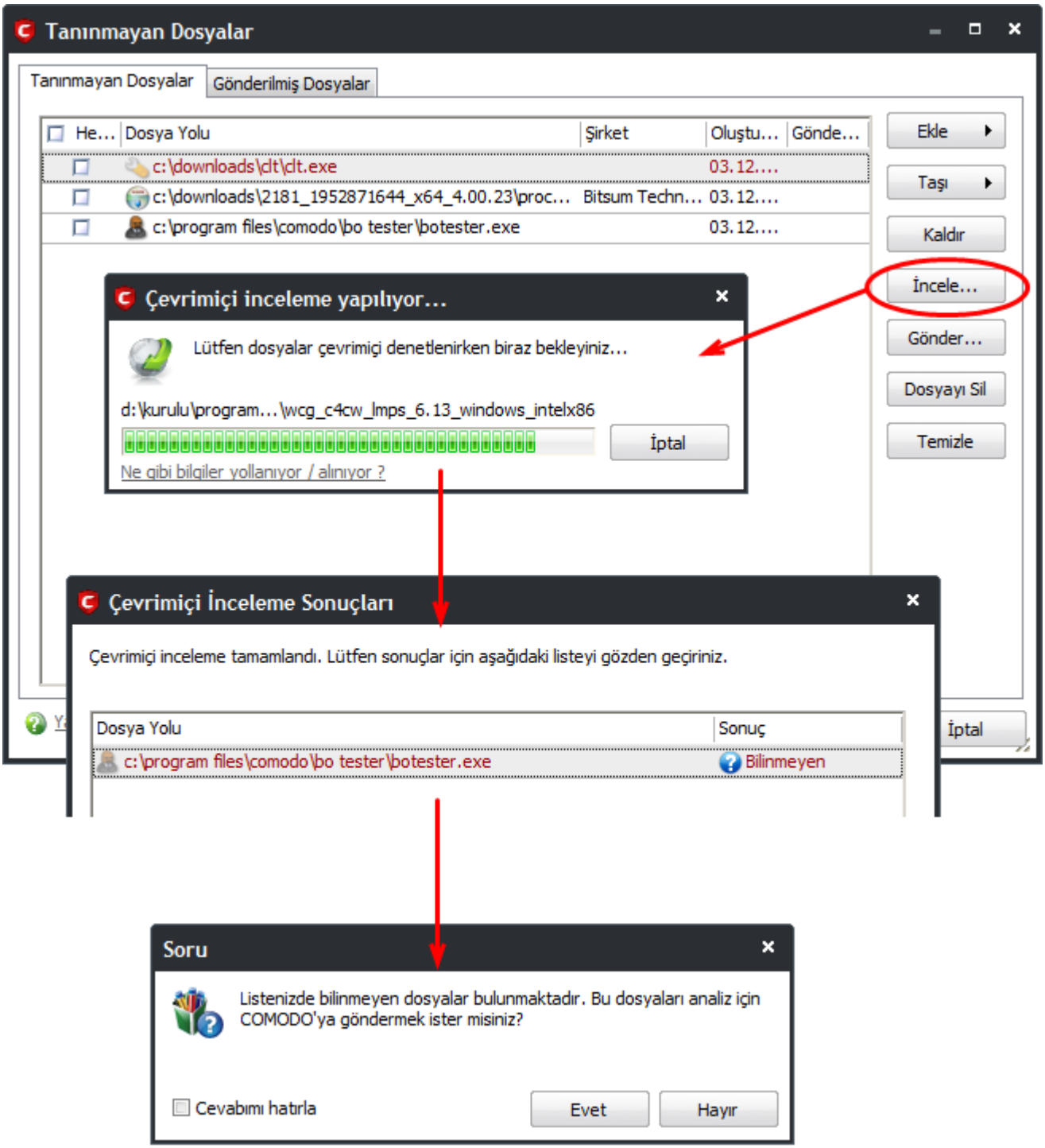
•Gönderilmiş Dosyalar - Analiz için Comodo'ya gönderilen dosyalar.

4.4.1 Tanınmayan Dosyalar

Savunma+ tarafından şüpheli olarak belirlenen dosyaların listesi ve elle eklenen dosyalar. Analiz için dosyaları Comodo'ya gönderebilirsiniz.



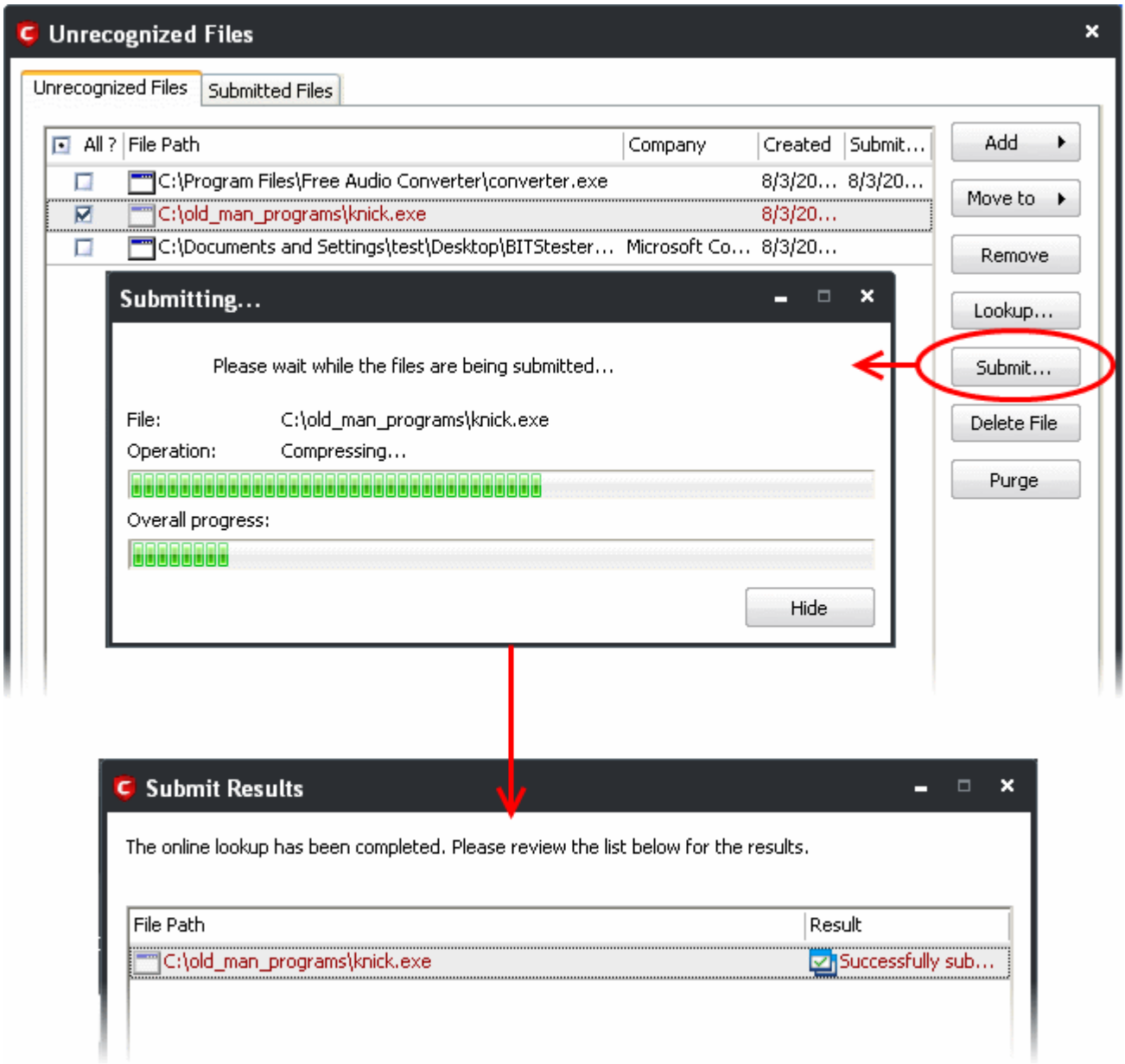
'İncele...' özelliği ile Comodo ana güvenli listesinden dosya imzasına bakabilirsiniz. İmza bulunmuyorsa şu seçenekler size sunulur:



Dosya gönderildikten sonra güvenlik tehdidi oluşturup oluşturmadığına Comodo teknisyenleri tarafından bakılır. Güvenli ise beyaz listeye eklenir.

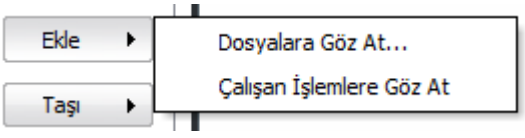
Dosyaları elle Comodo'ya göndermek için

Dosyayı seçin ve 'Gönder' düğmesine tıklayın.

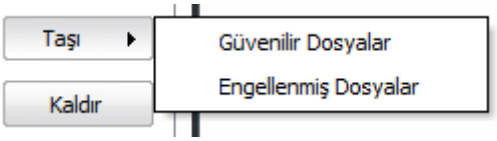


Gönderim sırasında ilerleme çubuğu ve tamamlandığında sonuç penceresi görünür.

'Ekle' düğmesini kullanarak elle bu bölüme dosya ekleyebilirsiniz:

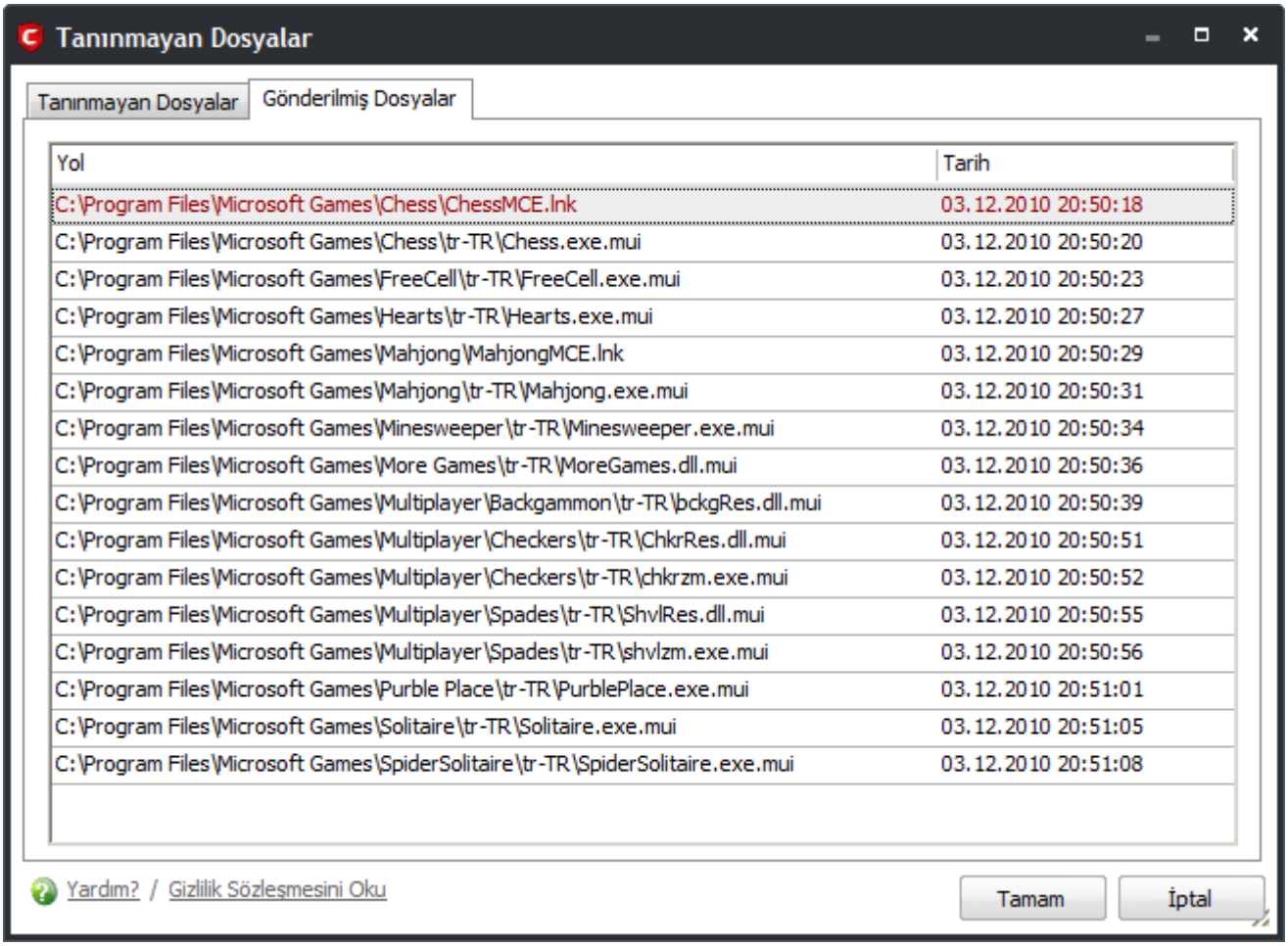


'Taşı' düğmesi ile dosyaları diğer listelere aktarabilirsiniz.:



4.4.2 Gönderilmiş Dosyalar

Savunma+ Görevleri > Tanınmayan Dosyalar ve Antivirüs görevleri > Dosyaları Gönder bölümlerinden analiz için

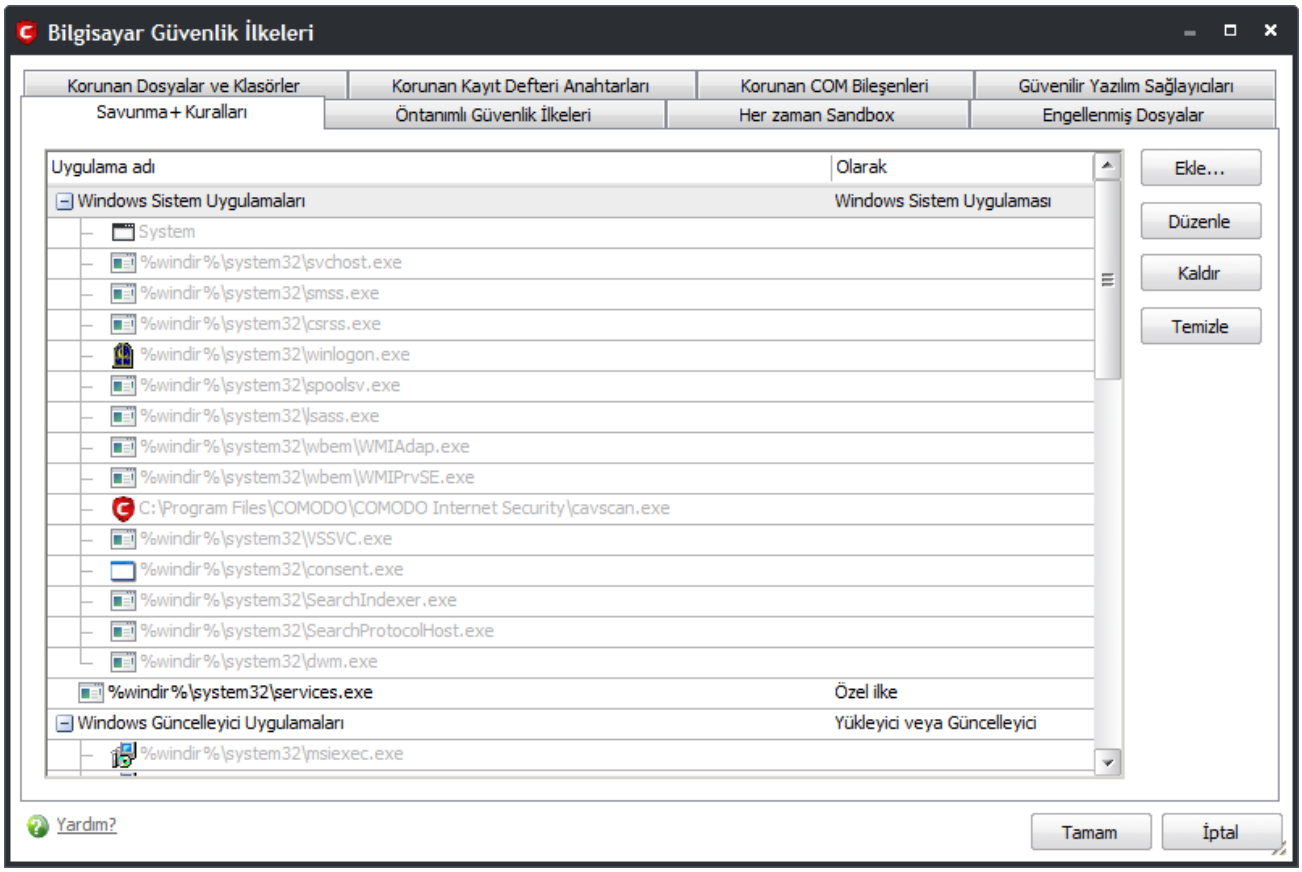


Comodo'ya gönderilen dosyaların listesini içerir.

4.5 Bilgisayar Güvenlik İlkeleri

Bilgisayar Güvenlik İlkeleri bölümü kullanıcıların uygulamalara uygulanan Savunma+ güvenlik ilkelerini görüntülemesine ve düzenlemesine, Öntanımlı Güvenlik İlkeleri, korunan Dosyalar ve Klasörler, Kayıt Defteri Anahtarları, COM Arabirimleri, dosyaların her zaman sandbox içinde çalıştırılmasını, Güvenilir Yazılım Sağlayıcıları tanımlamasına vs. olanak sağlar.

Bilgisayar Güvenlik İlkeleri bölümüne erişmek için Savunma+ Görevleri > Bilgisayar Güvenlik İlkeleri bölümünü kullanın.



Bilgisayar Güvenlik İlkeleri bölümü aşağıdaki sekmeleri içerir:

•Bilgisayar Güvenlik İlkeleri

•Öntanımlı Güvenlik İlkeleri

•Her zaman Sandbox

•Engellenmiş Dosyalar

•Korunan Dosyalar ve Klasörler

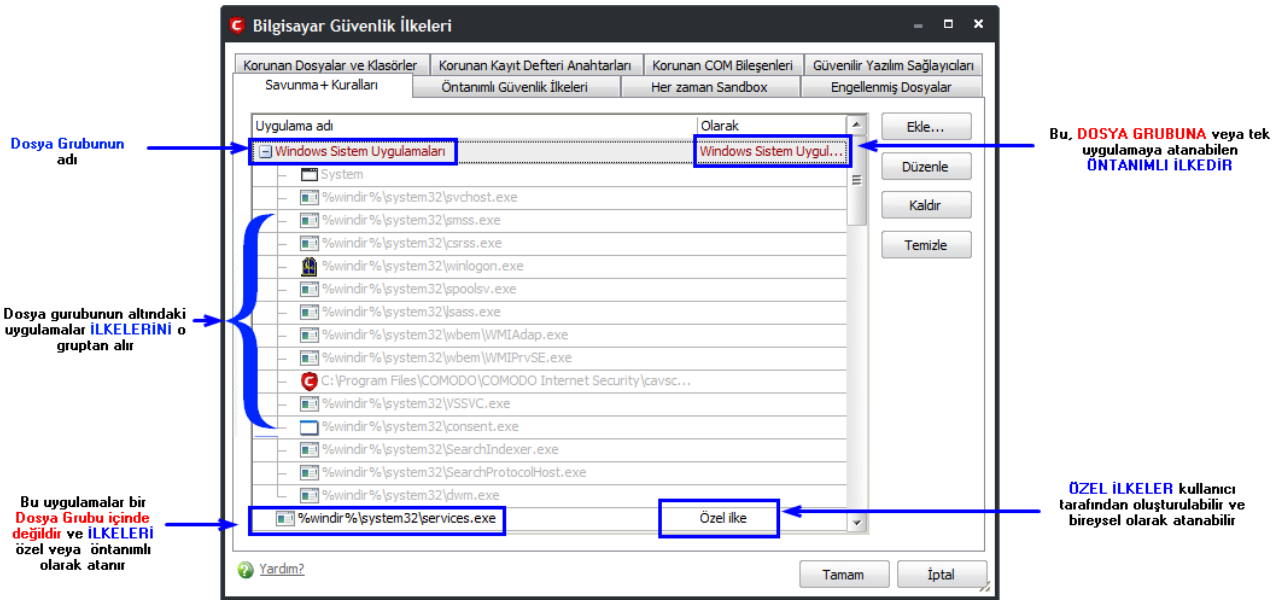
•Korunan Kayıt Defteri Anahtarları

•Korunan COM Arabirimleri

•Güvenilir Yazılım Sağlayıcıları

4.5.1 Bilgisayar Güvenlik İlkeleri

Bilgisayar Güvenlik İlkeleri sekmesi sisteminizde kurulu değişik uygulama gruplarını ve onlara uygulanan güvenlik ilkelerini listeler. Seçili uygulamalara uygulanan ilkeleri değiştirebilir ve ayrıca onlara özel ilkeler uygulayabilirsiniz.



İlk sütun, **Uygulama Adı**, uygulama adını veya dosya grubunun adını gösterir. Dosya grubuna uygulanan bir ilke o grup altındaki tüm dosyalara uygulanır. İkinci sütun, **Olarak,** uygulanan ilkenin adını gösterir.

Genel Gezinti:

- **Ekle... – Listeye yeni uygulama ekledikten sonra ona ilke oluşturmanıza olanak salar. Ayrıca bakınız 'Savunma+ Güvenlik İlkesi Oluşturulması veya Değiştirilmesi'.**
- **Düzenle... – Seçili uygulamanın ilkesini değiştirebilirsiniz. Ayrıca bakınız 'Savunma+ Güvenlik İlkesi Oluşturulması veya Değiştirilmesi'.**
- **Kaldır – Bulunan ilkeyi siler.**

Not: Gruplardaki uygulamaları bu arayüzü kullanarak kaldıramazsınız. Bunun için 'Gruplar' arayüzünü kullanmalısınız.

- **Temizle – Listedeki uygulamaların yollarını denetler ve geçersiz olanları kaldırır.**

Kullanıcılar ilkeleri önceliğe göre *yeniden sıralamak* için sürükle bırak ile uygulamaları veya dosya gruplarını aşağı yukarı taşıyabilirler. Grup içindeki dosyalar için 'Gruplar' arayüzünü kullanabilirsiniz.

Savunma+ Güvenlik İlkesi Oluşturulması veya Değiştirilmesi

Uygulamanın Savunma+ ilkesini tanımlamaya başlamak için

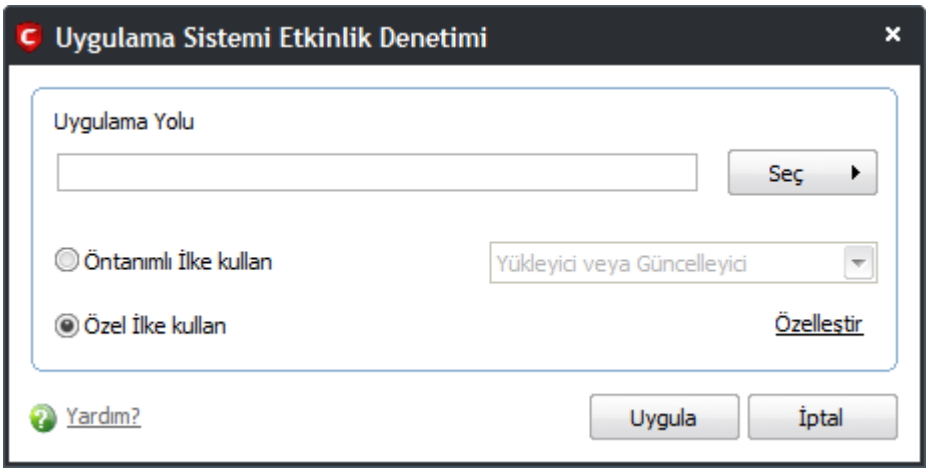
(1) İlke uygulamak istediğiniz uygulamayı veya dosya grubunu seçin.

(2) Güvenlik ilkesini bu uygulama için yapılandırın.

(1) İlke uygulamak istediğiniz uygulamayı veya dosya grubunu seçin

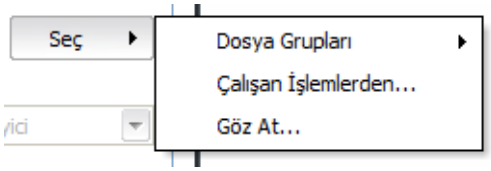
Listede olmayan bir uygulamaya ilke tanımlamak istiyorsanız ‘Ekle’ düğmesine tıklayın.

Bu aşağıda görünen 'Uygulama Sistem Etkinlik Denetimi' arayüzünü açar.



Listede bulunmayan yeni bir uygulama için ilke tanımladığınız için ‘Uygulama Yolu’ boştur.

‘Seç’ düğmesine tıklayın.



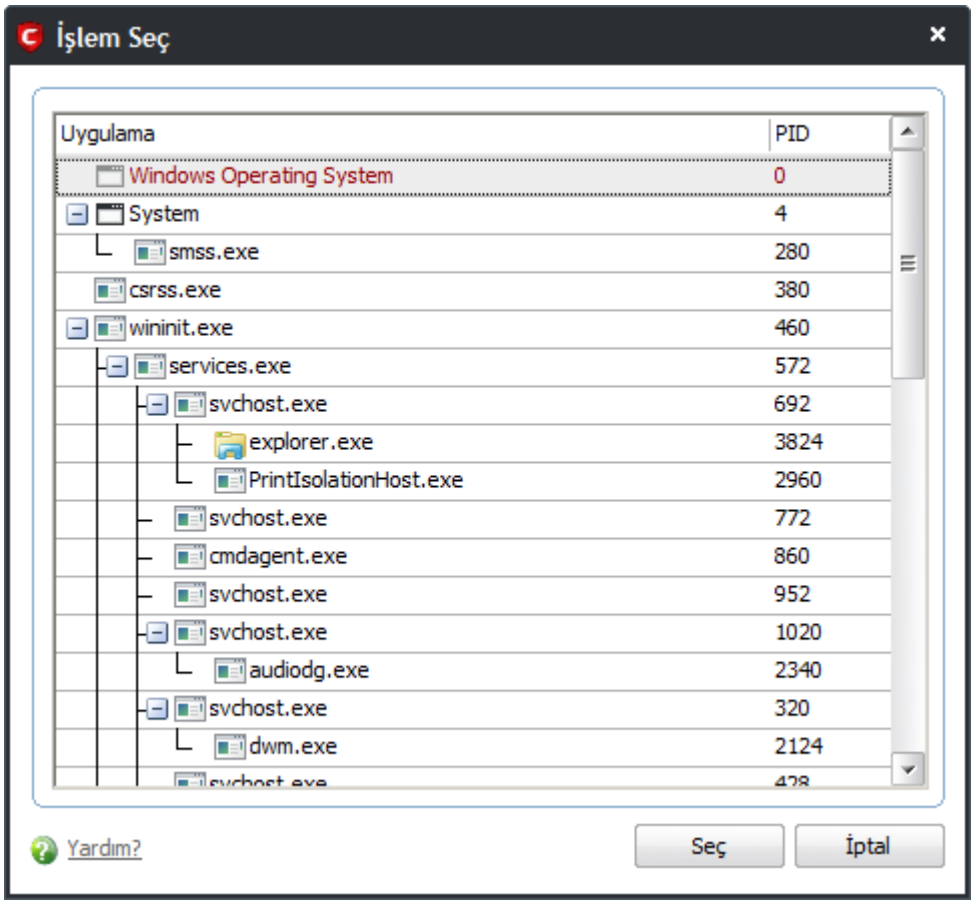
3 değişik yöntemle seçim yapabilirsiniz. Dosya Grupları; Çalışan İşlemler ve Göz At.

1. Dosya Grupları – Önceden tanımlanmış dosya gruplarından seçim yapabilirsiniz.

'Gruplar’ arayüzüne aşağıdaki şekilde erişebilirsiniz:

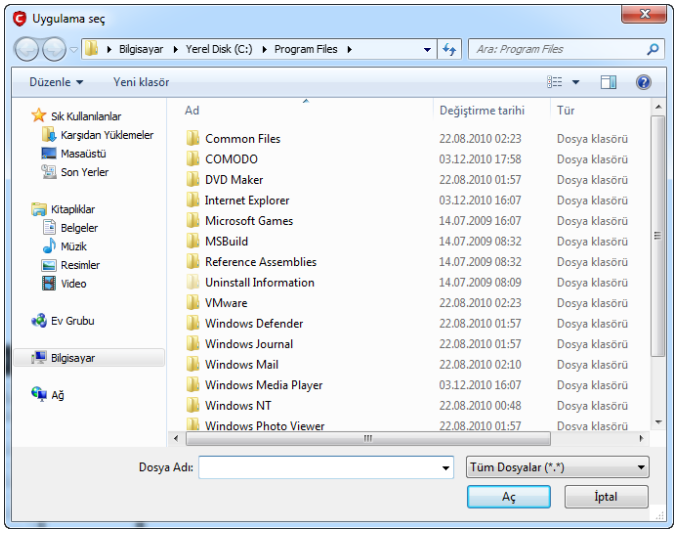
- **Savunma+ > Bilgisayar Güvenlik İlkeleri > Korunan Dosyalar ve Klasörler daha sonra ‘Gruplar…’ düğmesine tıklayın.**

1. Çalışan İşlemler – Sisteminizde çalışan işlemlerden seçim yapabilirsiniz.



Seçiminiz onaylamak için 'Seç' düğmesine tıklayın.

2. Göz At... - Uygula seç penceresinden istediğiniz uygulamayı bularak seçebilirsiniz.



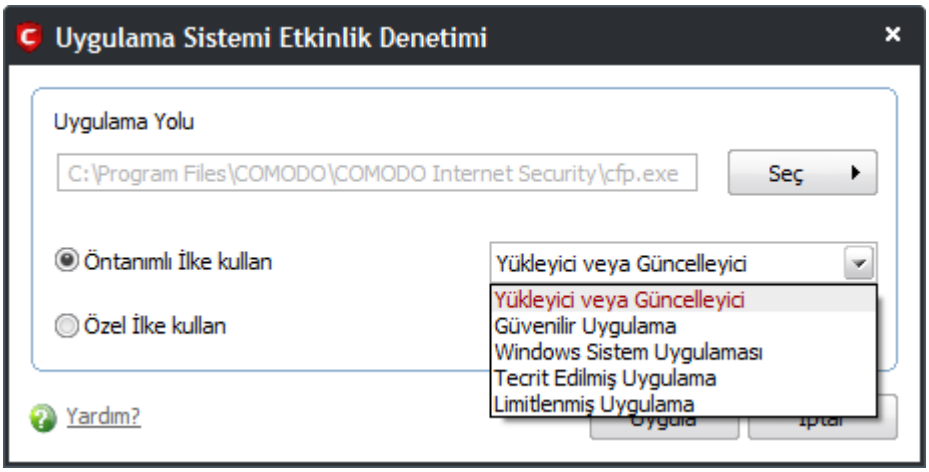
Aşağıdaki örnekte Opera web tarayıcısı gösterilmiştir.

Seçimden sonraki adım, uygulama kurallarının yapılandırılmasıdır.

(2) Güvenlik ilkesini bu uygulama için yapılandırın

Uygulamaya ilke tanımlamak için iki seçenek bulunmaktadır - Öntanımlı Güvenlik İlkesi Kullanmak veya Özel İlke Kullanmak.

1. Öntanımlı Güvenlik İlkesi Kullanmak – Öntanımlı ilkelerden birini hızlıcana hedef uygulamaya atayabilirsiniz. Aşağıdaki örnekte, 'Limitlenmiş Uygulama' seçilmiştir. Öntanımlı güvenlik ilkesi Bilgisayar Güvenlik İlkeleri arayüzünde 'Olarak' sütununda görünür.

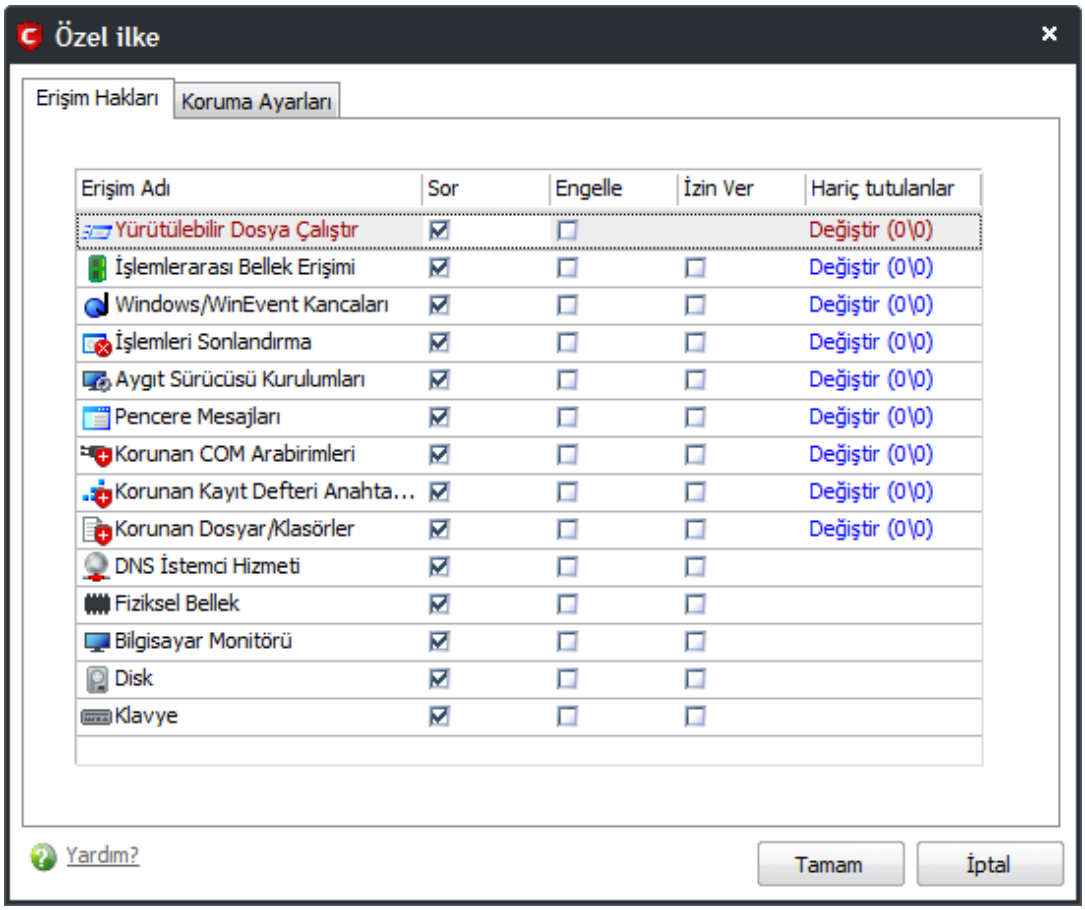


Not: Burada seçilen öntanımlı ilkeyi düzenlemek için 'Öntanımlı Güvenlik İlkeleri' arayüzünü kullanmalısınız. Daha esnek ilkeler oluşturmak istiyorsanız öntanımlı ilke yerine Özel İlke kullanmalısınız.

2. Özel İlke Kullanmak - Deneyimli kullanıcılar için tasarlanmıştır, **Özel İlke** seçeneği ilkeler üzerinde tam denetim sağlar. Özel İlke bölümünde iki temel yapılandırma alanı bulunur - Erişim Hakları ve Koruma Ayarları.

Basit olarak, 'Erişim Hakları' uygulamanın diğer işlemlere veya nesnelere ne yapabileceğini belirlerken 'Koruma Ayarları' uygulamaya diğer işlemler tarafından ne yapılabileceğini belirler.

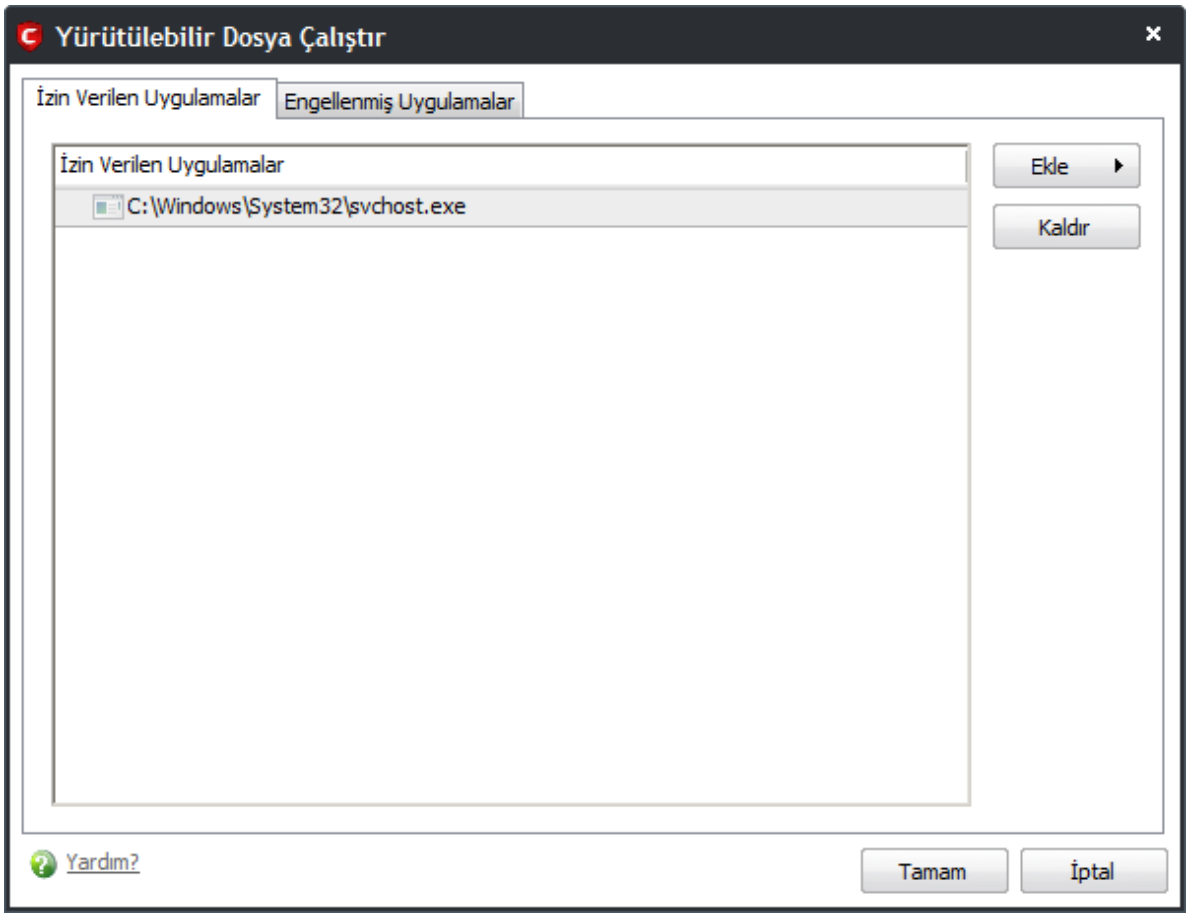
i. Erişim Hakları – Erişim Hakları arayüzü uygulamanın yürütebileceği etkinlikleri belirlemenize olanak sağlar.



Yukarıda listelenen Erişim Adlarının tanımları ve Sor, İzin Ver veya Engelle eylemlerinin her bir erişim adı için açıklamalarını görmek için buraya tıklayın.

'Sor', 'İzin Ver' veya 'Engelle' eylemlerinin hariç tutulanlarını yanlarındaki 'Değiştir' düğmesinden belirleyebilirsiniz.

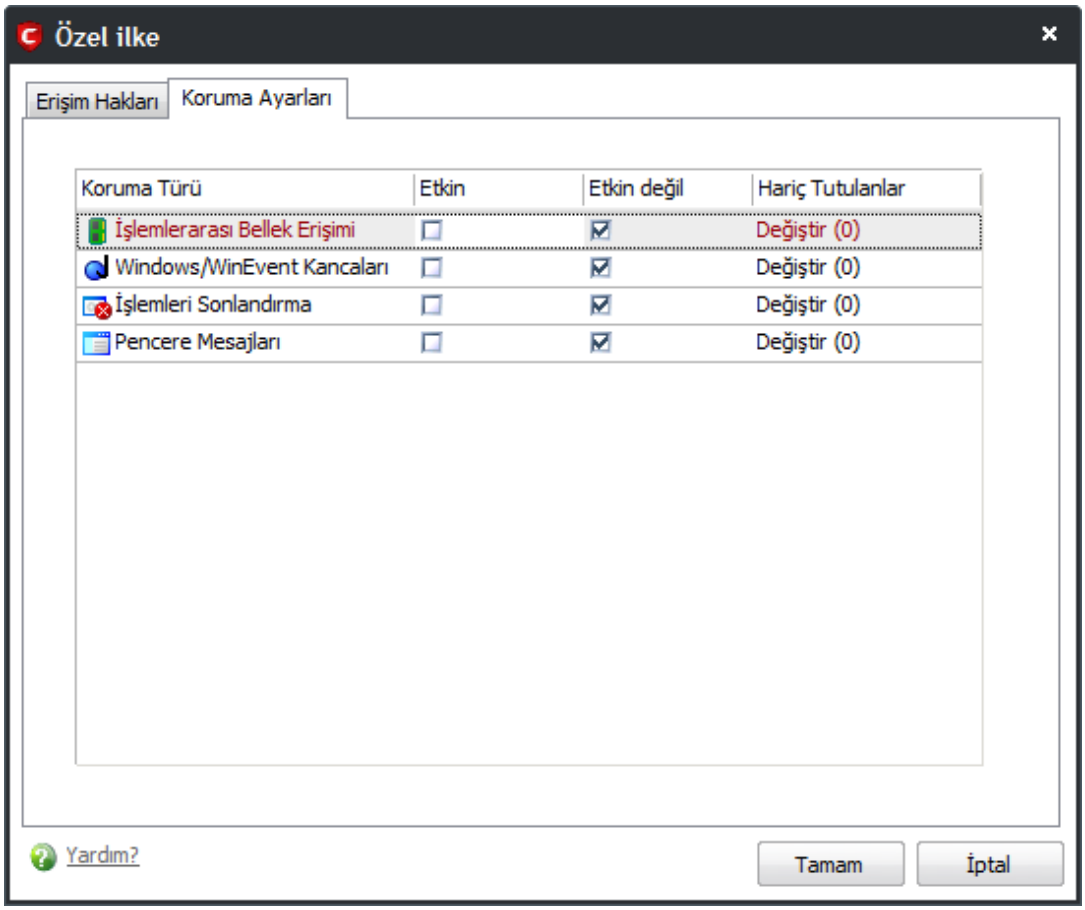
Hariç tutmak istediğiniz türe göre 'İzin Verilen Uygulamalar' veya 'Engellenmiş Uygulamalar' sekmelerinden birini seçin.



'Ekle' düğmesi ile uygulama veya dosya grubunu seçin. (Bulunan seçeneklerin açıklaması için buraya tıklayın)

Yukarıdaki örnekte, 'Yürütülebilir dosya çalıştır' için varsayılan eylem 'Sor' dur. Bu şu anlama gelir; 'Opera.exe' bir program yürütmeye çalışırsa Savunma+ bunun için izninizi isteyen bir uyarı gösterecektir. 'Değiştir' düğmesine tıklayarak 'oemig50.exe' uygulamasını 'İzin Verilen Uygulamalar' listesine ekleyerek bu kural için bu uygulamayı hariç tutabilirsiniz. Opera.exe şimdi 'oemig50.exe' uygulamasını uyarı vermeden yürütebilir fakat listede bulunmayan uygulamalar için uyarı çıkacaktır.

ii. Koruma Ayarları – Koruma ayarları uygulamanın veya dosya grubunun diğer uygulamaların etkinliklerine karşı nasıl korunacağını belirler. Bu korumalar 'Koruma Türü' olarak adlandırılır.



Uygulama veya dosya grubunu diğer uygulamaların etkinliklerine karşı izlemeye almak ve korumak için 'Etkin' işaretleyin veya izleme ve koruma dışı bırakmak için 'Etkin değil' kutusunu işaretleyin.

Yukarıda listelenen 'Koruma Türleri' tanımları için buraya tıklayın.

'Değiştir' düğmesine tıklayarak hariç tutulanları seçebilirsiniz.

1. Ayarları onaylamak için 'Uygula' düğmesine tıklayın.

4.5.2 Öntanımlı Güvenlik İlkeleri

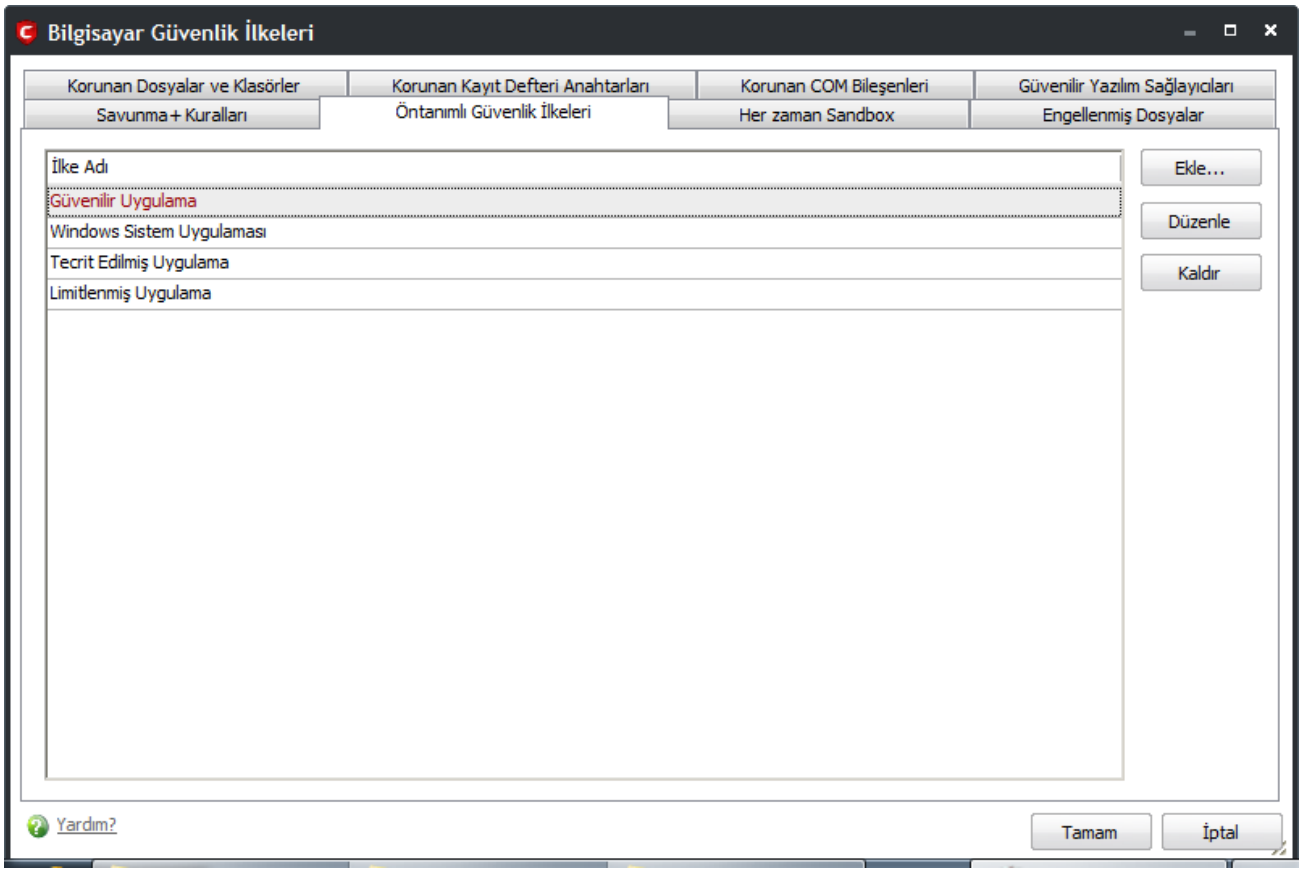
Yeniden kullanılabilir öntanımlı güvenlik ilkeleri oluşturabilirsiniz.

Not: Bu bölüm deneyimli kullanıcılar içindir. Ayrıntılı bilgi için Ağ Güvenlik İlkeleri bölümüne bakın.

İlkeler sistemde bulunan her bir uygulama için ayrı ayrı oluşturabilir fakat bu işlem çok zaman alacaktır. Bu yüzden uygulamalar için genel kapsamlı öntanımlı ilkeler bulunmaktadır Gereksinimlerinize göre bu ilkeleri uygulamalara atayabilir ve isteğinize göre bunları değiştirebilirsiniz.

Bu kategoriyi yapılandırmak için

•Savunma+ Görevleri > Bilgisayar Güvenlik İlkeleri > Öntanımlı Güvenlik İlkeleri. Bu listede dört tane varsayılan ilke bulunmaktadır.



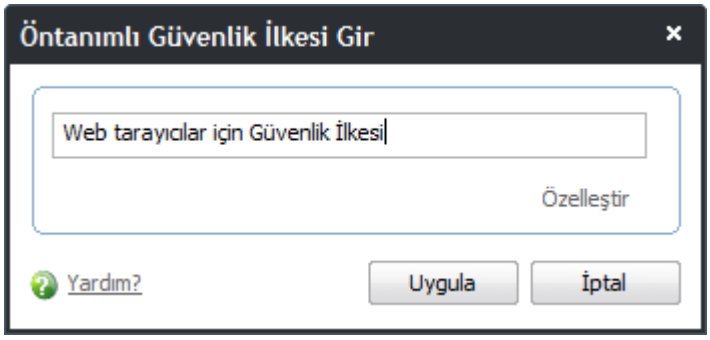
Bulunan öntanımlı ilkeyi görüntülemek veya düzenlemek için

1. Listeden İlke Adına çift tıklayın veya
2. Listeden İlke Adını seçin, sağ tıklayın ve 'Düzenle' seçin veya
3. İlke Adını seçin ve sağdan 'Düzenle' düğmesine tıklayın.

Buradan, ilke adlarını değiştirebilir, ilkenin 'Erişim Haklarını' ve 'Koruma Ayarlarını' düzenleyebilirsiniz. Burada yaptığını değişiklikler otomatik olarak o ilke altındaki tüm uygulamalara uygulanır.

Öntanımlı ilke oluşturmak için

•'Ekle' düğmesine tıklayın, ilke için ad girin, 'Özelleştir' bağlantısına tıklayın ve daha sonra yapılandırın.
Görüntülemek için buraya tıklayın.

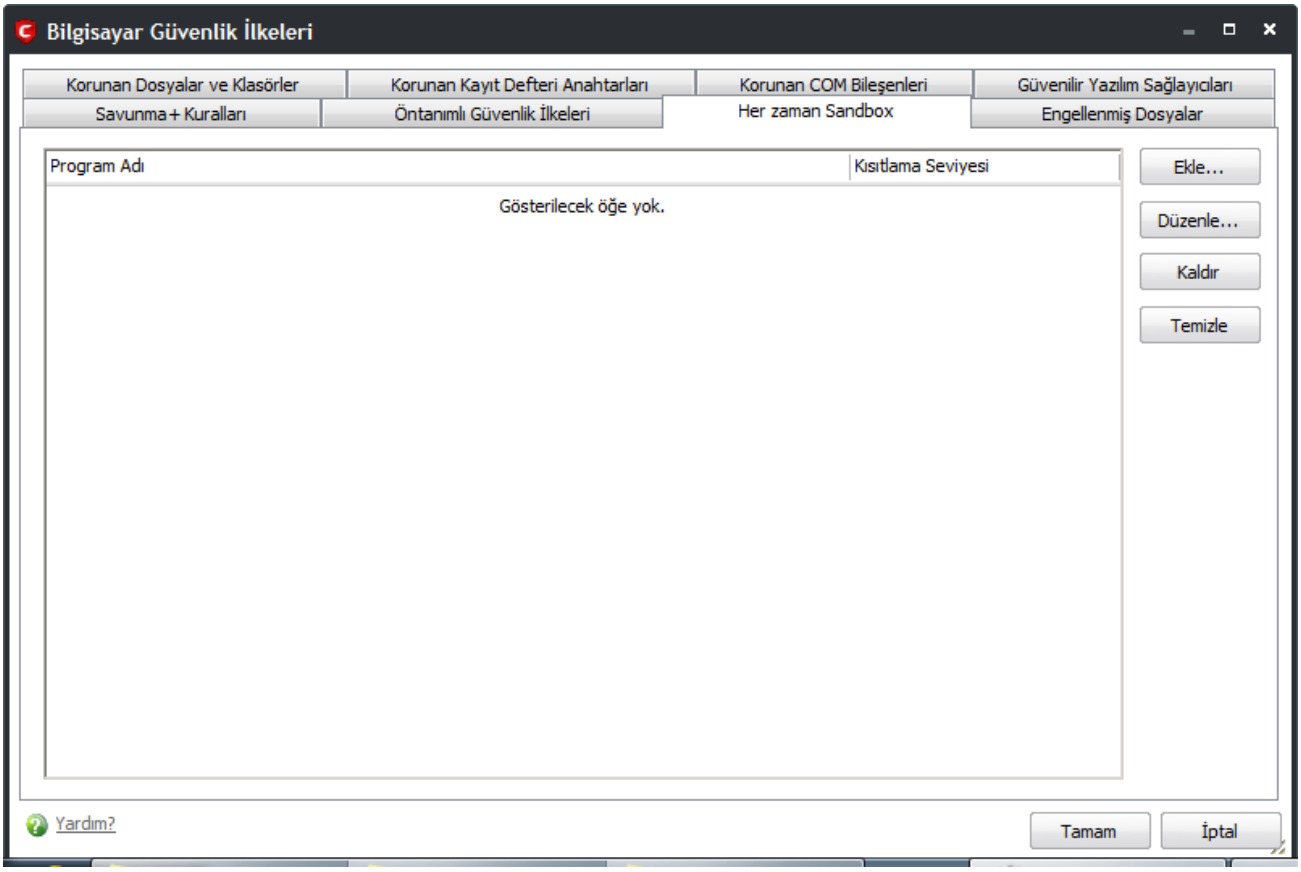


İlkeyi oluşturduktan sonra bu ilkeyi belirli uygulamalara veya dosya gruplarına Savunma+ Bilgisayar Güvenlik İlkeleri bölümünden atayabilirsiniz.

4.5.3 Her Zaman Sandbox

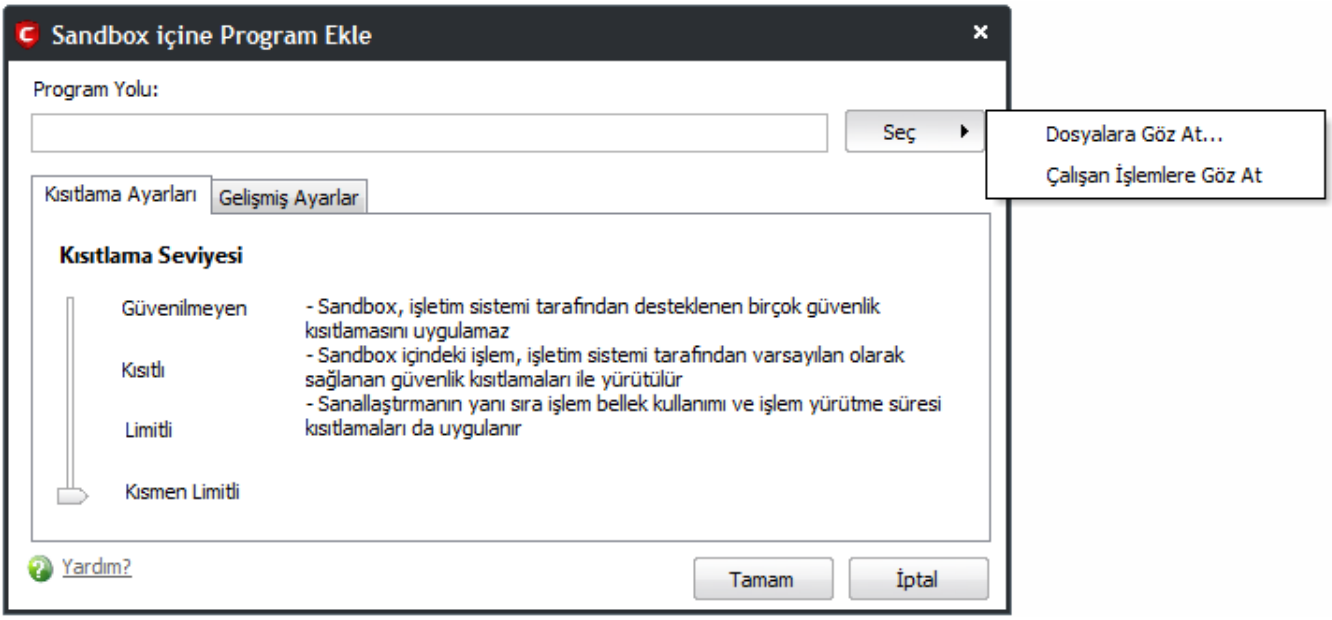
Bu bölüm, kalıcı veya uzun süreli olarak sandbox içinde çalıştırılmasına karar verilmiş kullanıcı tanımlı uygulamaları listeler. Bu liste kullanıcının şüphelendiği veya başka kaygıları (sandbox içinde beta yazılım testi gibi) olduğu uygulamaları içerebilir. Bu uygulamalar sistemde normal programlar olarak görünür fakat sandbox altında kısıtlanmış haklar ile çalışacaktır.

'Her zaman Sandbox' arayüzünü açmak için, Savunma+ > Bilgisayar Güvenlik İlkeleri > Her zaman Sandbox.

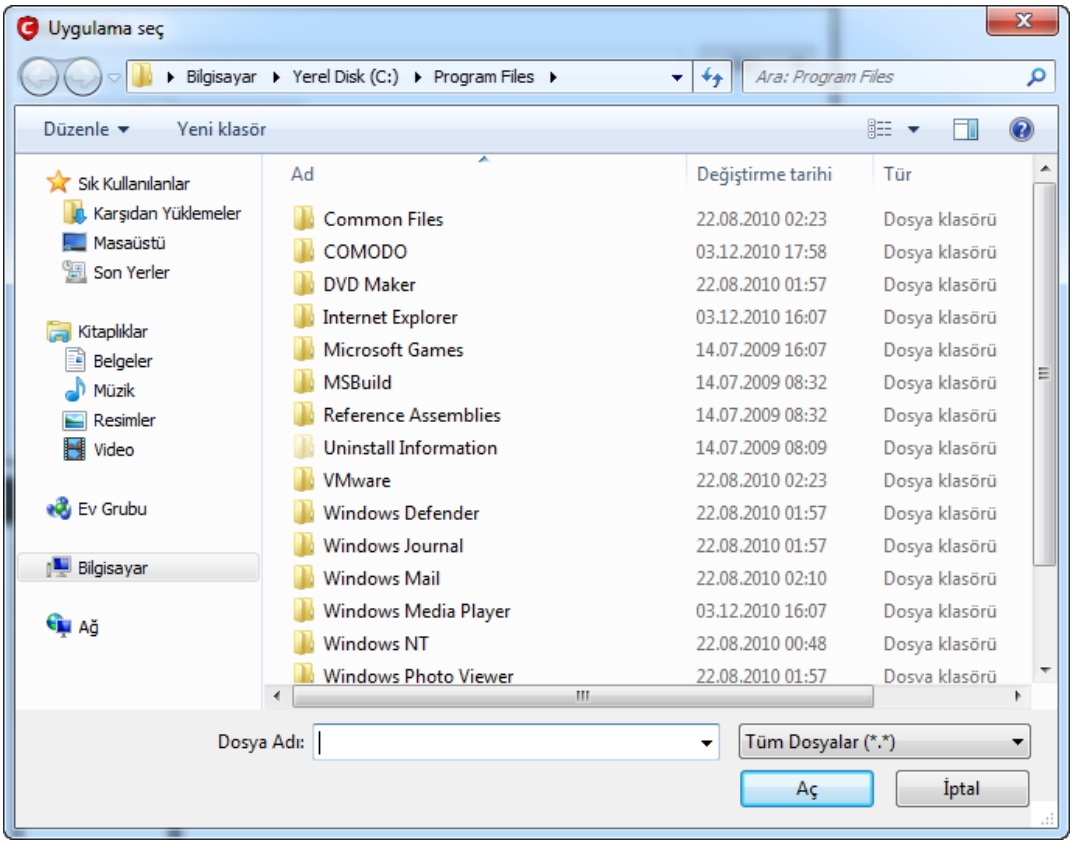


Programları (kalıcı) olarak sandbox içine eklemek için

1. Arayüzden 'Ekle...' düğmesine tıklayın. Bu 'Sandbox içine Program Ekle' diyaloğunu açar.
2. 'Seç' düğmesine tıklayın ve eklemek istediğiniz programı veya çalışan işlemlerden seçin.



3. ‘Aç’ düğmesine tıklayın. Aşağıdaki örnekte opera.exe’yi ekliyoruz.



4. 'Kısıtlama Ayarları' seçin.

   i. Güvenilmeyen – Uygulama işletim sisteminin hiçbir kaynağına erişemez. Uygulama bir seferde 10’dan fazla işlem yürütemez ve limitli erişim haklarıyla çalışır. Gelişmiş Ayarlar altında tanımlanan diğer

kısıtlamalar uygulanır.

Not: Kullanıcı etkileşimi gerektiren bazı uygulamalar bu ayarlar altında düzgün çalışmayabilir.

ii. Kısıtlı – Uygulama çok az sayıda işletim sistemi kaynağına erişebilir. Uygulama bir seferde 10'dan fazla işlem yürütemez ve çok limitli erişim hakları ile çalışır. Gelişmiş Ayarlar altında tanımlanan diğer kısıtlamalar uygulanır.

Not: Oyunlar gibi bazı uygulamalar bu ayarlar altında düzgün çalışmayabilir.

iii. Limitli – Uygulama yalnızca belirli işletim sistemi kaynaklarına erişilebilir. Uygulama bir seferde 10'dan fazla işlem yürütemez ve Yönetici hesap ayrıcalıkları olmadan çalışır. Gelişmiş Ayarlar altında tanımlanan diğer kısıtlamalar uygulanır.

iv. Kısmen Limitli - Uygulama tüm işletim sistemi kaynaklarına erişilebilir. Korunan dosyalara/kayıt anahtarlarına erişemez. Hata ayıkla, sürücü yükleme gibi ayrıcalıklı işlemler gerçekleştiremez. Gelişmiş Ayarlar altında tanımlanan diğer kısıtlamalar uygulanır.

1. 'Gelişmiş Ayarlar' seçin

Bu sekme sistem kaynakları kullanımı ve diğer dosyalara erişimi yapılandırmak içindir. Bulunan seçenekler şunlardır:

i. En fazla bellek tüketimi (MB) – Uygulamanın kullanabileceği en yüksek bellek miktarını belirler (MB olarak).

ii. Program çalışma süresini limitle (saniye) – Uygulamanın çalışabileceği en yüksek süre limitini belirler (saniye olarak).

iii. Dosya sistemi sanallaştırmasını etkinleştir – Sandbox içindeki uygulamalar 'gerçek' dosya sistemi üzerinde değişiklik yapamaz. Bunun yerine oluşturulan sanal dosya sistemi kullanılır. Bu seçenek etkin değilse uygulamalar gerekli girdileri yapamayacağı için düzgün çalışmayabilir.

Deneyimli kullanıcılar için: Sanal dosya sistemi sandbox çalışma klasörü içinde oluşturulur (ör. c:\sandbox\<uygulama adı>).

Sandbox Ayarlarında dosya sistemi sanallaştırması etkin değilse bu seçenek etkin olsa bile sanallaştırma yapılmaz.

iv. Kayıt defteri sanallaştırmasını etkinleştir - Sandbox içindeki uygulamalar 'gerçek' kayıt defteri üzerinde değişiklik yapamaz. Bunun yerine oluşturulan sanal kayıt defteri kullanılır. Bu seçenek etkin değilse uygulamalar gerekli girdileri yapamayacağı için düzgün çalışmayabilir.

Deneyimli kullanıcılar için: Sanal kayıt defteri sandbox anahtarı içinde oluşturulur (ör. HKEY_LOCAL_MACHINE\SYSTEM\Sandbox\...).

Sandbox Ayarlarında kayıt defteri sanallaştırması etkin değilse bu seçenek etkin olsa bile sanallaştırma yapılmaz

1. Ayarların geçerli olması için 'Tamam' düğmesine tıklayın.

Bu noktadan sonra uygulamalar sandbox içinde çalışacaktır. Daha sonra kaldırmak isterseniz listeden uygulamayı seçin ve 'Kaldır' düğmesine tıklayın. Uygulamayı sandbox içinde bir kerelik çalıştırmak istiyorsanız 'Sandbox içinde Program Çalıştır' kullanın.

•Sandbox içindeki uygulamanın kısıtlama ayarlarını düzenlemek istiyorsanız uygulamayı seçin ve 'Düzenle' düğmesine tıklayın.

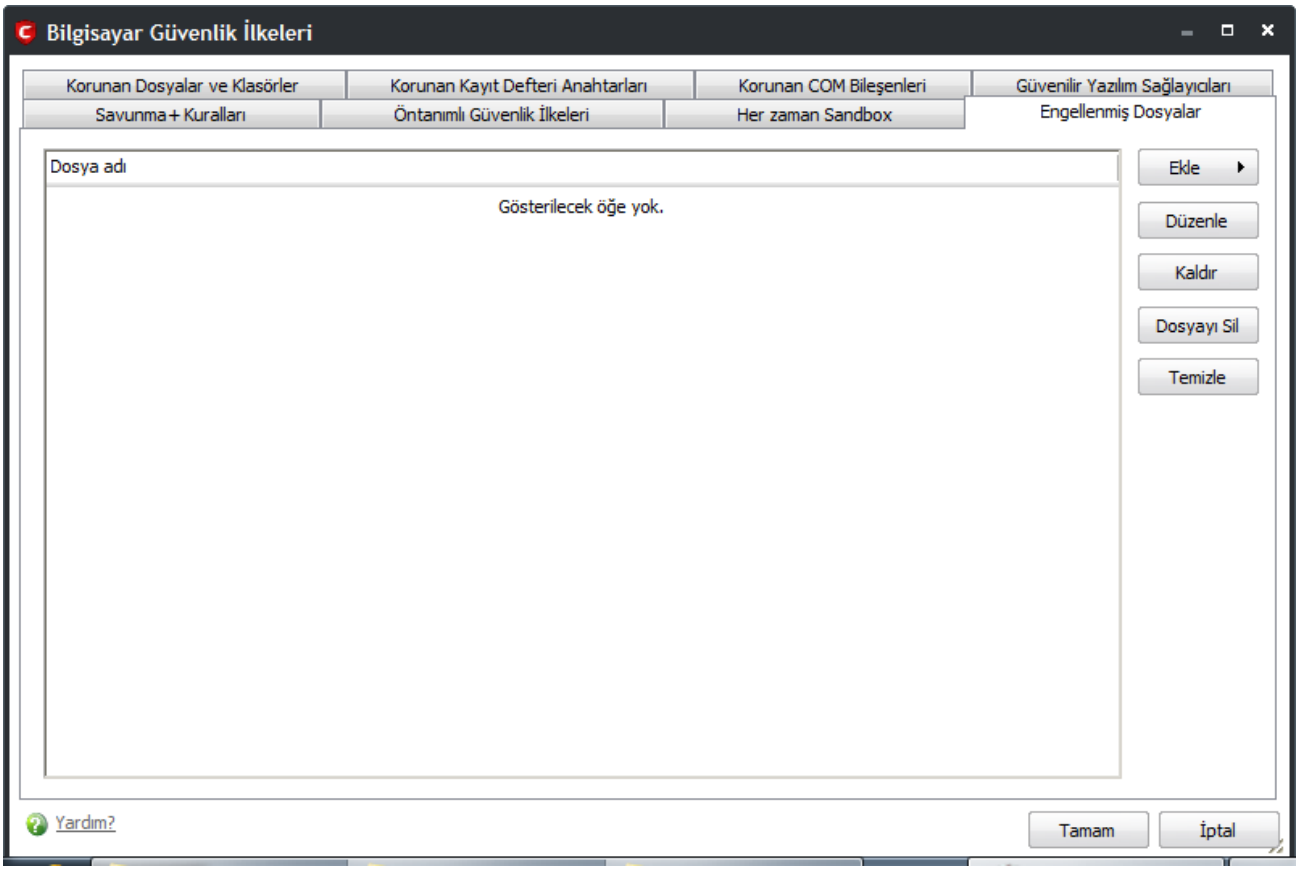
- Uygulamayı kaldırmak için 'Kaldır' düğmesine tıklayın. Uygulamayı bir sonraki çalıştırışınızda bu uygulama sandbox dışında çalışacaktır. (kötü niyetli olarak saptanmadığını veya sandbox içinde çalıştırma süreci sonunda otomatik olarak sandbox içinde çalıştırılmadığını varsayarsak)
- Geçersiz girdileri kaldırmak için 'Temizle' düğmesine tıklayın.

4.5.4 Engellenmiş Dosyalar

Savunma+ dosyaları ve klasörleri tamamen kitleyerek onlara diğer işlemler veya kullanıcılar tarafından yapılan tüm erişimi engellemenize olanak sağlar. Engellediğiniz dosya bir yürütülebilirse ne siz ne başka bir şey o programı çalıştıramaz. 'Korunan Dosyalar ve Klasörler' bölümünde bulunan dosyaların aksine kullanıcılar herhangi bir işlemi seçerek engellenmiş dosyalara erişim izni veremez.

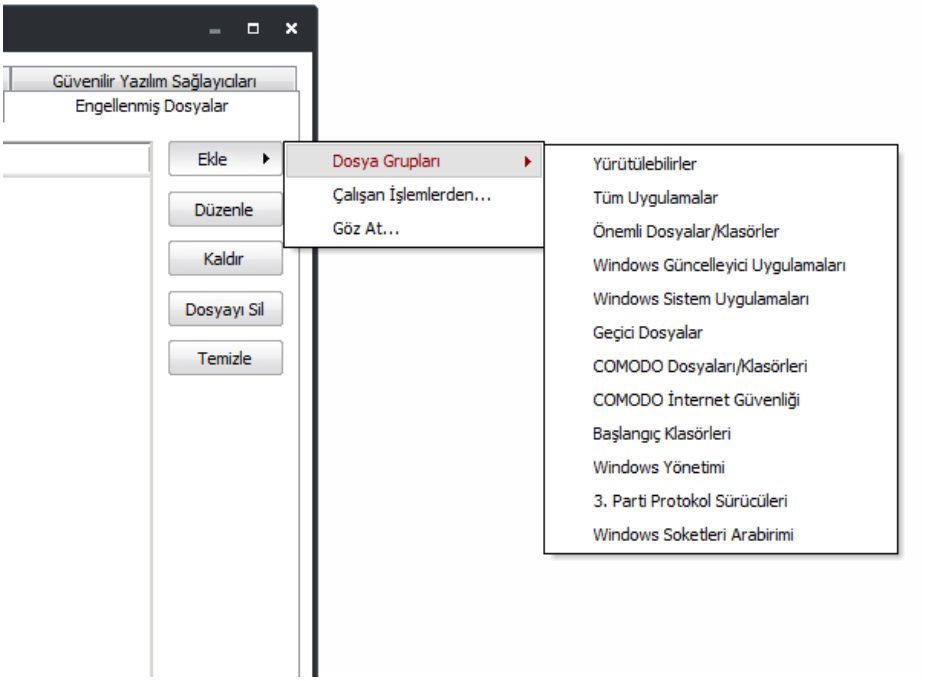
Engellenmiş Dosyalar arayüzüne erişmek için

•Savunma+ Görevleri > Bilgisayar Güvenlik İlkeleri > Engellenmiş Dosyalar.



Elle dosya, dosya grubu veya işlem eklemek için

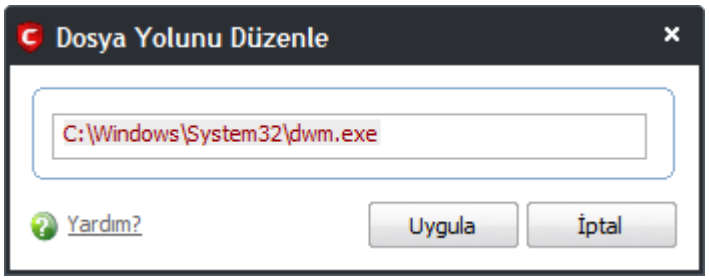
1. 'Ekle' düğmesine tıklayın. Dosya seçimi için bulunan seçenekleri görmek için buraya tıklayın.



Alternatif olarak, 'Tanınmayan Dosyalar' ve 'Güvenilir Dosyalar' bölümlerinden 'Taşı' özelliğini kullanarak da **Engellenmiş Dosyalara** aktarım yapabilirsiniz.

Bulunan girdi yolunu düzenlemek için

1. Girdiyi seçin ve 'Düzenle' düğmesine tıklayın. Dosya yolunu değiştirmek için 'Düzenle' diyaloğu açılır.



2. Gerektiği gibi dosya yolunu değiştirin ve 'Uygula' düğmesine tıklayın.

Bulunan girdi yolunu kaldırmak için

•Girdiyi seçin ve 'Kaldır' düğmesine tıklayın. Dosya yalnızca listeden kaldırılır, sistemden değil.

Kalıcı olarak dosyayı sistemden silmek için (dosya grubu veya yürütülebilir dosya)

•Girdiyi seçin ve 'Dosyayı Sil' düğmesine tıklayın.

Gerçersiz girdileri kaldırmak için,

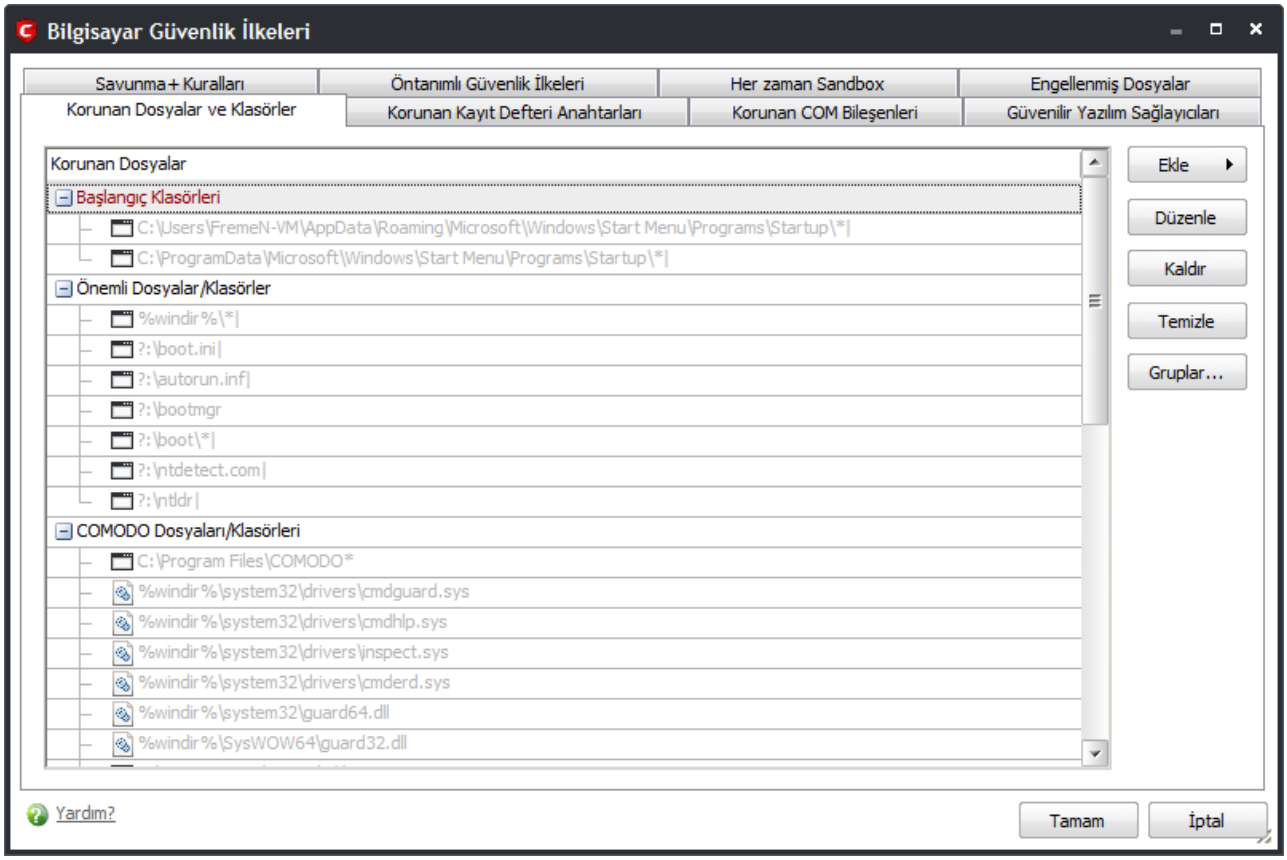
•'Temizle' düğmesine tıklayın.

- Ayarları uygulamak için 'Tamam' düğmesine tıklayın.

4.5.5 Korunan Dosyalar ve Klasörler

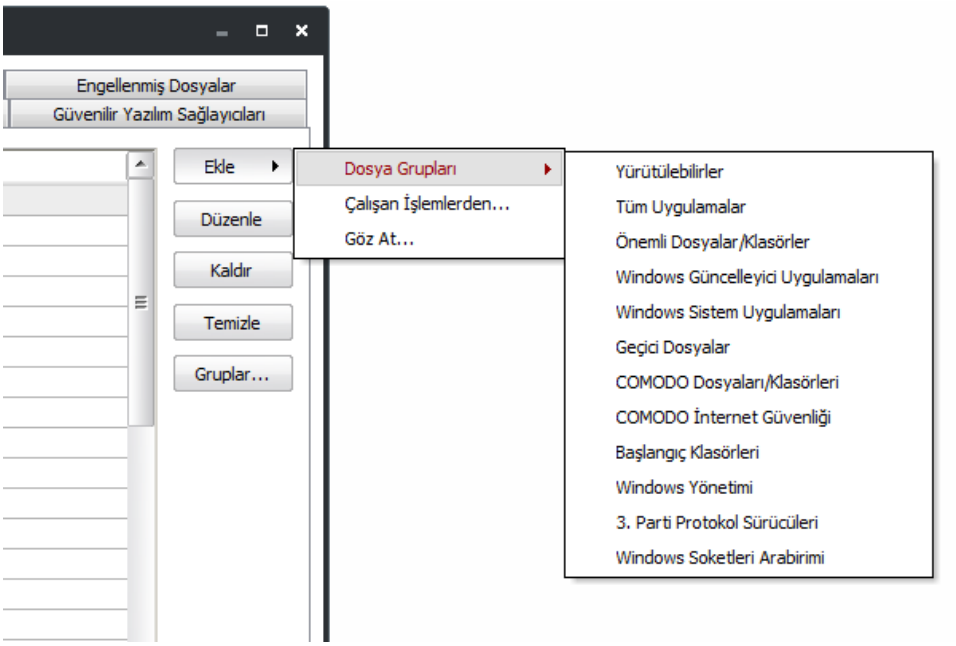
Korunan Dosyalar ve Klasörler ayarı belirli dosyaları ve klasörleri izinsiz değişikliklerden korur. Ayrıca değerli dosyalarınızı da korumakta kullanışlıdır. Dosya 'Korunuyorsa' kullanıcı tarafından hala erişilebilir ve okunabilir fakat değiştirilemez. 'hosts' dosyası bunun için iyi bir örnektir. (c:\windows\system32\drivers\etc\hosts). Bunun 'Korunan Dosyalar ve Klasörler' alanına eklenmesi web tarayıcısının bu dosyaya erişmesine ve okumasına izin verir. Ancak, bu dosyayı değiştirme girişiminde bulunan işlemler Comodo Internet Security tarafından engellenir ve 'Korunan Dosya Erişimi' uyarısı çıkartır.

Bu bölümüne erişmek için: Savunma+ Görevleri > Bilgisayar Güvenlik İlkeleri > Korunan Dosyalar ve Klasörler.



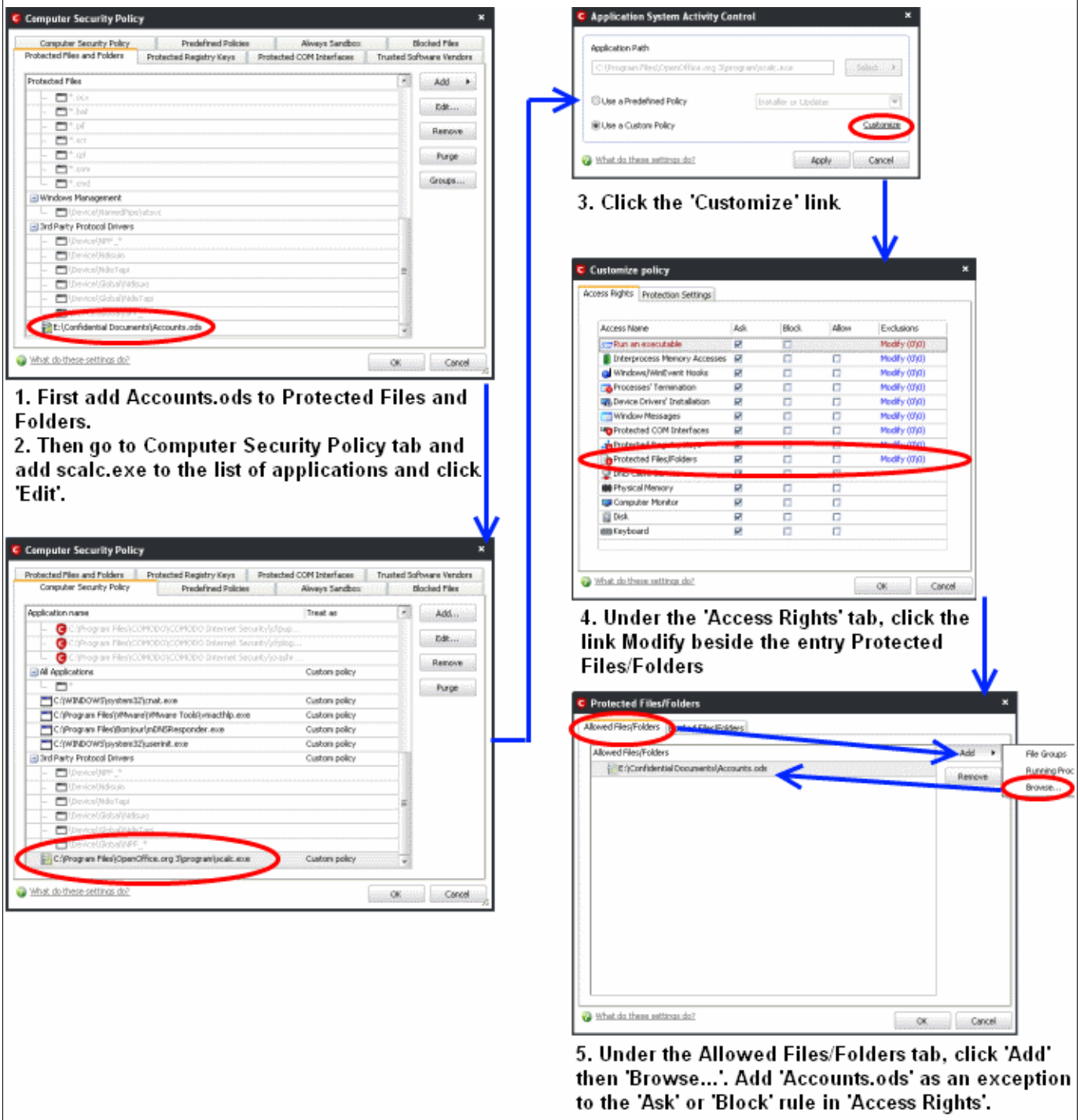
Elle dosya, dosya grubu veya işlem eklemek için

1. 'Ekle' düğmesine tıklayın. Dosya seçimi için bulunan seçenekleri görmek için buraya tıklayın.

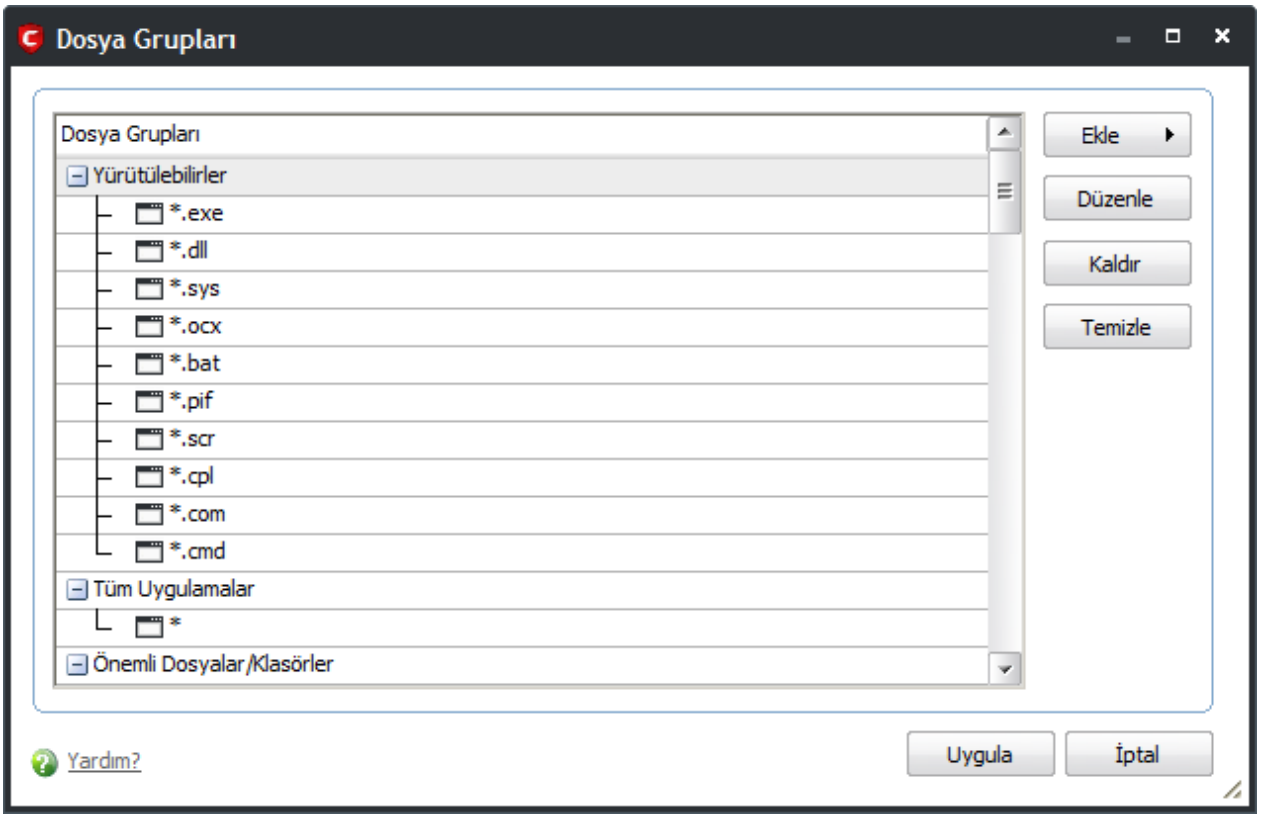


Hariç Tutulanlar

Kullanıcılar başka bir uygulamaya (veya dosya grubuna) korunan dosyaları değiştirmek için 'Bilgisayar Güvenlik İlkeleri' altından gerekli Erişim Haklarını atayarak izin verebilir. Basit bir örnek olarak hayali 'Accounts.ods' dosyasını ele alalım. Open Office Calc (scalc) programının bu dosyayı değiştirebilmesini istiyorsunuz fakat kötü niyetli programlar tarafından değiştirilmesini istemiyorsunuz. İlk olarak bu dosyayı 'Korunan Dosyalar ve Klasörler ' bölümünden 'Ekle' düğmesini kullanarak korunan dosyalara ekleyin. Ekledikten sonra 'Bilgisayar Güvenlik İlkelerine' gidin ve 'scalc' ilkesini özelleştirerek 'Accounts.ods' dosyasını hariç tutulanlarda izin ver bölümüne ekleyin.



'Grup...' düğmesi kullanıcının ‘Dosya Grupları’ arayüzüne erişmesine izin verir.



Dosya grupları kullanışlıdır, bir veya daha çok dosya türünü öntanımlı olarak gruplanması. Dosya grupları Bilgisayar Güvenlik İlkeleri altından hızlıca seçim yapmanızı sağlar.

Bu arayüz şunlara izin verir

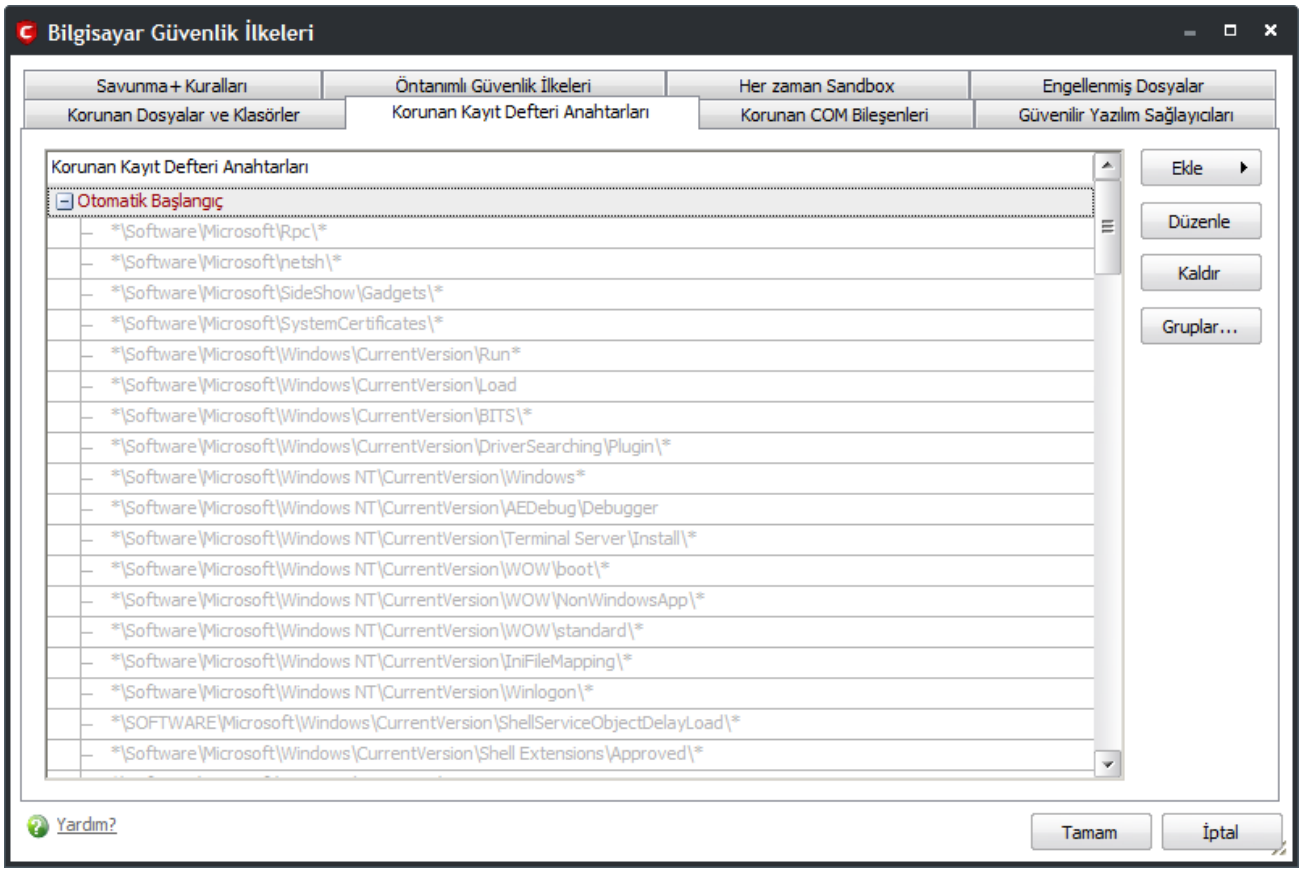
- **'Ekle' ile yeni Dosya Grupları oluşturabilirsiniz.**
- **'Düzenle' ile bulunan Dosya Gruplarını veya Dosyaları düzenleyebilirsiniz.**
- **'Ekle > Seç' ile bulunan bir dosya grubuna ekleme yapabilirsiniz.**
- **Sürükle bırak ile dosyaları gruplar arasında taşıyabilirsiniz.**

Not: Bu bölüm yalnızca dosya grupları oluşturmak veya değiştirmek içindir. Güvenlik ilkelerini buradan ayarlayamazsınız. Bunu yapmak için Bilgisayar Güvenlik İlkeleri veya Öntanımlı İlkeler arayüzünü kullanmalısınız.

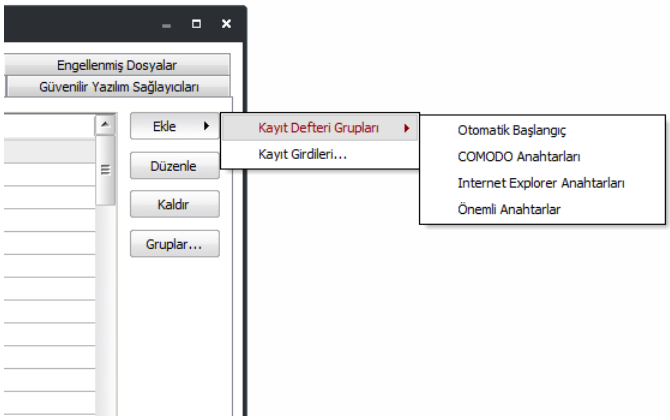
4.5.6 Korunan Kayıt Defteri Anahtarları

Comodo Internet Security otomatik olarak kritik kayıt defteri anahtarlarını değişikliklere karşı korur. Sistem anahtarları bozulursa veya değiştirilirse geri döndürülemez hasara yol açabilir. Kayıt defteri anahtarlarının saldırılara karşı korunması gereklidir.

Bu arayüze erişmek için: Savunma+ Görevleri > Bilgisayar Güvenlik İlkeleri > Korunan Kayıt Defteri Anahtarları.



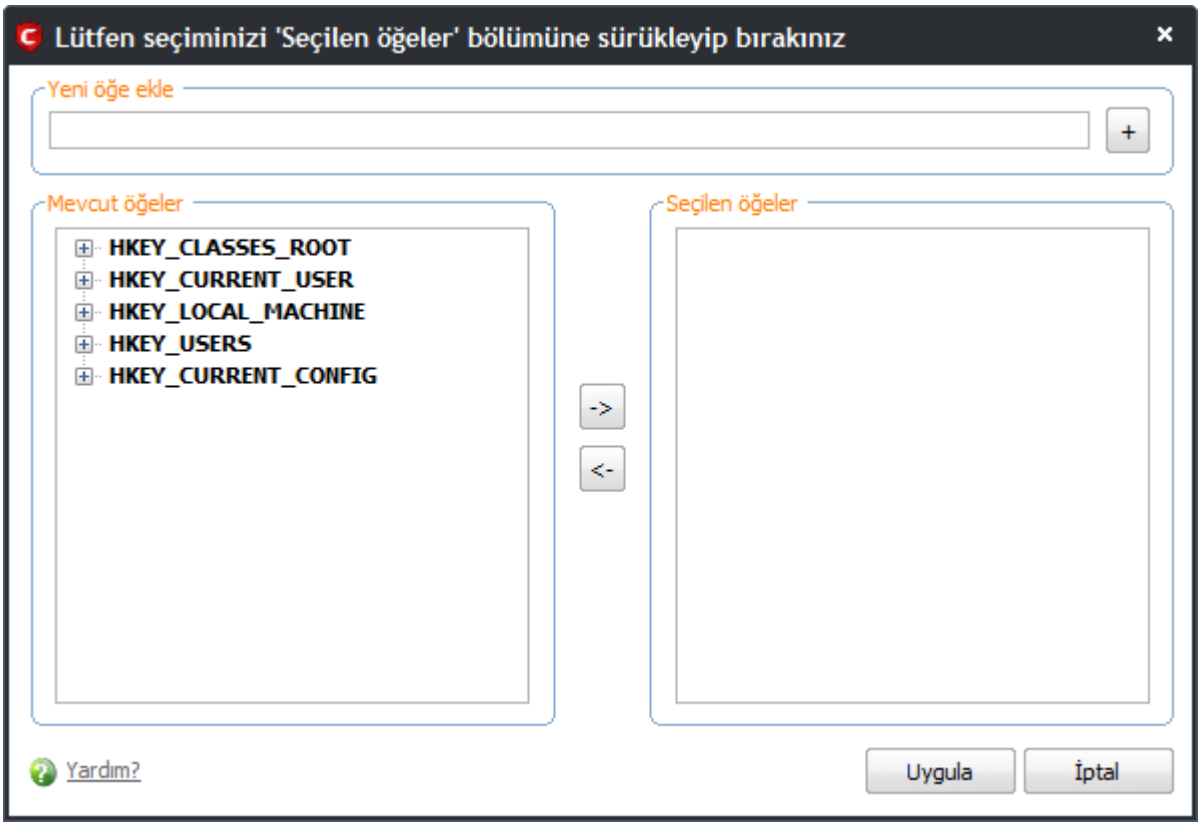
'Ekle' düğmesi ile bu listeye eklemeler yapabilirsiniz:



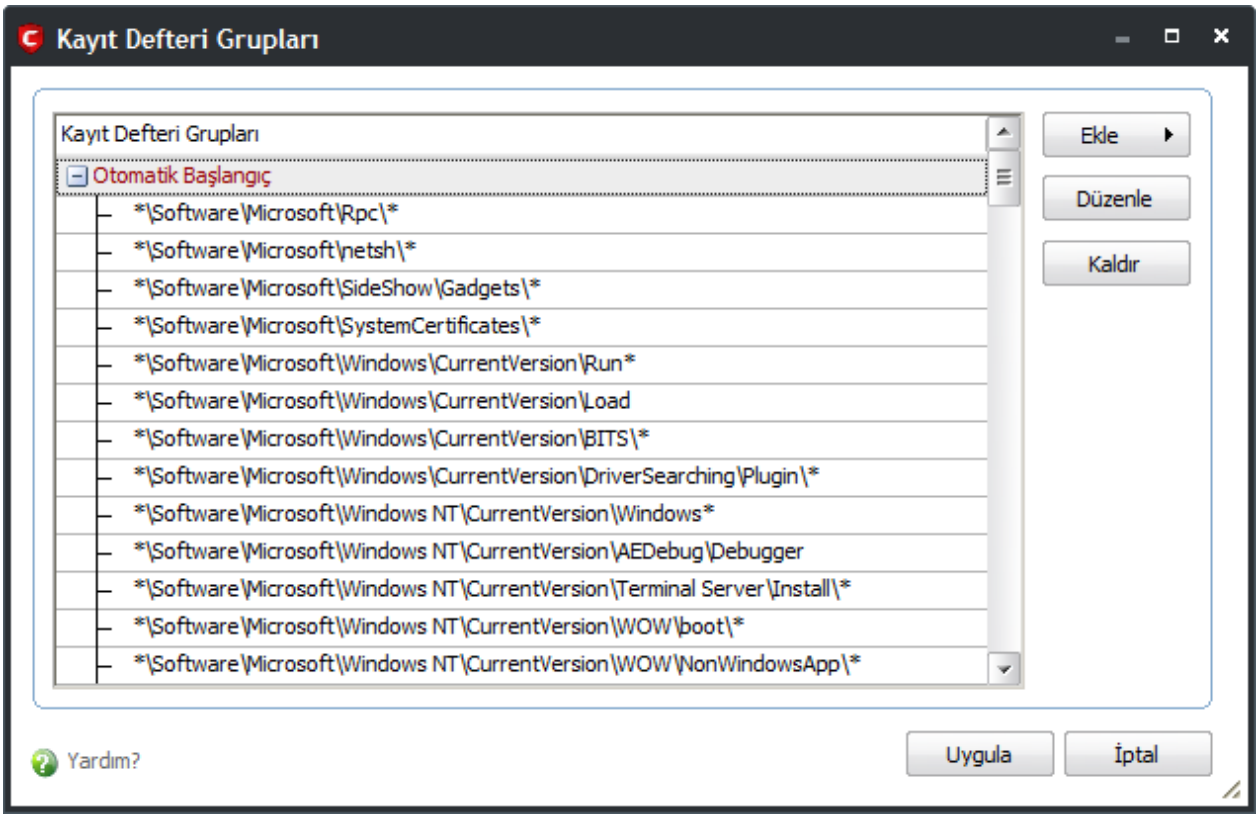
'Kayıt Defteri Grupları' seçeneği toplu ve öntanımlı grupları eklemenize izin verir. Comodo Internet Security varsayılan olarak 'Otomatik Başlangıç' (anahtarları), 'Comodo Anahtarları', 'Internet Explorer Anahtarları' ve 'Önemli Anahtarları' grupları ile gelir.

'Kayıt Girdileri...' seçeneği CIS arayüzü içinde Windows kayıt defterini açar ve anahtar seçmenizi sağlar.

Kayıt ağacına 'Mevcut öğeler' göz atarken istediğiniz öğeleri elle sürükle ve bırak ile sağ panele 'Seçilen öğeler' taşıyarak ekleyebilirsiniz. Elle anahtar adını girdikten sonra '+' düğmesi ile öğe ekleyebilirsiniz.



'Gruplar...' düğmesi 'Kayıt Defteri Grupları' arayüzüne erişmenize izin verir.



Kayıt defteri grupları kullanışlıdır, öntanımlı gruplama veya önemli kayıt defteri anahtarları.

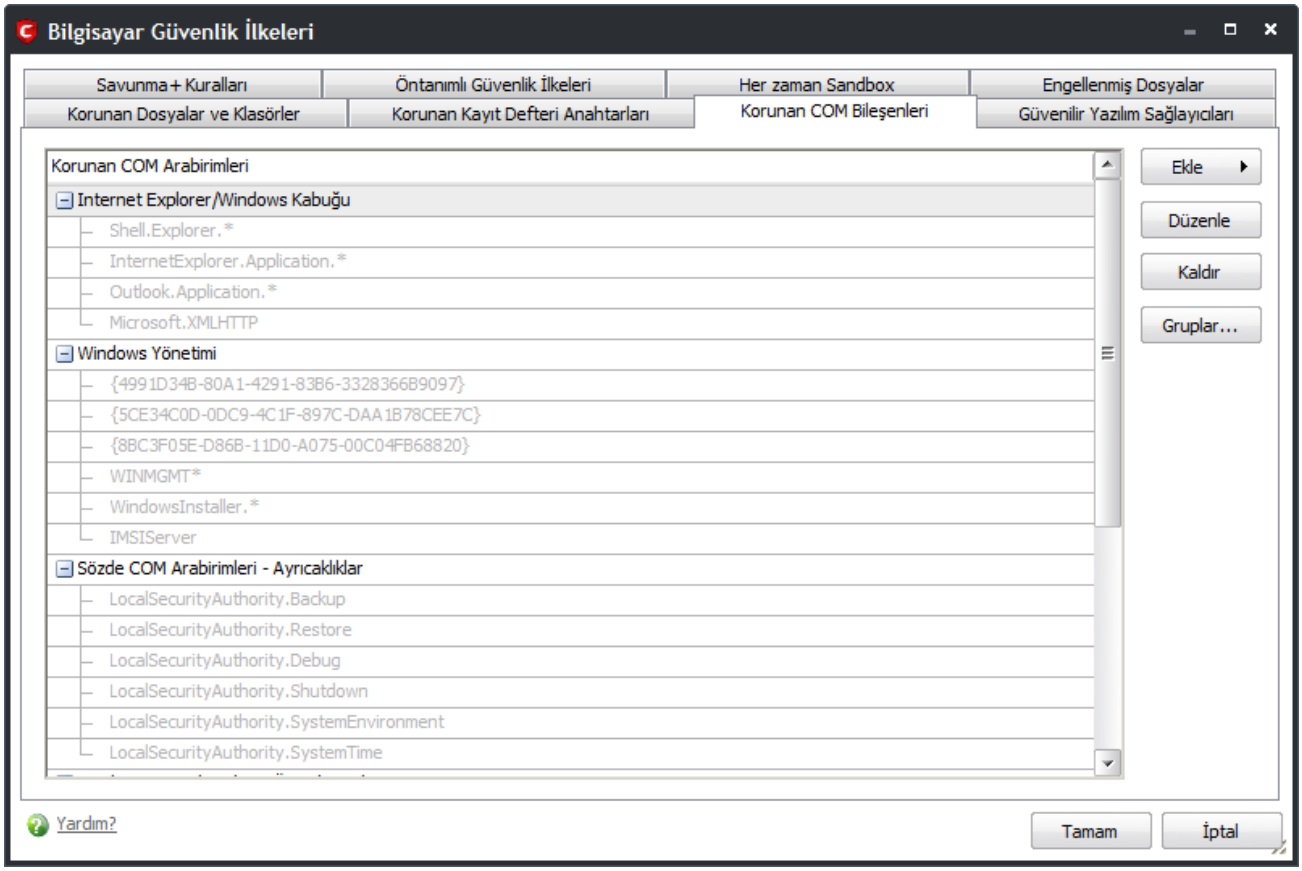
Bu arayüz şunlara izin verir:

- **'Ekle' ile yeni kayıt defteri anahtarı grubu oluşturabilirsiniz.**
- **Yeni grup adını seçerek ona 'Ekle > Seç > Kayıt Anahtarı…' ile anahtar ekleyebilirsiniz.**
- **Bulunan grup adını seçerek ona 'Ekle > Seç > Kayıt Anahtarı…' ile anahtar ekleyebilirsiniz.**
- **Grupları veya anahtarları seçerek sağ tık 'Düzenle' ile onları düzenleyebilirsiniz.**
- **Sürükle bırak ile anahtarları gruplar arasında taşıyabilirsiniz.**

4.5.7 Korunan COM Arabirimleri

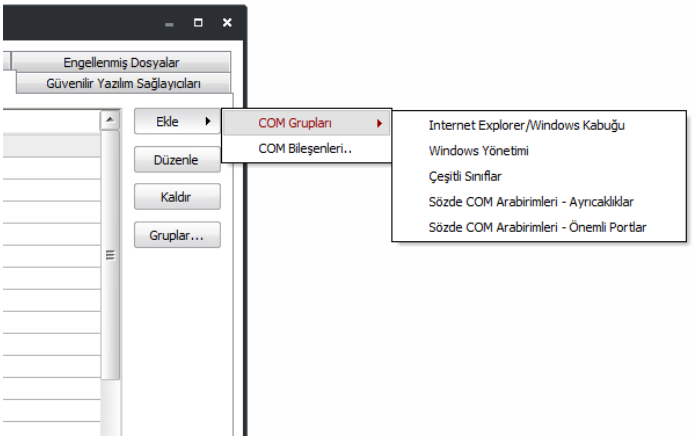
Bileşen Nesne Modeli (Component Object Model (COM)) Microsoft'un nesneye yönelimli programlama modelidir, nesnelerin tek uygulama içinde veya uygulamalar arası nasıl etkileşimde bulunacağını tanımlar. COM, Active X ve OLE temelinde kullanılır – Saldırganların ve kötü niyetli programların en favori iki hedefidir. Bu yüzden COM Arabirimlerinin korunması güvenlik için önemlidir.

Comodo Internet Security otomatik olarak COM arabirimlerini kötü niyetli programlar tarafından yapılacak değişikliklere, bozulmalara ve etkilemeye karşı korur. Öntanımlı COM Arabirim grupları 'Gruplar' düğmesi kullanılarak açılabilir.



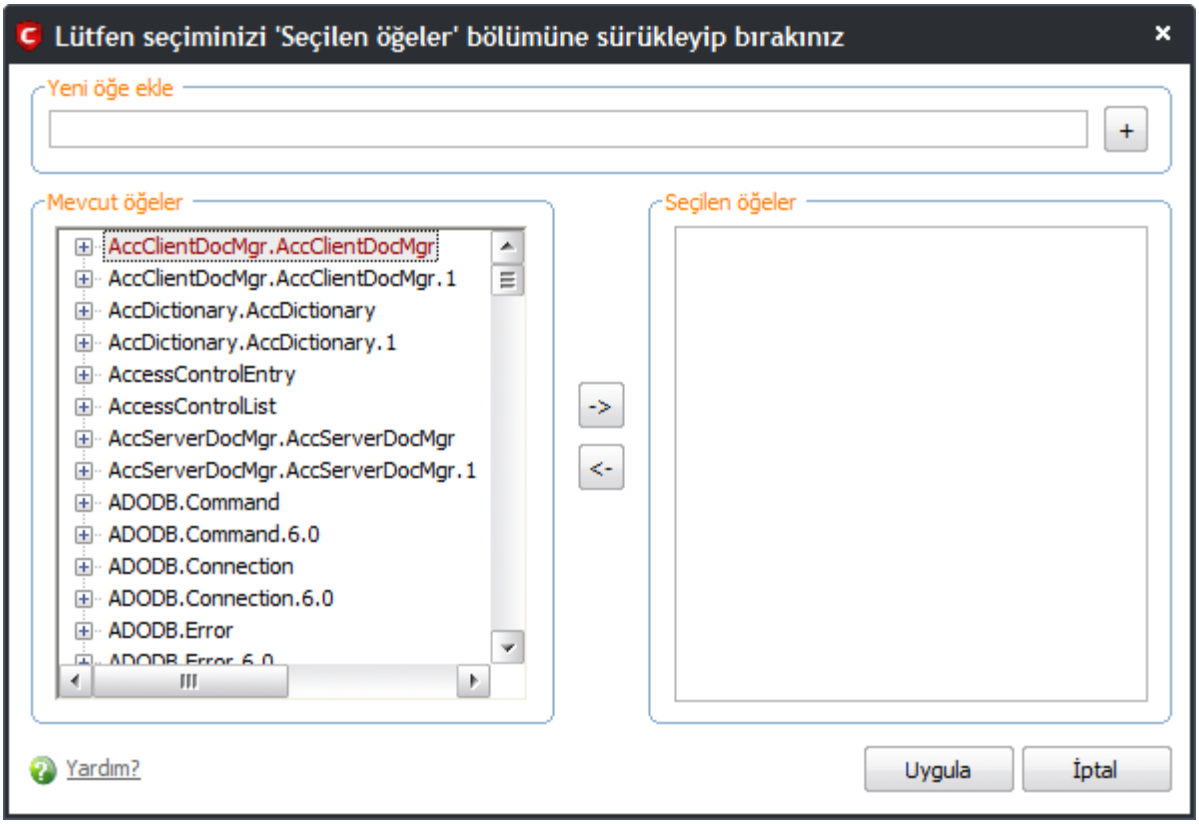
'Korunan COM Arabirimleri' arayüzüne erişmek için: Savunma+ Görevleri > Bilgisayar Güvenlik İlkeleri > Korunan COM Arabirimleri.

‘Ekle’ ile korunmasını istediğiniz COM arabirimini ekleyebilirsiniz.



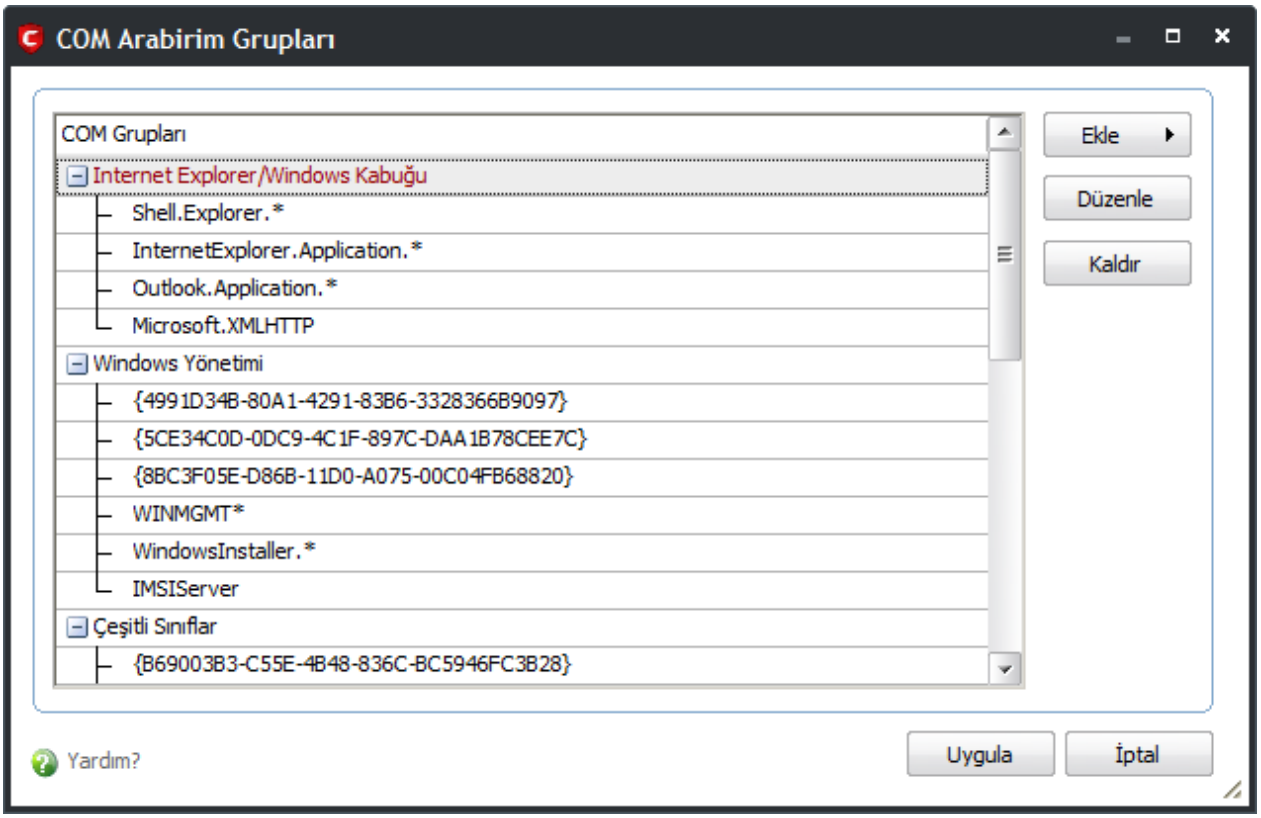
'COM Grupları' seçeneği toplu ve öntanımlı COM arabirimlerini eklemenize izin verir.

'COM Bileşenleri...' seçeneği COM bileşenlerini tek olarak eklemenize olanak sağlar. Bileşenlere elle ‘Mevcut öğeler’ göz atarken istediğiniz öğeleri elle sürükle ve bırak ile sağ panele ‘Seçilen öğeler’ taşıyarak ekleyebilirsiniz. Elle bileşen adını girdikten sonra ‘+’ düğmesi ile öğe ekleyebilirsiniz.



'COM Arabirim Grupları' erişmek için

•‘Gruplar’ düğmesine tıklayın.



COM grupları kullanışlıdır, öntanımlı gruplar.

Bu arayüz şunlara izin verir:

- **'Ekle' ile yeni COM grubu oluşturabilirsiniz.**
- **Yeni grup adını seçerek ona 'Ekle > Seç > COM Bileşenleri…' ile bileşen ekleyebilirsiniz.**
- **Bulunan grup adını seçerek ona 'Ekle > Seç > COM Bileşenleri…' ile bileşen ekleyebilirsiniz.**
- **Grupları veya bileşenleri seçerek sağ tık 'Düzenle' ile onları düzenleyebilirsiniz.**
- **Sürükle bırak ile bileşenleri gruplar arasında taşıyabilirsiniz.**

4.5.8 Güvenilir Yazılım Sağlayıcıları

Comodo Internet Security'de, bir uygulamanın güvenli olarak sayılabilmesi için iki temel yöntem vardır. Ya 'Beyaz Listede' bulunmalıdır veya 'Güvenilir Yazılım Sağlayıcıları Listesindeki' sağlayıcılardan biri tarafından sayısal olarak imzalanmış olmalıdır.

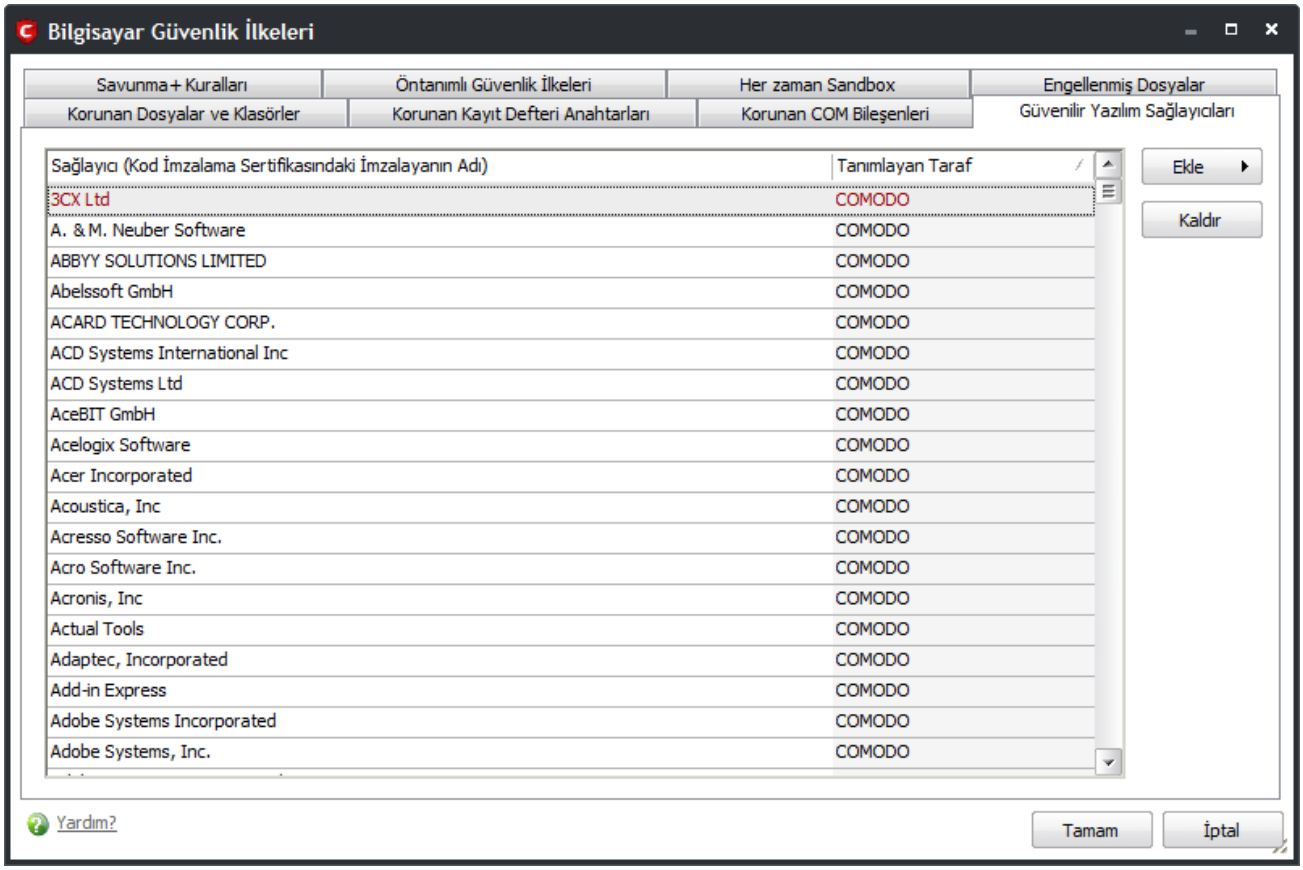
Bu noktadan:

- EĞER sağlayıcı 'Güvenilir Yazılım Sağlayıcıları' listesinde bulunuyorsa VE kullanıcı tarafından 'Trust Applications that are digitally signed by Trusted Software Vendors' seçeneği işaretlemişse SONUÇ olarak uygulamaya güvenilecektir ve çalışmasına izin verilecektir.

- EĞER sağlayıcı 'Güvenilir Yazılım Sağlayıcıları' listesinde bulunmuyorsa VEYA kullanıcı tarafından 'Trust

Applications that are digitally signed by Trusted Software Vendors' seçeneği işaretlenMEmişse SONUÇ olarak uygulama sandbox içinde çalıştırılacaktır. Söz konusu uygulama bir yükleyici ise CIS yükseltilmiş ayrıcalık uyarısı üretecektir.

'Güvenilir Yazılım Sağlayıcıları' bölümünü açmak için: Savunma+ Görevleri > Bilgisayar Güvenlik İlkeleri > Güvenilir Yazılım Sağlayıcıları.



Yazılımların sayısal olarak imzalanması hakkındaki notu okumak için buraya tıklayın

Kullanıcı tanımlı güvenilir sağlayıcıların nasıl Ekleneceğini / Tanımlanacağını öğrenmek için buraya tıklayın

Yazılım Sağlayıcıları - Yazılımlarınızı bu listeye nasıl ekleteceğinizi öğrenmek için buraya tıklayın

Not

Çoğu yazılım sağlayıcısı yazılımlarını sayısal olarak imzalar. Bu son kullanıcının yazılımı doğrulamasına yardımcı olur:

i. İçerik Kaynağı: İndirdikleri ve yüklemek üzere oldukları yazılımın gerçek yayıncısı tarafından geldiğini gösterir.

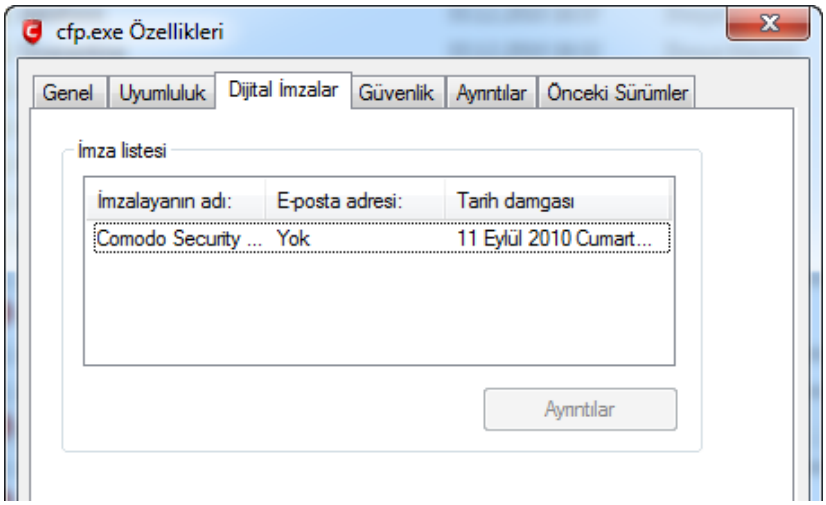
ii. İçerik Bütünlüğü: İndirdikleri ve yüklemek üzere oldukları yazılımın imzalandığından beri değiştirilmediğini ve bozulmadığını gösterir.

Eğer sağlayıcı 'Güvenilir Yazılım Sağlayıcıları' listesinde bulunuyorsa ve kullanıcı tarafından 'Trust Applications that are digitally signed by Trusted Software Vendors' seçeneği işaretlemişse sonuç olarak CIS otomatik olarak uygulamanın çalışmasına izin verecektir (Sayısal imzalama hakkında daha fazla bilgi için http://www.instantssl.com/code-signing/ sayfasına bakın).

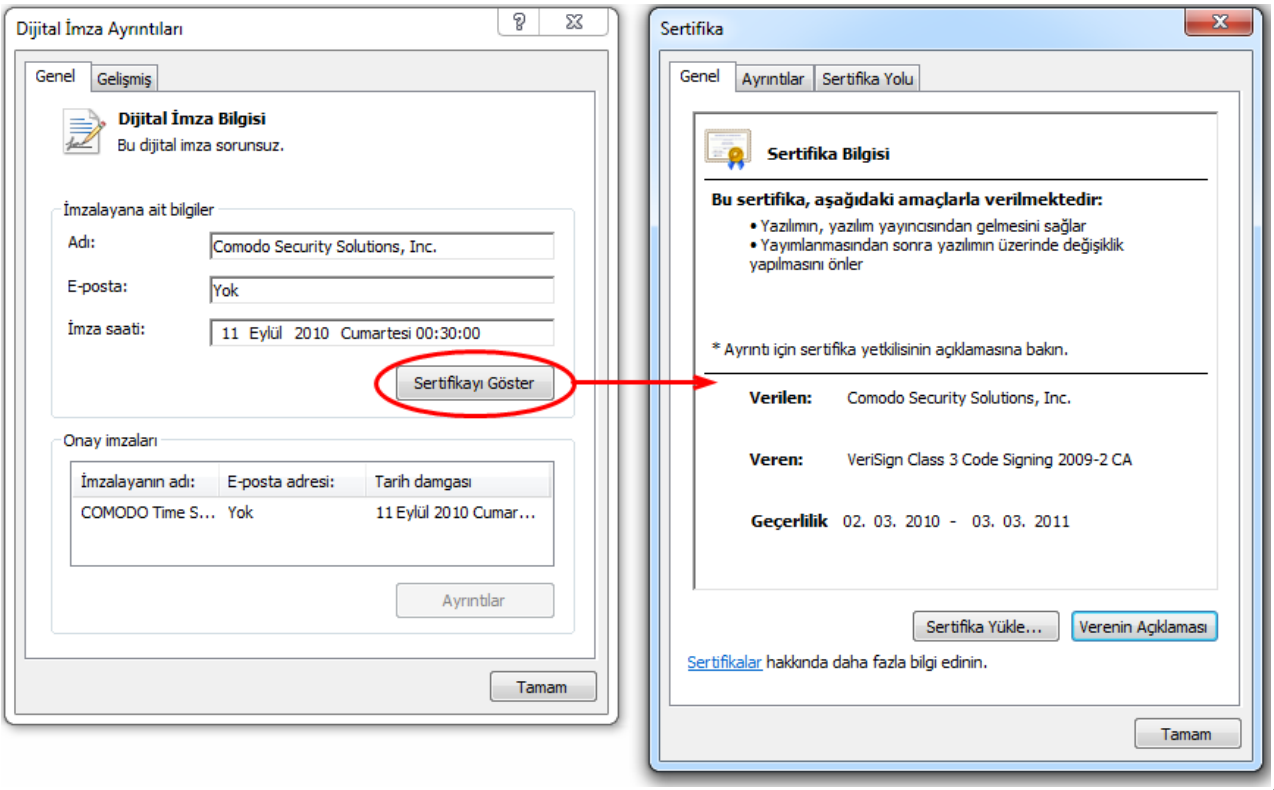
Dosya özelliklerinden dosyanın sayısal olarak imzalanıp imzalanmadığına bakabilirsiniz. Örneğin, Comodo Internet Security'nin cfp.exe dosyası sayısal olarak imzalanmıştır.

- **Comodo Internet Security kurulum klasörüne gidin.**
- **cfp.exe üzerine sağ tıklayın.**
- **Açılan içerik menüsünden 'Özellikleri' seçin.**
- **'Dijital İmzalar' sekmesine tıklayın (bu sekme yoksa dosya sayısal olarak imzalanmamıştır).**

Bu aşağıda göründüğü gibi yazılımı imzalayan CA'nın (Sertifika Yetkilisi) adını görüntüler:



Sertifika bilgilerini görüntülemek için 'Ayrıntılar' düğmesine tıklayın. 'Sertifikayı Göster' düğmesine tıklayarak asıl kod imzalama sertifikasını inceleyebilirsiniz. (aşağı bakın)

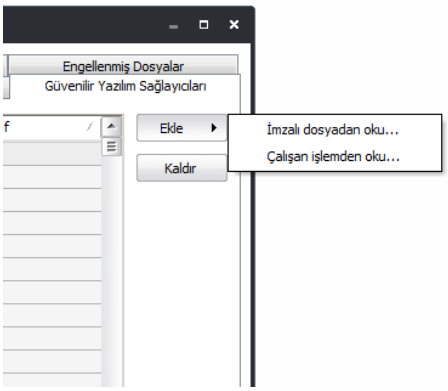


Yukarıdaki örnek özel bir durumdur, Comodo 'cfp.exe' uygulamasının hem geliştiricisi hem de imzalayıcısıdır (Güvenilir Sertifika Yetkilisi olarak). ('Onay imzaları' bölümüne bakın). Çoğunlukla bunlar farklıdır. Ayrıntılar için bu örneğe bakın.

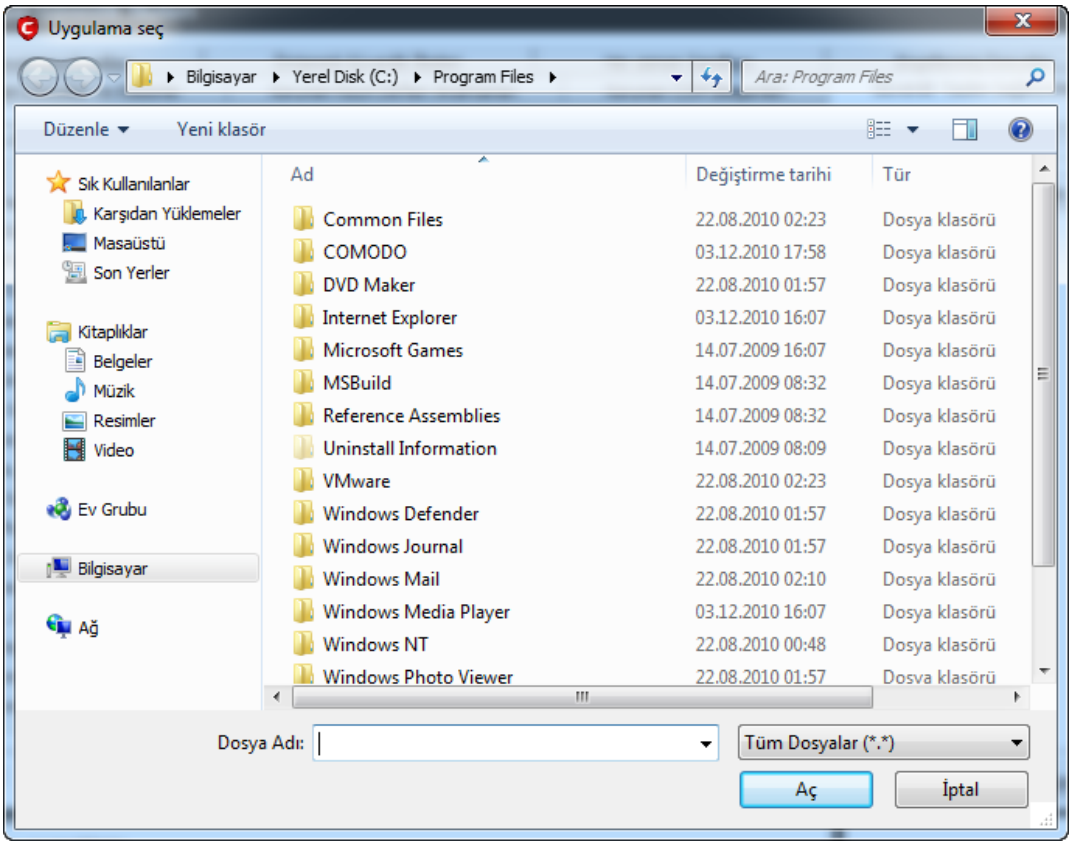
Kullanıcı tarafından Güvenilir Sağlayıcı Eklenmesi ve Tanımlanması

Yazılım sağlayıcısı yerel 'Güvenilir Yazılım Sağlayıcıları' listesine iki yolla eklenebilir:

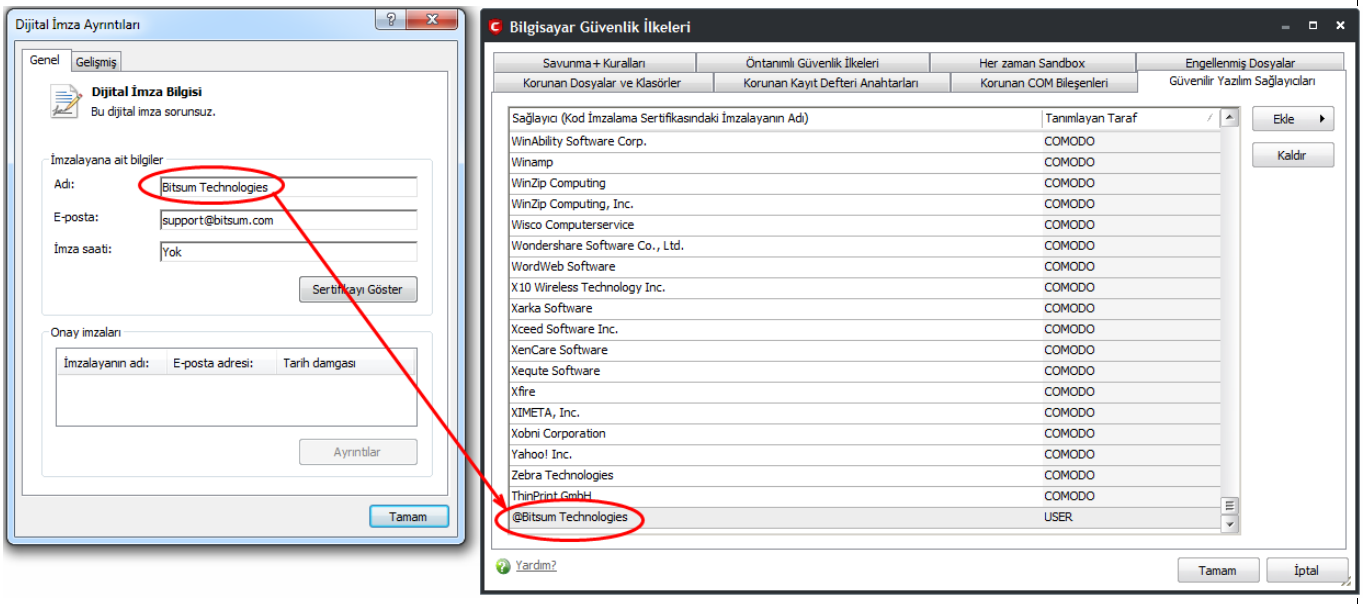
- **Yerel diskteki dosyanın imzası okunarak**
- **Çalışan işlemlerden dosyanın imzası okunarak**



Ekle düğmesine tıklayın ve 'Çalışan işlemden oku' seçin. Yürütülebilir dosyanın bulunduğu konuma gidin ve seçin. Aşağıdaki örnekte 'YahooMessenger.exe' kullanılmıştır.

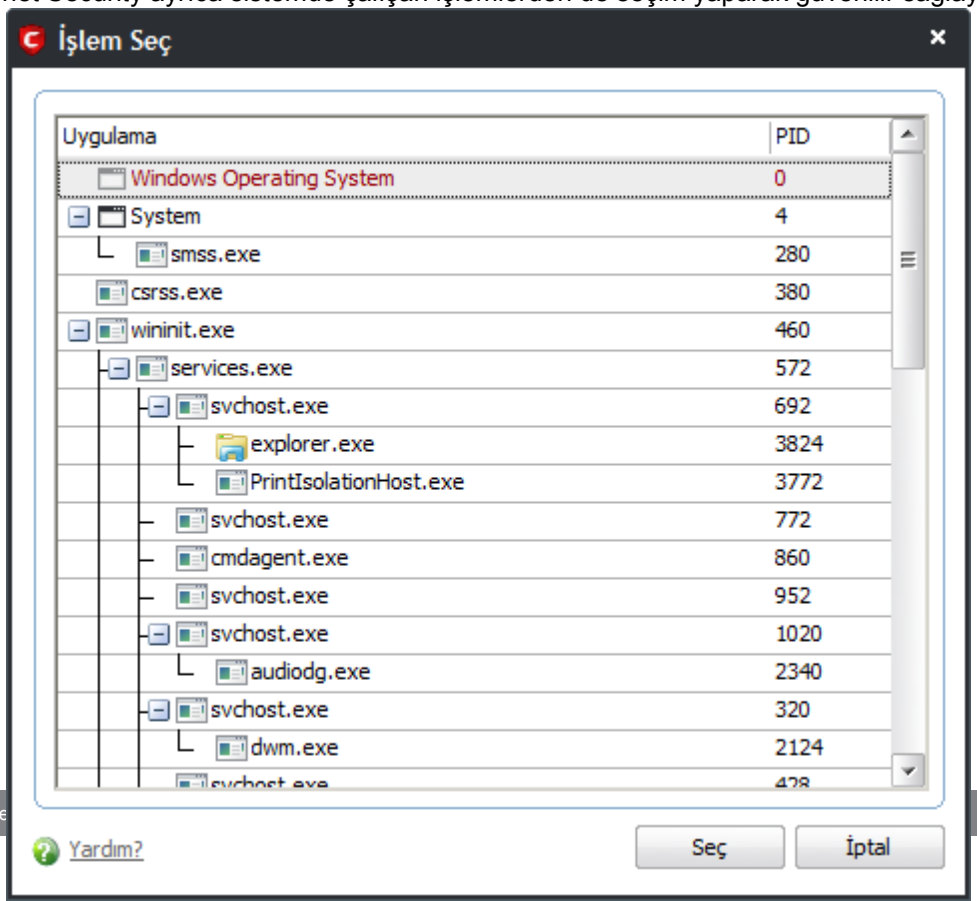


'Aç' düğmesine tıkladıktan sonra CIS dosyanın sağlayıcı tarafından imzalandığını ve Güvenilir Sertifika Yetkilisi tarafından onaylandığını denetler. Öyleyse, sağlayıcı (yazılımı imzalayan) Güvenilir Sağlayıcı listesine (Trusted Vendor list (TVL)) eklenir:



Yukarıdaki örnekte Comodo Internet Security 'YahooMessenger.exe' üzerindeki imzayı doğrulayabildi ve sağlayıcıya güvendi çünkü dosya güvenilir CA 'Verisign' tarafından onaylanmıştı. Yazılımı imzalayan 'Yahoo! Inc' Güvenilir Yazılım Sağlayıcıları listesine eklendi. Bu sağlayıcı tarafından imzalanmış diğer yazılımlara da ayarlardan değiştirilmediği sürece ileride güvenilecektir. (Savunma+ Ayarları > Genel Ayarlar altındaki bu ayar).

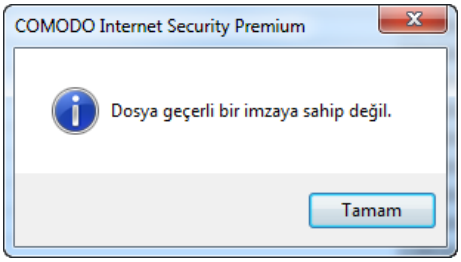
Comodo Internet Security ayrıca sistemde çalışan işlemlerden de seçim yaparak güvenilir sağlayıcılara ekleme



yapmanıza izin verir. Bunu yapmak için, 'Ekle…' düğmesine tıklayın ve 'Çalışan işlemden oku' seçin:

Güvenmek istediğiniz yürütülebiliri seçin ve 'Seç' düğmesine tıklayın. Comodo Internet Security yukarıda anlatıldığı gibi sertifikayı denetler.

Eğer Comodo Internet Security yazılım sertifikasının güvenilir CA tarafından onaylandığını doğrulayamazsa yazılımı sağlayıcı listesine eklemez. Bu durumda aşağıdaki hata mesajını görürsünüz.



Not: 'Güvenilir Yazılım Sağlayıcıları' listesi iki tür yazılım sağlayıcısı gösterir:

- **Kullanıcı tanımlı güvenilir yazılım sağlayıcıları – Kullanıcı tarafından eklenen sağlayıcılardır ve 'Kaldır' düğmesi ile listeden kaldırabilirsiniz.**
- Comodo tanımlı güvenilir yazılım sağlayıcıları – Comodo tarafından eklenen sağlayıcılardır.

Yazılım Geliştiricileri için Güvenilir Sağlayıcı Prıgramı

Yazılım geliştiricileri http://internetsecurity.comodo.com/trustedvendor/signup.php adresindeki başvuru formunu doldurarak ve yazılımlarının Comodo teknikerleri tarafından indirilebilir olduğundan emin olmalıdırlar. Teknikerlerimiz yazılımı Güvenilir Sağlayıcı listesine eklemeden önce:

- **Yazılımın güvenilir CA tarafından sağlanan kod imzalama sertifikası ile imzalanıp imzalanmadığını;**
- **Yazılımın kullanıcının sistemine karşı bir tehdit oluşturup oluşturmadığını;**

denetler.

Daha fazla bilgi http://internetsecurity.comodo.com/trustedvendor/overview.php adresindedir.

4.6 Etkin İşlemler Listesini Göster

Etkin İşlemler Listesi sistemde çalışan etkin tüm işlemleri gösterir.

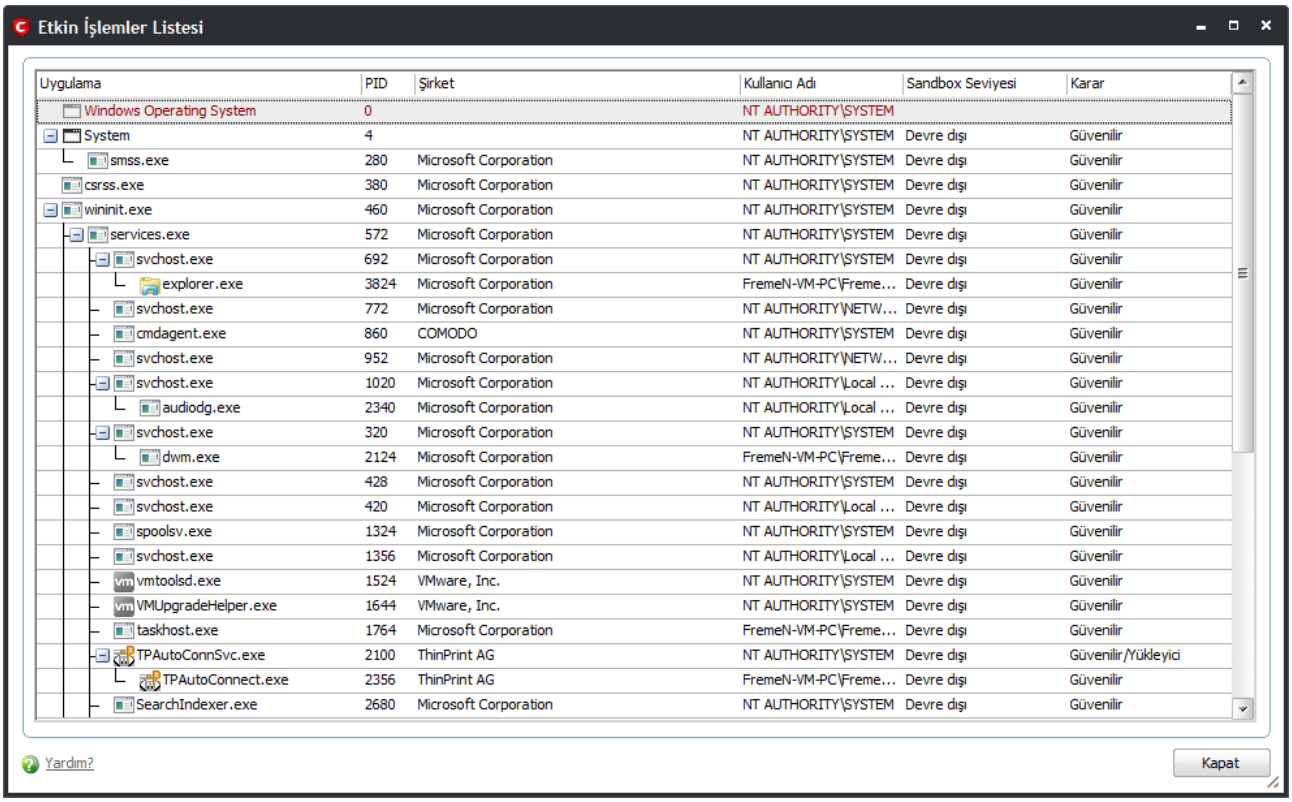
Etkin İşlem Listesini görüntülemek için

1. Savunma+ > Etkin İşlemler Listesi.

Sütun Açıklamaları

- **Uygulama – Uygulamanın adını gösterir.**

- **PID – İşlem Kimliği Numarasını (Process Identification Number) gösterir.**
- **Şirket – Yazılımı geliştirenin adını gösterir**
- **Kullanıcı Adı – İşlemi başlatan kullanıcı hesabının adını gösterir**
- **Sandbox Seviyesi – Programa uygulanan sandbox seviyesini gösterir**
- **Karar – Uygulamaya güvenilip güvenilmediğini gösterir.**



Uygulama	PID	Şirket	Kullanıcı Adı	Sandbox Seviyesi	Karar
Windows Operating System	0		NT AUTHORITY\SYSTEM		
System	4		NT AUTHORITY\SYSTEM	Devre dışı	Güvenilir
smss.exe	280	Microsoft Corporation	NT AUTHORITY\SYSTEM	Devre dışı	Güvenilir
csrss.exe	380	Microsoft Corporation	NT AUTHORITY\SYSTEM	Devre dışı	Güvenilir
wininit.exe	460	Microsoft Corporation	NT AUTHORITY\SYSTEM	Devre dışı	Güvenilir
services.exe	572	Microsoft Corporation	NT AUTHORITY\SYSTEM	Devre dışı	Güvenilir
svchost.exe	692	Microsoft Corporation	NT AUTHORITY\SYSTEM	Devre dışı	Güvenilir
explorer.exe	3824	Microsoft Corporation	FremeN-VM-PC\Freme...	Devre dışı	Güvenilir
svchost.exe	772	Microsoft Corporation	NT AUTHORITY\NETW...	Devre dışı	Güvenilir
cmdagent.exe	860	COMODO	NT AUTHORITY\SYSTEM	Devre dışı	Güvenilir
svchost.exe	952	Microsoft Corporation	NT AUTHORITY\NETW...	Devre dışı	Güvenilir
svchost.exe	1020	Microsoft Corporation	NT AUTHORITY\Local ...	Devre dışı	Güvenilir
audiodg.exe	2340	Microsoft Corporation	NT AUTHORITY\Local ...	Devre dışı	Güvenilir
svchost.exe	320	Microsoft Corporation	NT AUTHORITY\SYSTEM	Devre dışı	Güvenilir
dwm.exe	2124	Microsoft Corporation	FremeN-VM-PC\Freme...	Devre dışı	Güvenilir
svchost.exe	428	Microsoft Corporation	NT AUTHORITY\SYSTEM	Devre dışı	Güvenilir
svchost.exe	420	Microsoft Corporation	NT AUTHORITY\Local ...	Devre dışı	Güvenilir
spoolsv.exe	1324	Microsoft Corporation	NT AUTHORITY\SYSTEM	Devre dışı	Güvenilir
svchost.exe	1356	Microsoft Corporation	NT AUTHORITY\Local ...	Devre dışı	Güvenilir
vmtoolsd.exe	1524	VMware, Inc.	NT AUTHORITY\SYSTEM	Devre dışı	Güvenilir
VMUpgradeHelper.exe	1644	VMware, Inc.	NT AUTHORITY\SYSTEM	Devre dışı	Güvenilir
taskhost.exe	1764	Microsoft Corporation	FremeN-VM-PC\Freme...	Devre dışı	Güvenilir
TPAutoConnSvc.exe	2100	ThinPrint AG	NT AUTHORITY\SYSTEM	Devre dışı	Güvenilir/Yükleyici
TPAutoConnect.exe	2356	ThinPrint AG	FremeN-VM-PC\Freme...	Devre dışı	Güvenilir
SearchIndexer.exe	2680	Microsoft Corporation	NT AUTHORITY\SYSTEM	Devre dışı	Güvenilir

Herhangi bir işleme sağ tıklayın:

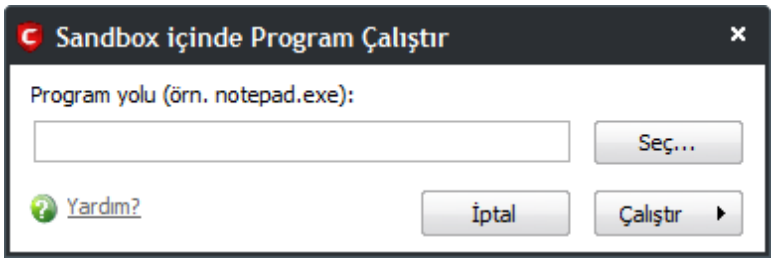
- **Tam Yolu Göster: Uygulama adına ek olarak dosyanın konumunu da gösterir.**
- **Yalnızca Sandbox içindekileri göster: Yalnızca Sandbox içinde çalışan işlemleri gösterir.**
- **Sonlandır: Seçili işlemi sonlandırır.**
- **Sonlandır & Engelle: Seçili işlemi sonlandırır ve dosyayı Savunma+ Engellenmiş Dosyalara ekler.**
- **Güvenilir Dosyalara Ekle:** Seçili programı Güvenilir Dosyalar listesine ekler.
- **Çevrimiçi İncele:** Seçili programın güvenilir olup olmadığına Comodo çevrimiçi veritabanından bakılır.
- **Gönder:** Seçili uygulama analiz için Comodo'ya gönderilir.

4.7 Sandbox içinde Program Çalıştır

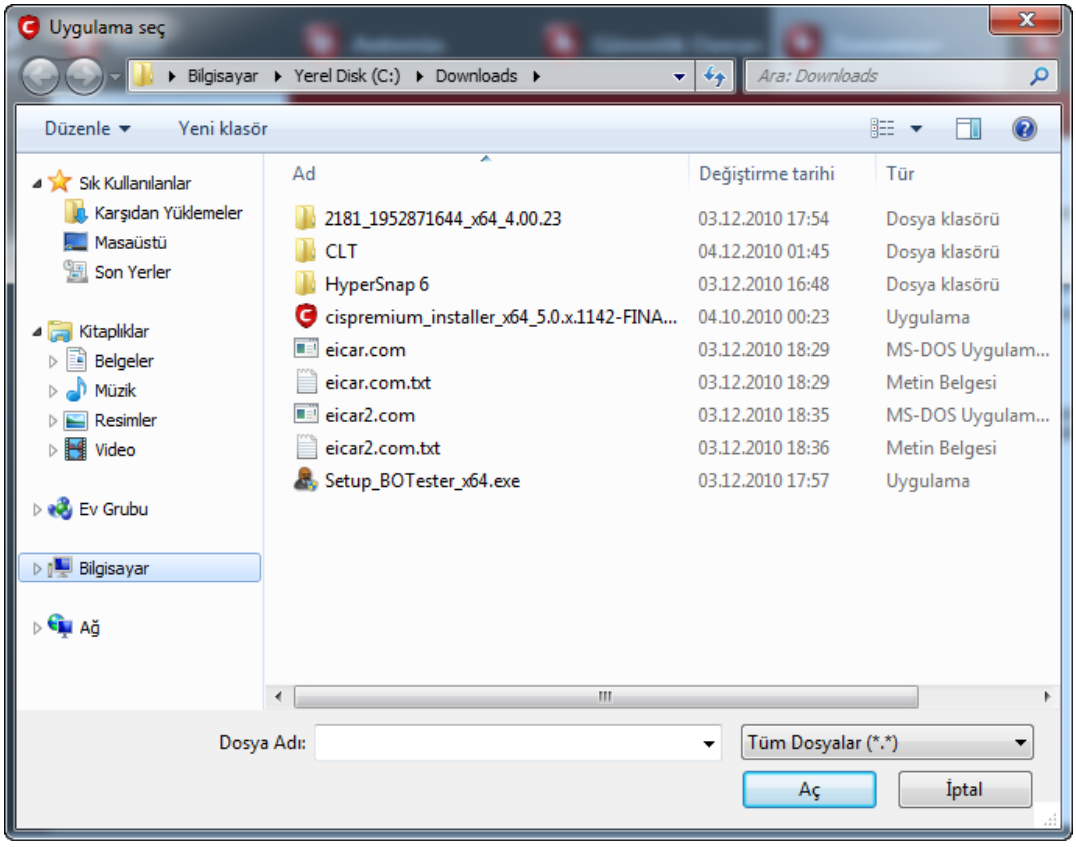
Comodo Internet Security programları özel olarak sandbox içinde çalıştırmanıza olanak sağlar. Bu programları test etmenizde ve onlara güvenip güvenemeyeceğinize karar vermenize yardımcı olur. Bu şekilde çalıştırılan programlar bir kerelik sandbox içinde çalışır. Sonraki çalıştırmalarda sandbox içinde çalıştırılmaz (Sandboxlama sürecini geçtiğini varsayarsak). Uzun süreli olarak uygulamaları sandbox içinde çalıştırmak istiyorsanız Her zaman Sandbox arayüzünü kullanın.

Uygulamayı Sandbox içinde çalıştırmak için

1. Savunma+ arayüzünden 'Sandbox içinde Program Çalıştır' bağlantısına tıklayın. Aşağıdaki diyalog açılacaktır:

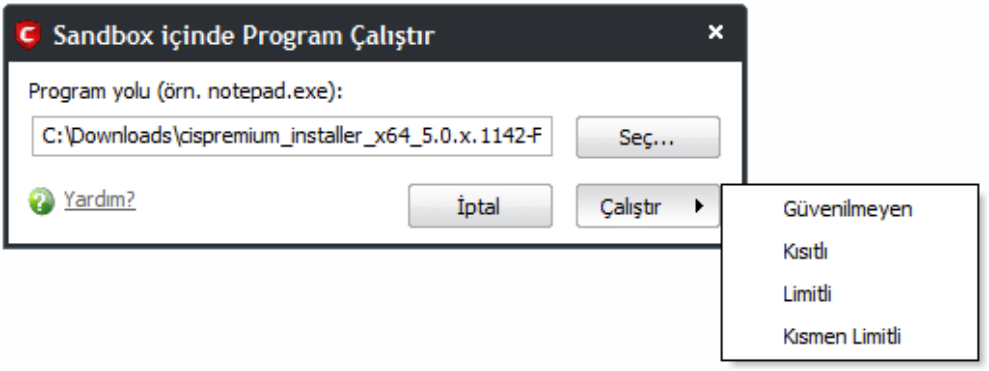


2. Sandbox içinde çalıştırılmasını istediğiniz programı seçin ve 'Seç' düğmesine tıklayın.



3. Uygulamaya gidin ve 'Aç' düğmesine tıklayın. Aşağıdaki örnekte Opera.exe seçilmiştir.

4. ‘Çalıştır’ düğmesine tıklayın ve menüden kısıtlama seviyesini seçin.



- **Güvenilmeyen - Uygulama işletim sisteminin hiçbir kaynağına erişemez. Uygulama bir seferde 10’dan fazla işlem yürütemez ve limitli erişim haklarıyla çalışır.**

Not: Kullanıcı etkileşimi gerektiren bazı uygulamalar bu ayarlar altında düzgün çalışmayabilir.

- **Kısıtlı - Uygulama çok az sayıda işletim sistemi kaynağına erişebilir. Uygulama bir seferde 10’dan fazla işlem yürütemez ve çok limitli erişim hakları ile çalışır.**

Not: Oyunlar gibi bazı uygulamalar bu ayarlar altında düzgün çalışmayabilir.

- **Limitli - Uygulama yalnızca belirli işletim sistemi kaynaklarına erişilebilir. Uygulama bir seferde 10’dan fazla işlem yürütemez ve Yönetici hesap ayrıcalıkları olmadan çalışır.**
- **Kısmen Limitli - Uygulama tüm işletim sistemi kaynaklarına erişilebilir. Korunan dosyalara/kayıt anahtarlarına erişemez. Hata ayıkla, sürücü yükleme gibi ayrıcalıklı işlemler gerçekleştiremez.**

Program seçtiğiniz kısıtlama seviyesinde bir kerelik sandbox içinde çalıştırılacaktır.

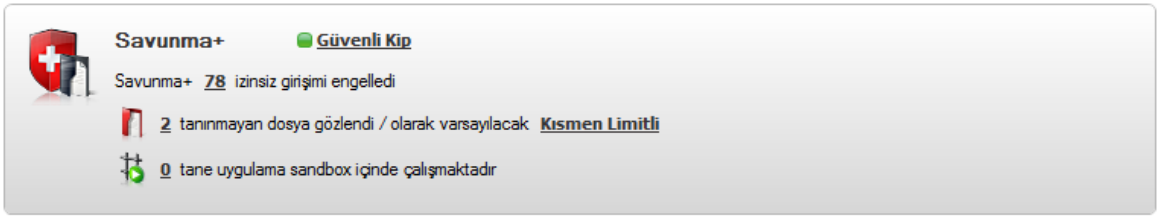
4.8 Savunma+ Ayarları

Savunma+ bilgisayarınızdaki tüm yürütülebilir dosyaları sürekli olarak izler. Savunma+ açıkken, HER defasında bilinmeyen uygulama yürütülebiliri (.exe, .dll, .sys, .bat vb.) çalıştırılırken kullanıcı uyarılır. Çalıştırılmasına izin verilen yürütülebilirler yalnızca sizin izin verdiklerinizdir. İzin verme işlemi çeşitli yollarla yapılabilir; Bilgisayar Güvenlik İlkelerinden elle onlara işlem yürütmesi hakkı tanıyarak; Savunma+ uyarısından karar vererek veya uygulama Comodo güvenli listesinde yer alıyorsa. Savunma+ ayrıca otomatik olarak kritik sistem dosyalarını ve klasörlerini, kayıt defterini izinsiz değişikliklere karşı korur. Bu tür koruma kötücül yazılımların çalışmasını ve sistem dosyalarında değişiklik yapmasını önleyerek Comodo Internet Security’nin savunmasına ek bir katman ekler.

Deneyimsiz kullanıcolar için Not: Bu sayfa sıklıkla ‘yürütülebilir’ (veya ‘yürütülebilir dosyalar’) değinir. ‘Yürütülebilir’ bilgisayarınıza görevler veya işlevler gerçekleştirmesi için talimat verebilen dosyadır. Bilgisayarınızda çalışan her program, uygulama ve aygıt başlamak için yürütülebilir dosyaya gerek duyar. En çok

tanınan yürütülebilir dosya '.exe'dir. Diğerleri ise cpl .dll, .drv, .inf, .ocx, .pf, .scr, .sys dir.

Savunma+ Ayarları alanı hızlıcana güvelik seviyesini ayarlamanıza izin verir. Bu ayarlara 'Savunma+' arayüzünden ve daha hızlı olarak Özet Ekranından (aşağıda göründüğü gibi) erişilebilir.



Bu ayarlar aşağıdaki sekmeler kullanılarak yapılabilir.

•Genel Ayarlar sekmesi

•Yürütme Denetimi Ayarları sekmesi

•Sandbox Ayarları sekmesi

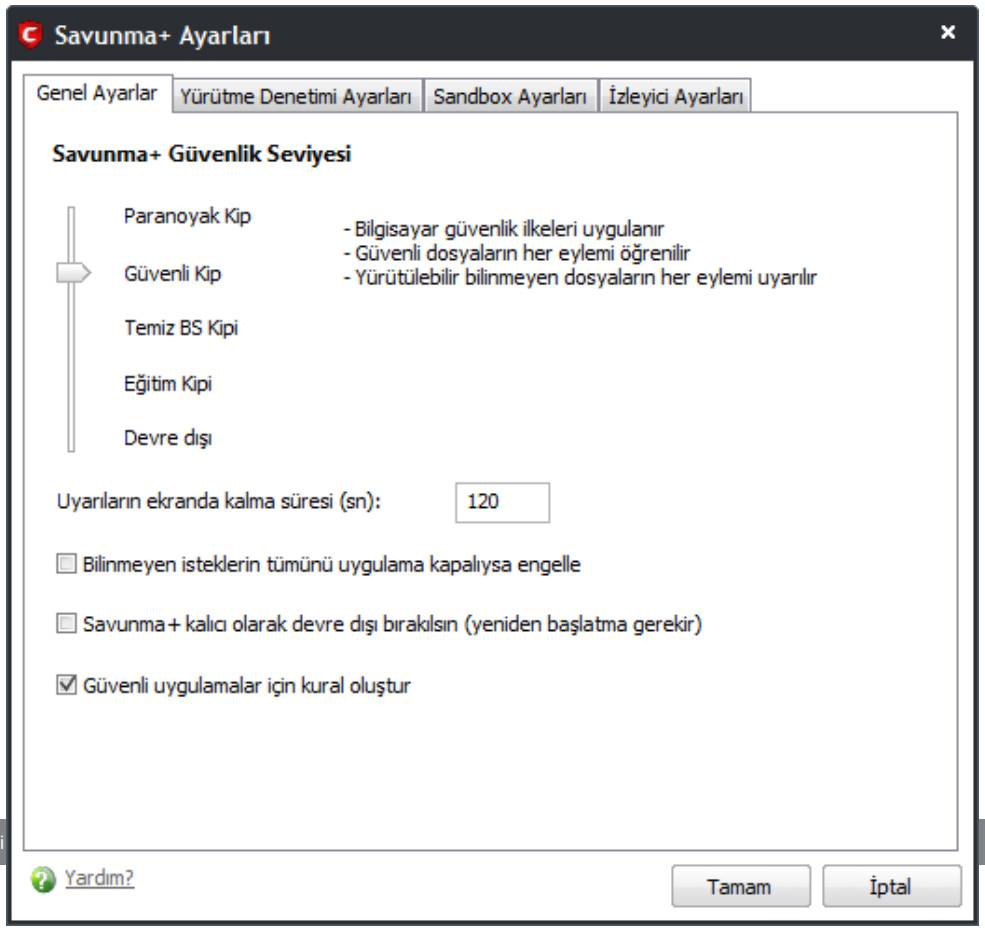
•İzleyici Ayarları sekmesi

4.8.1 Genel Ayarlar

Kaydırıcı Seçenekleri

Comodo Internet Security güvenlik seviyesi kaydıracı ile Savunma+ güvenlik seviyesini ayarlamanıza izin verir.

Bulunan seçenekler: **Paranoyak Kip, Güvenli Kip, Temiz PC Kipi, Eğitim Kipi ve Devre Dışıdır**. Burada seçilen



ayar CIS özet ekranında da görüntülenir.

- **Paranoyak Kip: Bu en yüksek güvenlik seviyesi ayarıdır ve Savunma+ tüm yürütülebilirleri izler ve denetler. Comodo Internet Security yalnızca kullanıcı tanımlı ilkelere uyar, otomatik olarak uygulamaların davranışlarını öğrenmez ve 'İzin Ver' kuralı oluşturmaz. Savunma+ bu seviyede çok fazla uyarı verir bu yüzden bu seçeneği yalnızca deneyimli kullanıcılara öneririz.**
- **Güvenli Kip: Savunma+ 'Güvenli' uygulamalara izin verir ve 'Güvenli uygulamalar için kural oluştur' seçeneği işaretli ise 'İzin Ver' kuralı da oluşturulur. Sertifikalı olmayan, bilinmeyen uygulamalar için uyarı verilir. Uyarıdan öntanımlı 'Güvenilir Uygulama' ilke seçerek bu uygulamaları da güvenli olarak tanıtabilirsiniz. Eğer bilgisayarınız yeni değilse veya temiz değilsse bu kipi kullanmanızı öneririz.**
- **Temiz PC Kipi:** Savunma+ bu seviyeye ayarlandıktan sonra yüklenen uygulamaları izler ve denetler ve sistemde kurulu olan uygulamaların etkinliklerini öğrenir. Bu seviye yeni veya temiz olan sistemler içindir. *Bu noktadan sonra* Savunma+ yeni, tanınmayan uygulamalar için uyarı verir. Bu kipte 'Tanınmayan Dosyalar' bölümünden kaldırılan dosyalar temiz olarak varsayılır.
- **Eğitim Kipi:** Savunma+ tüm yürütülebilirlerin etkinliklerini seviye değiştirilene kadar öğrenir. BU kipte uyarı almazsınız. Bu kipe bilgisayarınızdaki tüm uygulamalar güvenli ise geçmenizi öneririz.

İpucu: Bu kip 'Oyun Kipi' olarak kullanılabilir. Bu ayar bilinmeyen fakat güvenli olan veya oyunu ilk defa çalıştırıyorsanız kullanışlı olabilir. Bu uyarıları bastırırken uygulama için gerekli kuralları öğrenir. Daha sonra başka bir kipe geçebilirsiniz.

- **Devre Dışı:** Savunma+ korumasını kapatır. Sisteminizde alternatif başka koruma yüklü değilse bu seviyeye ayarlamayın.

İşaret Kutusu Seçenekleri

- **Uyarıların ekranda kalma süresi (sn) -** Uyarıların ne kadar süre görüntülenmesi gerektiğini ayarlayabilirsiniz. Varsayılan değer 120 sn'dir.
- **Güvenilir Yazılım Sağlayıcıları tarafından imzalanan uygulamalara güven –** Güvenilir Yazılım Sağlayıcıları Listesindeki sağlayıcıların imzaladığı uygulamalar güvenli olarak sayılır. Daha fazla bilgi için Güvenilir Yazılım Sağlayıcıları bölümüne bakın.
- **Bilinmeyen isteklerin tümünü hizmet çalışmıyorsa engelle –** Comodo Internet Security hizmeti çalışmıyorsa Bilgisayar Güvenlik İlkelerinde bulunmayan isteklerin tümünü engeller.
- **Savunma+ kalıcı olarak devre dışı bırakılsın (yeniden başlatma gerekir)** – Savunma+ kalıcı olarak devre dışı bırakılır. Alternatif bir korumanız (HIPS) yoksa bu seçeneği işaretlemenizi tavsiye etmiyoruz.
- **Güvenli uygulamalar için kural oluştur –** Güvenli uygulamalar için otomatik olarak Bilgisayar Güvenlik İlkelerinde kural oluşturulur.

Not: Savunma+ şu durumlarda uygulamalara güvenir:

- **Uygulama/dosya Savunma+ Görevleri altındaki Güvenilir Dosyalarda bulunuyorsa**

- **Savunma+ Görevleri altındaki Güvenilir Yazılım Sağlayıcıları listesinden bir sağlayıcı tarafından imzalanmış ise.**
- **Comodo Beyaz Listesinde yer alıyorsa.**

Varsayılan olarak CIS otomatik olarak kural oluşturmaz böylece yapılandırma gereksiz yere büyümemiş olur.

Bu seçenek etkinleştirilse CIS otomatik olarak 'izin ver' kuralı oluşturmaya başlar. Bu kurallar Bilgisayar Güvenlik İlkeleri arayüzünde listelenir. Deneyimli kullanıcılar bunları isteklerine ve gereksinimlerine göre değiştirebilirler.

4.8.2 Yürütme Denetimi Ayarları

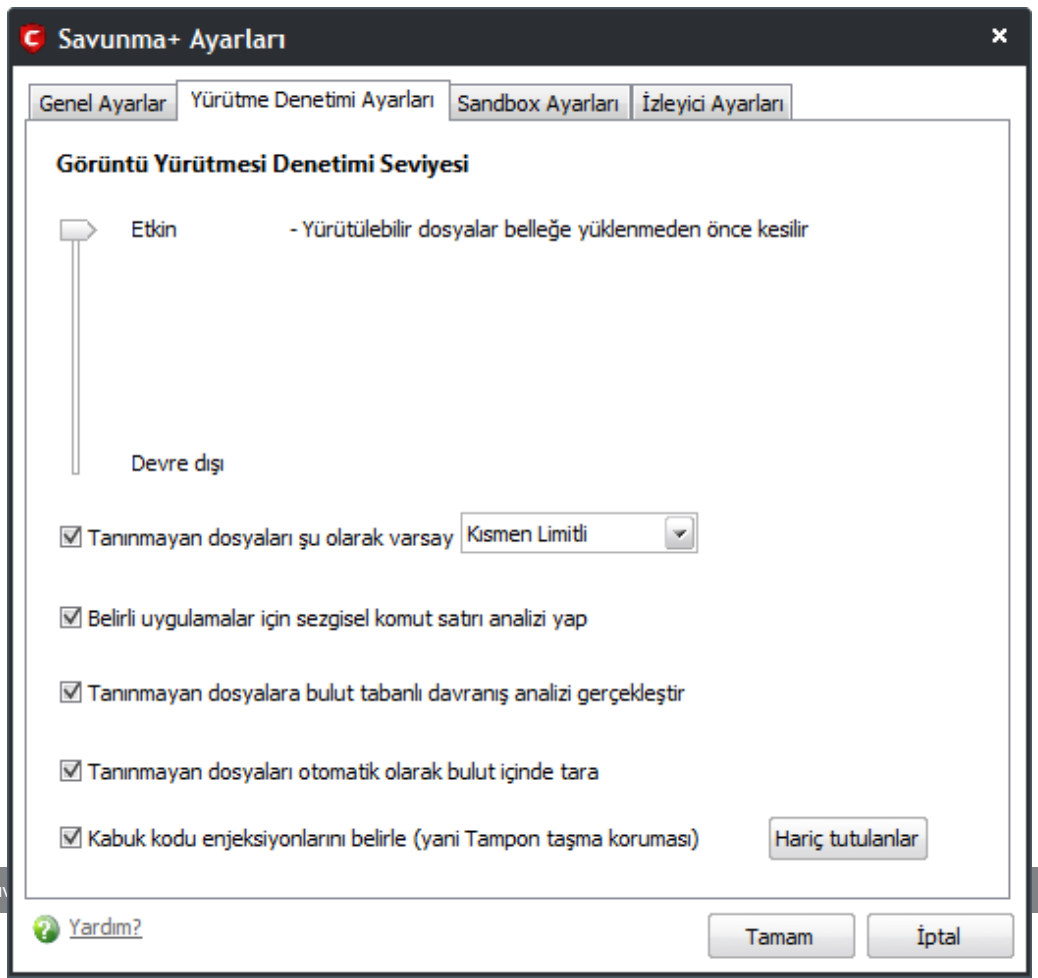
Yürütme Denetimi Savunma+ motorunun iç parçalarından biridir. Savunma+ Güvenlik Seviyesi 'Öğrenim Kipi' veya 'Temiz BS Kipi' olarak ayarlandığında belleğe yüklenen yürütülebilirlerin görüntülerinin doğrulanmasından sorumludur.

Comodo Internet Security yürütülebilirin belleğe yüklenme girişiminde imzasını hesaplar ve Comodo güvenli listesiyle karşılaştırır. Karşılaştırma sonucu imzanın karşılığı bulunursa uygulama güvenlidir değilse tanınmıyordur ve uyarı çıkar.

Bu alan izleyicinin ne kadar korumacı olmasını ve ne tür dosyaların denetlenmesini hızlıcana belirlemenize olanak sağlar.

Görüntü Yürütmesi Denetimi Seviyesi Kaydırgacı

Ayarlar arayüzündeki kaydırgaç güvenlik seviyesini **Etkin** ve **Devre Dışı** durumları arasında değiştirmenize izin verir. Savunma+ kalıcı olarak Savunma+ Ayarları arayüzünden kapatılmışsa bu ayarın etkisi olmaz.



•**Etkin** – Savunma+ yürütülebilir dosyaları belleğe yüklenmeden önce keser.

•**Devre Dışı** – Yürütülebilir dosyaların yürütmesi denetlenmez.

İşaret Kutuları

Tanınmayan dosyaları şu olarak varsay – Beş seçenek vardır ve seçili olan uygulanır.

•**Kısmen Limitli -** Uygulama tüm işletim sistemi kaynaklarına erişilebilir. Korunan dosyalara/kayıt anahtarlarına erişemez. Hata ayıkla, sürücü yükleme gibi ayrıcalıklı işlemler gerçekleştiremez. Gelişmiş Ayarlar altında tanımlanan diğer kısıtlamalar uygulanır.

•**Limitli -** Uygulama yalnızca belirli işletim sistemi kaynaklarına erişilebilir. Uygulama bir seferde 10'dan fazla işlem yürütemez ve Yönetici hesap ayrıcalıkları olmadan çalışır. Gelişmiş Ayarlar altında tanımlanan diğer kısıtlamalar uygulanır.

•**Kısıtlı -** Uygulama çok az sayıda işletim sistemi kaynağına erişebilir. Uygulama bir seferde 10'dan fazla işlem yürütemez ve çok limitli erişim hakları ile çalışır. Gelişmiş Ayarlar altında tanımlanan diğer kısıtlamalar uygulanır.

Not: Oyunlar gibi bazı uygulamalar bu ayarlar altında düzgün çalışmayabilir.

•**Güvenilmeyen -** Uygulama işletim sisteminin hiçbir kaynağına erişemez. Uygulama bir seferde 10'dan fazla işlem yürütemez ve limitli erişim haklarıyla çalışır. Gelişmiş Ayarlar altında tanımlanan diğer kısıtlamalar uygulanır.

Not: Kullanıcı etkileşimi gerektiren bazı uygulamalar bu ayarlar altında düzgün çalışmayabilir.

•**Engellenmiş –** Uygulamanın çalışmasına izin verilmez.

Belirli uygulamalar için sezgisel komut satırı analizi yap – Toplu komut dosyalarını veya betikleri yürüten ana uygulamalar için komut satırı denetimi yapılır. (wscript.exe, cmd.exe, java.exe, javaw.exe, mshta.exe gibi). Örneğin, "cmd.exe zararlı.bat' gibi.

- Not**:** 'Sezgisel' tarama, dosya kodunun incelenerek tipik zararlı kodu içerip içermediğine bakılmasıdır. Sezgisel tarama dosya imzalarına bakmak yerine dosyanın zararlı davranışları veya özellikleri içerip içermediğine bakar. Bu sayede tarama motoru şüpheli betikleri ve programları virüs veritabanında bulunmasalar bile saptayabilir.

Tanımayan dosyalara bulut tabanlı davranış analizi gerçekleştir – Tanınmayan ve Comodo'nun beyaz listesinde bulunmayan dosyalar Comodo Anında Kötücül Yazılım Analizi (CIMA) sunucularına yollanarak davranış analizinden geçer. Her bir dosya Comodo sunucularındaki sanal ortamda çalıştırılır ve kötü niyetli kodlar içerip içermediğine bakılır. Sonuçlar bilgisayarınıza kısa sürede (15 dk) geri yollanır.

Tanınmayan dosyaları otomatik olarak bulut içinde tara – Tanınmayan dosyalar otomatik olarak Comodo sunucularına gönderilir ve taranır.

Kabuk kodu enjeksiyonlarını belirle (yani Tampon taşma koruması) – Tampon taşma korumasını etkinleştirir.

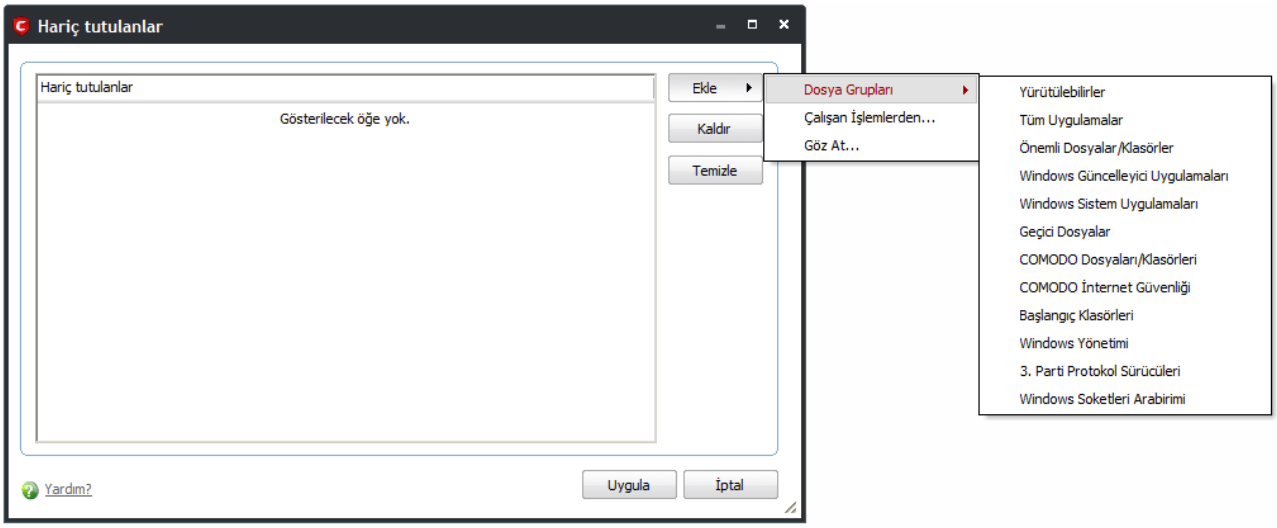
Uygulama tamponun işleyebileceğinden daha fazla veriyi tampona göndermesiyle meydana gelir. Bu olası bir korsan saldırısı olabilir.

Bu korumanın açılması Comodo Internet Security'nin her olası saldırıda uyarı vermesini sağlar. Yazılıma ve sağlayıcısına göre işlemin yürütülmesi isteğine izin verebilir veya engelleyebilirsiniz. Bu uyarı hakkında daha fazla bilgi için buraya tıklayın.

Comodo bu seçeneğin her zaman işaretli olmasını tavsiye eder.

Kabuk kodu enjeksiyonlarından bazı dosyaları veya dosya türlerini hariç tutmak için.

1. 'Hariç tutulanlar' düğmesine tıklayın.



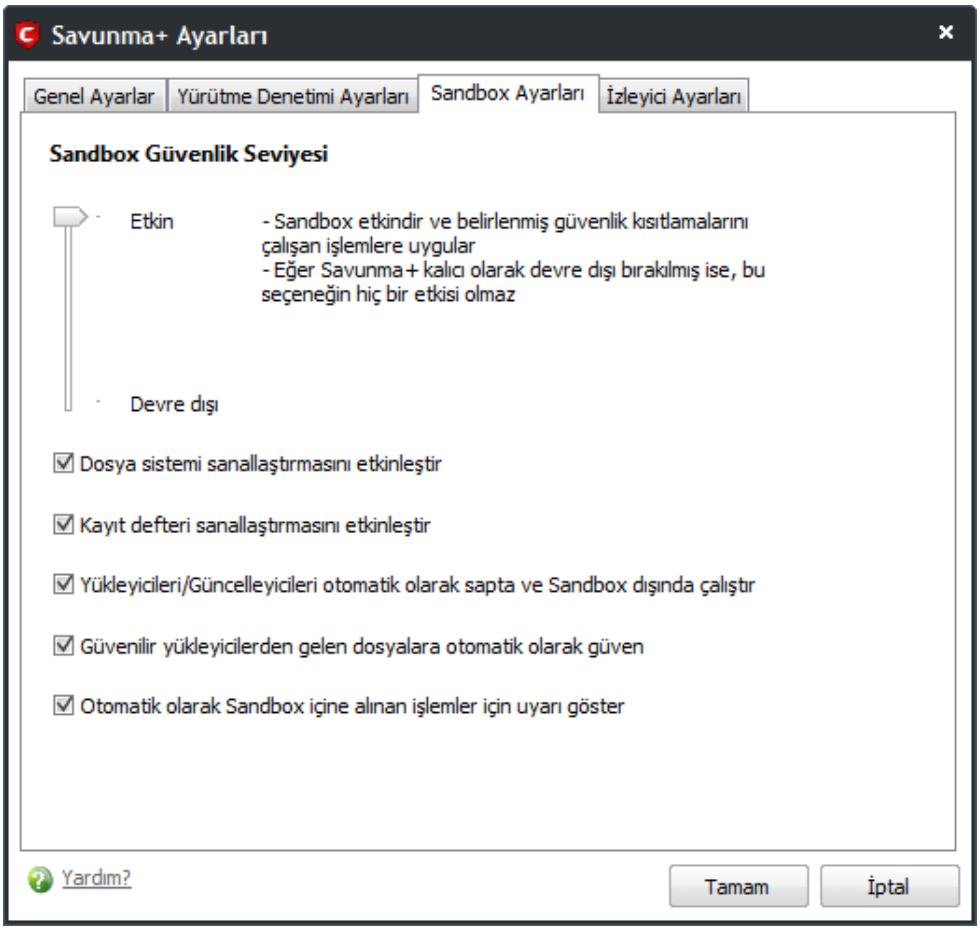
2. 'Ekle' ile hariç tutulacak dosyayı veya dosya grubunu seçin. Bulunan tüm seçim seçeneklerini görmek için buraya tıklayın.
3. Listeden kaldırmak için girdi seçin ve 'Kaldır' düğmesine tıklayın.
4. Geçersiz girdileri kaldırmak için 'Temizle' düğmesine tıklayın.

Not: Bu ayarlar yalnızca deneyimli kullanıcılar içindir.

5. Ayarları uygulamak için 'Uygula' düğmesine tıklayın.

4.8.3 Sandbox Ayarları

Sandbox Ayarları alanı sandbox davranışını ve yapılandırmasını değiştirmenize izin verir. Sandbox Ayarlarına erişmek için 'Savunma+ Ayarları' sonra 'Sandbox Ayarları' sekmesine gidin. Daha fazla bilgi için 4.1 - Sandbox - Tanıtım bölümüne bakın.



Sandbox Güvenlik Seviyesi Kaydırgacı

Ayarlar arayüzündeki Güvenlik Seviyesi kaydırgacı güvenlik seviyesini **Etkin** ve **Devre Dışı** durumları arasında değiştirmenize izin verir. Savunma+ kalıcı olarak Savunma+ Ayarları arayüzünden kapatılmışsa bu ayarın etkisi olmaz.

İşaret Kutuları

Dosya sistemi sanallaştırmasını etkinleştir – Sandbox içindeki uygulamalar 'gerçek' dosya sistemi üzerinde değişiklik yapamaz. Bunun yerine oluşturulan sanal dosya sistemi kullanılır. Bu seçenek etkin değilse uygulamalar gerekli girdileri yapamayacağı için düzgün çalışmayabilir.

> **Deneyimli kullanıcılar için**: Sanal dosya sistemi sandbox çalışma klasörü içinde oluşturulur (ör. c:\sandbox\<uygulama adı>).
>
> Sandbox Ayarlarında dosya sistemi sanallaştırması etkin değilse bu seçenek etkin olsa bile sanallaştırma yapılmaz.

Kayıt defteri sanallaştırmasını etkinleştir - Sandbox içindeki uygulamalar 'gerçek' kayıt defteri üzerinde değişiklik

yapamaz. Bunun yerine oluşturulan sanal kayıt defteri kullanılır. Bu seçenek etkin değilse uygulamalar gerekli girdileri yapamayacağı için düzgün çalışmayabilir.

Deneyimli kullanıcılar için: Sanal kayıt defteri sandbox anahtarı içinde oluşturulur (ör. HKEY_LOCAL_MACHINE\SYSTEM\Sandbox\...).

Sandbox Ayarlarında kayıt defteri sanallaştırması etkin değilse bu seçenek etkin olsa bile sanallaştırma yapılmaz.

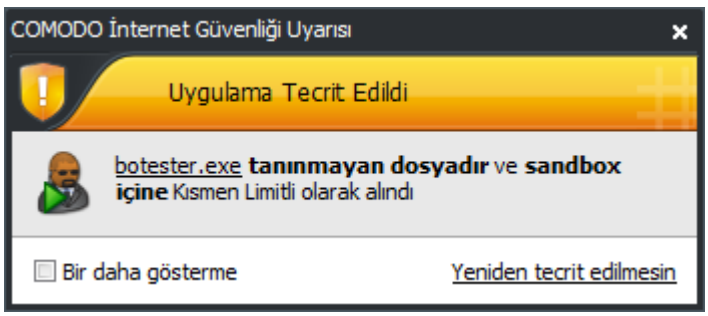
Aşağıdaki tablo bu arayüzden ve Bilgisayar Güvenlik İlkleri > Her zaman Sandbox > Ekle > Gelişmiş Ayarlar altından yapılan sanallaştırma ayarlarının önceliğini gösterir.

Sandbox Ayarları	Her zaman Sandbox > Gelişmiş Ayarlar	Ayar belirli bir uygulama için etkin mi?
Evet	Evet	Evet
Evet	Hayır	Hayır
Hayır	Evet	Hayır
Hayır	Hayır	Hayır

Yükleyicileri/Güncelleyicileri otomatik olarak sapta ve Sandbox dışında çalıştır – Yükleyici/Güncelleyici yürütülünce sandbox dışında çalıştırır. Yalnızca güvenilir sağlayıcılardan gelen yükleyicileri / güncelleyicileri çalıştıracaksanız bu seçeneği işaretleyin.

Güvenilir yükleyicilerden gelen dosyalara otomatik olarak güven – Güvenilir yükleyici tarafından oluşturulan dosyalara da güvenilir. Yani bunlar da sandbox dılında çalıştırılır.

Otomatik olarak Sandbox içine alınan işlemler için uyarı göster – Varsayılan olarak CIS otomatik olarak sandbox içine alınan işlemler için uyarı gösterir. Bu seçenek ile bunu açıp kapatabilirsiniz.



Ayarların geçerli olması için 'Tamam' düğmesine tıklayın.

Ek bilgi:

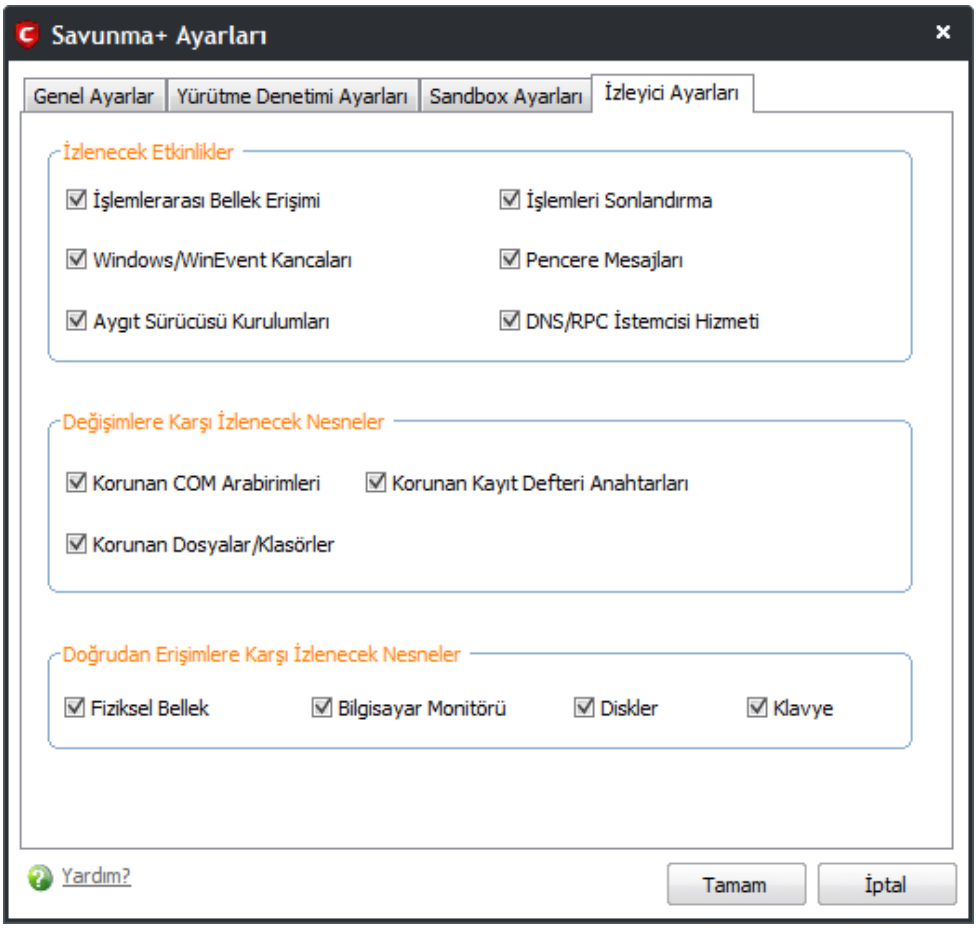
- Ayrıca bakınız 'Sandbox Uyarıları'
- Ayrıca bakınız 'Bilinmeyen dosyalar: Sandbox içine Alma ve Tarama Süreci.

4.8.4 İzleyici Ayarları

'İzleyici Ayarları' sekmesi Savunma+ tarafından hangi etkinliklerin, birimlerin ve nesnelerin izlenmesi gerektiğini yapılandırmanıza izin verir.

Not: Burada seçtiğiniz ayarlar genele uygulanır.

- **Burada devre dışı bıraktığınız etkinlikler, birimler ve nesneler genel olarak kapatılır ve onlara genel olarak 'İzin Ver'miş olursunuz. Bu 'İzin Ver' ayarı 'Erişim Hakları' ve 'Koruma Ayarları' ilkelerinde tanımlanmış kuralları geçersiz kılar.**



İzlenecek Etkinlikler:

- **İşlemlerarası Bellek Erişimi –** Kötücül yazılımlar değişik türde saldırılar için (tuş kaydetme, uygulamanın davranışını değiştirme, özel bilgileri diğer işlemlere yollayarak çalma, uygulamanın kimliğini çalma veya uygulamayı taklit etme) bellek alanına kötü niyetli kodlar enjekte ederler. Bu tür saldırıları önlemek için bu seçeneği işaretli bırakın. Böylece Savunma+ bu tür girişimlerde uyarı verecektir.
- **Windows/WinEvent Kancaları –** Microsoft Windows işletim sisteminde olaylar (mesajlar, fare eylemleri, tuş girişleri gibi) uygulamaya erişmeden *önce* bunların önünü kesebilen mekanizma kancalardır. İşlev

olaylara göre hareket edebilir, bazı durumlarda onları değiştirebilir veya eleyebilir. Asıl olarak kancalar yasal uygulama geliştiricilerinin daha güçlü ve kullanışlı uygulamalar yapabilmeleri için geliştirilmiştir. Kancalar ayrıca bilgisayar korsanları tarafından sömürülerek daha güçlü kötücül yazılımlar yapmalarına da olanak sunar. Örneğin, tuşları girişlerini kaydeden zararlılar. Bu tür saldırıları önlemek için bu seçeneği işaretli bırakın. Böylece Savunma+ bu tür girişimlerde uyarı verecektir.

- **Aygıt Sürücüsü Kurulumları –** Aygıt sürücüleri uygulamaların veya işletim sisteminin bilgisayardaki donanımlar ile etkileşimine izin veren küçük programlardır. (Disk sürücüleri, CPU, USB aygıtları, ekran kartı, monitör gibi). Kötü niyetli aygıt sürücüsünün yüklenmesi bilgisayara zarar verebilir hatta o donanımın denetimini bilgisayar korsanına verebilir. Bu tür saldırıları önlemek için bu seçeneği işaretli bırakın. Böylece Savunma+ bu tür girişimlerde uyarı verecektir.
- **İşlemleri Sonlandırma –** İşlem bir programın çalışan kopyasıdır. (örneğin, Comodo Internet Security işlemi 'cfp.exe' dir. 'Ctrl+Alt+Delete' basın ve sistemde çalışan tüm işlemleri görmek için 'İşlemler' sekmesine gidin). İşlem sonlandırmak programı sonlandırır. Zararlı yazılımlar genellikle güvenlik yazılımını atlatmak için onun işlemlerini sonlandırmayı dener. Bu tür saldırıları önlemek için bu seçeneği işaretli bırakın. Böylece Savunma+ bu tür girişimlerde uyarı verecektir.
- **Pencere Mesajları –** Bu ayar ile Comodo Internet Security uygulamaların diğer uygulamaların davranışını değiştirmek için özel Pencere Mesajları gönderme girişiminde bulunmasını izler ve saptar (örneğin, WM_PASTE komutunu kullanarak).
- **DNS İstemcisi Hizmeti –** Bu ayar uygulamalar 'Windows DNS hizmetine' erişim girişiminde bulunduğu zaman sizi uyarır – DNS özyinelemeli saldırısı başlatmak için kullanılabilir. DNS özyinelemeli saldırısı bir tür DDOS saldırısıdır ve özyinelemeli (recursive) saldırılarla ağdaki bir veya birden çok DNS sunucusunu isteklere cevap veremez hale getirme girişimidir. Sorgularla taşmış bir DNS sunucusunda CPU kullanımı sonuçta en yüksek düzeye ulaşır ve DNS Sunucusu hizmeti kullanılamaz hale gelir. Ağda tam olarak çalışan bir DNS sunucusu olmadan, ağ kullanıcıları, DNS üzerinden öğrenilen ağ hizmetlerini kullanamaz. Bu tür saldırıları önlemek için bu seçeneği işaretli bırakın. Böylece Savunma+ bu tür girişimlerde uyarı verecektir.

Not: DNS (Domain Name System ; Etki Alanı İsim Sistemi), ağdaki bilgisayarları ve ağ hizmetlerini adlandırmak için kullanılan bir sistemdir. DNS adlandırması, Internet gibi TCP/IP ağlarında,

bilgisayarları ve hizmetleri hatırlanması kolay adlarla tanımlamak için kullanılır. Kullanıcı bir uygulamaya bir DNS adı girdiğinde, DNS hizmetleri bu adı çözümleyip kaynağa ulaşılmasını

sağlayan bir IP adresi bilgisini kullanıcıya temin eder.

Değişimlere Karşı İzlenecek Nesneler:

- **Korunan COM Arabirimleri burada belirtilmiş COM arabirimlerini izler.**
- **Korunan Kayıt Defteri Anahtarları burada belirtilmiş Kayıt anahtarlarını izler.**
- **Korunan Dosyalar/Klasörler burada belirtilmiş dosyaları ve klasörleri izler.**

Doğrudan Erişimlere Karşı İzlenecek Nesneler:

Comodo Internet Security'nin bilgisayarınızdaki kritik sistem nesnelerini doğrudan erişimlere karşı izleyip izlemeyeceğini belirler. Kötü niyetli uygulamalar doğrudan erişim yöntemini kullanarak depolama aygıtlarından veri

elde edebilir, diğer yürütülebilir yazılımı değiştirebilir veya yazılama bulaşabilir, tuşları kaydedebilir ve dahası… Comodo ortalama kullanıcılar için bu ayarların etkin olarak bırakılmasını tavsiye eder:

- **Fiziksel Bellek:** Bilgisayarınızın belleğini uygulamalar veya işlemler tarafından doğrudan erişime karşı izler. Kötü niyetli programlar geniş çaplı sömürüler çalıştırmak için fiziksel belleğe erişim girişiminde bulunur – en ünlüsü 'Hafıza Taşırma' sömürüsüdür.
- **Bilgisayar Monitörü:** Comodo Internet Security işlemler bilgisayar monitörüne doğrudan erişme girişiminde bulunduğunda uyarı verir. Yasal uygulamalar bazen buna erişme gereği duyduğu halde, yeni gelişen casus yazılımlar da bunu kullanıcı etkinliklerini izlemek için kullanmaktadır. (örneğin, ekran görüntüsü almak, tarayıcı etkinliklerinin kaydı için vs.)
- **Diskler:** Yerel disklerinizi çalışan işlemlerin doğrudan erişimine karşı izler. Bu, kötü niyetli yazılımların doğrudan disklere erişerek disklerde depolanan verileri almasına, disk üzerindeki dosyaları yok etmesine veya dosya sistemine gereksiz veriler yazarak bozmasına karşı korumada yardımcı olur.
- **Klavye:** Klavyeyi doğrudan erişimlere karşı izler. 'Tuş Kaydediciler' olarak bilinen kötü niyetli yazılımlar klavyeden girdiğiniz tuşları kaydedebilir ve bunu parolalarınızı, kredi kartı numaralarınızı ve diğer kişisel bilgilerinizi çalmak için kullanabilir. Bu ayar seçiliyken Comodo Internet Security her doğrudan klavye erişimi girişiminde uyarı verir.

5 Daha Seçenekleri - Tanıtım

Daha Seçenekler arayüzü hem genel yapılandırmayla ilgili değişik alanlar hem de Comodo Internet Security tecrübenizi arttıracak ve geliştirecek kullanışlı araçlar ve kısayollar içerir.

Erişmek için gezinti panelinden 'Daha' 

bağlantısına tıklayın.

Bu bölümdeki alanların ayrıntılı açıklamalarını görmek için aşağıdaki bağlantılara tıklatın.

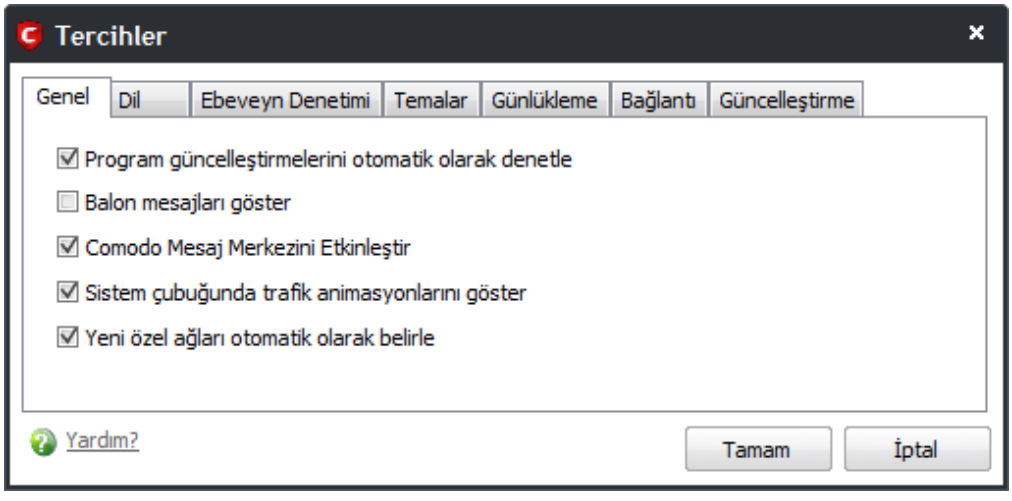
- **Tercihler:** Kullanıcının Comodo Internet Security genel ayarlarını yapılandırmasına izin verir (parola koruması, güncelleştirme seçenekleri, dil, tema ve buna benzer.)
- **Yapılandırmalarımı Yönet:** Kullanıcının Comodo Internet Security yapılandırma profillerini yönetmesine, içeri veya dışarı aktarmasına izin verir.
- **Hata Tanılayıcı:** Kurulumunuzla ilgili problemleri tanılamanıza yardımcı olur.
- **Güncelleştirmeleri Denetle:** Comodo Internet Security güncelleştiricisini başlatır.
- **Destek Forumlarına Göz At:** Comodo Kullanıcı Forumlarına yönlendirir.

- **Yardım**: Bu yardım dosyasını açar.
- **Hakkında**: Ürün sürümü ve telif hakları bilgisini görüntüler.

5.1 Tercihler

Daha bölümündeki **Tercihler** menüsü Comodo Internet Security'nin çalışmasıyla ilişkili çeşitli seçenekleri yapılandırmanıza izin verir.

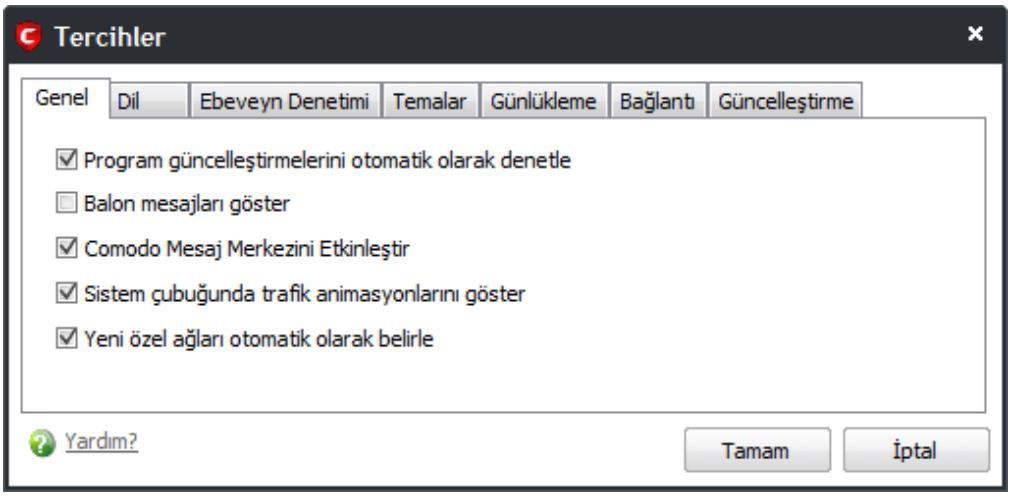
Tercihler diyalog kutusunu açmak için



- 'Daha' içinden 'Tercihler' bölümüne gidin.

Ayarlarınızı yapmak için aşağıdaki sekmeler bulunur:

- Genel
- Dil
- Ebeveyn Denetimi
- Temalar
- Bağlantı
- Güncelleştirme



5.1.1 Genel Ayarlar

- **Program güncelleştirmelerini otomatik olarak denetle –** Bu seçenek Comodo Internet Security'nin program güncelleştirmelerini otomatik olarak denetleyip denetlemeyeceğini belirler. Bu seçenek işaretliyken Comodo Internet Security her 24 saatte bir VE bilgisayarınızı her yeniden başlattığınızda güncelleştirmeleri denetler. Güncelleştirme bulunursa otomatik olarak indirilir ve yüklenir. Bu seçenek işaretli değilse kullanıcılar 'Daha' altındaki 'Güncelleştirmeleri Denetle' bölümünden elle güncelleştirmeleri denetleyebilir.
- **Balon mesajları göster –** Bunlar ekranın sağ alt köşesinde çıkan bilgilendirme mesajlarıdır. Bunlar genellikle '…öğreniyor' mesajlarıdır. Bu mesajları görmek istemiyorsanız bu kutudaki işareti kaldırın.
- **Sistem çubuğunda trafik animasyonlarını göster –** Varsayılan olarak, sistem çubuğundaki 'Kalkan' işaretinde her trafik olduğunda animasyon görünür.

Trafik giden ise, kalkanın sağında yeşil ok yukarı doğru çıkar; trafik gelen ise, kalkanın solunda kırmızı ok aşağı doğru iner şekilde animasyon görünür. Bu animasyonu görmek istemiyorsanız bu kutudaki işareti kaldırın.

- **Yeni özel ağları otomatik olarak belirle –** Güvenlik duvarı yeni ağları otomatik olarak belirler.
- **Comodo Mesaj Merkezini etkinleştir** – Bu seçenek işaretliyse Comodo Internet Security düzenli aralıklarla Comodo Mesaj Merkezi penceresini görüntüler.

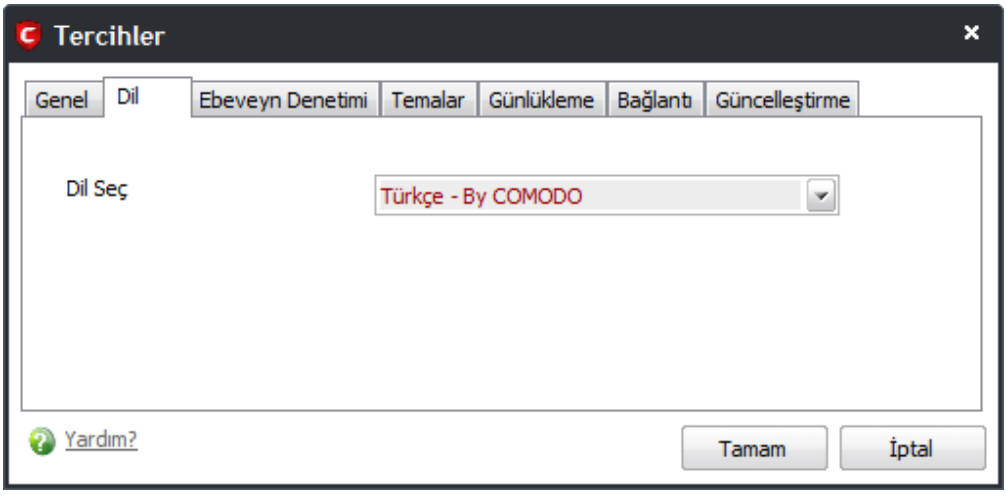
Comodo Mesaj Merkezi penceresi Güvenlik Uyarılarını, Comodo Internet Security ile ilgili haberleri ve önemli güvenlik güncelleştirmeleri hakkında bilgileri gösterir. 'Daha fazla bilgi' bağlantısına tıklanması sizi Comodo Forumlarına (http://forums.comodo.com) yönlendirir. Kayıt olmak ücretsizdir.

5.1.2 Dil Ayarları

Comodo Internet Security birçok dilde mevcuttur. Açılır menüden seçerek dil değiştirebilirsiniz.

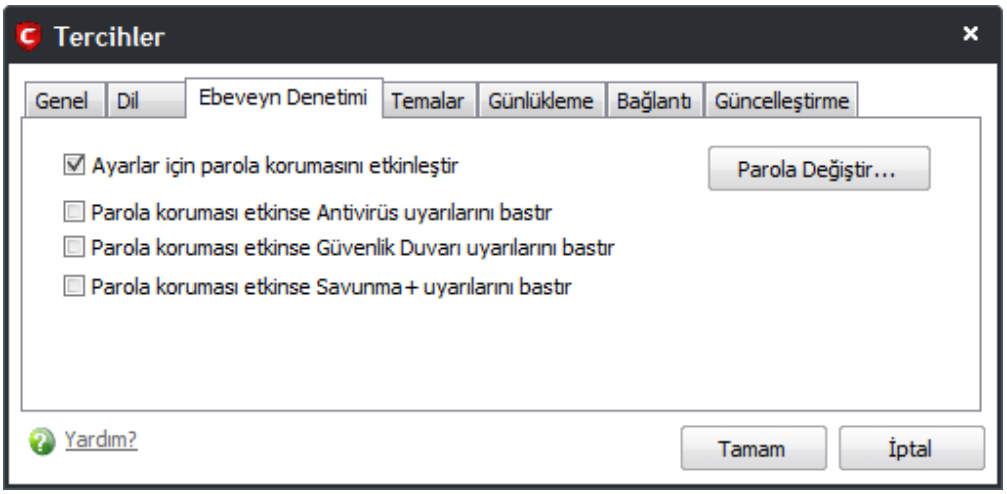
Seçiminizin etkili olabilmesi için Comodo Internet Security uygulamasını yeniden başlatmanız gerekir. Bunu şu yollarla yapabilirsiniz:

- **Bilgisayarınızı yeniden başlatarak (önerilen); veya**
- **Sistem çubuğundaki kalkan simgesine sağ tıklayın 'Çıkış' seçin ve Programlar menüsünden Başlat > Programlar > COMODO > Comodo Internet Security veya masaüstündeki simgeye çift tıklayarak yeniden başlatın. Yeniden başladıktan sonra seçtiğiniz dilde görünecektir.**

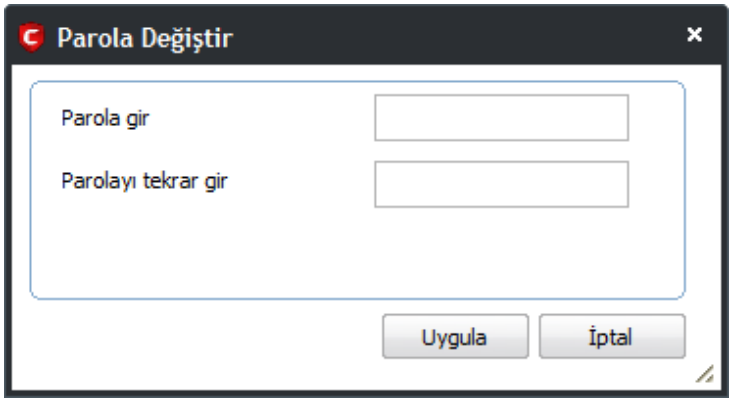


5.1.3 Ebeveyn Denetimi Ayarları

'Ebeveyn Denetimi' sekmesi Comodo Internet Security'nin parola korumasını yapılandırmanıza izin verir.



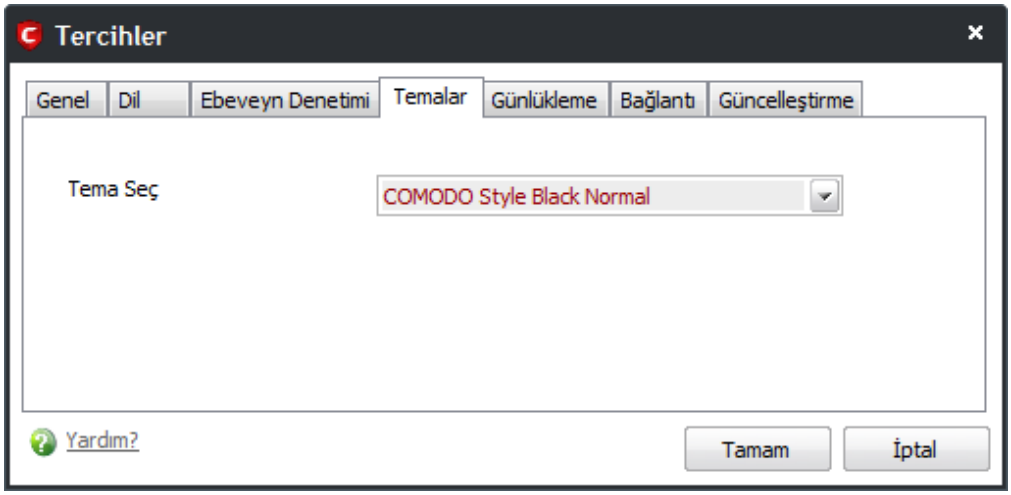
- **Ayarlar için parola korumasını etkinleştir –** Bu seçenek tüm önemli yapılandırma bölümleri için parola korumasını etkinleştirir. Bu seçeneği seçtiyseniz, 'Parola Değiştir' düğmesine tıklayarak parola girmeli ve onu doğrulamalısınız. Önemli bölümlere erişmeye çalıştığınız her zaman bu parola sorulur.



- **Parola koruması etkinse Antivirüs uyarılarını bastır –** Seçiliyse, Antivirüs uyarılarını bastırır. Bilgisayarı deneyimsiz birileri kullanırken onların uyarılara vereceği yanlış cevaplar sonucu sisteme gelebilecek zararları önlemek için bu seçeneği kullanabilirsiniz. Antivirüs bir zararlı saptadığı zaman uyarı görüntülemeden bu zararlı etkinliğini engeller.
- **Parola koruması etkinse Güvenlik Duvarı uyarılarını bastır -** Seçiliyse, Güvenlik Duvarı uyarılarını bastırır. Bilgisayarı deneyimsiz birileri kullanırken onların uyarılara vereceği yanlış cevaplar sonucu sisteme gelebilecek zararları önlemek için bu seçeneği kullanabilirsiniz. Güvenlik Duvarı bir izinsiz girişim saptadığı zaman uyarı görüntülemeden bu girişimi engeller.
- **Parola koruması etkinse Savunma+ uyarılarını bastır -** Seçiliyse, Savunma+ uyarılarını bastırır. Bilgisayarı deneyimsiz birileri kullanırken onların uyarılara vereceği yanlış cevaplar sonucu sisteme gelebilecek zararları önlemek için bu seçeneği kullanabilirsiniz. Savunma+ bir izinsiz girişim saptadığı zaman uyarı görüntülemeden bu zararlı etkinliğini engeller.

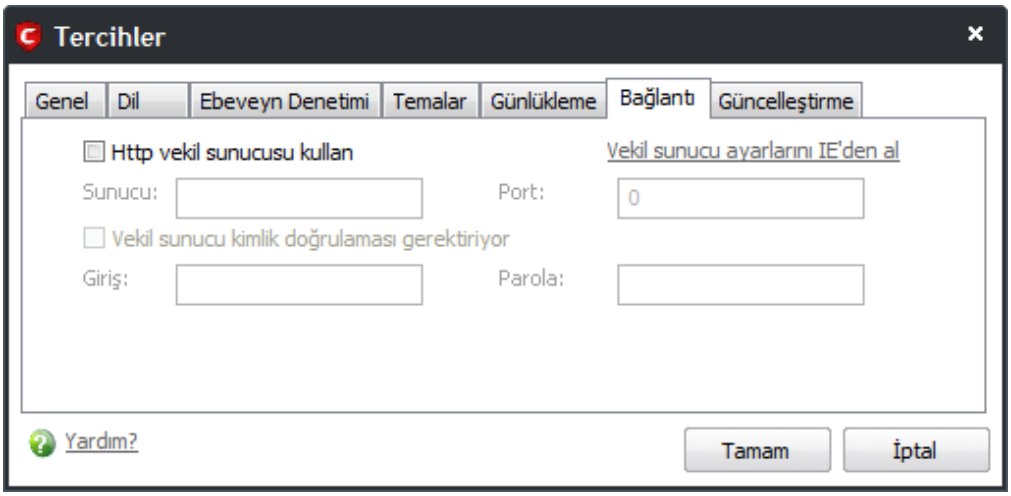
5.1.4 Temalar

Temalar sekmesi Comodo Internet Security görünümünü değiştirmenize izin verir. Açılır menüden seçerek tema değiştirebilirsiniz.



5.1.5 Bağlantı Ayarları

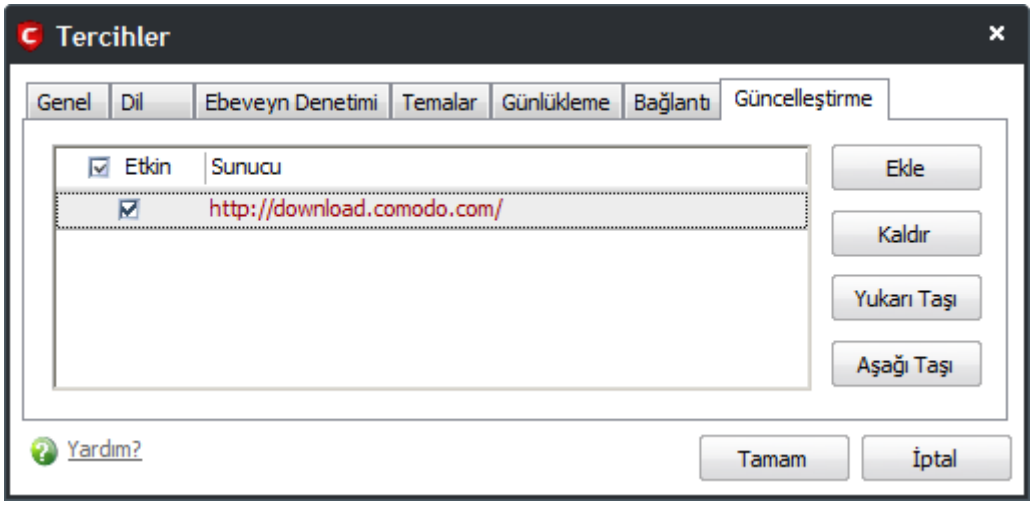
Bağlantı sekmesi Comodo Internet Security'nin güncelleştirmeleri almak vs. için Comodo sunucularına nasıl bağlanacağını yapılandırmanıza izin verir. Ağınızda Vekil Sunucu kullanıyorsanız veya CIS'in vekil sunucu kullanmasını istiyorsanız Vekil Sunucu ayarlarını bu arayüzden yapabilirsiniz.



- **'Http vekil sunucu kullan' seçin ve 'Sunucu' alanına IP adresi veya ad girin, 'Port' alanına da port numarası girin.**
  - Vekil sunucusu kimlik doğrulaması gerektiriyor ise 'Vekil sunucu kimlik doğrulaması gerektiriyor' seçeneğini işaretleyin. 'Giriş' ve 'Parola' alanlarını doldurun.
- **Eğer Comodo Internet Security'nin vekil sunucu ayarlarını Internet Explorer'dan almasını istiyorsanız 'Vekil sunucu ayarlarını IE'den al' bağlantısına tıklayın.**

5.1.6 Güncelleştirme Ayarları

Güncelleştirme sekmesi AV veritabanı güncelleştirmelerini açıp kapatmanıza ve güncelleştirmelerin hangi sunucudan indirilmesi gerektiğini seçmenize izin verir. Varsayılan olarak, Comodo Sunucusunun URL'si girilidir.



•Comodo sunucularından indirmek istiyorsanız ayarı olduğu gibi bırakabilirsiniz.

•Yerel ağa bağlıysanız ve CIS program güncelleştirmeleri ağdaki HTTP sunucusunda veya başka bir makinada çalışan Comodo Çevrimdışı Güncelleyicisinde bulunuyorsa bu bilgisayarları bu alana ekleyebilirsiniz.

Not:: Comodo Çevrimdışı Güncelleyicisi kullanıcıların yerel HTTP sunucusu üzerinden güncelleştirmeleri sağlamasına izin verir. Deneyimli kullanıcılar bu aracı http://enterprise.comodo.com/security-solutions/endpoint-security/endpoint-security-manager/free-trial.php adresinden indirebilirler.

•Sunucu eklemek için 'Ekle' düğmesine tıklayın ve URL veya IP adresi girin.

•Çoklu sunucu eklemek için bu işlemi tekrarlayın.

•Yukarı Taşı ve Aşağı Taşı düğmelerini kullanarak sunucu seçin.

CIS çevrimdışı olsanız bile tanımlanmış sunuculardan güncelleştirmeleri indirir.

•Ayarların geçerli olması için 'Tamam' düğmesine tıklayın.

5.2 Yapılandırmalarımı Yönet

Comodo Internet Security güvenlik ayarlarınızın yapılandırmalarını kaydetmenize ve dosyaya aktarmanıza izin verir. Bu aynı yapılandırmayı birçok bilgisayara yüklemek isteyen sistem yöneticileri için kullanışlıdır. Eğer sisteminiz yükseltiyorsanız ve CIS'i kaldırıp yeniden kurmanız gerekiyorsa yapılandırmanızın yedeğini alıp daha sonra geri yükleyebilirsiniz. Birden fazla bilgisayara elle ayar yapmak yerine bu şekilde bir bilgisayarda yaptığınız ayarları hızlıcana diğerlerine uygulayabilirsiniz.

5.2.1 Comodo Ön Ayarlı Yapılandırmaları

Varsayılan olarak Comodo Internet Security üç ön ayarlı yapılandırma ile gelir. Yükleme seçiminize göre bu yapılandırmalardan biri ETKİN YAPILANDIRMA olarak ayarlanır. CIS sistem simgesine sağ tıklayarak istediğiniz zaman yapılandırmalar arası geçiş yapabilirsiniz.

Her bir yapılandırma hakkında daha fazla bilgi için aşağıdaki bağlantılara tıklayın:

- COMODO - Internet Security
- COMODO - Proactive Security
- COMODO - Firewall Security

Önemli Not: Yapılan değişiklikler etkin olan yapılandırmaya kaydedilir.

Üç ön ayarlı yapılandırma ile sağlanan varsayılan güvenlik seviyeleri hakkında ayrıntılı açıklama aşağıda verilmiştir:

COMODO - Internet Security – Antivirüs ve Güvenlik Duvarı bileşenleri yüklendiği zaman bu varsayılan yapılandırmadır. Güvenlik Duvarı her zaman Güvenli Kipe ayarlıdır. Fakat kurulum sırasında gerçekleştirilen tarama sonucunda sistem temiz çıkarsa Savunma+ kipi Temiz BS Kipine ayarlanır. Değilse, varsayılan Güvenli Kiptir. Bu kipte,

- **Yürütme Denetimi devre dışıdır.**
- **Bilgisayar Monitörü/Disk/Klavye/DNS İstemcisi erişimi/Pencere Mesajları izlenmez.**
- **Yalnızca genel olarak bulaşılan dosyalar/klasörler bulaşmaya karşı korunur.**
- **Yalızca genel olarak sömürülen COM arabirimleri korunur.**
- **Savunma+ sisteme zararlı bulaşmasını önlemeye göre ayarlanmıştır.**

Internet Security seçeneğini değiştirmek istiyorsanız, bunun için Yapılandırmalarım arayüzünü kullanabilirsiniz.

COMODO - Proactive Security – Bu yapılandırma CIS korumasını en yüksek seviyeye çıkartır. Mümkün tüm korumalar ve izlemeler etkinleştirilmiştir. Eğer yalnızca kurulumda Comodo Güvenlik Duvarı seçilmişse bir sonraki ekranda kullanıcıya hangi yapılandırmayı varsayılan olarak kullanmak istediği sorulur. Güvenlik Duvarı her zaman Güvenli Kipe ayarlıdır. Fakat kurulum sırasında gerçekleştirilen tarama sonucunda sistem temiz çıkarsa Savunma+ kipi Temiz BS Kipine ayarlanır. Değilse, varsayılan kip Güvenli Kiptir.

Proactive Security seçeneğini değiştirmek istiyorsanız, bunun için Yapılandırmalarım arayüzünü kullanabilirsiniz.

COMODO - Firewall Security – Bu yapılandırma Güvenlik Duvarı ve Savunma+ için optimum koruma seçilyse etkinleştirilir. Güvenlik Duvarı her zaman Güvenli Kipe ayarlıdır. Fakat kurulum sırasında gerçekleştirilen tarama sonucunda sistem temiz çıkarsa Savunma+ kipi Temiz BS Kipine ayarlanır. Değilse, varsayılan kip Güvenli Kiptir.

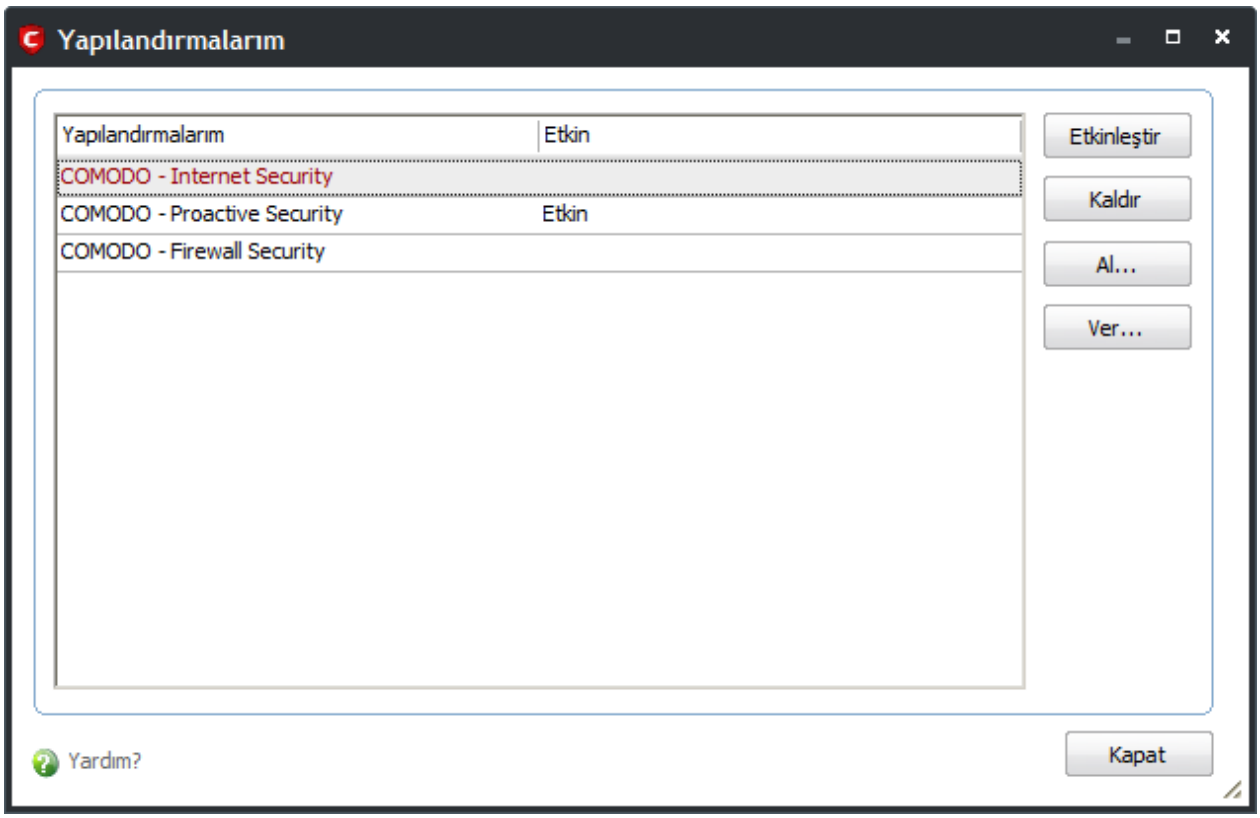
- **Yürütme Denetimi kullanıcı tarafından başlatılmayan uygulamaları denetlemeye ayarlıdır.**

- **Bilgisayar Monitörü/Disk/Klavye izlenmez.**
- **Yalnızca genel olarak bulaşılan dosyalar/klasörler bulaşmaya karşı korunur.**
- **Yalızca genel olarak sömürülen COM arabirimleri korunur.**
- **Savunma+ sisteme zararlı bulaşmasını önlemeye göre ve Internet erişimi sızıntılarını saptamaya yönelik ayarlanmıştır (zararlı bulaşmış olsa bile).**

Firewall Security seçeneğini değiştirmek istiyorsanız, bunun için Yapılandırmalarım arayüzünü kullanabilirsiniz.

5.2.2 Alma/Verme ve Kişisel Yapılandırmaların Yönetilmesi

Yapılandırma arayüzüne erişmek için



1. 'Daha > Yapılandırmalarımı Yönet' bölümüne gidin.

Bu arayüze ilk defa erişiyorsanız şu üç ön ayarlı seçimi görebilirsiniz.:

- COMODO - Internet Security
- COMODO - Proactive Security
- COMODO - Firewall Security

'Etkin' olarak belirtilen yapılandırma kullanımda olan yapılandırmadır.

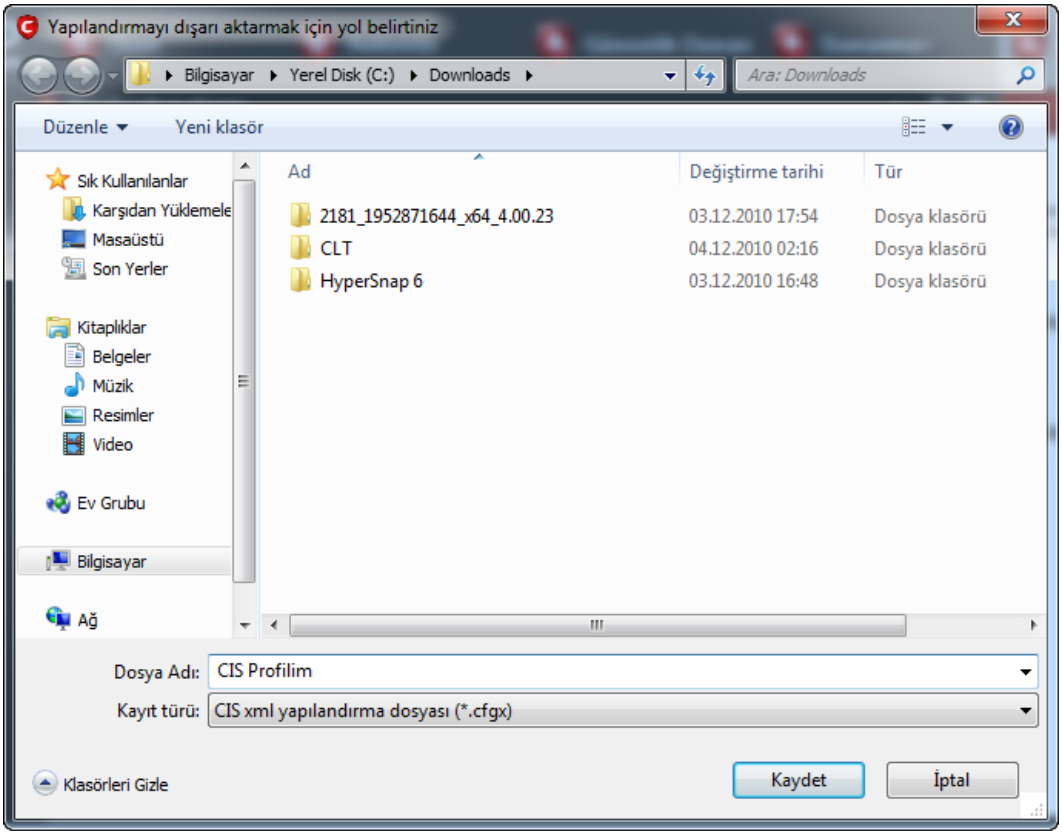
1. Daha fazla bilgi almak istediğiniz alanlara tıklayın:
    - Yapılandırmamı dosyaya çıkart
    - Dosyadan kayıtlı yapılandırmamı al

- Farklı yapılandırma ayarını etkinleştir
- Etkin olmayan yapılandırmayı sil

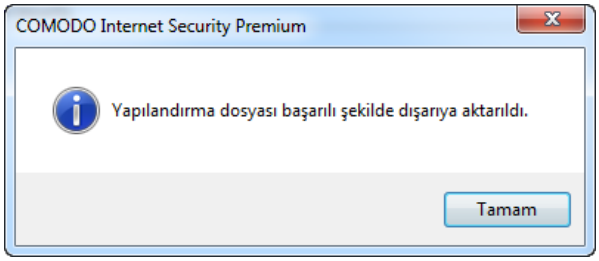
Yapılandırmamı dosyaya çıkart

Etkin yapılandırmayı dosyaya çıkartmak için

1. 'Ver' düğmesine tıklayın.
2. Profil için dosya adı girin ve seçtiğiniz konuma kaydedin.



Onay diyaloğu başarılı çıkartma sonrası görünür.



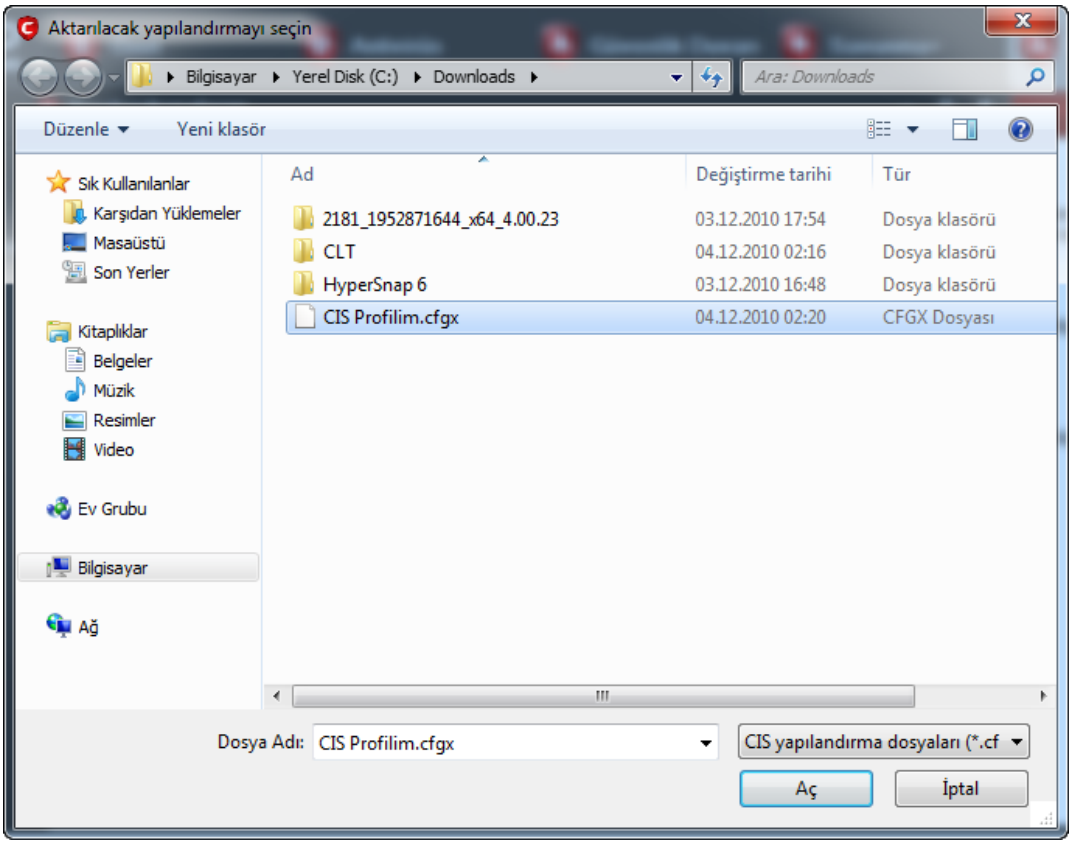
Dosyadan kayıtlı yapılandırmamı al

Yapılandırma profilinin alınması Comodo Internet Security içinde herhangi bir profili depolamanıza izin verir. Alınan

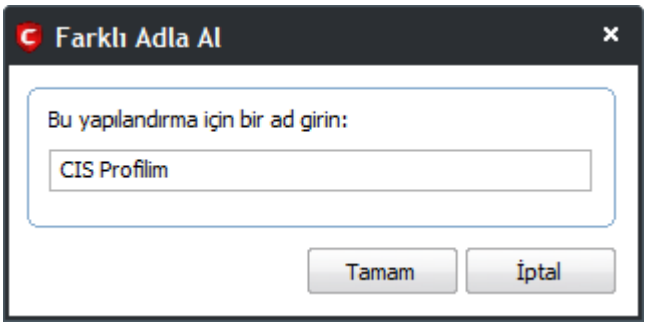
yapılandırma profilleri siz seçene kadar etkin olmaz.

Profil almak için

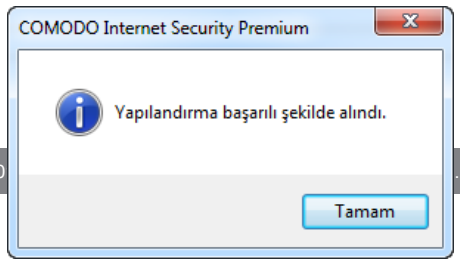
1. 'Al' düğmesine tıklayın.
2. Kayıtlı profilin konumuna gidin ve 'Aç' düğmesine tıklayın.



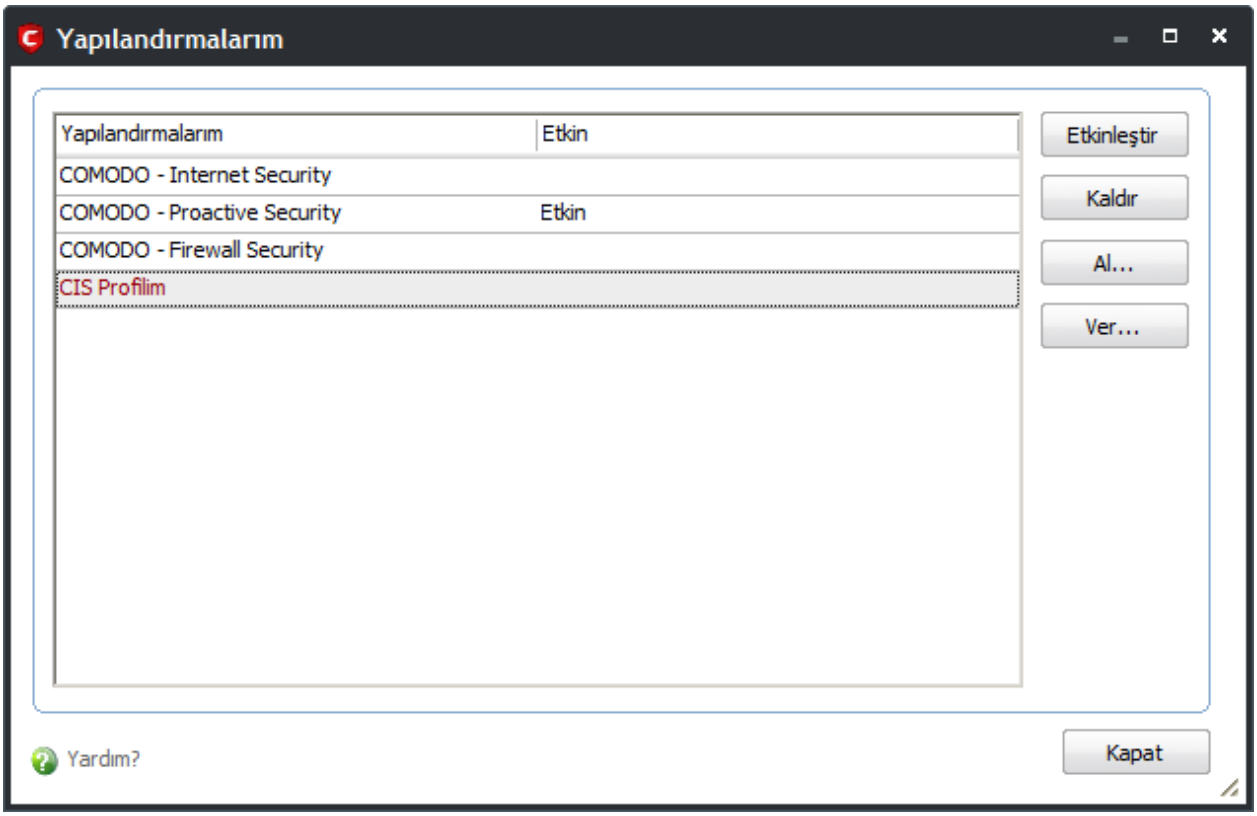
3. 'Farklı Adla Al' diyaloğu görünür, profil için istediğiniz adı girin ve 'Tamam' düğmesine tıklayın.



Onay diyaloğu başarılı çıkartma sonrası görünür.



Alındıktan sonra, yapılandırma profili atanmaya hazırdır.



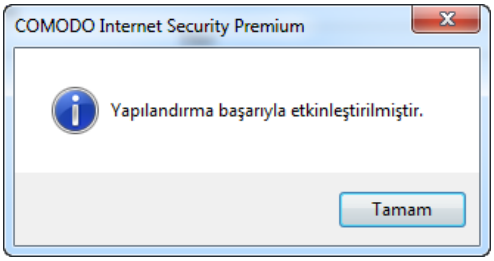
Farklı yapılandırma ayarını etkinleştir

Etkinleştir seçeneği hızlıcana yapılandırmalar arası geçiş yapmanıza izin verir.

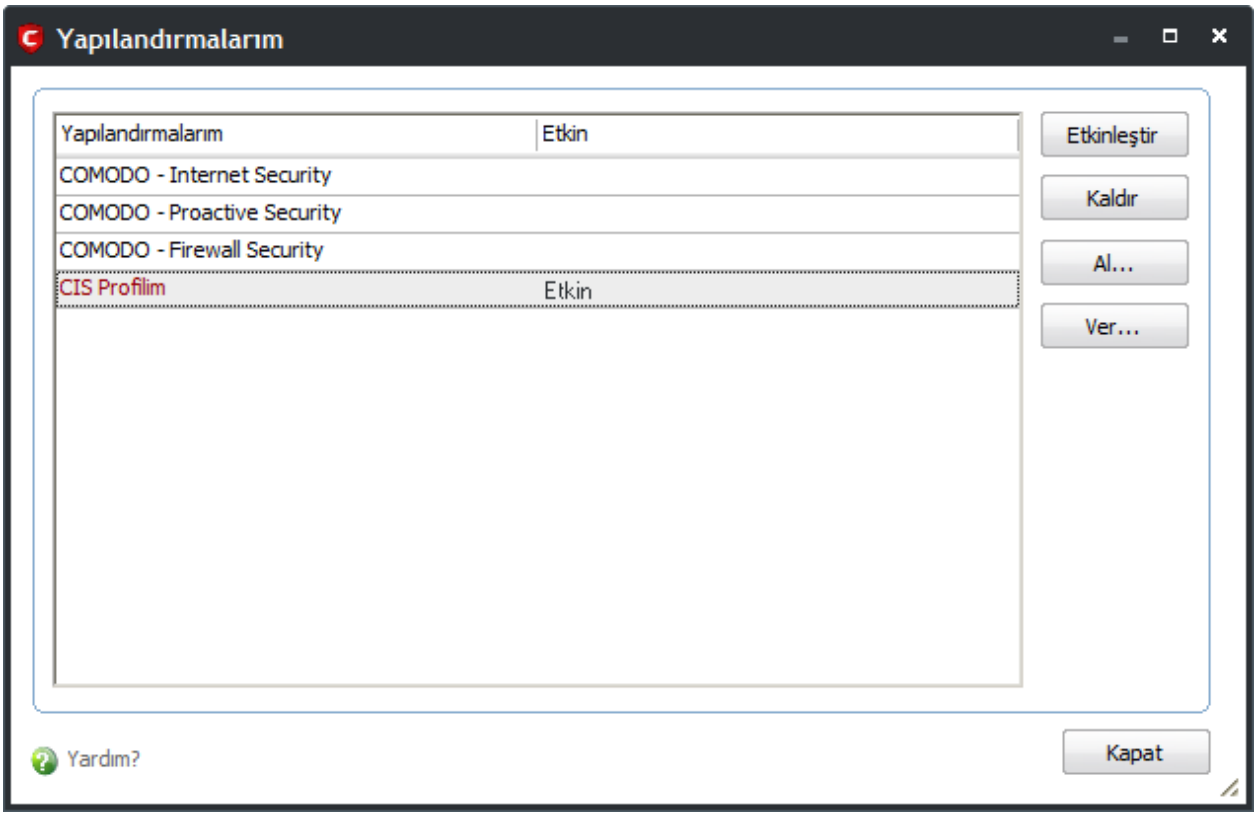
Farklı yapılandırma seçmek için

1. Etkinleştirmek istediğiniz profili seçin ve etkinleştirin.
2. 'Etkinleştir' düğmesine tıklayın.

Onay diyaloğu görünür.



Seçilen yapılandırma etkindir.

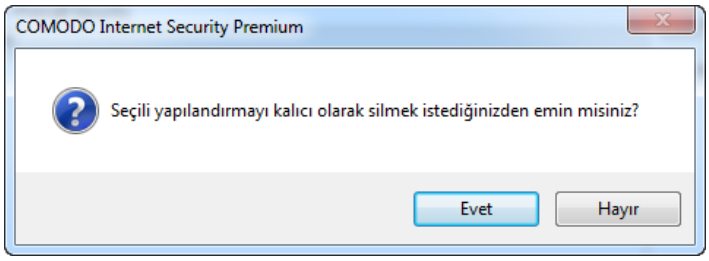


Etkin olmayan yapılandırmayı sil

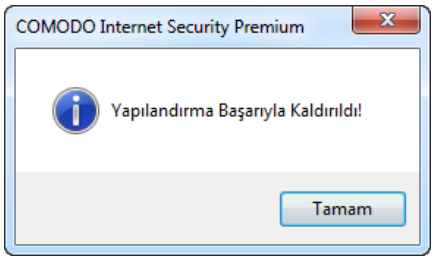
İstenmeyen yapılandırma profillerini 'Kaldır' düğmesi ile silebilirsiniz. Etkin olan yapılandırmayı silemezsiniz. Yalnızca etkin olmayan yapılandırmaları silebilirsiniz.

İstenmeyen profili kaldırmak için

1. Profili seçin ve 'Kaldır' düğmesine tıklayın. Onay diyaloğu görünür.



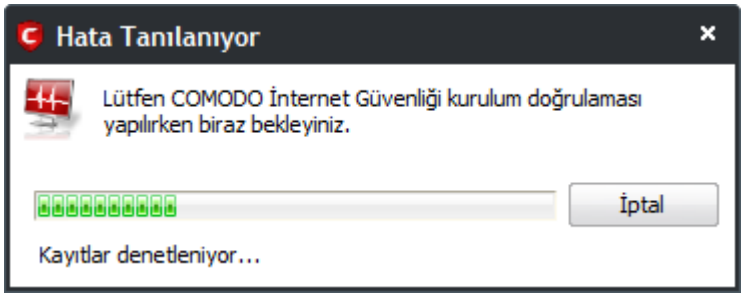
2. Silmek istediğinizden eminseniz 'Evet' düğmesine tıklayın. Seçilen profil listeden kaldırılır ve onay diyaloğu görünür.



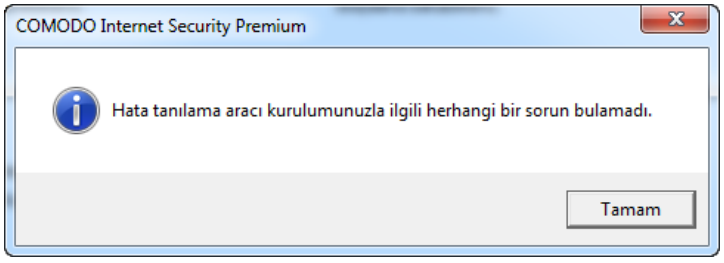
5.3 Hata Tanılayıcı

Comodo Internet Security'nin kendi bütünlük denetimi vardır. Bu denetim sisteminiz tarar ve doğru yüklendiğinden emin olur. Bilgisayarınızın şu bölümlerini denetler:

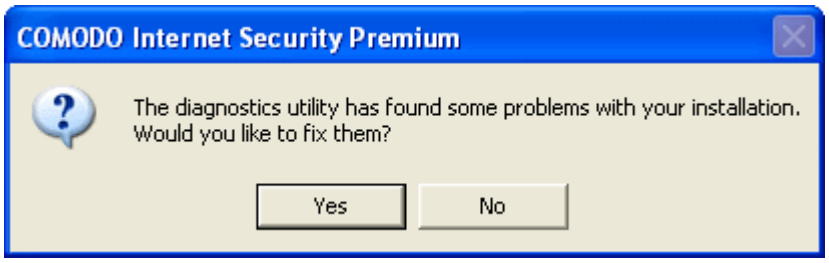
- **Dosya Sistemi – Tüm Comodo dosyalarının bulunup bulunmadığını ve doğru yüklenip yüklenmediğini denetler.**
- **Kayıt Defteri - Tüm Comodo kayıt anahtarlarının bulunup bulunmadığını ve doğru yüklenip yüklenmediğini denetler.**
- **Comodo Internet Security ile çakışan yazılımlara bulunup bulunmadığına karşı denetler.**



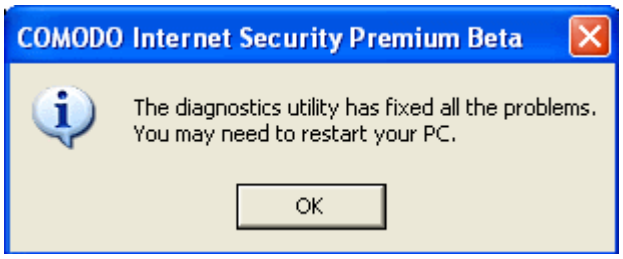
Açılır pencerede tarama sonuçları görünür. Yüklemenizde hata yoksa aşağıdaki diyalog görüntülenir.



Hata tanılama aracı yüklemenizle ilgili hata bulduysa, aşağıdaki diyalog görüntülenir.



Hata tanılayıcı 'Evet' düğmesine tıkladığınızda hataları otomatik olarak düzeltir ve sistemin yeniden başlatılması için sorar.



Değişikliklerin geçerli olması için bilgisayarınızı yeniden başlatın.

5.4 Güncelleştirmeleri Denetle

'Daha' seçenekleri arayüzündeki 'Güncelleştirmeleri Denetle' bağlantısına tıklayarak yeni güncelleştirme olup olmadığını denetleyebilirsiniz.

Güncelleştirmelerin bulunabirliğini denetlemek için

- **'Başlat'** düğmesine tıklayın.

Denetlenme tamamlandığında, panel güncelleştirme bulunabirliğini gösterir.

'Güncelleştirme Ayrıntıları' bağlantısı sizi sürüm notlarının bulunduğu web sayfasına yönlendirir.

Güncelleştirme işlemini başlatmak için

- **'Başlat'** düğmesine tıklayın**.**

Not: Güncelleştirmeleri daha sonra indirip yüklemek istiyorsanız 'İptal' düğmesine tıklayın.

Yükleme işlemi tamamlandıktan sonra, 'Evet' düğmesine tıklayın. Sistemin yeniden başlatılması istenir.

- Şimdi yeniden başlatmak için 'Evet' düğmesine daha sonra yeniden başlatmak için 'Hayır' düğmesine tıklayın.

5.5 Destek Forumlarına Göz At

Comodo Internet Security hakkında daha fazla destek almak için sorularınızı Comodo Forumlarına yazabilirsiniz.

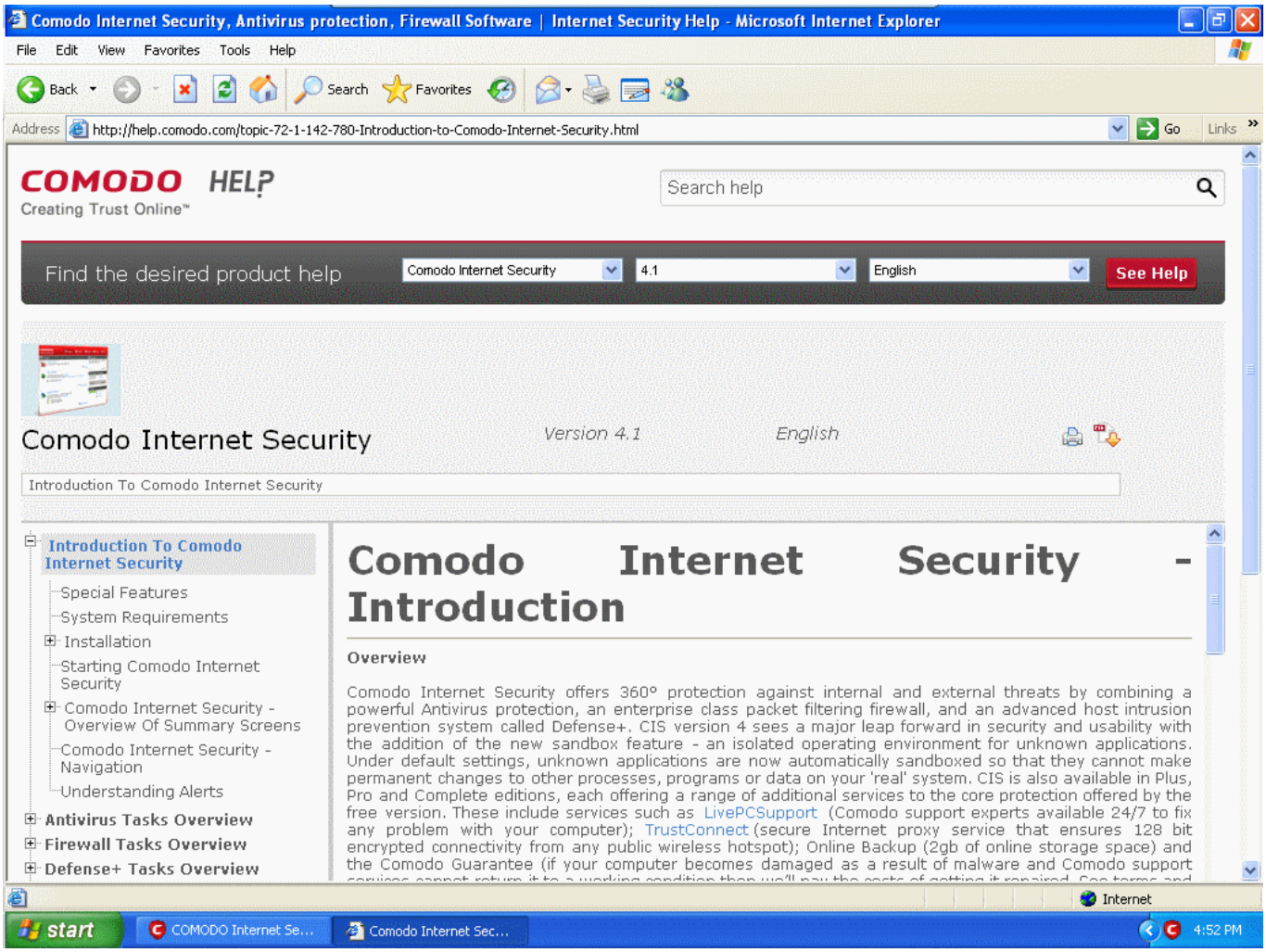
- **Destek Forumlarına Göz At bağlantısına tıklayarak doğrudan http://forums.comodo.com adresindeki web sayfasına yönlendirilirsiniz. Kaydolmak ücretsizdir.**

Çevrimiçi Bilgi Tabanı

Ayrıca http://support.comodo.com adresinde çevrimiçi bilgi tabanımız ve destek bilet sistemimiz de vardır. Kaydolmak ücretsizdir.

5.6 Yardım

Daha bölümündeki **Yardım** bağlantısı bu çevrimiçi yardım rehberini açar. Her alan kendine adanmış sayfalara sahiptir ve uygulamanın işlevleri ayrıntılı olarak açıklamaktadır.



Ayrıca web sayfasındaki yardım rehberini yazdırabilir veya pdf biçimindeki yardım rehberi dosyasını indirebilirsiniz.

5.7 Hakkında

'Daha' ekranından 'Hakkında' bağlantısına tıklayarak 'Hakkında' bilgi diyaloğunu görebilirsiniz.

Bilgisayarınızda yüklü olan Comodo Internet Security'nin sürüm bilgilerini ve yüklemenize özgün seri numarasını görebilirsiniz. Seri numarası destek amaçlı olarak yüklemenizin kimliğini doğrulamak içindir.

Live PC Desteği

Comodo Internet Security Pro ve Complete müşterileri Live PC Desteği ile bilgisayar problemlerine hızlı ve kapsamlı olarak yardım alabilirler. 'Live Support' düğmesine tıklayarak kolaycana Comodo güvenlik uzmanlarından yardım alabilirsiniz. Uzak masaüstü bağlantısı ile bilgisayarınıza bağlanılarak sorunlarınız çözülür. Bu hizmeti test etmek isteyenler 30 günlük deneme süresinden faydalanabilirler.

Lütfen ürün hakkında daha fazla bilgi için http://www.livepcsupport.com adresini ziyaret ediniz. Lütfen Comodo Internet Security Pro'ya kaydolmak için http://personalfirewall.comodo.com adresine gidiniz.

- **Hizmetlerin Tanıtımı**
- **İstemcinin Başlatılması ve Hizmet Talebi**
- **LivePCSupport İstemcisinin Kaldırılması**

5.8 Hizmetlerin Tanıtımı

Comodo uzmanları tarafından uzak masaüstü bağlantısı ile bilgisayarınıza bağlanılarak sorunlarınız gözünüzün önünde çözülür.

- **Uzmanlarımız günün 24 saati mevcuttur herhangi bir hizmeti gerçekleştirmek veya destek sorunuza yanıt vermek için**

- **3 ev veya çalışma bilgisayarınıza kadar limitsiz destek. Her Comodo Internet Security Pro veya Complete lisansı aşağıda listelenen hizmetler için istediğiniz kadar Live PC Desteği talep etmenize izin verir.**
- **Her ne zaman olursa Çevrimiçi Konuşma oturumu başlatabilirsiniz. İsterseniz uzmanlarımız uzaktan bağlanarak sorunlarınızı çözecektir.**
- **Bir kez daha bilgisayarınızı sorunsuz olarak kullanmanın tadını çıkarın!**

Comodo Internet Security Pro ve Complete aboneleri LivePCSupport alırlar:

•Virüs Teşhisi / Temizliği – Bilgisayarınız zararlılara karşı taranır ve zararlı bulunursa temizlenerek önceki durumuna getirilir.

- **PC Ayarlaması – İnce ayarlar yapılarak bilgisayarınızın çalışma hızı arttırılır.**
- **Internet Giriş Koruması – Bilgisayarınızın temek güvenlik ayarları etkinleştirilerek veri hırsızlığına ve kimlik bilgisi hırsızlığına karşı önlem alınır.**
- **Eposta Hesabı Kurulumu – Internet tabanlı eposta hesabınız ayarlanır. Herhangi bir sağlayıcı, herhangi bir hesap olabilir.**
- **Yazılım Yüklenmesi – Comodo ürünleriniz yüklenir ve yapılandırma en yüksek güvenlik ve verim için özelleştirilir.**
- **Yazıcı Kurulumu ve Sorun Çözümü – Yazıcı sürücüleri yüklenir veya güncellenir, mürekkep seviyeleri denetlenir ve ağınızda çalışıcak şekilde yapılandırılır.**
- **Yeşil PC – Bilgisayarınızın güç seçenekleri ayarlanarak elektrik faturasından tasarruf yapmanız sağlanır.**
- **Bilgisayar Sorun Çözümü – Temel donanım çakışmaları için denetlenir.**

Not 1: Her durumda, abonelik numaranızı hazır bulundurmalsınız. Abonelik numaranız epostanızda, ürün kutusunda veya içinde bulunmaktadır.

Not 2: Yukarıda listelenen hizmetler *yalnızca* Pro ve Complete paketlerinin bileşeni olan LivePCSupport içindir. Pro ve Complete paketlerinin tüm ayrıntılarını görmek için buraya tıklayınız.

5.9 İstemcinin Başlatılması ve Hizmet Talebi

Live PC Destek hizmeti için Live PC Destek istemcisi yüklü olmalıdır. CIS Pro ve Complete yüklerken istemci otomatik olarak yüklenir. Aşağıdaki yöntemleri kullanarak istemciyi başlatabilirsiniz:

- LivePCSupport masaüstü simgesine çift tıklayarak 

- LivePCSupport sistem simgesine tıklayarak 

- LivePCSupport istemcisini doğrudan Windows Başlat Menüsü – Tüm Programlar > COMODO > LivePCSupport > Comodo LivePCSupport tıklayarak.

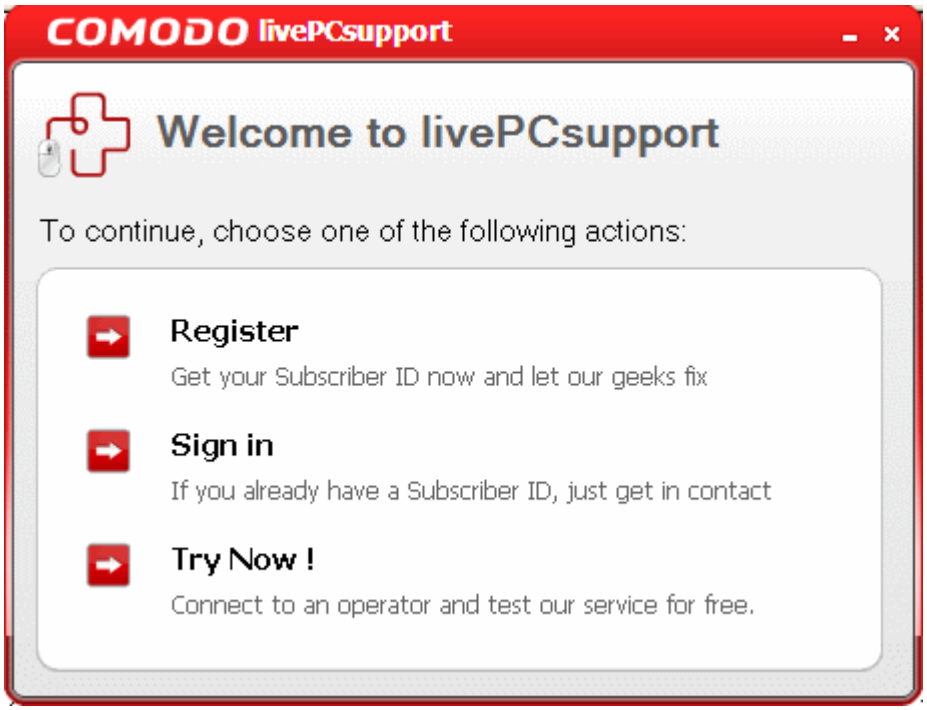
LivePCSupport giriş seçenekleri görüntülenecektir:

Gereken hizmeti seçin:

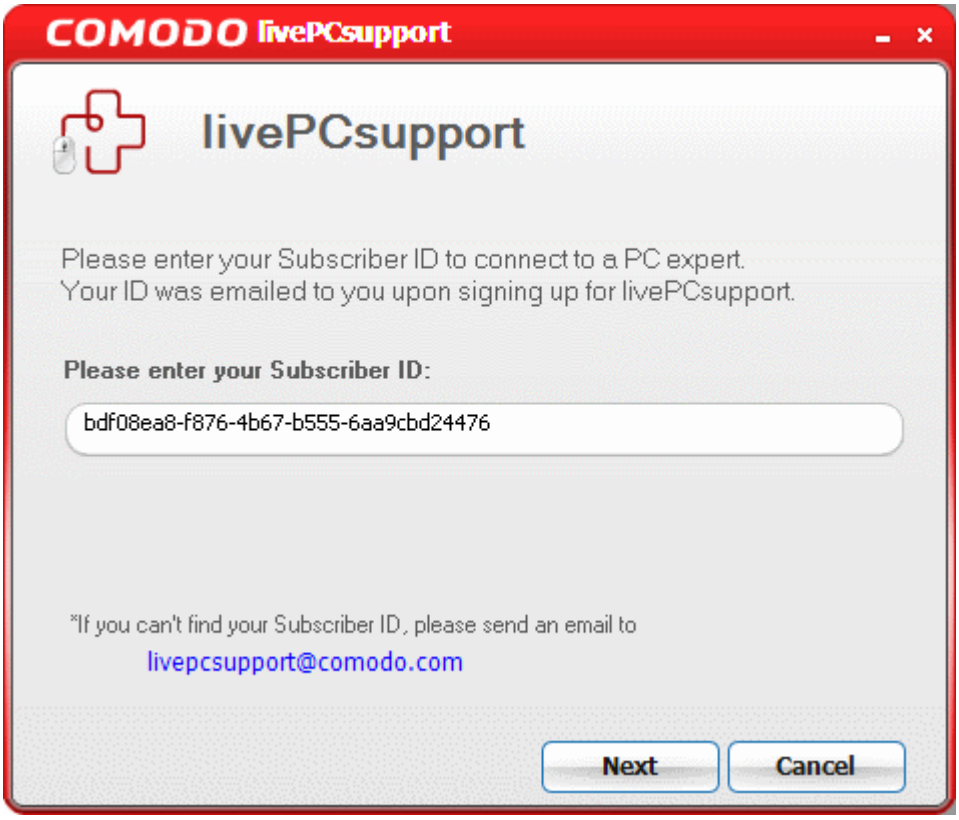
- **Virüs Bulaşması** - Virüs temizliğinde yardım gerekiyorsa tıklayın.

- **Diğer** - Kayıt defteri hataları, gizlilik sorunları, gereksiz dosyalar ve diğer Windows/Sistem kaynaklı problemler konusunda yardım için tıklayın.

Belirlenen alanda uzman teknisyene bağlanacaksınız. Bu seçeneklerden birine tıklanması kayıt ekranını açacaktır.

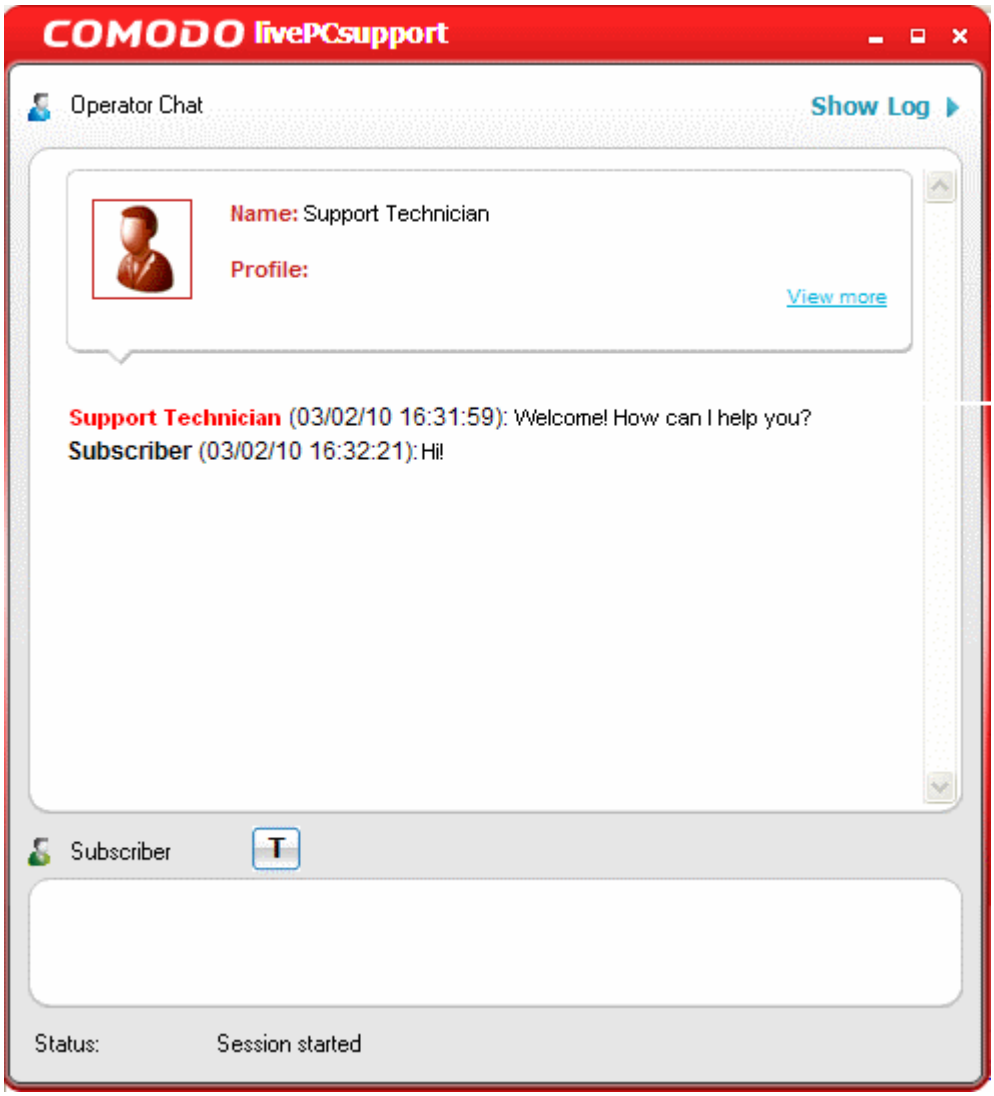


'Oturum aç'... tıklayın



...ve 'Subscriber ID:' metin kutusuna Abonelik Numaranızı girin ve 'Next' tıklayın.

Saniyeler içinde, Comodo Destek Teknisyeni konuşma penceresinden yanıt verir ve probleminiz açıklamanızı ister.



Metin kutusuna sorunuzu yazın ve Enter tuşuna basın.

Comodo güvenlik teknisyeni her sorunuza cevap verecektir. Gerekirse sorununuzu çözmek için uzaktan sisteminize bağlanacaktır ve sisteminiz düzeltecektir.

5.10 Live PC Support İstemcisinin Kaldırılması

Live PC Support İstemcisini Kaldırmak için

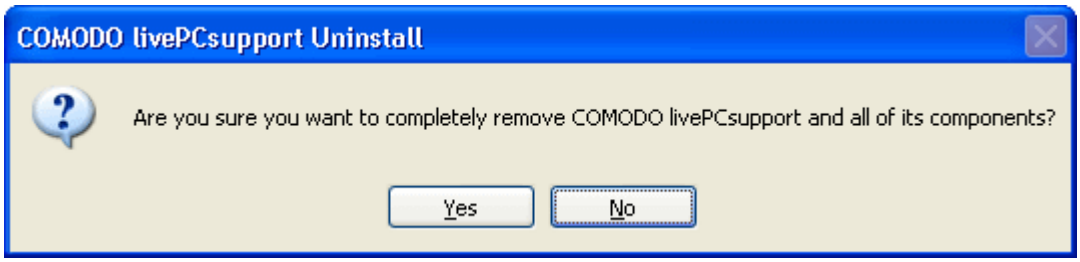
Tüm Programlar > COMODO > LivePCSupport > Kaldır.

Veya

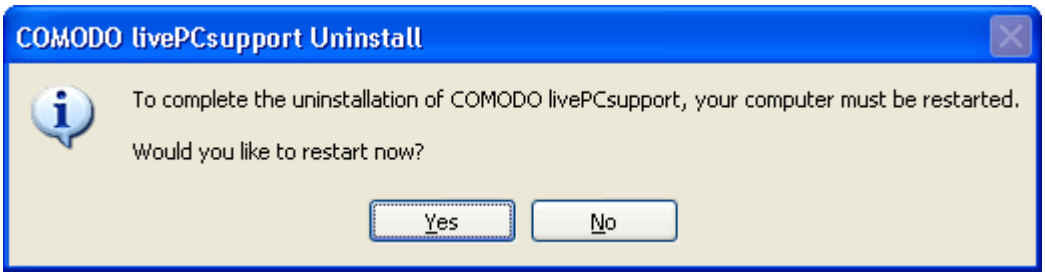
1. Denetim Masasını açın.

2. 'Program Ekle/Kaldır' tıklayın.
3. 'Comodo LivePCSupport' seçin.
4. 'Kaldır' tıklayın.

Kaldırmak onay diyaloğu görünür.



5. 'Evet' tıklayın. Kaldırma ilerleyişi görüntülenir. Değişikliklerin geçerli olması için sisteminizi yeniden başlatmanız gereklidir.



6. 'Evet' tıklayarak sistemi yeniden başlatın.

Sorularınız için bu eposta adresine yazabilirsiniz: cisquestions@comodo.com

Teknik ürün soruları için bu adresi ziyaret edin: https://support.comodo.com/ (Comodo Müşteri Hizmetleri için ücretsiz hizmet hesabı gerekmektedir.)

6 TrustConnect Tanıtımı

Comodo TrustConnect genel kablosuz ağlar üzerindeki oturumlarınızı şifreleyen güvenli bir Internet vekil sunucu hizmetidir. Bu kablosuz oturumlar kolaylıkla kesilebildiğinden dolayı veriler için önemli bir açık oluşturmaktadır.

TrustConnect bu tür veri hırsızlıklarını önlemek için tasarlanmıştır. Ayrıca tüm internet trafiğinizi şifreler. Hizmete bağlandıktan sonra, TrustConnect yazılımı trafiğin sisteminizden çıktığı gibi şifrelendiğini belirtir. (Web site adresleri, anında mesajlaşmalar, kişisel bilgiler, sade metin olarak giden kullanıcı adları ve parolalar ve diğer önemli bilgiler dahil). Veri hırsızları ve korsanlar verilerinizi kesemez veya 'yakalayamaz' – veriler SSL şifreli VPN bağlantısı ile TrustConnect sunucuları üzerinden internete gittiği için bilgilerin sizden geldiği belirlenemez. Genel,

siber suçlular bu yayınları kolaylıkla kesebilirler.

Comodo TrustConnect kurulumu kolaydır. Çoğu işletim sisteminde çalışır (Windows, Mac OS X), ek olarak çoğu güvenlik duvarı uygulamasıyla da çalışır. Kurulum üç dakikadan kısa sürer. TrustConnect istemcisi Windows, Mac OS, Linux ve iPhone mobil cihazları için bulunur ve aşağıdaki adrese giriş yapılaak indirilebilir https://accounts.comodo.com/account/login . Comodo Internet Security Suite Pro/Complete onay epostanızda bilgileriniz bulunmaktadır. Giriş yaptıktan sonra, TrustConnect sekmesinden abonelik ekleyelebilir, ödeme ve iletişim bilgilerinizi değiştirebilir ve kullanım durumunuza bakabilirsiniz. Comodo Internet Security Suite Pro/Complete paketiyle gelen TrustConnect hizmetinde 10 GB/aylık veri taransferi vardır.

Comodo Internet Security Pro/Complete müşterileri ayrıca $99 değerinde 'Total Security and Support' LivePCSupport paketi alırlar. Ürün hakkında daha fazla bilgi için http://www.livepcsupport.com adresini ziyaret edin. Comodo Internet Security Pro oturumu açmak için http://personalfirewall.comodo.com adresine gidin.

TrustConnect Sistem Gereksinimleri

- **Windows Vista**
- **Windows XP**
- **Mac OS X**
- **Linux (kernel 2.4 veya üstü)**
- **FreeBSD, OpenBSD**

TrustConnect Kurulumu

•Microsoft Windows

•MAC OS X

•Linux

•iPhone / iPod Touch

6.1 Microsoft Windows – Yapılandırma ve Bağlantı

Bu bölüm yüklü olduğu varsayılan Trustconnect yapılandırmasını ve bağlantısını anlatır. Yüklü değilse:

•Lütfen CIS Pro veya CIS Complete yükleyicisini çalıştırın ve seçeneklerden 'TrustConnect Kur' seçin

•Alternatif olarak, TrustConnnect istemcisi http://www.comodo.com/trustconnect veya Comodo hesabınızın 'TrustConnect' alanından http://accounts.comodo.com/login ayrı olarak indirilebilir.

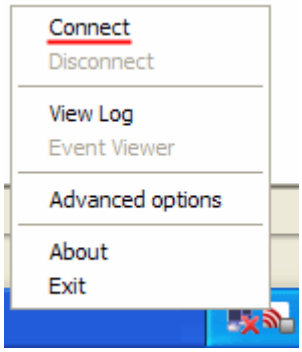
•TrustConnect yüklenmesi Bölüm 1.3.3.4 TrustConnect Kurulumu altında anlatılmıştır.

TrustConnect Bağlantısının Kurulması

Yükleme tamamlandıktan sonra, TrustConnect aşağıdaki yollar kullanılarak başlatılabilir:

- **Windows 'Başlat' menüsü aracılığıyla. 'Başlat > Programlar > Comodo > Trust Connect > Trust Connect' tıklayın**
- **TrustConnect sistem simgesine çift tıklayarak**:

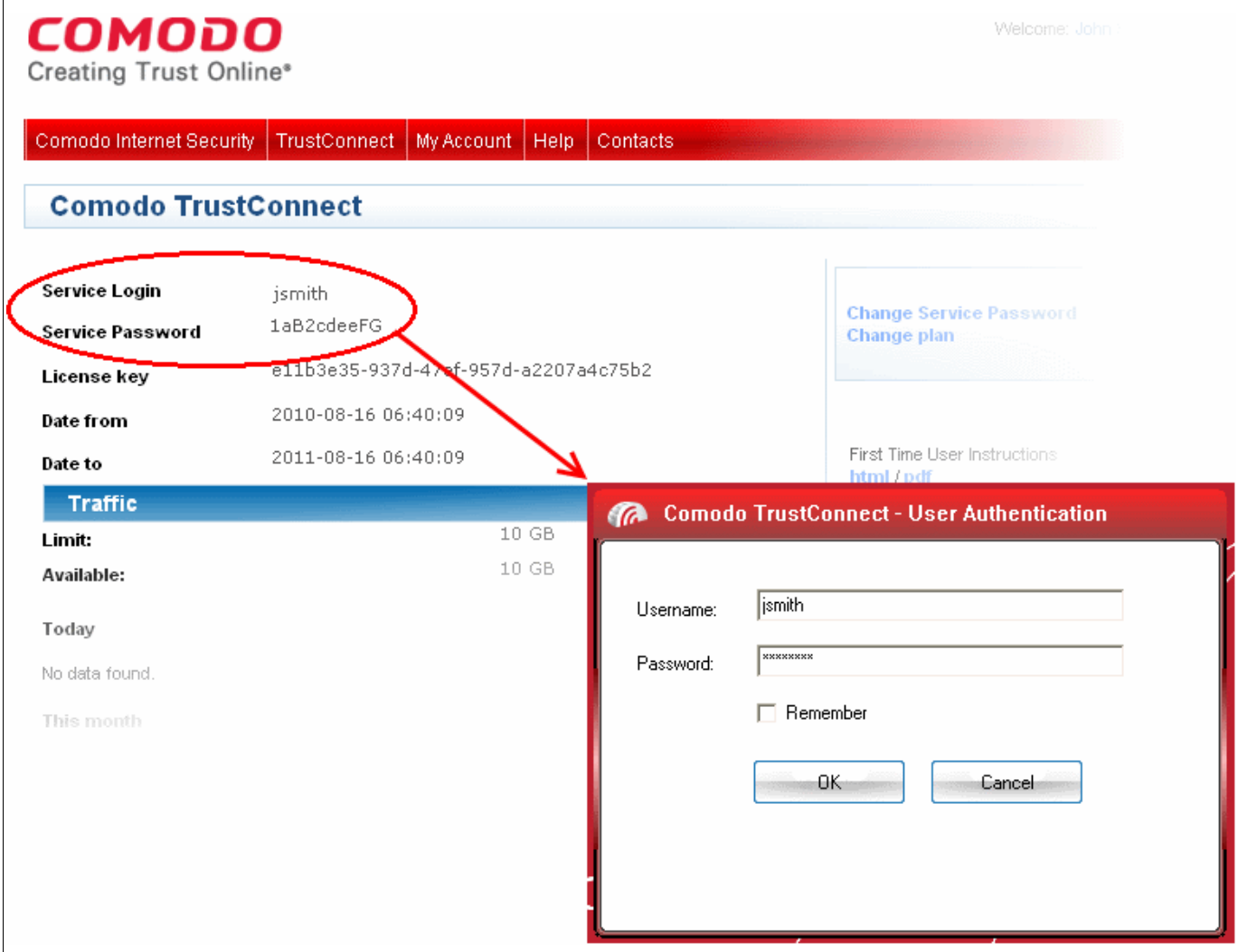
- **TrustConnect sistem simgesine sağ tıklayıp 'Bağlan (Connect)' seçerek:**



Varsayılan olarak, TrustConnect dünya üzerine dağılmış konumunuza en uygun, sunucu ve sizin aranızdaki uzaklık ve sunucu yük durumuna göre en uygun sunucuyu seçerek bağlantı kurar. Bağlanmak istediğiniz sunucuyu, bu sayfanın altında açıklandığı gibi Gelişmiş Seçenekler (Advanced Options) bölümünden değiştirebilirsiniz.

TrustConnect başladıktan sonra hizmet kullanıcı adınızı ve parolanızı girmelisiniz.

Not: Bu parola Comodo Hesabınızın parolası ile aynı değildir. TrustConnect hizmetini etkinleştirirken oluşturulan hizmete özgün paroladır. Gerekirse , 'Change Service Password' düğmesini kullanarak parolanızı değiştirebilirsiniz.



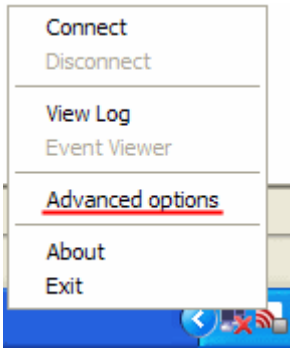
'Evet' düğmesine tıklayarak onaylayın ve bağlanın. Giriş bilgilerinizin başarılı olarak doğrulanması sonrası sistem simgesi başarılı olarak bağlandığınızı belirten yeşil renge döner:

TrustConnect bağlı değil	*TrustConnect bağlantı girişimi yapılıyor*	*TrustConnect başarılı olarak bağlandı*

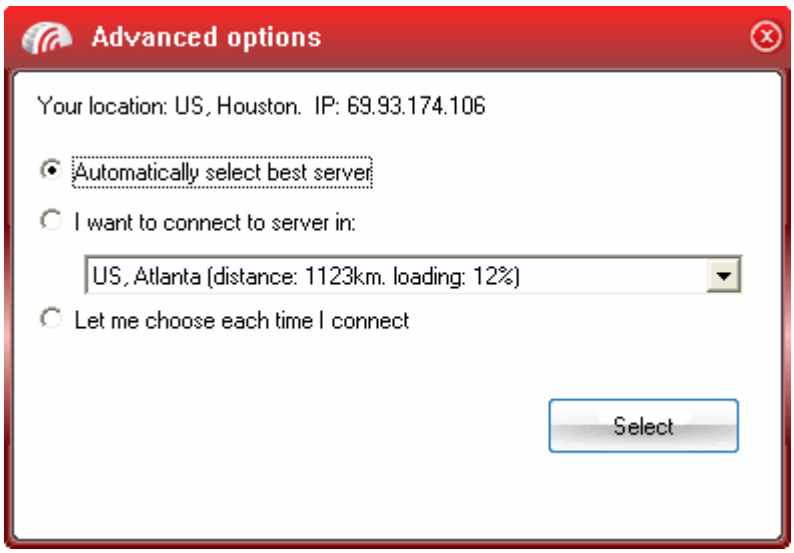
Gelişmiş Seçenekler

Comodo TrustConnect bu bölümden bağlanmak istediğiniz sunucuyu değiştirmenize izin verir. Bunu otomatik olarak veya her zaman elle seçmek için de ayarlayabilirsiniz.

Gelişmiş seçenekler paneline erişmek için, sistem simgesine sağ tıklayın ve 'Advanced Options' seçin.



Panel mevcut konumu ve IP adresini gösterir.



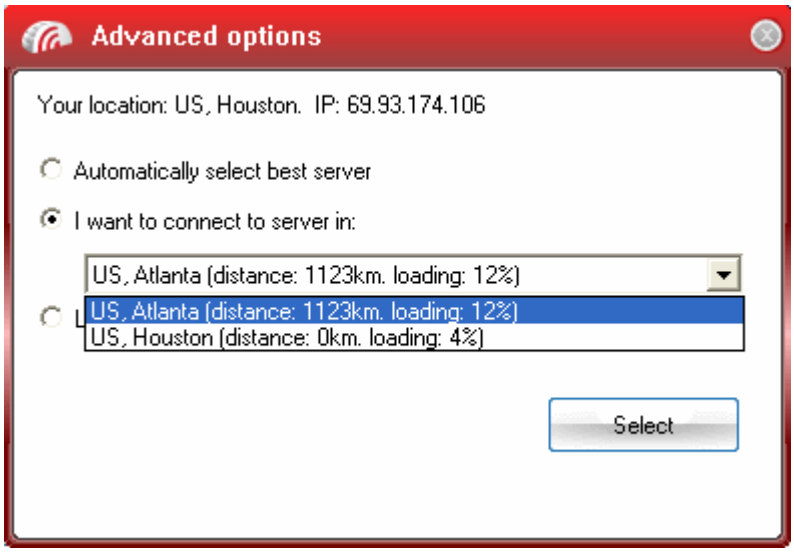
Sunucu seçimini seçeneklerden şu şekilde yapılandırabilirsiniz:

- **Otomatik olarak en iyi sunucuyu seç (Automatically select the best server);**
- **Şu sunucuya bağlanmak istiyorum (I want to connect to server in);**
- **Her bağlandığımda ben seçeyim (Let me choose each time I connect).**

Seçeneği işaretleyin ve seçimin geçerli olması için Select (Seç) düğmesine tıklayın.

Otomatik olarak en iyi sunucuyu seç – En uygun yük ve konumdaki sunucuyu otomatik olarak seçer. Varsayılan seçenektir ve tüm kullanıcılara önerilir.

Şu sunucuya bağlanmak istiyorum: Sizin seçtiğiniz ve varsayılan olarak belirlediğiniz sunucuya her açıldığında otomatik olarak bağlanır. Her sunucunun bulunduğu konum, uzaklık ve yük durumu yüzde olarak yanında belirtilir.



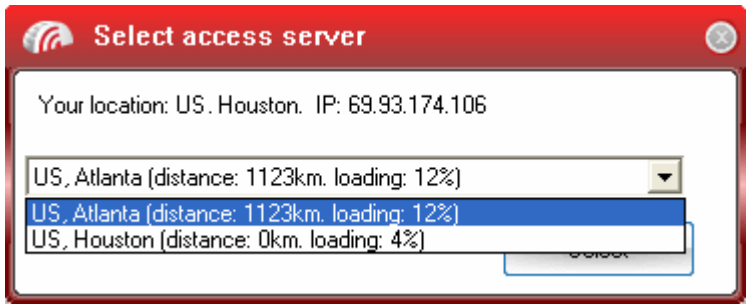
- **Varsayılan olarak atanmasını istediğiniz sunucuyu ayarlayın ve 'Select (Seç)' düğmesine tıklayın.**

Not: Daha hızlı erişim için en yakın konumun seçilmesi önerilir.

TrustConnect seçtiğiniz ve varsayılan olarak belirlediğiniz sunucuya her açıldığında otomatik olarak bağlanır. Bunu Advanced Options (Gelişmiş Seçenekler) bölümünden değiştirebilirsiniz.

Her bağlandığımda ben seçeyim – Her bağlandığında farklı bir sunucuyu elle seçmenize izin verir.

TrustConnect hizmeti her başlatıldığında bağlanmak istediğiniz sunucu seçimini yapmanız için sorulur. Bağlantı kurulduktan sonra 'Select access server (Erişim sunucusu seç)' diyaloğu görünür.



Açılır liste menüsü değişik bölgelerde bulunan TurstConnect erişim sunucularını gösterir. Her sunucunun bulunduğu konum, uzaklık ve yük durumu yüzde olarak yanında belirtilir.

- **Bağlanmak istediğiniz sunucuyu ayarlayın ve 'Select (Seç)' düğmesine tıklayın. Seçili sunucu ile erişim kurulur.**

Not: Daha hızlı erişim için en yakın konumun seçilmesi önerilir.

6.2 Mac OS X – Yapılandırma ve Bağlantı

TrustConnect OpenVPN istemcisinin yüklenmesi ve yapılandırılması

1. TrustConnect OpenVPN istemcisini Mac OS X 10.4 (veya üstü) Tunnelblick project sitesinden indirin - http://code.google.com/p/tunnelblick. 'Featured downloads' bölümünden indirilebilir.

   Alternatif olarak, doğrudan aşağıdaki bağlantıdan indirilebilir:
   http://tunnelblick.googlecode.com/files/Tunnelblick_3.0b26.dmg
2. İstemciyi yükleyin. Yükleme sürecini başlatmak için indirdiğiniz dmg uzantılı dosyaya çift tıklayın. Kurulum tamamlandıktan sonra 'Tunnelblick' simgesi masaüstünde görünür. Tunnelblick hakkında daha fazla bilgi için http://code.google.com/p/tunnelblick adresindeki proje sitesine bakın.
3. TrustConnect paketinize uygun istemci yapılandırma dosyasını indirin:

   •TrustConnect aboneleri VEYA 7 günlük deneme sürümü için:
   https://accounts.comodo.com/download/trustconnect/client.conf

   •ÜCRETSİZ TrustConnect kullanıcıları için:
   http://download.comodo.com/trustconnect/free_client.conf

1. İndirmiş olduğunuz 'client.conf' veya 'free_client.conf' dosyasının adını 'openvpn.conf' olarak değiştirin
2. TrustConnect CA sertifikasını indirin.
3. Yeniden adlandırılmış **yapılandırma dosyasını** ve kök **CA sertifikasını** belirtilen klasöre kopyalayın: *~/Library/Application/Support/Tunnelblick/Configurations*
4. **Tunnelblick.app** başlatın ve **Connect 'openvpn'** seçin.
5. TrustConnect giriş bilgilerinizi girin.

6.3 Linux / Open VPN – Yapılandırma ve Bağlantı

Linuz kullanıcıları için aşağıdaki seçenekler bulunmaktadır:

- **OpenVPN İstemcisinin İndirilmesi ve Yüklenmesi**
- **RedHat İstemcisinin İndirilmesi ve Yüklenmesi**
- **Ubuntu İstemcisinin İndirilmesi ve Yüklenmesi**

TrustConnect OpenVPN İstemcisinin İndirilmesi ve Yüklenmesi

TrustConnect hizmetine bağlanmak için ilk önce TrustConnect OpenVPN istemci yazılımını indirmeniz ve yüklemeniz gerekmektedir.

1. TrustConnect OpenVPN istemcisinin Linux için indirilmesi. Buraya tıklayarak doğrudan indirebilirsiniz.

2. RPM paketinin kullanılması

RPM paketlerini destekleyen (SuSE, Fedora, Redhat, etc.) dağıtımlardan birini kullanıyorsanız, bu tekniği kullanarak yüklemeniz en iyisidir. Kendi RPM dosyanızı **derleyebilirsiniz**:

```
rpmbuild -tb openvpn-[version].tar.gz
```

RPM dosyası oluşturulduktan sonra, aşağıdaki gibi **yükleyebilirsiniz**:

```
rpm -ivh openvpn-[details].rpm
```

RPM paketi ile OpenVPN yüklenmesi için şu **bağımlılıklar** gerekmektedir:
openssl, lzo, pam. LZO kütüphaneleri buradan indirilebilir.

1. RPM paketi olmadan

Eğer Debian, Gentoo, veya RPM tabanlı olmayan Linux dağıtımı kullanıyorsanız, dağıtımınızın paket yöneticisini de kullanarak OpenVPN istemcisini yükleyebilirsiniz. Ayrıca OpenVPN istemcisini Linux üzerinde evrensel `./configure` metoduyla da yükleyebilirsiniz.

İlk olarak dosyayı `.tar.gz` çıkartın:

```
tar -xfz openvpn-[version].tar.gz
```

cd komutu ile üst seviyedeki klasöre gidin ve şunu yazın:

```
./configure
make
make install
```

Daha ayrıntılı bilgi için resmi OpenVPN 2.0 'How To' sayfasına bakın.

TrustConnect OpenVPN İstemcisinin Yapılandırılması

1. TrustConnect paketinize uygun istemci yapılandırma dosyasını indirin:
   - TrustConnect aboneleri VEYA 7 günlük deneme sürümü için:
     https://accounts.comodo.com/download/trustconnect/client.conf
   - ÜCRETSİZ TrustConnect kullanıcıları için:
     http://download.comodo.com/trustconnect/free_client.conf

1. TrustConnect CA sertifikasını indirin.
2. Kök CA sertifikasını ve yapılandırma dosyasını OpenVPN yapılandırma klasörüne kopyalayın, örneğin `/etc/openvpn/`.
3. TrustConnect OpenVPN istemci programını başlatın:

```
openvpn--openvpn config /etc/openvpn/client.conf
```

4. TrustConnect giriş bilgilerinizi girin.

TrustConnect RedHat İstemcisini İndirin ve Yükleyin

TrustConnect istemcisini RedHat sistemine yüklemek için (Fedora, RHEL)

1. RPM paketini buradan indirin:

   https://accounts.comodo.com/download/trustconnect/tcclient-1.0-1.noarch.rpm

2. Konsolu açın, root olarak giriş yapın ve şu komutu yürütün:

rpm -Uhv PATH/TO/RPM/tcclient-1.0-1.noarch.rpm

İstemci RedHat Fedora 8, 9, 10 üzerinde test edilmiştir.

Not: TrustConnect RedHat İstemcisi ücretsiz hizmet kullanıcıları için mevcut değildir. Ücretsiz hizmet kullanıcıları bu belgede önceden açıklandığı gibi OpenVPN istemcisini kurabilirler.

TrustConnect Ubuntu İstemcisini İndirin ve Yükleyin

TrustConnect istemcisini Ubuntu sistemine yüklemek için

1. DEB paketini buradan indirin:

https://accounts.comodo.com/download/trustconnect/tcclient_1.0-1_all.deb

2. Konsolu açın, root olarak giriş yapın ve şu komutu yürütün:

dpkg -i PATH/TO/DEB/tcclient_1.0-1_all.deb

İstemci Ubuntu 8.0, 8.1 üzerinde test edilmiştir.

Kullanım:
Trustconnect istemcisini çalıştırın: "Uygulamalar Menüsü" -> "Internet" -> "TrustConnect Client"

Not: TrustConnect Ubuntu İstemcisi ücretsiz hizmet kullanıcıları için mevcut değildir. Ücretsiz hizmet kullanıcıları bu belgede önceden açıklandığı gibi OpenVPN istemcisini kurabilirler.

6.4 Apple iPhone / iPod Touch – Yapılandırma ve Bağlantı

OpenVPN hesap sayfasını açın. Gidin **Setting** > **General** > **Network** > **VPN** > **Settings**.

1. PPTP seçin ve TrustConnect VPN hesap bilgilerinizi girin:

•'Server' alanında, lütfen aşağıdaki adreslerden birini kullanın:

- us1.vpn.comodo.com (ücretli aboneler için)
- us2.vpn.comodo.com (ücretli aboneler için)
- us3.vpn.comodo.com (ücretsiz kullanıcılar için)

1.TrustConnect hesap bilgilerinizi girin.

1. 'Save' düğmesine tıklayın ve VPN ana sayfasına geri dönün (`Setting > General > Network > VPN`).
2. Trust Connect VPN bağlantısını başlatın. 'VPN' ayarını 'ON' olarak değiştirin.

6.5 TrustConnect SSS

Genel Sorular

TrustConnect Uygulamasını Nasıl Ayarlarım ve Sunucuya Bağlanırım?

Kullanıcı Adım ve Parolam Neden Çalışmıyor?

TrustConnect Hangi İşletim Sistemlerini Destekliyor?

TrustConnect Sunucusuna Bağlanmak için Hangi İstemcileri Kullanmalıyım?

Bizim tüm İnternet (http & HTTPS) bağlantılarımız vekil sunucu üzerinden yapılıyor. Bu durumda TrustConnect kullanarak nasıl bağlanırım?

Comodo TrustConnect gibi Güvenli Bağlantıya neden ihtiyacım var?

Koklayıcı nedir?

Ne tür TrustConnect Hesapları mevcuttur?

Tam hizmette ne tür Abonelik Planları mevcuttur?

Windows Yapılandırması

Windows Vista Yapılandırması

iPhone/iPod İstemci Yapılandırması

Genel Sorular

TrustConnect Uygulamasını Nasıl Ayarlarım ve Sunucuya Bağlanırım?

1. İlk olarak, https://accounts.comodo.com adresinden Comodo Hesap sayfasına giriş bilgilerinizi kullanarak girin.
2. Gezinti çubuğundan 'TrustConnect' sekmesine geçin.

3. İşletim sisteminize uygun TrustConnect İstemci yazılımını indirin, yükleyin ve yapılandırın. Tüm gerekli yazılımlar ve talimatlar hesabınızın 'TrustConnect' alanında bulunmaktadır. Alternatif olarak aşağıdaki bağlantılara bakabilirsiniz:

Windows

TrustConnect Windows Client Configuration Guide (pdf) indirin

Windows TrustConnect Client indirin

MAC OS X

TrustConnect MAC OS X Client Configuration Guide (pdf) indirin

Linux / OpenVPN

TrustConnect Linux Client Configuration Guide (pdf) indirin

iPhone / iPod Touch

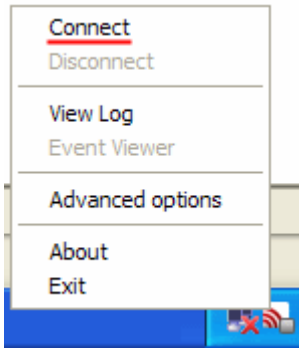
TrustConnect IPOD Client Configuration Guide (pdf) indirin

4. Yüklendikten sonra TrustConnect İstemcinizi başlatın.

Aşağıdaki örnek Windows istemcisini kullanarak nasıl bağlanacağınızı gösterir:

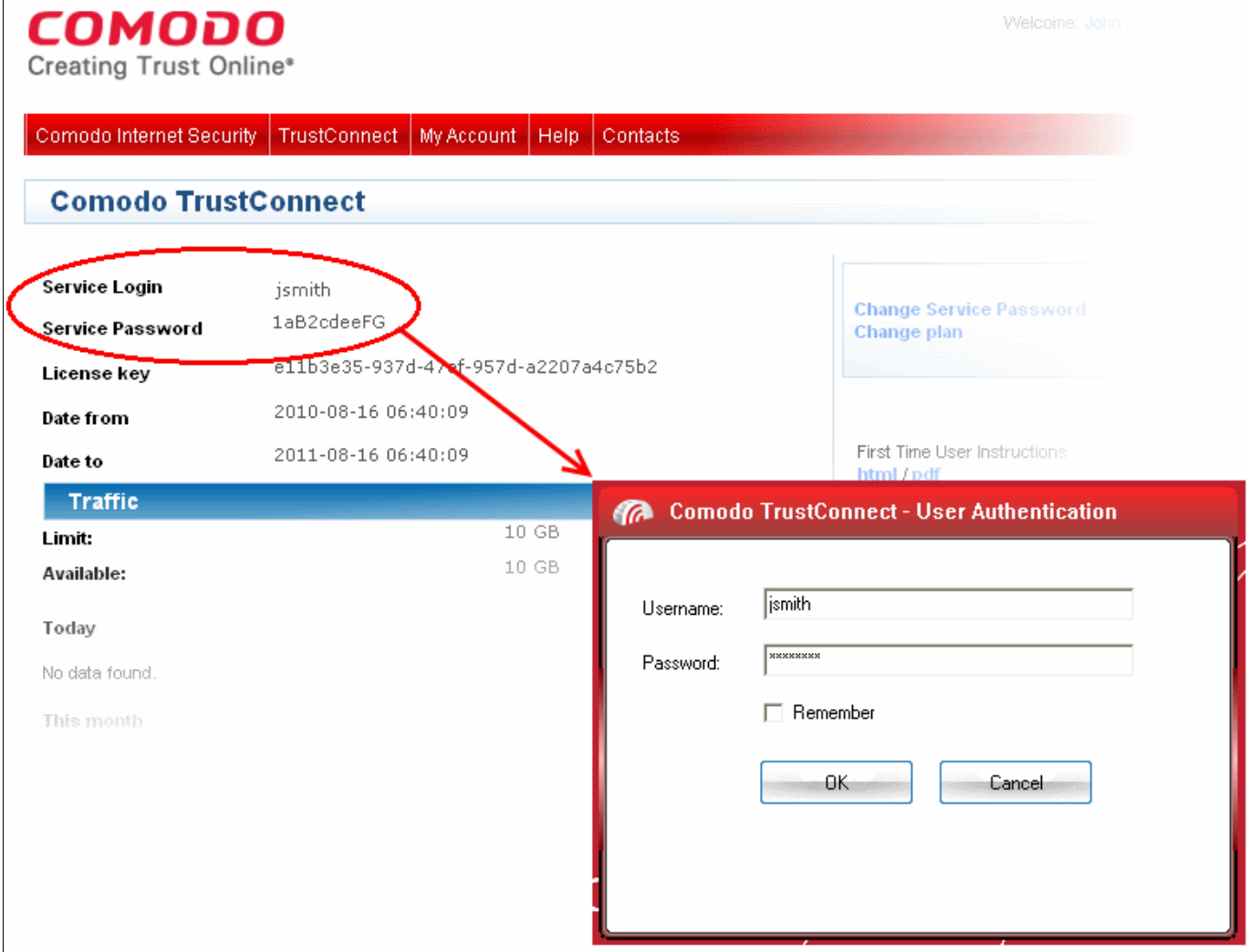
Başlat > Programlar > Comodo > Trust Connect > Trust Connect

Veya, eğer TrustConnect çalışır durumdaysa, sistem simgesine sağ tıklayın ve 'Connect' seçin:



1. Giriş kutusuna hizmet giriş bilgilerinizi girin.

Not: Bu parola Comodo Hesabınızın parolası ile aynı değildir. TrustConnect hizmetini etkinleştirirken oluşturulan hizmete özgün paroladır. Gerekirse , 'Change Service Password' düğmesini kullanarak parolanızı değiştirebilirsiniz.



6. Başarılı bağlantı sonrası sistem simgesi başarılı olarak bağlandığınızı belirten yeşil renge döner:



TrustConnect bağlı değil	*TrustConnect bağlantı kurmaya çalışıyor*	*TrustConnect başarılı olarak bağlandı*

Kullanıcı Adım ve Parolam Neden Çalışmıyor?

Comodo hesabınızın değil TrustConnect Hizmetinizin giriş bilgilerini kullandığınızdan emin olun.

TrustConnect müşterisi olarak (veya CIS Pro/Complete müşterileri) iki set giriş bilgisi vardır:

Comodo Hesap Bilgileri. Bu kullanıcı adı ve parolası https://accounts.comodo.com adresindeki hesabınızı yönetmeniz içindir. Bunu üye olurken oluşturdunuz (TrustConnect veya CIS Pro/Complete için).

TrustConnect Hizmet Bilgileri. Bu kullanıcı adı ve parolası TrustConnect sunucularına bağlanmak içindir.

TrustConnect Hizmet Bilgilerini görüntülemek için:

- https://accounts.comodo.com adresine Comodo Hesap Bilgileri ile giriş yapın
- Gezinti çubuğundan 'TrustConnect' düğmesine tıklayın
- Hizmet bilgileriniz listelenir. 'Change Service Password' düğmesi ile parola değiştirebilirsiniz.

TrustConnect Hangi İşletim Sistemlerini Destekliyor?

TrustConnect Windows 2000, Windows XP, Windows Vista, Linux ve Mac Os X üzerinde başarılı olarak test edilmiştir. Ayrıca iPod/iPhone gibi mobil aygıtları da destekler.

TrustConnect Sunucusuna Bağlanmak için Hangi İstemcileri Kullanmalıyım?

İşletim sisteminize uygun TrustConnect İstemci yazılımını indirin, yükleyin ve yapılandırın. Tüm gerekli yazılımlar ve talimatlar hesabınızın 'TrustConnect' alanında bulunmaktadır. Alternatif olarak aşağıdaki bağlantılara bakabilirsiniz:

Windows

TrustConnect Windows Client Configuration Guide (pdf) indirin

Windows TrustConnect Client indirin

MAC OS X

TrustConnect MAC OS X Client Configuration Guide (pdf) indirin

Linux / OpenVPN

TrustConnect Linux Client Configuration Guide (pdf) indirin

iPhone / iPod Touch

TrustConnect IPOD Client Configuration Guide(pdf) indirin

Bizim tüm İnternet (http & HTTPS) bağlantılarımız vekil sunucu üzerinden yapılıyor. Bu durumda TrustConnect kullanarak nasıl bağlanırım?

Windows istemcisi kullanıyorsanız, şöyle yapmalısınız:

i. TrustConnect hedef (komut) yolu değiştirin:
   - 'TrustConnect' simgesine sağ tıklayın;
   - 'Özellikler' -> 'Kısayol' seçin;
   - Bu metini **--allow_proxy 1** 'Hedef' alanına ekleyin, aşağıdaki gibi:

"C:\Program Files\Comodo\TrustConnect\bin\TrustConnect.exe" --allow_proxy 1

ii. TrustConnect istemcisini başlatın

iii. Vekil sunucu ayarlarını girin:

- 'TrustConnect' sistem simgesine sağ tıklayın ve 'Proxy Settings' seçin;
- 'Manual Configuration' seçin ve vekil sunucu ayarlarını girin, örneğin:

HTTP proxy, Adres: 192.168.0.1, Port: 3128

iv. TrustConnect bağlanın.

Linux/Unix veya MAC OS X istemcisi kullanıyorsanız, istemci yapılandırma dosyasına http-proxy direktifini eklemeniz gerekmektedir. Örneğin: http-proxy 192.168.0.1 3128.

iPhone/iPod istemcisi kullanıyorsanız:

- VPN ayarlarından vekil suncuyu ayarlayın: 'Ayarlar' -> ' Genel' -> 'Ağ' -> 'VPN' -> 'Ayarlar' -> 'Vekil sunucu'

Comodo TrustConnect gibi Güvenli Bağlantıya neden ihtiyacım var?

Genel kablosuz ağlar üzerinden bağlanıyorsanız tüm bilgileriniz okunabilir, düz metinler siber suçlular tarafından koklanabilir. Ek olarak, çoğu otelde koklanabilir kablolu ağlar bulunmaktadır. Gezerken tüm bilgileriniz görünebilir, bunlar kurumsal gizli ve kişisel bilgilerinizi içerebilir.

Koklayıcı nedir?

Genel anlamda, bilgisayar yalnızca kendi TCP/IP adresine yönlendirilmiş trafiği alır. Koklayıcı yazılımlar bilgisayarın tüm yerel ağdaki trafiği kaydetmesine imkan verir.

Ne tür TrustConnect Hesapları mevcuttur?

3 ana 'türde' TrustConnect Hesabı bulunur:

- **TAM** – Ücretli abonelik. Kullanıcılar TrustConnect hizmetinin tüm özelliklerini kullanabilir.
- **DENEME** – 7 günlük deneme süresi boyunca kullanıcılar TrustConnect hizmetinin tüm özelliklerini kullanabilir.
- **ÜCRETSİZ** – 'Ömür boyu ücretsiz' hizmeti bazı kısıtlamalar içerir. Daha fazla bilgi için 'Ücretli ve ücretsiz hizmet arasındaki farklılıklar nelerdir?' sorununa bakınız.

Tam hizmette ne tür Abonelik Planları mevcuttur?

The following plans are available for the TrustConnect service:

- Günlük – 24 saatlik erişim $3.99
- Aylık - $6.99 aylık, 1 kullanıcı hesabı, limitsiz trafik
- Yıllık - $49.99 yıllık, 1 kullanıcı hesabı, limitsiz trafik

Aşağıdaki gibi iş paketleri mevcuttur:

- Kurumsal Aylık - $25.00 aylık, 5 kullanıcı hesabı, 500 GB toplam trafik
- Kurumsal Yıllık - $200.00 aylık, 5 kullanıcı hesabı, 500 GB toplam trafik

Gerektiğinde ek trafik satın alabilir miyim?

Evet, istediğiniz zaman ek trafik hesabınıza eklenebilir.

- https://accounts.comodo.com adresinden Comodo hesabınıza girin
- Gezinti çubuğundan 'TrustConnect' sekmesine gidin (veya 'Service' menüsünden 'TrustConnect' seçin)

- 'Buy extra traffic' tıklayın ve size uyan plana kaydolun

Ücretli ve ücretsiz hizmet arasındaki farklılıklar nelerdir?

Ücretsiz hizmet:

- Aylık 10 GB trafik limit
- Konum hizmeti ücretsiz kullanıcılar için mevcut değildir (sunucu seçimi yapılamaz)
- Ücretsiz hizmet küçük reklamlar gösterir
- Ücretsiz hizmet belli protokollerin kullanımına izin vermez. Bunlar FTP, SMTP, NNTP ve NTP'dir.

Not: POP3 ve IMAP protokollerine izin verilir, böylece epostalarınızı (Gmail, Yahoo gibi) denetleyebilirsiniz. Anında mesajlaşma programları da kullanılabilir (MSN ve ICQ gibi).

- TrustConnect istemcisi RedHat ve Ubuntu Linux dağıtımlarını kullanan ücretsiz kullanıcılar için mevcut değildir. Bu kullanıcılar OpenVPN istemcisini kullanabilirler.

Bu limitleri kaldırmak için tam hesaba nasıl geçebilirim?

Ücretsiz hizmeti tam hizmete yükseltmek için:

- https://accounts.comodo.com adresinden Comodo hesabınıza girin
- Gezinti çubuğundan 'TrustConnect' sekmesine gidin (veya 'Service' menüsünden 'TrustConnect' seçin)
- 'Change Plan' tıklayın ve size uyan plana kaydolun

Comodo TrustConnect kullanabilmem için kablosuz bağlantı mı kullanmam gerekiyor?

Hayır. Bazı ağlarda, fiziksel olarak kablo ile bağlı olsalar bile, güvenli bağlantı mevcut değildir. Comodo TrustConnect hizmetini kullanarak kablolu bağlantılarda da bilgilerinizi şifreleyebilir ve gizleyebilirsiniz.

Evde WEP etkin kablosuz bağlantım var. Güvende miyim?

Hayır. Siber suçlular WEP şifrelemesini internetten kolayca elde edilebilen araçlar ile kırabilirler. Güvenlik duvarı bulunmayan bilgisayarlar saldırıya daha açık olurlar. Comodo TrustConnect evdeki kablosuz ağınızdan bağlanırken de bağlantınızın güvende olmasına yardımcı olur.

TrustConnect lisansı yalnızca bir bilgisayar için mi geçerlidir veya ev ağımdaki diğerlerine de yükleyebilir miyim?

TrustConnect istemci yazılımını istediğiniz kadar bilgisayara yükleyebilirsiniz fakat aynı anda bir bilgisayardan oturum açabilirsiniz.
Lisans sözleşmesini bu adresten okuyabilirsiniz: https://accounts.comodo.com/trustconnect/management/eula

TrustConnect üzerinden bağlantı hızı nedir?

Tüm TrustConnect bağlantıları 128 bit SSL üzerinden şifreli olarak gerçekleşir, bu yüzden genelde hız 1.5 – 3.0 Mbps aralığındadır.

TrustConnect Deneme süresi bitiminde ne olur?

7 günlük deneme süreniz bittikten sonra üye olduğunuz plana geçirilirsiniz.

Hesabımı nasıl iptal edebilirim?

TrustConnect hesabınızı iptal etmek istiyorsanız, bu isteğinizi belirten epostayı trustconnectcancel@comodo.com adresine gönderiniz. Lütfen kullanıcı bilgilerinizi, eposta adresinizi ve şipariş numaranızı iptal nedeninizle birlikte epostanıza eklemeyi unutmayın.

TrustConnect ne tür güvenlik önlemleri kullanır?

Tüm TrustConnect bağlantıları 128 bit SSL üzerindendir. Ek olarak, özel VPN oturum anahtarı her saat yeniden oluşturulur.

NAT-etkin yönlendirici arkasındaki bilgisayar TrustConnect ile çalışabilir mi?

Evet. Eğer bilgisayarınız İnternete NAT-etkin yönlendirici üzerinden bağlanıyorsa TrustConnect hizmetine bağlanırken bir sorun yaşamamalısınız.

Microsoft Windows Soruları

"Ağ Bağlantılarımda" görünen "TAP-Win32 Adapter" nedir?

"TAP-Win32 Adapter" sanal ağ kartıdır ve TrustConnect yüklenirken oluşturulur. Bu bağdaştırıcı TrustConnect Sunucusuna güvenli tünel oluşturmak için gereklidir.

Her şeyi doğru yaptığımdan eminim fakat hala sunucuya bağlanamıyorum.

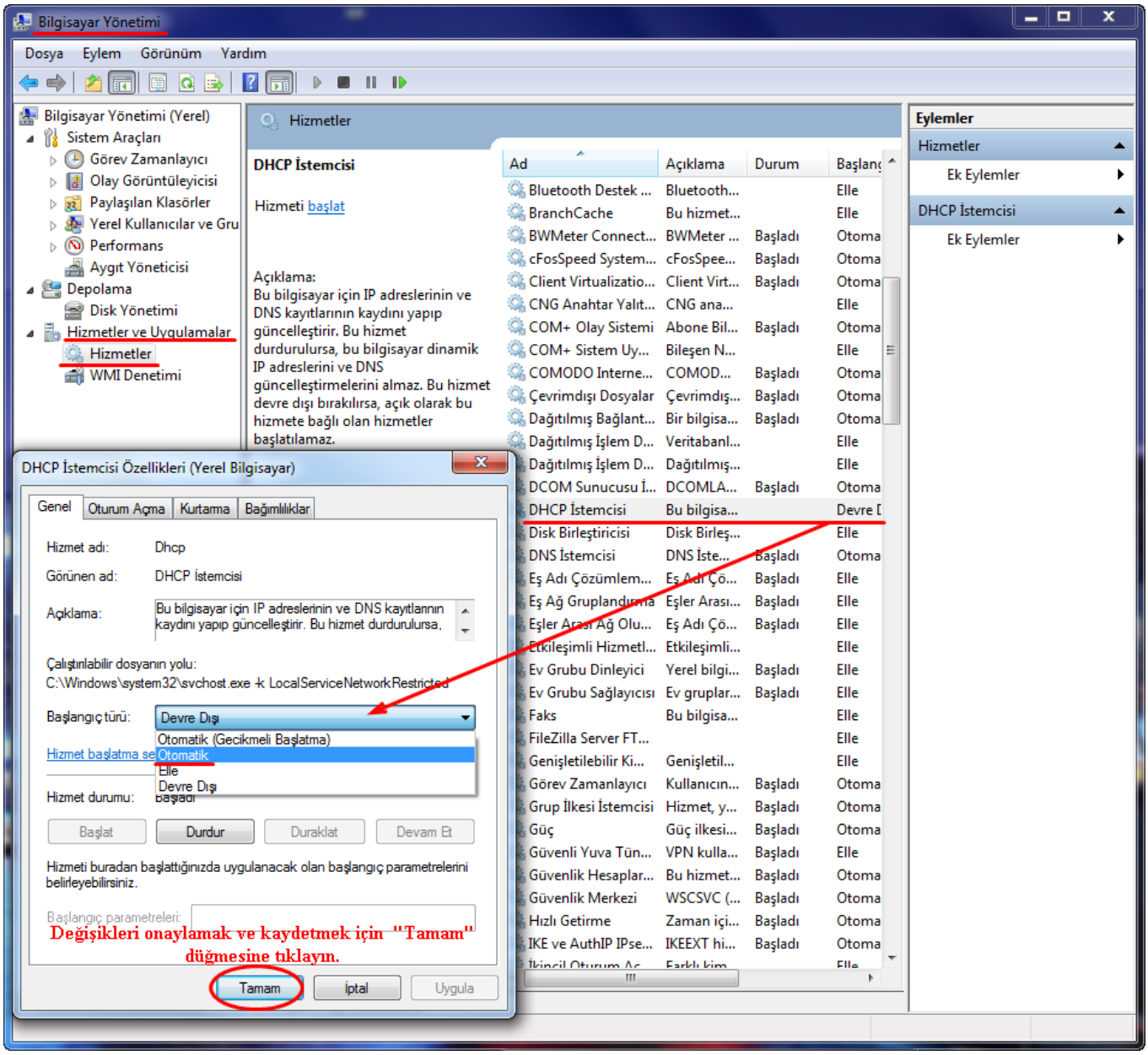
Hizmet giriş bilgilerinizi doğru girdiğinizden emin olun. Bu yanlışsa https://accounts.comodo.com/trustconnect/management adresine girin ve Hizmet Giriş bilgilerinizi denetleyin.

Sunucuya bağlanabiliyorum fakat sitelere erişemiyorum. IPCONFIG /ALL komutu TAP bağdaştırıcısı için 0.0.0.0 IP gösteriyor. Ne yanlış?

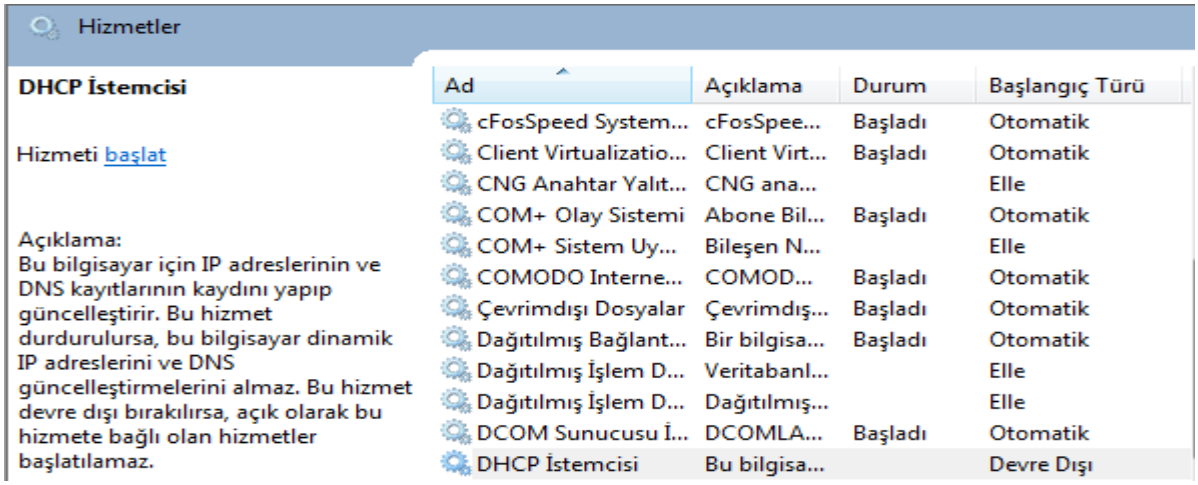
DHCP İstemcisi hizmeti etkin olmalıdır.

Bu hizmeti etkinleştirmek için, şunları yapmalısınız:

1. Windows "Bilgisayarım" simgesine sağ tıklayın.
2. ‘Bilgisayar Yönetimi’ aracını açmak için içerik menüsünden "Yönet" seçin.
3. ‘Hizmetler ve Uygulamalar’ bölümüne daha sonra ‘Hizmetler’ bölümüne girin.
4. Sağda listelenen hizmetlerin listesinden ‘DHCP İstemcisini’ seçin. Bu DHCP İstemci Özellikleri penceresini açar.
5. ‘Başlangıç türünün’ ‘Otomatik’ olarak ayarlı olduğundan emin olun.
6. Değişikleri onaylamak ve kaydetmek için “Tamam” düğmesine tıklayın.



- 'Hizmeti başlat' bağlantısı şimdi mevcuttur. Ona tıklayarak DHCP İstemcisini çalıştırın.



TrustConnect ile WEB bağlantısı yaparken güvenlik duvarı açık olmalı mı?

Evet. TrustConnect internet bağlantınızın güvenliğini sağlar fakat bilgisayarınızın portlarını güvenceye almaz (bu amaçla tasarlanmamıştır). Portlarınızı korumak için hala güvenlik duvarı gerekmektedir. Comodo kullanıcılara Comodo Internet Security yüklemelerini önerir.

TrustConnect tarafından hangi port numaraları kullanılır?

TrustConnect yalnızca 443. Portu kullanır.

Microsoft Windows Vista Soruları

Sunucuya bağlanamıyorum. Günlük dosyası "Bu sistemdeki tüm TAP-Win32 bağdaştırıcıları kullanımdadır" girdisini içeriyor. Fakat "Ağ Bağlantılarımda" herhangi bir bağdaştırıcı bulamadım?

TrustConnect yazılımını her zaman Yönetici erişim hakları ile yükleyin ve çalıştırın.

Tüm bağdaştırıcılar doğru yerde fakat hala sunucuya bağlanamıyorum.
"Yönetici olarak çalıştır " kutusunu işaretlemeniz gerekmektedir:

- TrustConnect simgesine sağ tıklayın;
- 'Özellikler' --> 'Uyumluluk' seçin.

VEYA Windows Vista ve üzerinde "Yönetici olarak çalıştır" ile uygulamayı çalıştırın.

iPhone/iPod İstemci Soruları

Bağlanmayı denediğimde sunucu yanıt vermiyor.

Ağ ayarlarınızı ve internet erişiminizi denetleyin.

TrustConnect sunucu adresleri nelerdir?

IPod / IPhone istemcileri için aşağıdaki sunucuları kullanabilirsiniz:

- us1.vpn.comodo.com (ücretli abonelik için)
- us2.vpn.comodo.com (ücretli abonelik için)
- us3.vpn.comodo.com (ücretsiz abonelik için)

TrustConnect, iPod istemcisi için hangi port numaralarını kullanıyor?

TrustConnect IPOD istemcisi 1723. Portu kullanır (PPTP hizmeti).

7 Ek 1 Comodo Secure DNS Hizmeti

Giriş

Comodo Secure DNS hizmeti kullanımda olan DNS sunucularınızı değiştirerek DNS isteklerini Comodo Sunucularından çözümler. Çoğu ağ ISS tarafından sağlanan veya kendi küçük çaplı DNS sunucularını kullanmaktadır fakat hızlı ve güvenli DNS çözümlemesi için güvenli ve geniş dağıtılmış olarak hizmet veren DNS sunucuları gerekmektedir.

Not: İnternetteki her cihaz özgün 32-bit numara (IPv4) veya 128-bit numara (IPv6) ile tanımlanır. Bu bilgisayarlar için yeterli de olsa insanlar sayı dizeleri yerine adları daha rahat hatırlayabilirler. The Domain Name System/Alan Adı Sistemi (DNS) bu sayılar ve adlar arasındaki çeviriyi sağlar. Sanal olarak her yazılım, cihaz, aygıt ve hizmet İnternet üzerinden birbirleriyle iletişim kurmak için DNS kullanır. Ayrıca DNS bu bilgileri kullanıcıların uzaktan bulabilmesi için İnternet üzerinde yayar.

Comodo Secure DNS geniş olarak dağıtılmış DNS hizmetidir. Donanım veya yazılım gerektirmez ve daha sağlıklı, hızlı ve güvenli bir İnternet deneyimi sunar.

- **Sağlıklı – Comodo Secure DNS hizmeti dünya üzerinde beş kıtaya yayılmıştır. Bu her yerden daha sağlıklı bir DNS hizmeti almanızı sağlar. Her düğümde çoklu sunucular vardır ve birkaç Tier 1 taşıyıcıya bağlıdır.**
- **Daha Hızlı – Bizim stratejik olarak yerleştirilmiş düğümlerimiz İnternetin en uygun kesişim noktalarında konumlandırılmıştır. Çoğu DNS sağlayıcısının aksine, Comodo Secure DNS hizmeti "Anycast " yönlendirme teknolojisini kullanır. Bunun anlamı, yapmış olduğunuz DNS istekleri size en yakında bulunan düğüm tarafından çözümlenir. Bunu kocaman önbelleğimiz ile birleştirin ve aradığınız yanıtı herkesten daha hızlı ve sağlıklı olarak getirebiliriz.**
- **Daha Akıllı – Bulunmayan bir siteye gitmek istediğinizde Comodo'nun arama ve rehber sayfaları sizi istediğiniz yere götürür.**
- **Daha Güvenli – Lider İnternet Güvenlik Çözümleri sağlayıcısı olarak, Comodo İnternetteki tehditlerin farkındadır. Comodo zararlı web sitelerinin (örn. sahtekârlık siteleri, kötü niyetli yazılım bulunduran siteler, vs.) gerçek zamanlı olarak engellenme listesini (RBL) tutar, bunlara erişilmek istendiği zaman kullanıcıyı uyarır. Bilinen çevrimiçi tehlikelerden sizi ve sizin müşterilerinizi korumak için bize güvenebilirsiniz.**

Comodo Secure DNS hizmetini başlatmak için DNS ayarlarınızı bizim DNS sunucularımızın IP adreslerini gösterecek şekilde ayarlamanız gerekmektedir. Comodo Internet Security yüklenirken bu ayarların otomatik olarak yapılandırılmasını seçebilirsiniz. Bunu seçmediyseniz , bu ayarları daha sonra elle değiştirebilirsiniz. İstediğiniz zaman önceki ayarlarınıza da geri dönebilirsiniz.

Aşağıdaki bağlantılara tıklayarak bilgisayarınızın veya yönlendiricinizin DNS ayarlarını elle nasıl değiştirilebileceğini öğrenebilirsiniz.

- **Yönlendirici**
- **Windows XP**
- **Windows Vista**

7.1 Yönlendirici (Router) – Comodo Secure DNS Hizmetinin Elle Etkinleştirilmesi veya Devre Dışı Bırakılması

Comodo Secure DNS hizmetini yönlendiricinizin DNS ayarlarını elle değiştirerek etkinleştirebilir veya devre dışı bırakabilirsiniz. Comodo ağdaki her bilgisayarın DNS ayarlarını elle değiştirmek yerine yönlendirici üzerinden değişiklik yapılmasını önerir, böylece Comodo Secure DNS hizmeti ağdaki tüm bilgisayarlar tarafından kullanılabilir.

Comodo Secure DNS hizmetini etkinleştirmek için, DNS sunucusunun IP adreslerini aşağıdaki Comodo Secure DNS sunucu adresleri ile değiştirin. IP adresleri şunlardır:

Birincil DNS: 156.154.70.22

İkincil DNS: 156.154.71.22

Önemli Not: CIS yüklenirken İngilizce dışında bir dil seçtiyseniz, aşağıdaki adresleri kullanın:

Birincil DNS: 156.154.70.25

İkincil DNS: 156.154.71.25

Comodo Secure DNS himzetini durdurmak için

- **DNS sunucusu IP adreslerini önceki ayarına değiştirin.**

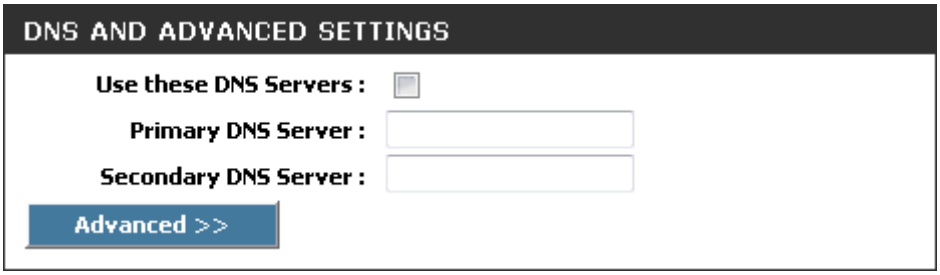
DNS ayarlarını değiştirmek için

1. Yönlendiriciye giriş yapın. Web tarayıcınısı açın ve yönlendiricinin yönetim sayfasına girin. Eğer yönlendiricinin yönetim sayfasının IP adresini bilmiyorsanız endişelenmeyin, genellikle aşağıdaki IP adreslerinden biridir:

http://192.168.0.1
http://192.168.1.1
http://192.168.10.1

Yönlendiriciye giriş için kullanıcı adını ve/veya parolasını unuttuysanız, en yaygın olarak kullanıcı adı için “admin” ve parola için boş, “admin” veya “password” kullanılır. Bunlar çalışmaz ise yönlendiricinizi sıfırlayarak deneyin.

1. DNS Sunucu Ayarlarını bulun. "DNS" girilecek alanı bulmaya çalışın.



2. DNS IP adreslerine Comodo Secure DNS sunucularını girin ve kaydedin.

Birincil DNS: 156.154.70.22

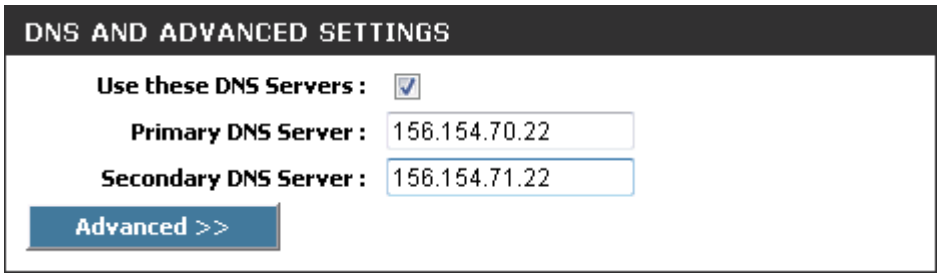
İkincil DNS: 156.154.71.22

Önemli Not: CIS yüklenirken İngilizce dışında bir dil seçtiyseniz, aşağıdaki adresleri kullanın:

Birincil DNS: 156.154.70.25

İkincil DNS: 156.154.71.25

Girdikten sonra aşağıdaki örnekteki gibi görünecektir.



Comodo Secure DNS hizmetini şu şekilde devre dışı bırakabilirsiniz:

- **DNS sunucu kullanımı ayarını iptal edin veya otomatik olarak ayarlayın.**

veya

- **Tercih edilen farklı ve alternatif DNS sunucu IP adresleri girerek.**

7.2 Windows XP – Comodo Secure DNS Hizmetinin Elle Etkinleştirilmesi veya Devre Dışı Bırakılması

Comodo Secure DNS hizmetini işletim sisteminizin Denetim Masası > Ağ Bağlantıları üzerinden erişilebilen DNS ayarlarını elle değiştirerek etkinleştirebilir veya devre dışı bırakabilirsiniz.

Comodo Secure DNS hizmetini etkinleştirmek için, DNS sunucusunun IP adreslerini aşağıdaki Comodo Secure DNS sunucu adresleri ile değiştirin. IP adresleri şunlardır:

Tercih edilen DNS: 156.154.70.22

Diğer DNS: 156.154.71.22

Önemli Not: CIS yüklenirken İngilizce dışında bir dil seçtiyseniz, aşağıdaki adresleri kullanın:

Birincil DNS: 156.154.70.25

İkincil DNS: 156.154.71.25

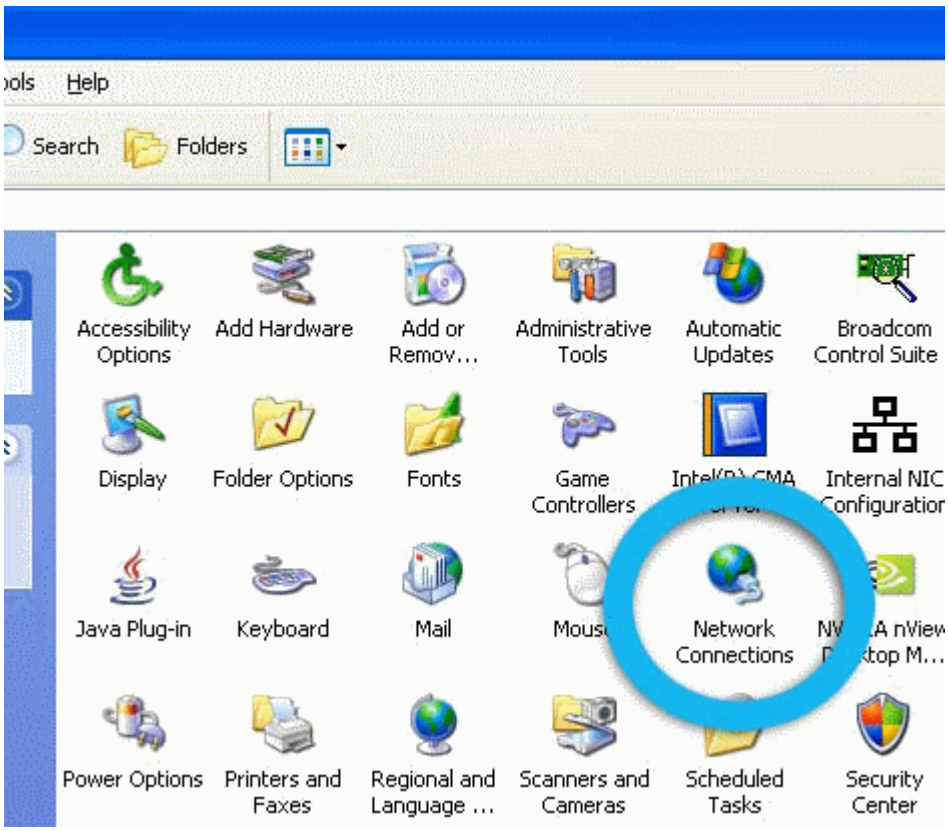
Comodo Secure DNS hizmetini durdurmak için

- **DNS sunucusu IP adreslerini önceki ayarına değiştirin.**

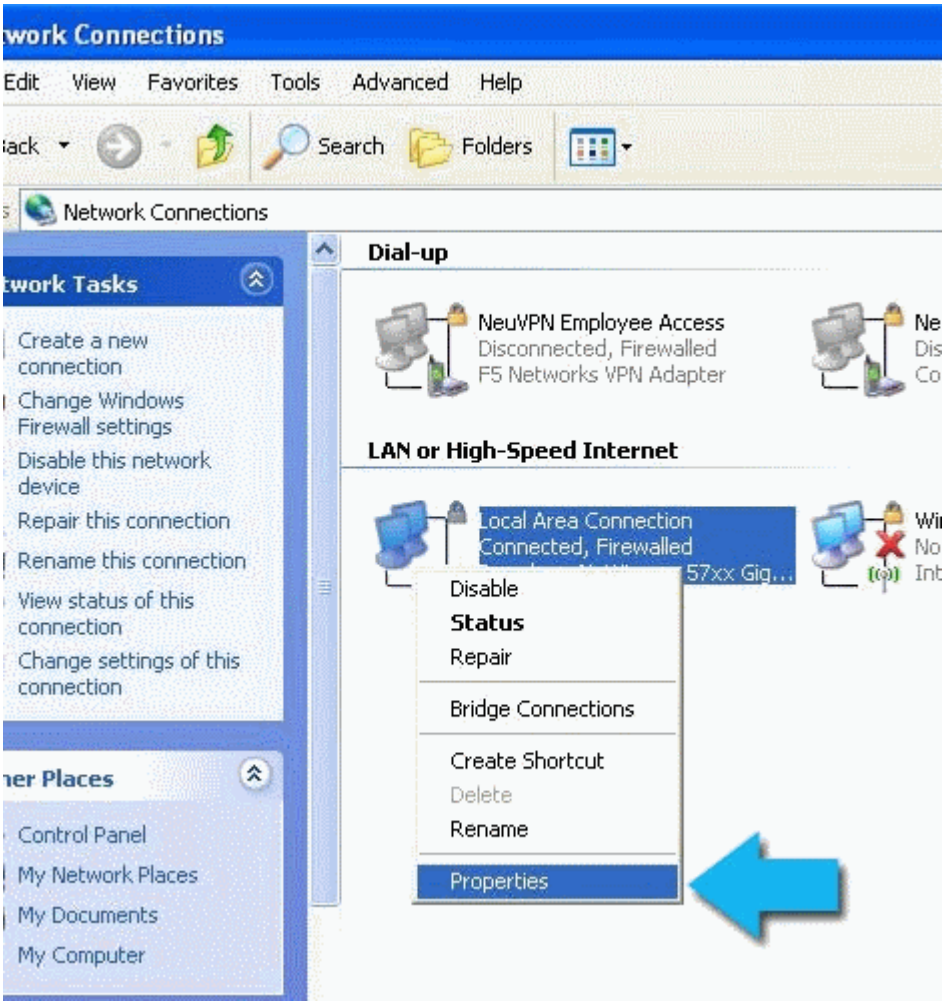
DNS ayarlarını değiştirmek için

1. Başlangıç Menüsünden 'Denetim Masası' seçin.

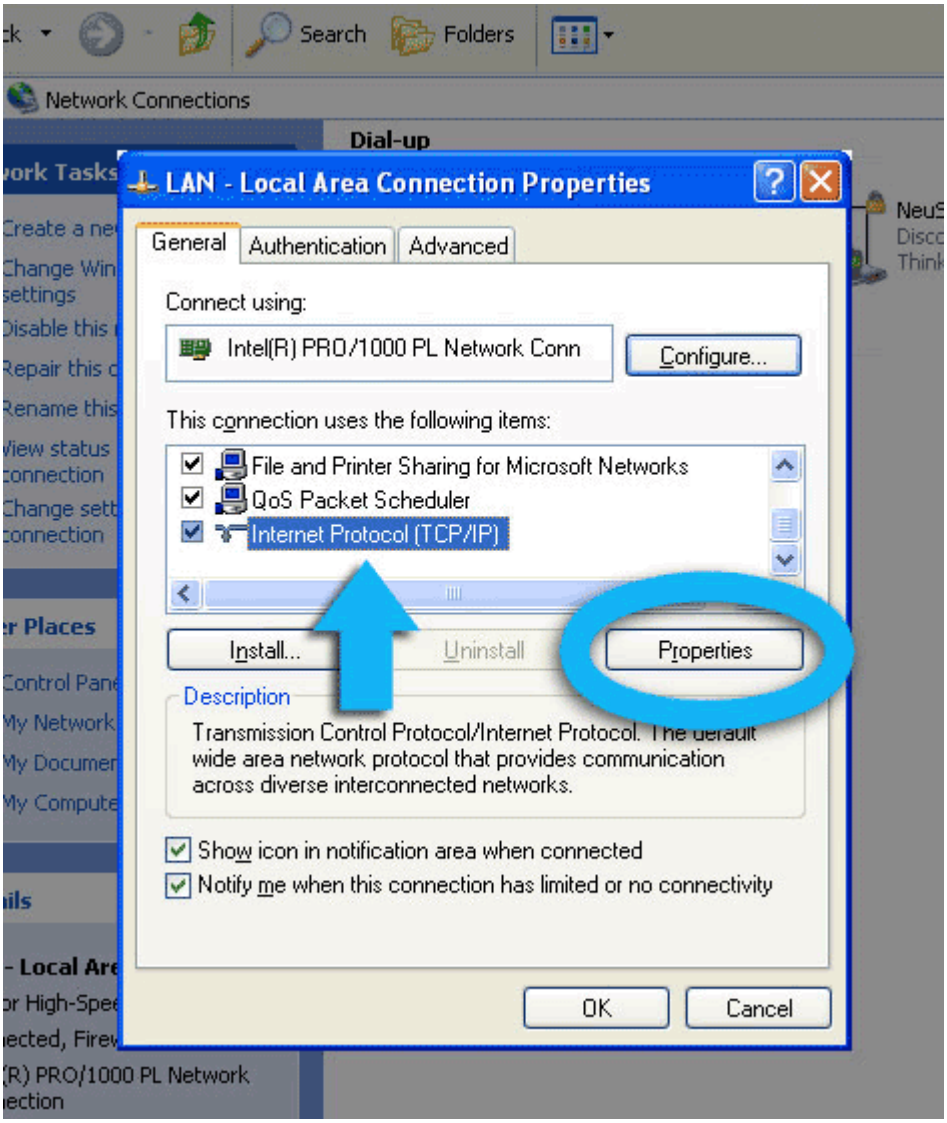
2. Denetim Masası seçeneklerinden 'Ağ Bağlantıları' öğesini seçin.



3. Ağ Bağlantılarından bağlantınıza sağ tıklayın ve 'Özellikler' seçeneğine tıklayın



4. 'Internet Protokolü (TCP/IP)' seçin ve 'Özellikler' seçeneğine tıklayın.



5. Radyo düğmesine tıklayın Aşağıdaki DNS sunucu adreslerini kullan kutusunu işaretleyin ve Comodo Secure DNS adreslerini Tercih edilen ve Diğer DNS sunucusu alanlarına girin.

Lütfen herhangi bir nedenle eski ayarlarınıza dönmek istediğiniz durumlar için Comodo Secure DNS adreslerini girmeden önce kullanmakta olduğunuz DNS adreslerini bir yere not ediniz.

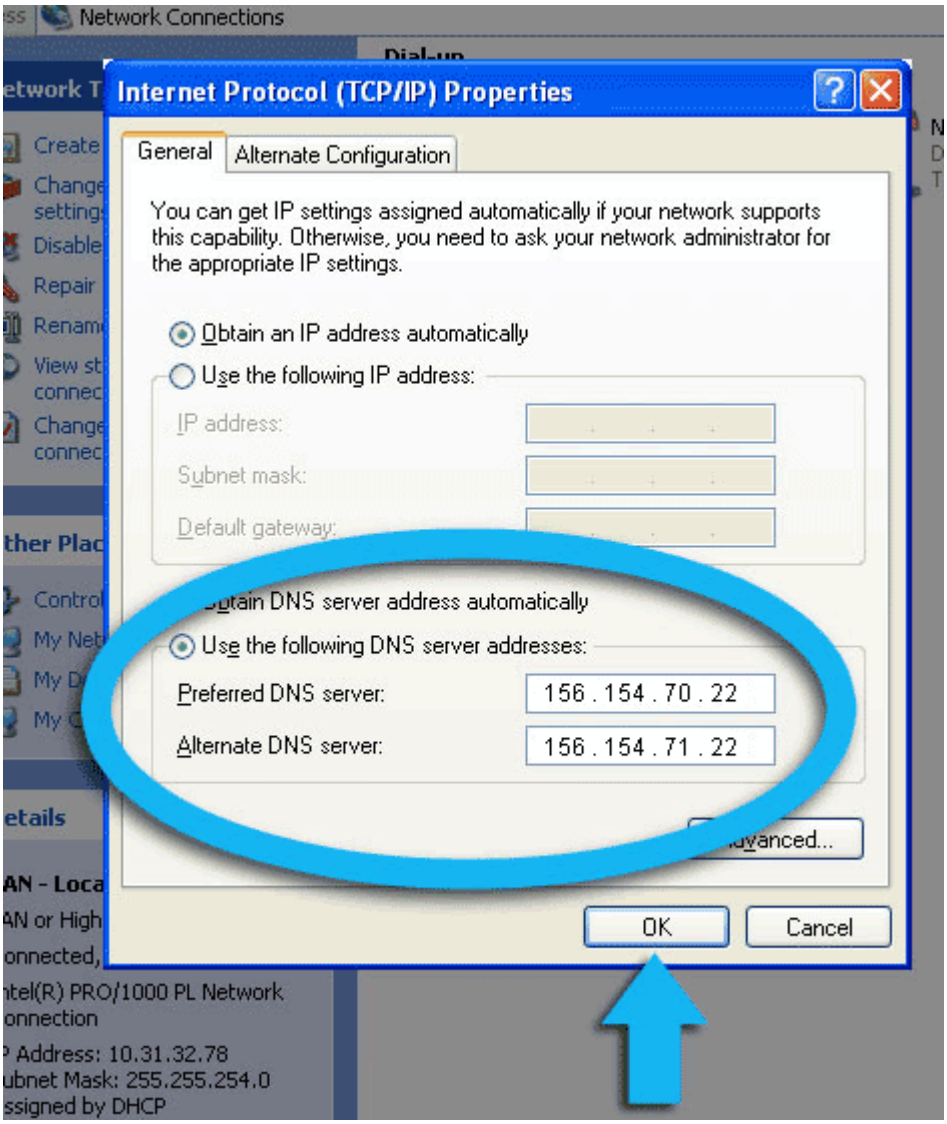
Tercih edilen DNS: 156.154.70.22

Diğer DNS: 156.154.71.22

Önemli Not: CIS yüklenirken İngilizce dışında bir dil seçtiyseniz, aşağıdaki adresleri kullanın:

Birincil DNS: 156.154.70.25

İkincil DNS: 156.154.71.25

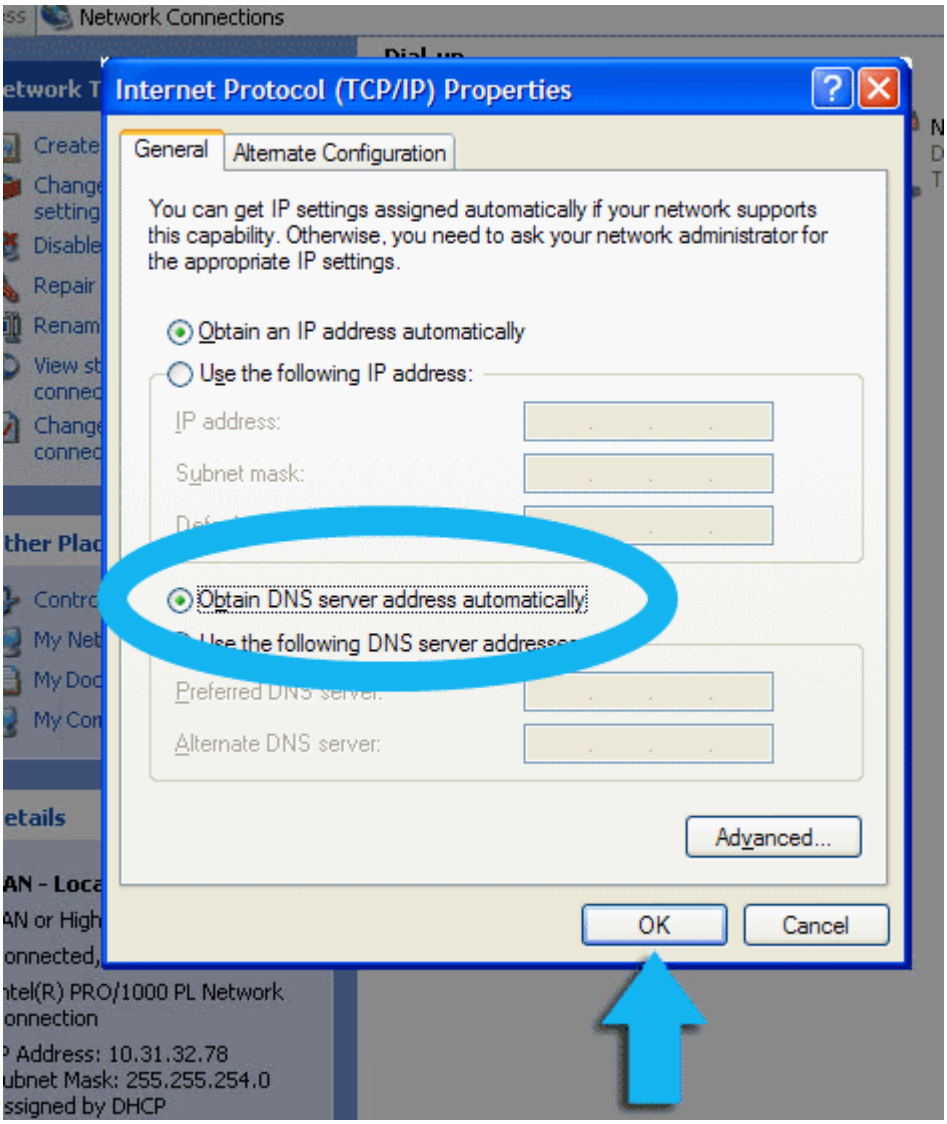


Comodo Secure DNS hizmetini şu şekilde devre dışı bırakabilirsiniz:

- **'DNS sunucu adresini otomatik olarak al' seçerek ISS tarafından sağlanan DNS adreslerini kullanmaya geri dönebilirsiniz.**

veya

- **Tercih edilen farklı ve alternatif DNS sunucu IP adresleri girerek.**



7.3 Windows Vista – Comodo Secure DNS Hizmetinin Elle Etkinleştirilmesi veya Devre Dışı Bırakılması

Comodo Secure DNS hizmetini işletim sisteminizin Denetim Masası > Ağ Bağlantıları üzerinden erişilebilen DNS ayarlarını elle değiştirerek etkinleştirebilir veya devre dışı bırakabilirsiniz.

Comodo Secure DNS hizmetini etkinleştirmek için, DNS sunucusunun IP adreslerini aşağıdaki Comodo Secure DNS sunucu adresleri ile değiştirin. IP adresleri şunlardır:

Tercih edilen DNS: 156.154.70.22

Diğer DNS: 156.154.71.22

Önemli Not: CIS yüklenirken İngilizce dışında bir dil seçtiyseniz, aşağıdaki adresleri kullanın:

Birincil DNS: 156.154.70.25

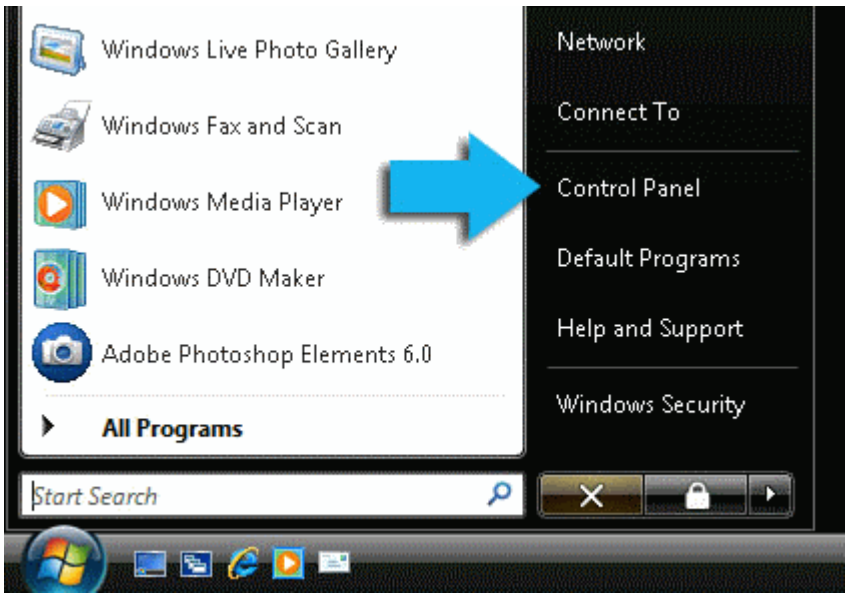
İkincil DNS: 156.154.71.25

Comodo Secure DNS hizmetini durdurmak için

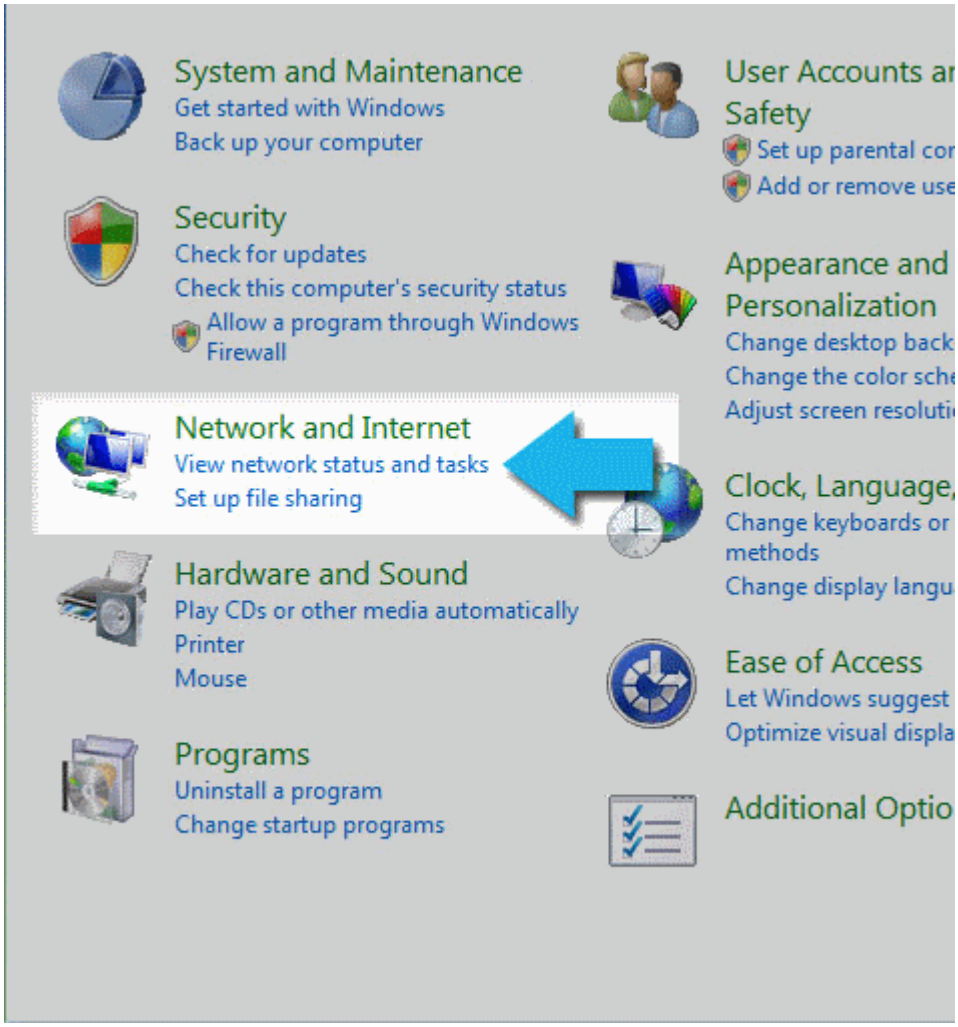
- **DNS sunucusu IP adreslerini önceki ayarına değiştirin.**

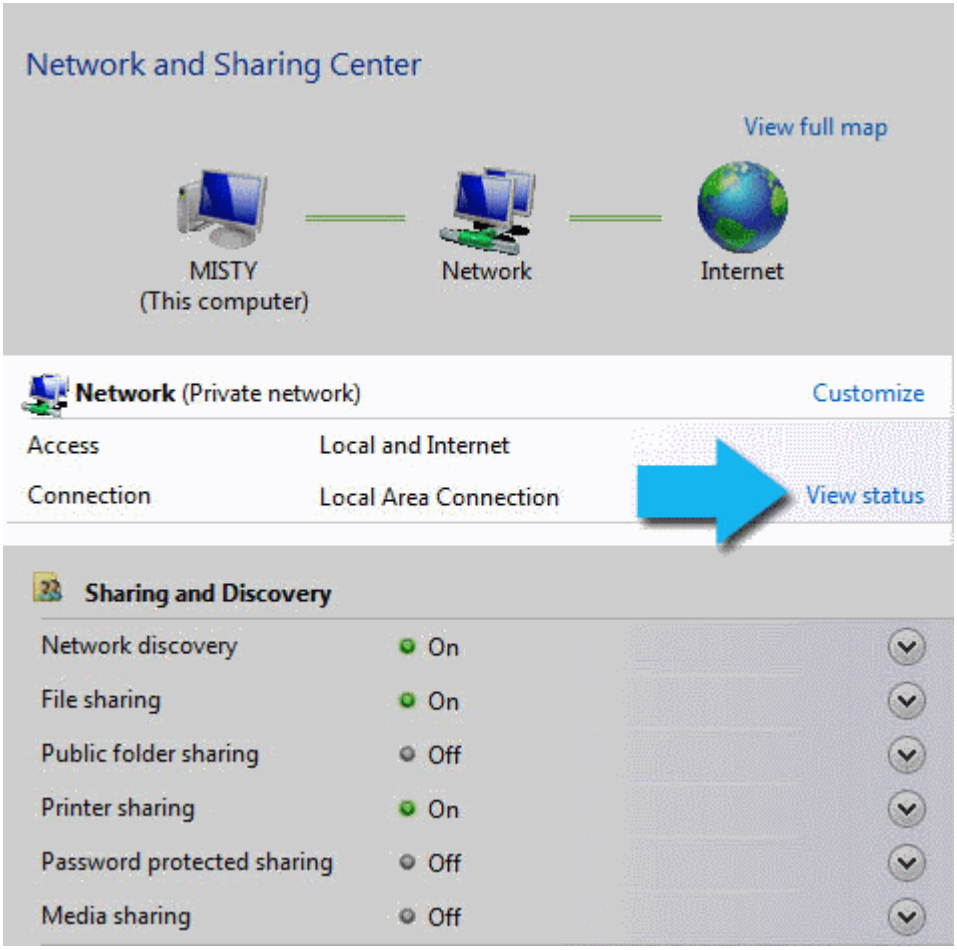
DNS ayarlarını değiştirmek için

1. 'Başlat' düğmesine tıklayın, daha sonra 'Denetim Masası' seçin.

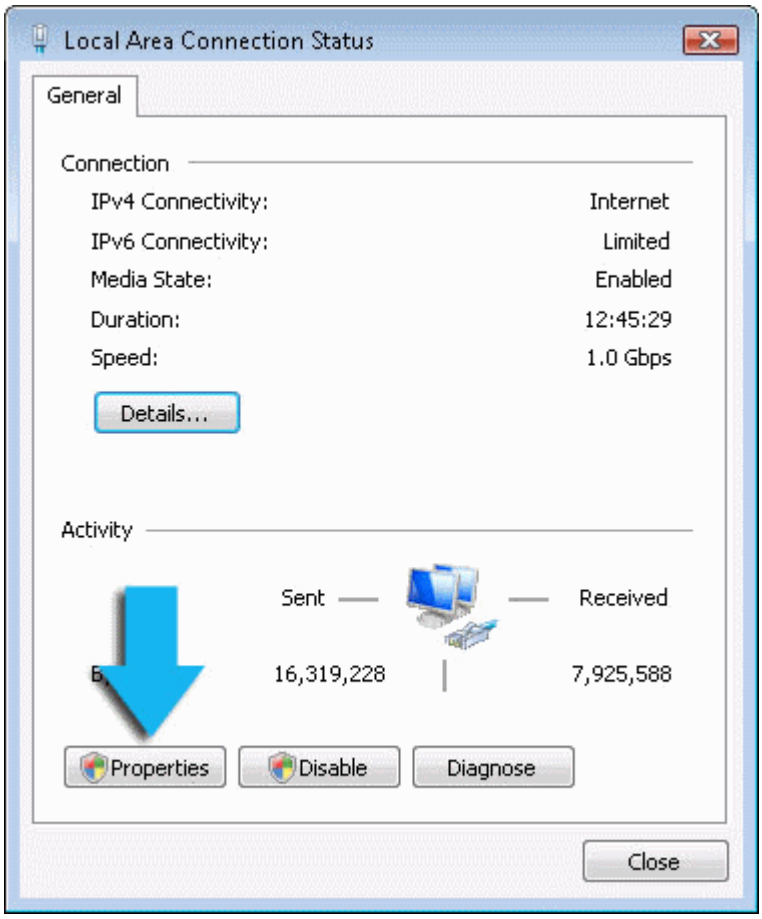


2. 'Ağ durumunu ve görevlerini görüntüle' bağlantısına tıklayın.

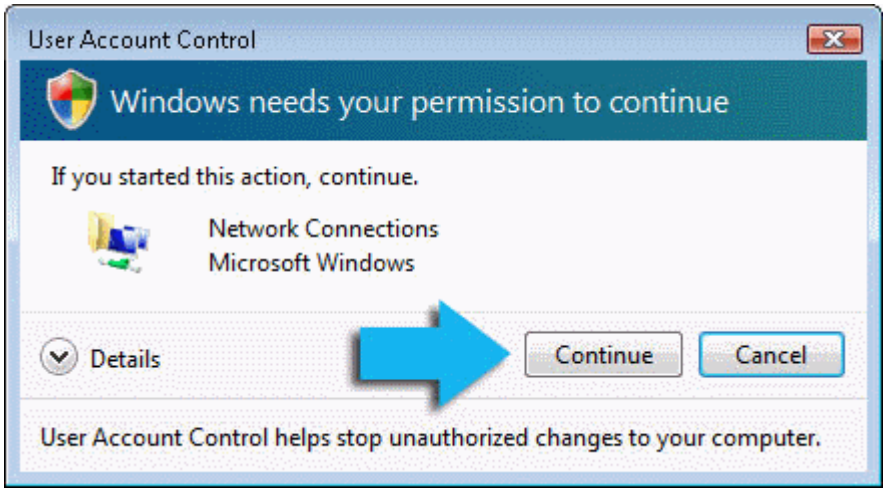




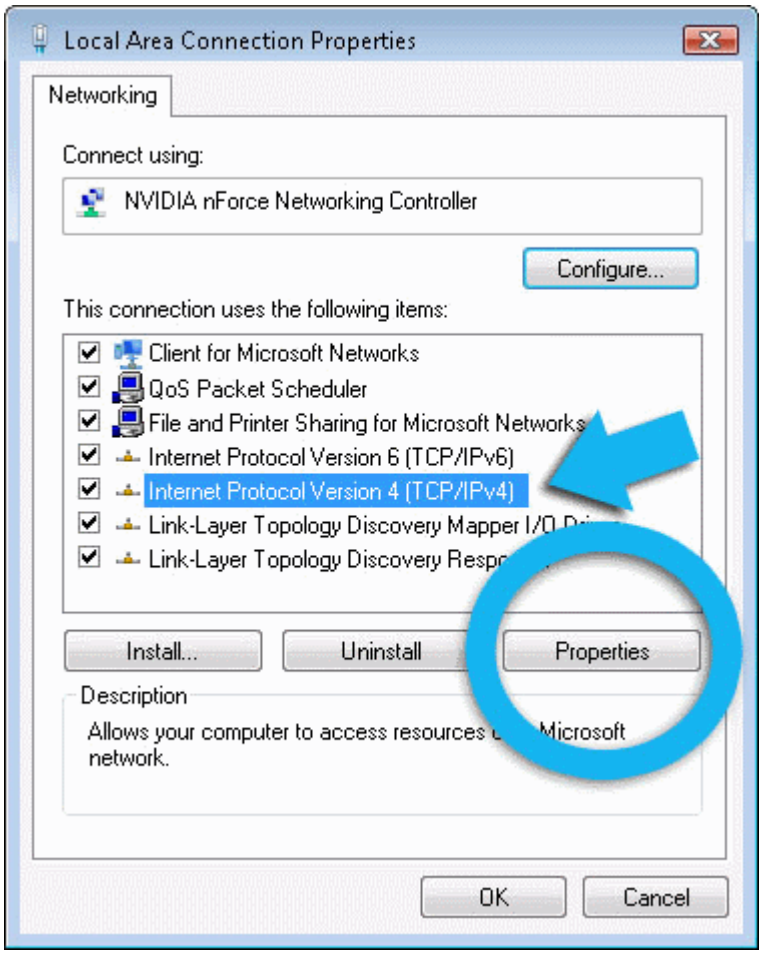
3. 'Durum Görüntüle' bağlantısına tıklayın.
4. 'Özellikler' düğmesine tıklayın.



5. Vista değişiklik yapabilmeniz için izin isteyebilir. Eğer isterse 'Devam/Evet' düğmesine tılayın.



6. 'Internet Protokolü sürüm 4 (TCP/IPv4)' seçin, daha sonra 'Özellikler' düğmesine tıklayın.



7. Radyo düğmesine tıklayın Aşağıdaki DNS sunucu adreslerini kullan kutusunu işaretleyin ve Comodo Secure DNS adreslerini Tercih edilen ve Diğer DNS sunucusu alanlarına girin.

Lütfen herhangi bir nedenle eski ayarlarınıza dönmek istediğiniz durumlar için Comodo Secure DNS adreslerini girmeden önce kullanmakta olduğunuz DNS adreslerini bir yere not ediniz.

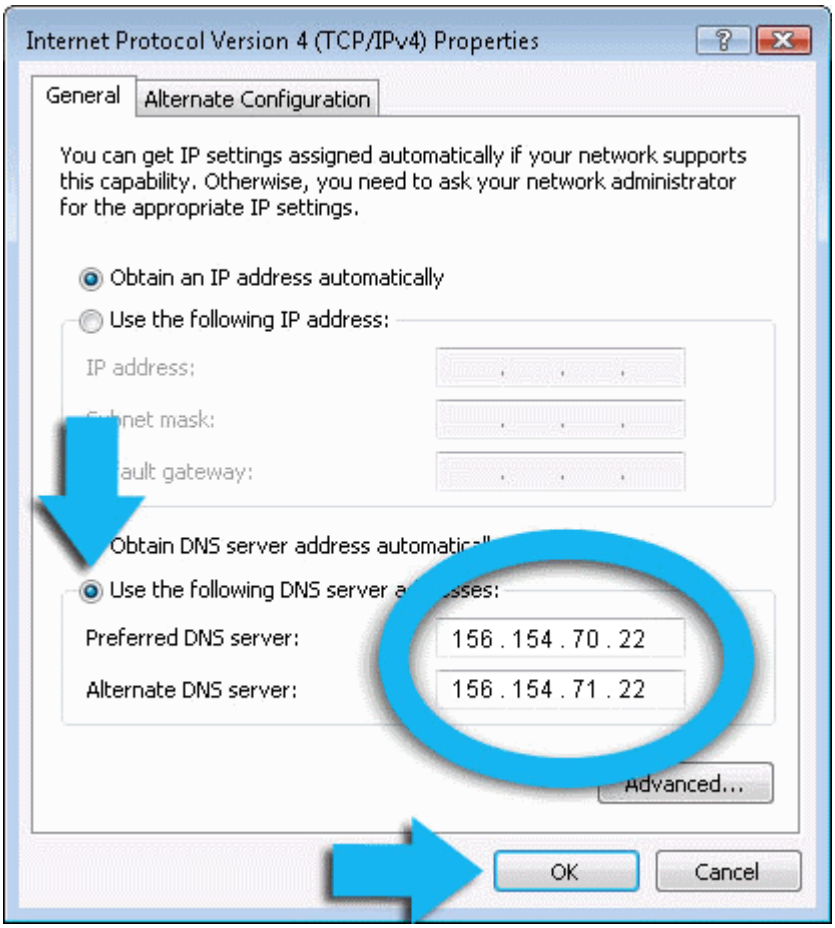
Tercih edilen DNS: 156.154.70.22

Diğer DNS: 156.154.71.22

Önemli Not: CIS yüklenirken İngilizce dışında bir dil seçtiyseniz, aşağıdaki adresleri kullanın:

Birincil DNS: 156.154.70.25

İkincil DNS: 156.154.71.25

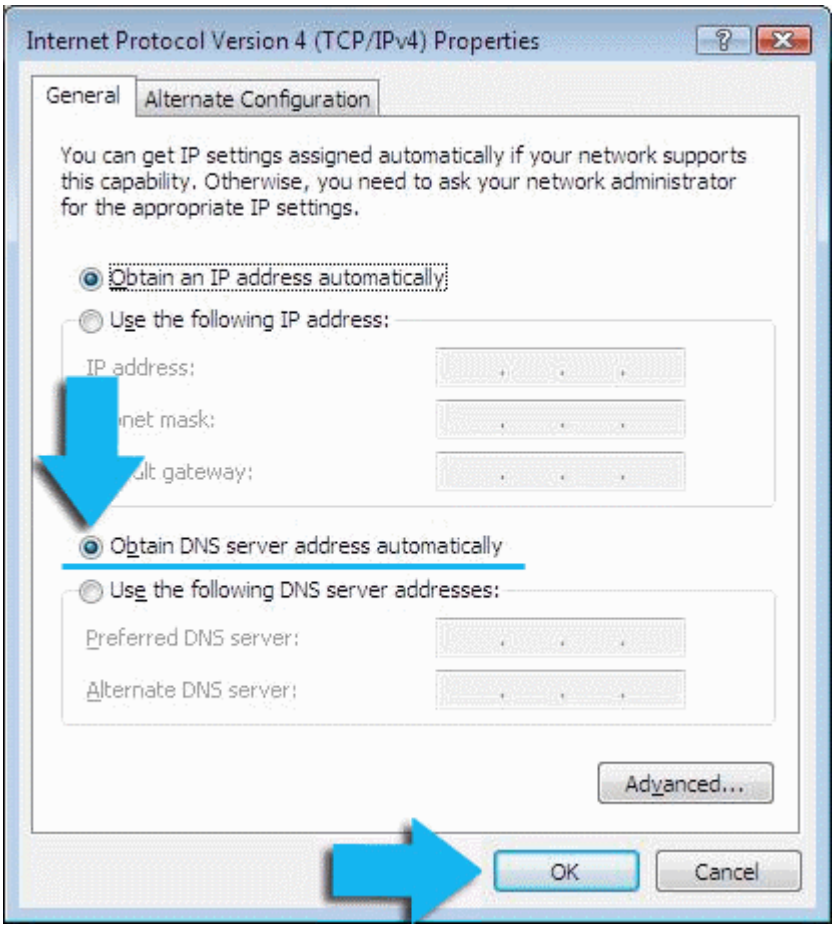


Comodo Secure DNS hizmetini şu şekilde devre dışı bırakabilirsiniz:

- **'DNS sunucu adresini otomatik olarak al' seçerek ISS tarafından sağlanan DNS adreslerini kullanmaya geri dönebilirsiniz.**

veya

- **Tercih edilen farklı ve alternatif DNS sunucu IP adresleri girerek.**



Comodo Hakkında

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

Comodo Security Solutions, Inc.

525 Washington Blvd.

Jersey City, NJ 07310

United States

Tel : +1.888.266.6361

Comodo CA Limited

3rd floor, Office Village Exchange Quay

Trafford Road, Salford, Manchester M5 3EQ

United Kingdom

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

Email: Sales@comodo.com

For additional information on Comodo - visit **http://www.comodo.com**

COMODO

Creating Trust Online™

www.comodo.com

Comodo Security Solutions Inc.
525 Washington Bvld,
Jersey City, NJ 07310
United States
Tel: +1.888.266.6361
Email : Sales@comodo.com