

# ESET Mobile Security

Business Edition řu iřletim sistemi iin: Windows Mobile

Yikleme El Kitabı ve Kullanıcı Kılavuzu



## ESET Mobile Security

Telif hakkı ©2011 ESET, spol. s r.o.

ESET Mobile Security, ESET, spol. s r.o. tarafından geliştirilmiştir. Daha fazla bilgi için [www.eset.com](http://www.eset.com) sitesini ziyaret edin.

Tüm hakları saklıdır. Bu belgenin hiçbir bölümü yazarından yazılı izin alınmadan yeniden üretilemez, yeniden kullanılabilirliği bir sistemde saklanamaz ya da herhangi bir biçimde veya herhangi bir araç (elektronik, mekanik, fotokopi, kayıt, tarama veya diğer) kullanılarak iletilemez.

ESET, spol. s r.o. açıklanan uygulama yazılımlarında önceden haber vermeden değişiklik yapma hakkını saklı tutar.

Dünya Geneline Müşteri Hizmetleri: [www.eset.com/support](http://www.eset.com/support)

REV. 2.5.2011

## İçindekiler

<b>1. ESET Mobile Security yazılımını yükleme.....</b>	<b>3</b>
1.1 Minimum sistem gereksinimleri.....	3
1.2 Yükleme.....	3
1.2.1 Aygıtınıza yükleme.....	3
1.2.2 Bilgisayarınızı kullanarak yükleme.....	3
1.3 Kaldırma.....	4
<b>2. Ürün etkinleştirme.....</b>	<b>5</b>
2.1 Kullanıcı adı ve parola kullanarak etkinleştirme.....	5
2.2 Kayıt anahtarı kullanarak etkinleştirme.....	5
<b>3. Güncelleme.....</b>	<b>6</b>
3.1 Ayarlar.....	6
<b>4. Aktif koruma.....</b>	<b>7</b>
4.1 Ayarlar.....	7
<b>5. İsteğe bağlı tarayıcı.....</b>	<b>8</b>
5.1 Bütün bir aygıt taraması çalıştırma.....	8
5.2 Bir klasörü tarama.....	8
5.3 Genel ayarlar.....	8
5.4 Uzantı ayarları.....	9
<b>6. Tehdit bulundu.....</b>	<b>10</b>
6.1 Karantina.....	10
<b>7. Anti-Theft.....</b>	<b>11</b>
7.1 Ayarlar.....	11
<b>8. Güvenlik duvarı.....</b>	<b>13</b>
8.1 Ayarlar.....	13
<b>9. Güvenlik denetlemesi.....</b>	<b>15</b>
9.1 Ayarlar.....	15
<b>10. Antispam.....</b>	<b>17</b>
10.1 Ayarlar.....	17
10.2 Beyaz Liste / Kara Liste.....	17
10.3 Spam iletilerini bulma.....	18
10.4 Spam iletilerini silme.....	18
<b>11. Uzaktan yönetim.....</b>	<b>19</b>
11.1 Ayarlar.....	19
<b>12. Günlükleri ve istatistikleri görüntüleme.....</b>	<b>20</b>
<b>13. Sorun giderme ve destek.....</b>	<b>22</b>
13.1 Sorun giderme.....	22
13.1.1 Başarısız yükleme.....	22
13.1.2 Güncelleme başarısız oldu.....	22
13.1.3 Dosya karşıdan yükleme zaman aşımına uğradı.....	22
13.1.4 Güncelleme dosyası eksik.....	22
13.1.5 Veritabanı dosyası bozuk.....	22
13.2 Teknik destek.....	22

# 1. ESET Mobile Security yazılımını yükleme

## 1.1 Minimum sistem gereksinimleri

Windows Mobile için ESET Mobile Security ürününü yükleyebilmeniz, ancak mobil aygıtınızın aşağıdaki sistem gereksinimlerini karşılamasıyla mümkündür:

	Minimum sistem gereksinimleri
İşletim sistemi	Windows Mobile 5.0 ve üzeri
İşlemci	200 MHz
Bellek	16 MB
Kullanılabilir boş alan	2,5 MB

## 1.2 Yükleme

Yükleme öncesinde tüm açık belgeleri kaydedin ve çalışan tüm uygulamalardan çıkın. ESET Mobile Security yazılımını doğrudan aygıtınıza yükleyebilir ya da yükleme için bilgisayarınızı kullanabilirsiniz.

Başarılı şekilde yüklendikten sonra, [Ürün etkinleştirme](#) bölümündeki adımları izleyerek ESET Mobile Security yazılımını etkinleştirin.

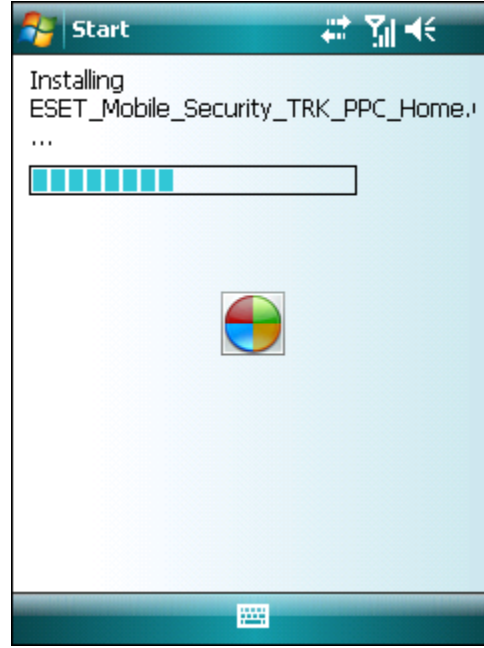
### 1.2.1 Aygıtınıza yükleme

ESET Mobile Security yazılımını doğrudan aygıtınıza yüklemek için Wi-Fi, Bluetooth, USB dosya aktarımı veya e-posta eki aracılığıyla .cab yükleme dosyasını aygıtınıza karşıdan yükleyin. Dosyayı bulmak için **Başlat > Programlar > Dosya Gezgini** yolunu izleyin. Dosyaya dokunarak yükleyiciyi başlatın ve ardından yükleme sihirbazındaki istemleri izleyin.



ESET Mobile Security ürününü yükleme

**NOT:** Windows Mobile kullanıcı arabirimi, aygıt modeline göre farklılık gösterir. Yükleme dosyası aygıtınızda farklı bir menüde ya da klasörde bulunabilir.

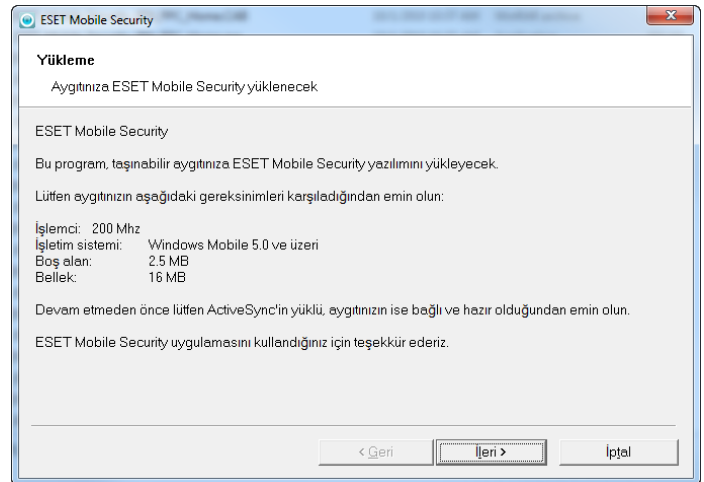


Yükleme işlemi

Yükleme sonrasında, program ayarlarını değiştirebilirsiniz. Bununla birlikte, varsayılan yapılandırma kötü amaçlı programlara karşı maksimum koruma sağlar.

### 1.2.2 Bilgisayarınızı kullanarak yükleme

ESET Mobile Security ürününü bilgisayarınızı kullanarak yüklemek için, mobil aygıtınızı ActiveSync (Windows XP'de) ya da Windows Mobile Aygıt Merkezi (Windows 7 ve Vista'da) aracılığıyla bilgisayara bağlayın. Aygıt tanındıktan sonra, karşıdan yüklenen yükleme paketini (.exe dosyası) çalıştırın ve yükleme sihirbazındaki talimatları izleyin.



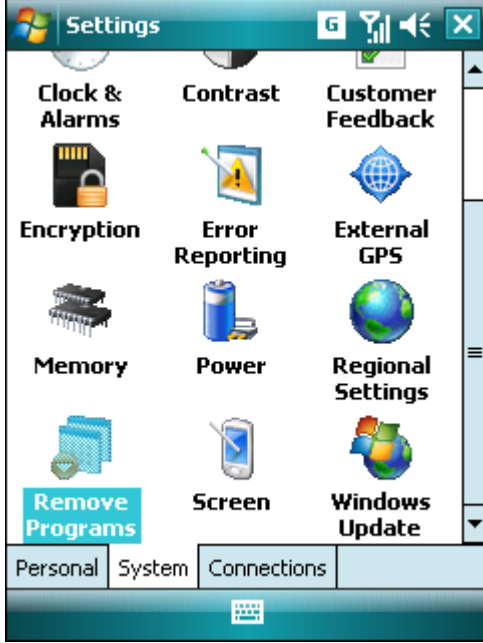
Bilgisayarınızdaki yükleyiciyi başlatma

Ardından mobil aygıtınızdaki istemleri izleyin.

### 1.3 Kaldırma

**Başlat** > **Ayarlar** yolunu izleyip **Sistem** sekmesine, ardından da **Program Kaldır** simgesine dokunarak ESET Mobile Security programını mobil aygıtınızdan kaldırabilirsiniz.

**NOT:** Windows Mobile kullanıcı arabirimi, aygıt modeline göre farklılık gösterir. Bu seçenekler aygıtınızda biraz farklı olabilir.



ESET Mobile Security programını kaldırma

ESET Mobile Security öğesini seçin ve **Kaldır**'a dokunun. Kaldırma işlemini onaylamanız istediğinde **Evet** seçeneğine dokunun.



ESET Mobile Security programını kaldırma

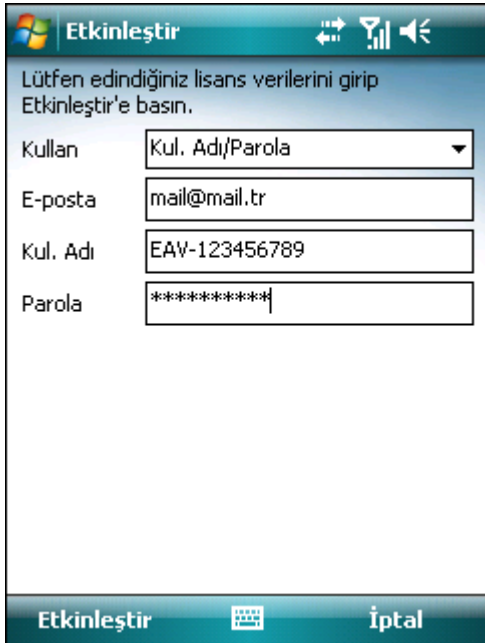
## 2. Ürün etkinleştirme

Ana ESET Mobile Security penceresi (**Başlat > Programlar > ESET Mobile Security**) bu el kitabındaki tüm talimatların başlangıç noktasıdır.



Ana ESET Mobile Security penceresi

Başarılı şekilde yüklendikten sonra, ESET Mobile Security programının etkinleştirilmesi gerekir. Ürününüzü etkinleştirmeniz istenmezse, **Menü > Etkinleştir** seçeneğine dokununuz.



Program etkinleştirme

İki farklı etkinleştirme yöntemi vardır; sizin için hangisinin geçerli olduğu, ESET Mobile Security ürününüzü satın alma şeklinize bağlıdır.

### 2.1 Kullanıcı adı ve parola kullanarak etkinleştirme

Ürününüzü bir dağıtımçıdan satın aldıysanız, size ürünle birlikte bir kullanıcı adı ve parola verilmiştir. **Kul. Adı/Parola** seçeneğini belirleyin ve **Kul. Adı** ve **Parola** alanlarına size verilen bilgileri girin. **E-posta** alanına geçerli iletişim adresinizi girin. Etkinleştirmeyi tamamlamak için **Etkinleştir**'e dokununuz. Ürünü başarıyla etkinleştirdiğinize dair bir onay e-postası alacaksınız.

### 2.2 Kayıt anahtarı kullanarak etkinleştirme

ESET Mobile Security ürününü yeni bir aygıtla birlikte (ya da kutulu bir ürün olarak) satın aldıysanız, size ürünle birlikte bir Kayıt anahtarı verilmiştir. **Kayıt anahtarı** seçeneğini belirleyin ve ardından **Anahtar** alanına size verilen bilgileri, **E-posta** alanına da geçerli iletişim adresinizi girin. Etkinleştirmeyi tamamlamak için **Etkinleştir**'e dokununuz. Yeni kimlik doğrulama verileriniz (Kullanıcı Adı ve Parola) otomatik olarak Kayıt anahtarının yerine geçecek ve belirttiğiniz e-posta adresine gönderilecektir.

Her etkinleştirme belirli bir süre için geçerlidir. Etkinleştirilen lisansın süresi sona erdiğinde program lisansını yenilemeniz gerekir (program sizi bu konuda önceden bilgilendirecektir).

**NOT:** Etkinleştirme sırasında, aygıtın Internet'e bağlı olması gerekir. Küçük miktarda veri indirilecektir. Bu aktarımlar, mobil iletişim sağlayıcınızla yaptığınız hizmet sözleşmesine göre ücretlendirilir.

### 3. Güncelleme

Varsayılan olarak ESET Mobile Security ile birlikte, programın düzenli olarak güncellenmesini sağlayacak bir güncelleme görevi yüklenmiştir. Güncellemeleri elle de gerçekleştirebilirsiniz.

Yüklemeden sonra, ilk güncellemeyi elle çalıştırmanızı öneririz. Bunu **Eylem > Güncelle** yolunu izleyerek yapabilirsiniz.

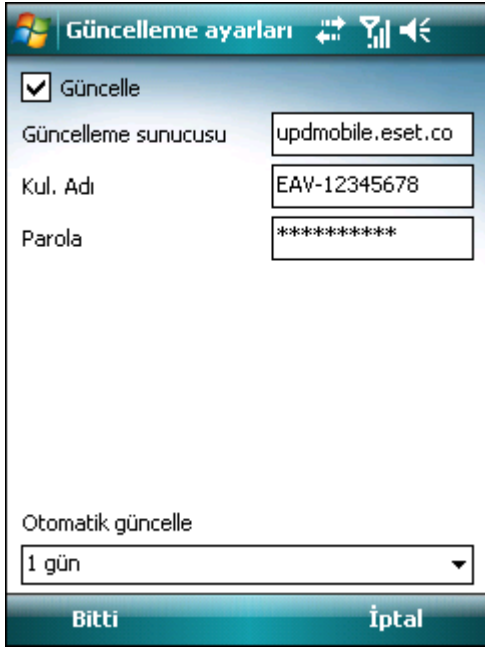
#### 3.1 Ayarlar

Güncelleme ayarlarını **Menü > Ayarlar > Güncelle** yolunu izleyerek yapılandırabilirsiniz.

**Güncelle** seçeneği otomatik güncellemeleri etkinleştirir ya da devre dışı bırakır.

Güncellemelerin karşidan yükleneceği **Güncelleme sunucusu** adresini belirleyebilirsiniz (*updmobile.eset.com* adresi varsayılan ayarını aynen bırakmanızı öneririz).

**Otomatik güncelle** seçeneğini kullanarak otomatik güncellemelerin zaman aralığını belirleyebilirsiniz.



#### Güncelleme ayarları

**NOT:** Yeni bir tehdit eklendiğinde, gereksiz bant genişliği kullanımını önlemek için, gerektiği şekilde virüs imza veritabanı güncellemeleri yayınlanır. Virüs imza veritabanı güncellemeleri etkin lisansınız sayesinde ücretsizdir, ancak mobil hizmet sağlayıcınız veri aktarımları için sizden ücret talep edebilir.

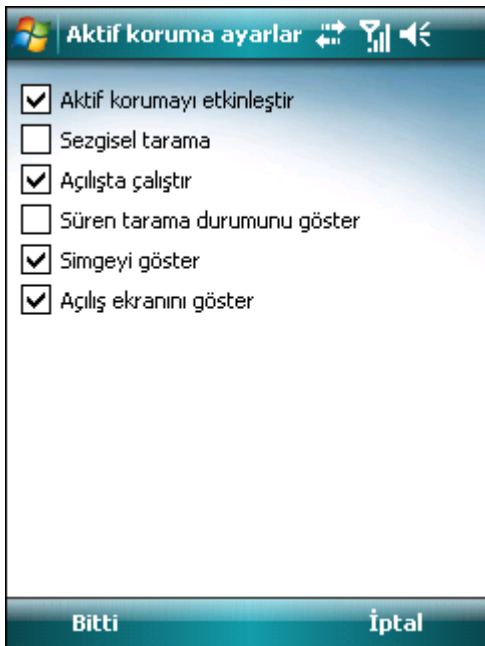
## 4. Aktif koruma

Aktif koruma, etkileşim kurduğunuz dosyaları gerçek zamanlı olarak denetler. Çalıştırılan, açılan ya da kaydedilen dosyalarda otomatik olarak tehdit denetlemesi yapılır. Tarama dosya üzerinde herhangi bir eylem gerçekleştirilmeden önce yapılarak varsayılan ayarlarla maksimum koruma sağlanır. Aktif koruma, sistem başlatıldığında otomatik olarak başlatılır.

### 4.1 Ayarlar

**Menü > Ayarlar > Aktif koruma** yolunu izleyerek aşağıdaki seçenekleri etkinleştirebilir ya da devre dışı bırakabilirsiniz:

- **Aktif korumayı etkinleştir** - etkinleştirilirse, Aktif koruma arka planda çalışır.
- **Sezgisel tarama** - Sezgisel tarama tekniklerini uygulamak için bu seçeneği belirleyin Sezgisel tarama, kodu analiz edip tipik virüs davranışlarını tanıyarak, virüs imza veritabanı tarafından henüz saptanmamış olan yeni kötü amaçlı yazılımları proaktif bir şekilde saptar. Olumsuz yönüyle taramanın tamamlanması için ek zaman gerektirmesidir.
- **Açılıştaki çalıştır** - Seçilirse, aygıtın yeniden başlatılmasından sonra Aktif koruma otomatik olarak başlatılır.
- **Süren tarama durumunu göster** - Bu seçeneği belirleyerek, tarama devam ederken sağ alt köşede tarama durumunu görüntüleyin.
- **Simgeyi göster** - Aktif koruma ayarlarının hızlı erişim simgesini görüntüler (Windows Mobile Başlat ekranının sağ alt köşesinde).
- **Açılış ekranını göster** - bu seçenek aygıtınız başlatılırken gösterilen ESET Mobile Security açılış ekranını kapatmanıza olanak tanır.



Aktif koruma ayarları

## 5. İsteğe bağlı tarayıcı

İsteğe bağlı tarayıcıyı mobil aygıtınızda sızıntı olup olmadığını denetlemek için kullanabilirsiniz. Önceden tanımlanan bazı dosya türleri varsayılan olarak taranır.

### 5.1 Bütün bir aygıt taraması çalıştırma

Bütün bir aygıt taraması bellek, çalışan işlemler, bağımlı dinamik bağlantı kitaplıkları (DLL) ile dahili ve çıkarılabilir depolama alanlarının parçası olan dosyaları denetler.

**Eylem > Tarama > Tüm aygıt** yolunu izleyerek bütün bir aygıt taraması çalıştırabilirsiniz.

**NOT:** Bellek tarama işlemi varsayılan olarak gerçekleştirilmez. Bu işlemi **Menü > Ayarlar > Genel** yolunu izleyerek etkinleştirebilirsiniz.

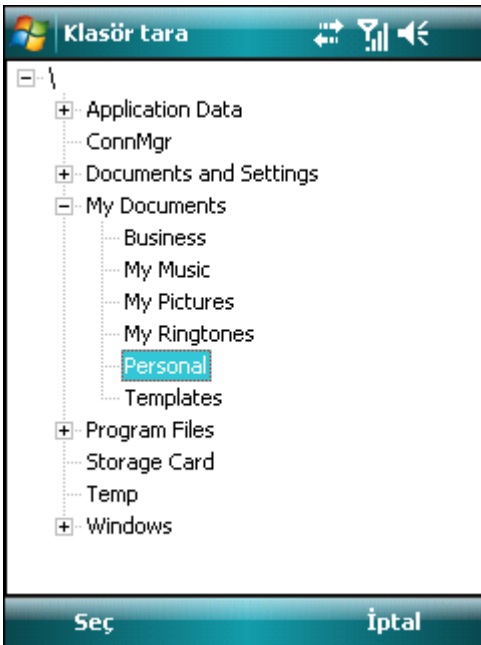
Program önce sistem belleğini tarar (çalışan işlemler ve bağımlı DLL'leri dahil) ve ardından dosyalar ile klasörleri tarar. Her taranan dosyanın tam yol ve dosya adı kısaca gösterilecektir.

**NOT: Eylem > Tarama > Taramayı durdur** yolunu izleyerek devam eden bir taramayı iptal edebilirsiniz.

### 5.2 Bir klasörü tarama

**Eylem > Tarama > Klasör** yolunu izleyerek aygıtınızdaki belirli bir klasörü tarayabilirsiniz.

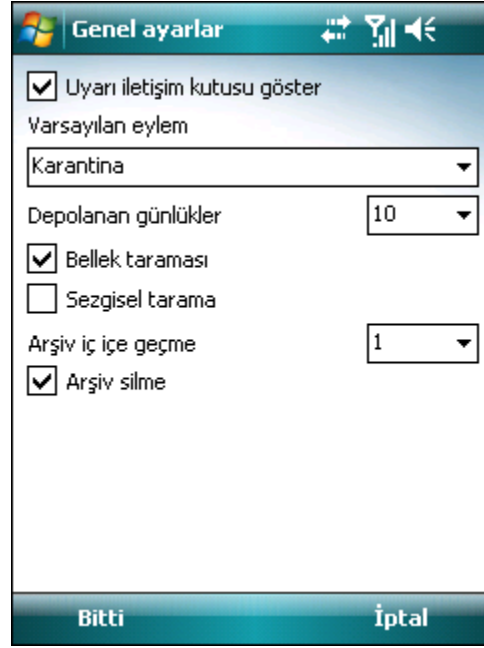
Taramak istediğiniz klasöre ve **Seç**'e dokununuz.



Taranacak klasörü seçme

### 5.3 Genel ayarlar

Tarama parametrelerini **Menü > Ayarlar > Genel** yolunu izleyerek değiştirebilirsiniz.



Genel ayarlar

Tehdit uyarı bildirimlerini görüntülemek için **Uyarı iletişim kutusu göster** seçeneğini belirleyin.

Etkilenen dosyalar algılandığında otomatik olarak gerçekleştirilecek bir varsayılan eylem belirleyebilirsiniz. Aşağıdaki seçeneklerden birini belirleyebilirsiniz:

- Karantina,
- Sil,
- Hiçbir şey yapma (önerilmez).

**Depolanan günlükler** seçeneği, **Menü > Günlükler > Tarama** bölümünde saklanacak maksimum günlük sayısını belirlemenizi sağlar.

**Bellek tarama** etkinse, asıl dosya taramasından önce aygıt belleğinde otomatik olarak kötü amaçlı program taraması yapılacaktır.

**Sezgisel tarama** seçeneği etkinse, ESET Mobile Security sezgisel tarama tekniklerini kullanacaktır. Sezgisel tarama, kodu analiz ederek tipik virüs davranışları arayan algoritma tabanlı bir algılama yöntemidir. Başlıca avantajı, geçerli virüs imza veritabanında henüz tanınmayan kötü amaçlı yazılımları algılayabilme kabiliyetidir. Olumsuz yönü ise taramanın tamamlanması için ek zaman gerektirmesidir.

**Arşiv iç içe geçme** seçeneği, taranacak iç içe geçmiş arşivlerin derinliğini belirlemenize olanak tanır. (Sayı ne kadar yüksekse, tarama da o kadar derin olacaktır.)

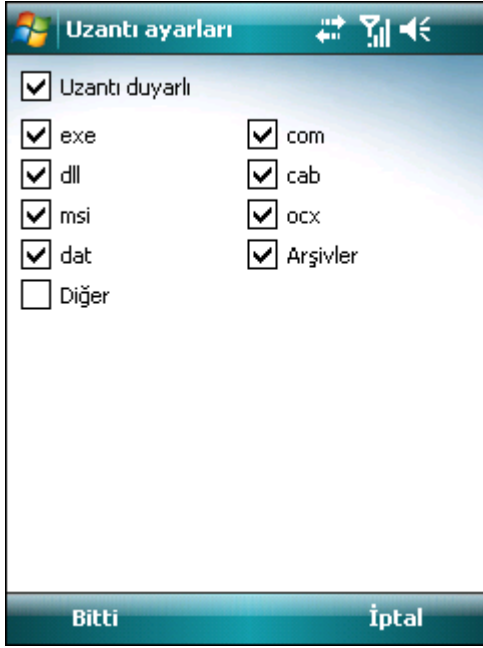
**Arşiv silme** seçeneği etkinse, etkilenen nesnelere içeren arşiv dosyaları (*zip*, *rar* ve *jar*) otomatik olarak silinecektir.

## 5.4 Uzantı ayarları

**Menü > Ayarlar > Uzantılar** yolunu izleyerek mobil aygıtınızda taranacak dosya türlerini belirleyebilirsiniz.

**Uzantılar** penceresi görüntülenecek ve size, sızıntıya maruz kalan en yaygın dosya türlerini gösterecektir. Taramak istediğiniz dosya türlerini seçin ya da taramanın dışında bırakmak istediğiniz uzantıların seçimini kaldırın. **Arşivler** seçeneğini etkinleştirirseniz, tüm desteklenen arşiv dosyaları (*zip, rar ve jar*) taranacaktır.

Tüm dosyaları taramak için **Uzantı duyarlı** onay kutusunun seçimini kaldırın.



Uzantı ayarları

## 6. Tehdit bulundu

Bir tehdit bulunursa, ESET Mobile Security sizden bir eylem gerçekleştirmenizi isteyecektir.



Tehdit uyarısı iletişim kutusu

**SİL** yolunu izlemenizi öneririz. **Karantina** seçeneğini belirlerseniz, dosya özgün konumundan karantina konumuna taşınacaktır. **Yoksay** yolunu izlerseniz, hiçbir eylem gerçekleştirilmeyecektir ve etkilenen dosya mobil aygıtınızda kalacaktır.

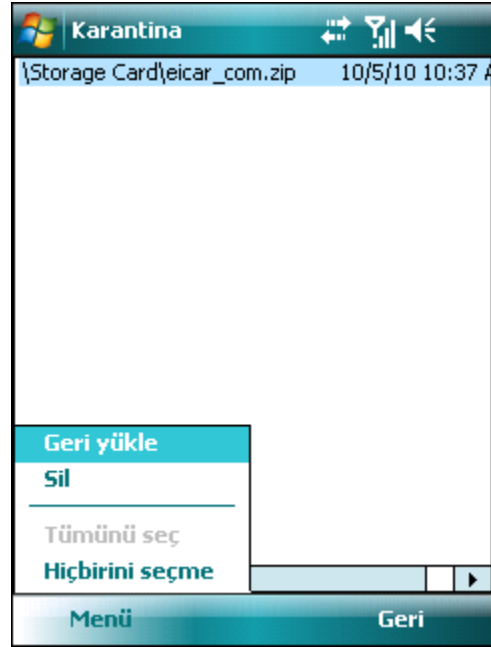
Bir arşivde (örn. .zip dosyasında) bir sızıntı algılanırsa, uyarı penceresinde **Arşivi sil** seçeneği görüntülenir. **SİL** seçeneğiyle birlikte bu seçeneği de belirleyerek arşivlenen tüm dosyaları silebilirsiniz.

**Uyarı iletişim kutusunu göster** seçeneğini devre dışı bırakırsanız, geçerli tarama sırasında uyarı penceresi görüntülenmez (uyarıları sonraki tüm taramalar için devre dışı bırakmak isterseniz bkz. [Genel ayarlar](#) (8)).

### 6.1 Karantina

Karantinanın ana görevi etkilenen dosyaları güvenli bir şekilde saklamaktır. Dosyalar temizlenemiyorsa, silinmeleri güvenli değilse ya da önerilmiyorsa ya da ESET Mobile Security tarafından hatalı bir şekilde algılanıyorsa, karantinaya alınmaları gerekir.

Karantina klasöründe saklanan dosyalar, karantinanın tarihi ile saatini ve etkilenen dosyanın özgün konumunu gösteren bir günlükte görüntülenebilir. Karantinayı **Menü > Görünüm > Karantina** yolunu izleyerek açabilirsiniz.



Karantina Listesi

Karantinaya alınan dosyaları **Menü > Geri yükle** yoluna dokunarak geri yükleyebilirsiniz (her bir dosya özgün konumuna geri yüklenir). Bu dosyaları kalıcı olarak kaldırmak istiyorsanız, **Menü > Sil**'e dokununuz.

## 7. Anti-Theft

Anti-Theft özelliği, mobil telefonunuzu yetkisiz erişimlere karşı korur.

Telefonunuzu kaybeder ya da çaldırırsanız ve çalan kişi SIM kartınızı (güvenilmeyen) bir yenisiyle değiştirirse, kullanıcı tanımlı bazı telefon numarasına ya da numaralarına gizlice bir Uyarı SMS'i gönderilir. Bu ileti o anda takılı olan SIM kartın telefon numarasını, IMSI (Uluslararası Mobil Abone Kimliği) numarasını ve telefonun IMEI (Uluslararası Mobil Donanım Kimliği) numarasını içerir. İleti Gönderilen klasöründen otomatik olarak silineceğinden yetkisiz kullanıcı iletinin gönderildiğini fark etmez.

Aygıtınızda kayıtlı tüm verileri (kişiler, iletiler, uygulamalar) ve o anda takılı olan çıkarılabilir medyayı silmek için, yetkisiz kullanıcının mobil numarasına aşağıdaki biçimde bir Uzaktan silme SMS'i gönderebilirsiniz:

#RC# DS parola

Burada *parola*, **Menü > Ayarlar > Parola** yolunu izleyerek ayarladığınız kendi parolanızdır.

### 7.1 Ayarlar

Öncelikle **Menü > Ayarlar > Parola** yolunu izleyerek parolanızı ayarlayın. Bu parola aşağıdakiler için gereklidir:

- aygıtınıza Uzaktan silme SMS'i göndermek,
- aygıtınızdaki Anti-Theft ayarlarına erişmek,
- aygıtınızdan ESET Mobile Security yazılımını kaldırmak.

Yeni bir parola ayarlamak için, parolanızı **Yeni parola** ve **Parolayı yeniden yazın** alanlarına yazın. **Anımsatıcı** seçeneği (ayarlıysa) parolanızı anımsamadığınız takdirde bir ipucu görüntüler.

Var olan parolayı değiştirmek için, önce **Geçerli parolayı girin** ve ardından yeni parolayı girin.

**ÖNEMLİ:** Aygıtınızdan ESET Mobile Security yazılımını kaldırırken gerekli olacağı için, lütfen parolanızı dikkatle seçin.

Bir güvenlik parolası ayarlama

Anti-Theft ayarlarına **Menü > Ayarlar > Anti-Theft** yolunu izleyip parolanızı girerek erişebilirsiniz.

Takılan SIM kartın (ve olası Uyarı SMS'i gönderiminin) otomatik denetimini devre dışı bırakmak için **SIM eşleştirmesini etkinleştir** seçeneğinin seçimini kaldırın.

Mobil aygıtınızda o anda takılı olan SIM kart güvenilen olarak kaydetmek istediğiniz SIM kartsa, **Geçerli SIM'e güveniliyor** onay kutusunu işaretlediğinizde, Güvenilen SIM listesine (**Trusted SIM** sekmesi) kaydedilir. **SIM diğer adı** metin kutusu otomatik olarak IMSI numarasıyla doldurulur.

Birden fazla SIM kart kullanıyorsanız, **SIM diğer adı** metin kutusunu değiştirerek (örn, *Ofis*, *Ev* vs.) her birini ayırt etmek isteyebilirsiniz.

**Uyarı SMS'i** bölümünde, aygıtınıza güvenilmeyen bir SIM kartı takıldıktan sonra önceden tanımlanmış numaraya/numaralara gönderilecek olan metin iletisini değiştirebilirsiniz.



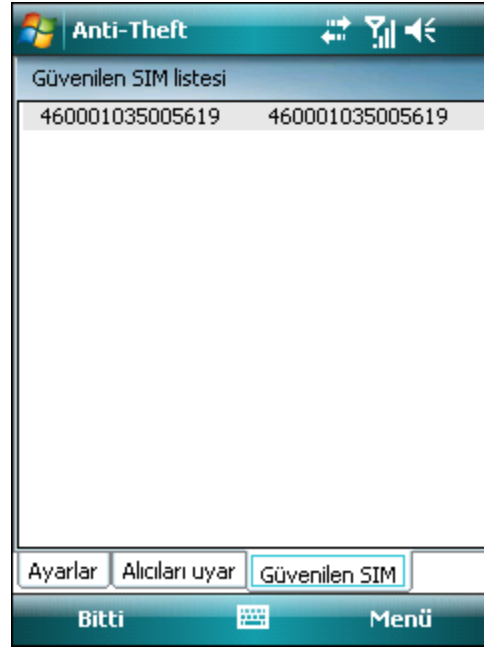
Anti-Theft ayarlar

**Alıcıları uyar** sekmesi, aygıtınıza güvenilmeyen SIM kart takıldıktan sonra Uyarı SMS'i alacak olan önceden tanımlanmış numaraların listesini gösterir. Yeni bir numara eklemek için **Menü > Ekle**'ye dokununuz. **Menü > Kişi ekle** yolunu izleyerek kişi listesinden bir numara ekleyebilirsiniz.

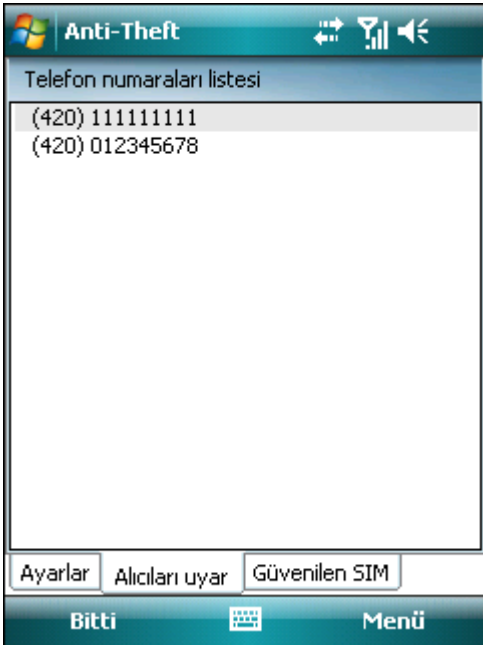
**NOT:** telefon numarasının uluslararası arama kodunun ardından asıl numarayı içermesi gerekir (örn. +1610552000).

**Güvenilen SIM** sekmesi güvenilen SIM kartlarının listesini gösterir. Her giriş, SIM diğer adı (sol sütun) ile IMSI numarasından (sağ sütun) oluşur.

Bir SIM'i listeden çıkarmak için, SIM'i seçin ve **Menü > Kaldır**'a dokununuz.



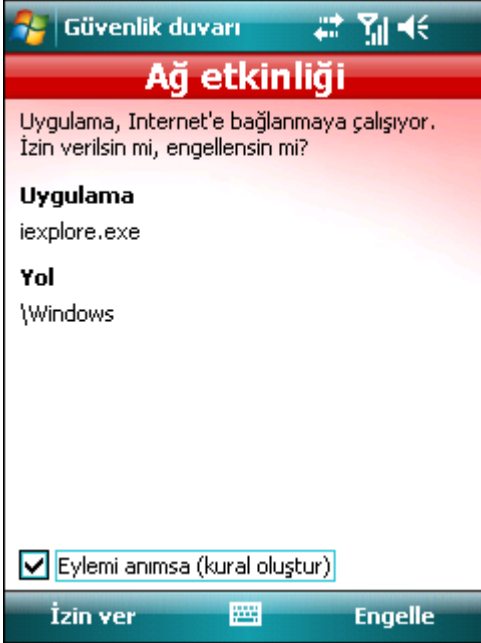
Güvenilen SIM listesi



Önceden tanımlanmış telefon numaraları listesi

## 8. Güvenlik duvarı

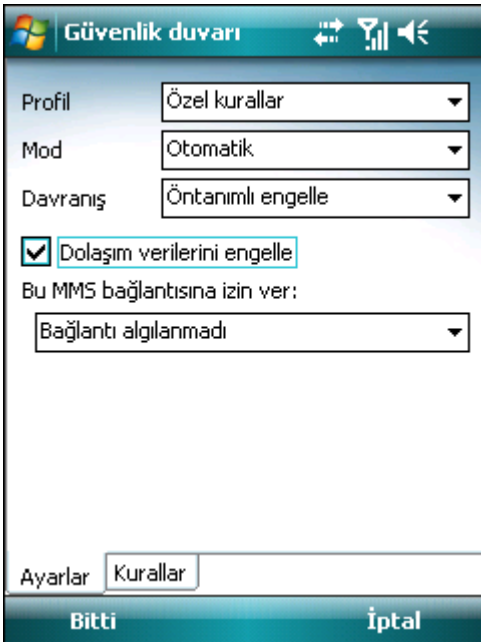
Güvenlik duvarı, filtre kurallarına göre her bir ağ bağlantısına izin vererek ya da bu bağlantıları engelleyerek gelen ve giden tüm ağ trafiğini denetler.



Güvenlik duvarı uyarısı

### 8.1 Ayarlar

Güvenlik duvarı ayarlarını **Menü > Ayarlar > Güvenlik duvarı** yoluna dokunarak değiştirebilirsiniz.



Güvenlik duvarı ayarları

Aşağıdaki profillerden birini seçebilirsiniz:

- **Tümüne izin ver** - tüm ağ trafiğine izin verir,
- **Tümünü engelle** - tüm ağ trafiğini engeller,
- **Özel kurallar** - kendi filtre kurallarınızı tanımlamanızı sağlar.

**Özel kurallar** profilindeyken, iki filtre modundan birini

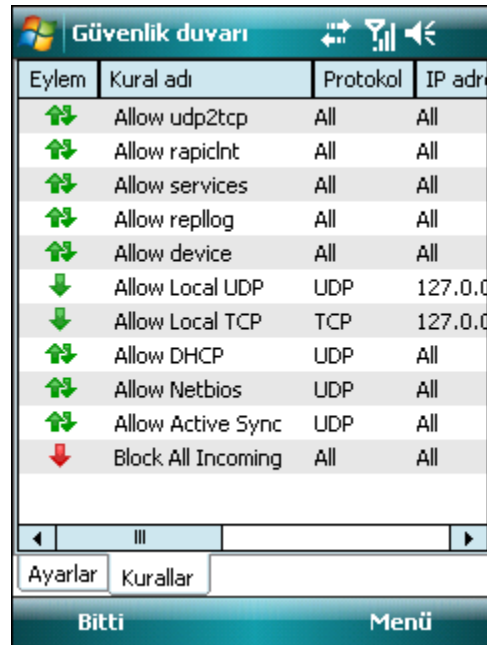
seçebilirsiniz:

- **Otomatik** - kural tanımlamaya gerek duymadan güvenlik duvarını kolay ve rahat bir şekilde kullanmayı tercih eden kullanıcılar için uygundur. Bu mod bütün giden trafiğe izin verir. Gelen trafik için, **Davranış** seçeneğinde varsayılan eylemi ayarlayabilirsiniz (**Öntanımlı izin ver** ya da **Öntanımlı engelle**).
- **Etkileşimli** - kişisel güvenlik duvarınızı özelleştirmenizi sağlar. Karşılık gelen bir kural olmadan bir iletişim algılandığında, bilinmeyen bir bağlantıyı bildiren bir iletişim penceresi görüntülenir. İletişim penceresi, iletişime izin verme ya da iletişimi engelleme ve bir kural oluşturma seçeneği sunar. Bir kural oluşturmayı seçerseniz, kurala göre gelecekteki tüm bu bağlantılara izin verilir ya da gelecekteki tüm bu bağlantılar engellenir. Kuralı olan bir uygulama değiştirilirse, bir iletişim penceresi size bu değişikliği kabul etme ya da reddetme seçeneği sunar. Var olan kural yanıtınıza göre değiştirilir.

**Dolaşım verilerini engelle** - etkinleştirilirse, ESET Mobile Security aygıtınızın bir dolaşım ağına bağlı olup olmadığını otomatik olarak algılar ve hem gelen hem giden verileri engeller. Bu seçenek, Wi-Fi ya da GPRS aracılığıyla alınan verileri engellemez.

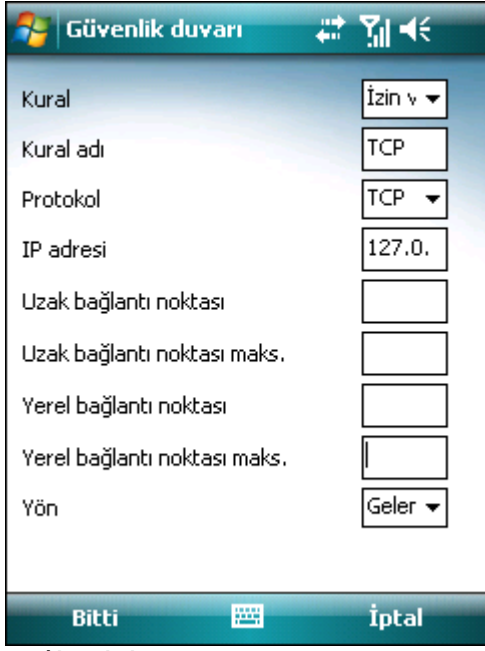
**Bu MMS bağlantısına izin ver:** - bir dolaşım ağına MMS iletilerinin alınması için bir bağlantı seçer. Diğer bağlantılardan gelen MMS iletileri ESET Mobile Security tarafından engellenir.

**Kurallar** sekmesinde, var olan filtre kurallarını düzenleyebilir ya da kaldırabilirsiniz.



Güvenlik duvarı kuralları listesi

Yeni bir kural oluşturmak için **Menü > Ekle** seçeneğine dokunun, tüm gerekli alanları doldurun ve **Bitti** seçeneğine dokunun.



The image shows a screenshot of the Windows Firewall rule creation dialog box. The title bar reads "Güvenlik duvarı" (Firewall). The dialog is divided into two main sections: a configuration area and a bottom action bar. The configuration area contains the following fields and controls:

Kural	İzin v ▾
Kural adı	TCP
Protokol	TCP ▾
IP adresi	127.0.
Uzak bağlantı noktası	
Uzak bağlantı noktası maks.	
Yerel bağlantı noktası	
Yerel bağlantı noktası maks.	
Yön	Geler ▾

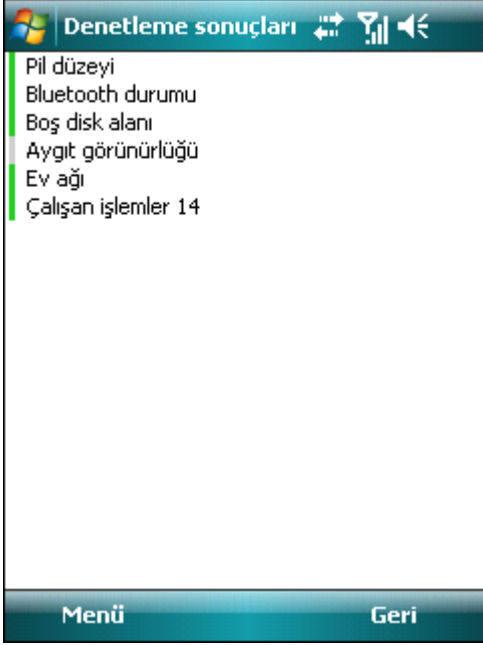
The bottom action bar contains three buttons: "Bitti" (Done), a keyboard icon, and "İptal" (Cancel).

Yeni kural oluşturma

## 9. Güvenlik denetlemesi

Güvenlik denetlemesi telefonun pil düzeyi, bluetooth durumu, boş disk alanı vb. ile ilgili durumunu denetler.

**Eylem > Güvenlik denetlemesi** yolunu izleyerek Güvenlik denetlemesini elle çalıştırabilirsiniz. Ayrıntılı bir rapor görüntülenecektir.

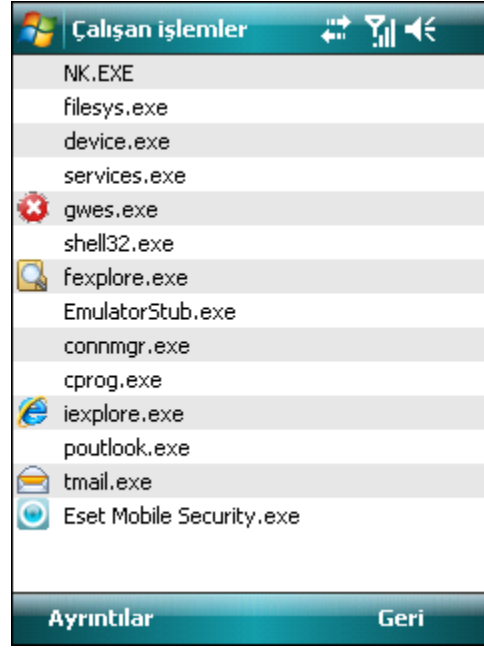


Güvenlik denetlemesi sonuçları

Her öğenin yanındaki yeşil renk, değer eşğin üstünde olduğunu ya da öğenin bir güvenlik riski oluşturmadığını belirtir. Kırmızı renkte değerin eşğin altında olduğu ya da öğenin olası bir güvenlik riski taşıyabileceği anlamına gelir.

**Bluetooth durumu** ya da **Aygıt görünürlüğü** kırmızıyla vurgulanmışsa, öğeyi seçip şu yolu izleyerek durumunu kapatabilirsiniz: **Menü > Düzelt**.

Her bir öğenin ayrıntılarını görmek için öğeyi seçip şu yolu izleyin: **Menü > Ayrıntılar**.



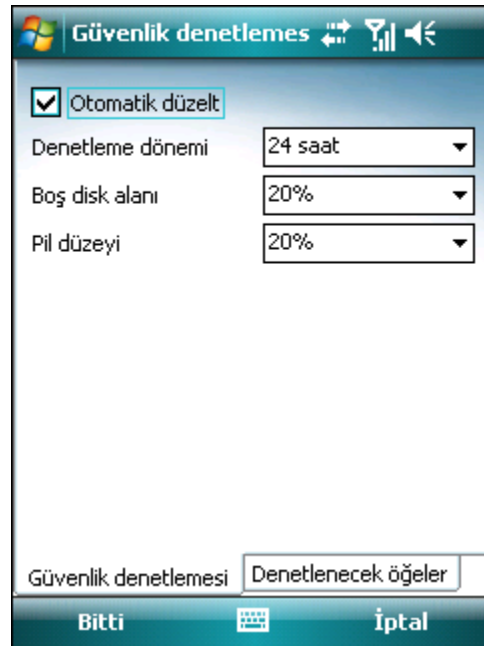
Çalışan işlemler

**Çalışan işlemler** seçeneği, aygıtınızda çalışan tüm işlemlerin listesini gösterir.

İşlem ayrıntılarını (işlemin tam yol adı ve bellek kullanımını) işlemi seçip **Ayrıntılar**'a dokunarak görebilirsiniz.

### 9.1 Ayarlar

Güvenlik denetlemesi parametrelerini **Menü > Ayarlar > Güvenlik denetlemesi** yoluna dokunarak değiştirebilirsiniz.



Güvenlik denetlemesi ayarları

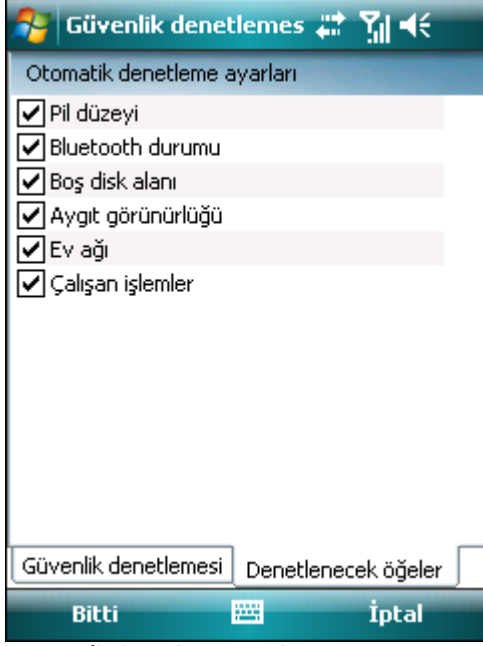
**Otomatik düzelt** seçeneği etkinse, ESET Mobile Security risk altındaki öğeleri (örn. Bluetooth durumu, aygıt görünürlüğü) kullanıcının müdahalesi olmadan, otomatik olarak düzeltmeye çalışır. Bu ayar yalnızca

otomatik (zamanlanmış) denetleme için geçerlidir.

**Denetleme dönemi** seçeneği otomatik denetlemenin ne sıklıkta yapılacağını seçmenizi sağlar. Otomatik denetlemeyi devre dışı bırakmak istiyorsanız, **Hiçbir zaman**'ı seçin.

**Boş disk alanı** ve **Pil düzeyi** öğelerinin düşük olarak değerlendirileceği eşik değerini ayarlayabilirsiniz.

**Denetlenecek öğeler** sekmesinde, otomatik (zamanlanmış) güvenlik denetlemesi sırasında denetlenecek öğeleri seçebilirsiniz.



Otomatik denetleme ayarları

## 10. Antispam

Antispam modülü, mobil aygıtınıza gönderilmiş istenmeyen SMS ve MMS iletilerini engeller.

İstenmeyen iletiler genellikle mobil telefon hizmet sağlayıcılarının reklamlarını ya da bilinmeyen veya belirtilmemiş kullanıcıların iletilerini içerir.

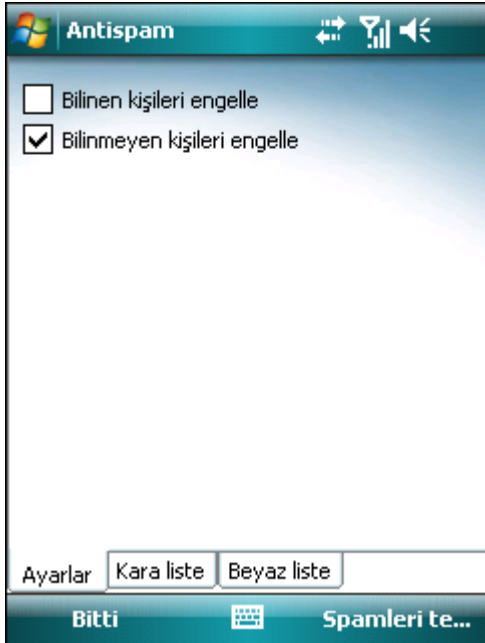
### 10.1 Ayarlar

Alınan ve engellenen iletiler hakkındaki istatistiksel bilgileri **Menü > Görünüm > İstatistikler** yolunu izleyerek görebilirsiniz.

Antispam ayarlarında (**Menü > Ayarlar > Antispam**), aşağıdaki filtre modları kullanılabilir:

- **Bilinmeyen kişileri engelle** - Bu seçeneği etkinleştirerek sadece adres defterinizdeki kişilerden ileti kabul edin.
- **Bilinen kişileri engelle** - Bu seçeneği etkinleştirerek sadece adres defterinizde bulunmayan kişilerden ileti alın.
- Bütün gelen iletileri otomatik olarak engellemek için hem **Bilinmeyen kişileri engelle** hem de **Bilinen kişileri engelle** seçeneklerini etkinleştirin.
- Antispam modülünü kapatmak için hem **Bilinmeyen kişileri engelle** hem de **Bilinen kişileri engelle** seçeneklerini devre dışı bırakın. Bu durumda tüm gelen iletiler kabul edilecektir.

**NOT:** Beyaz liste ve Kara liste girişleri bu seçenekleri geçersiz kılar ([Beyaz Liste / Kara Liste](#) bölümüne bakın).

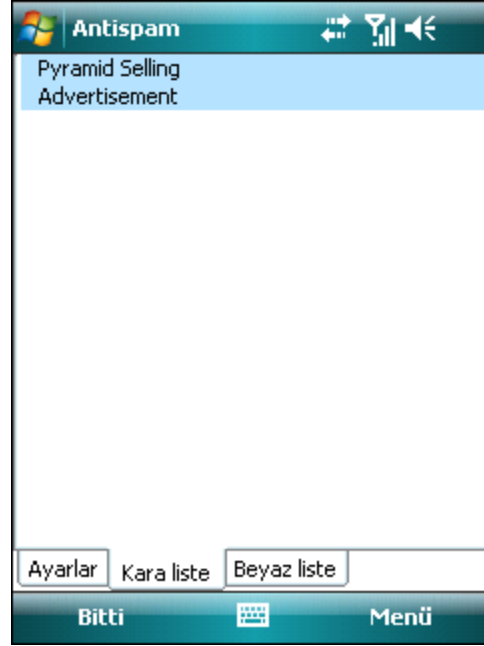


Antispam ayarları

### 10.2 Beyaz Liste / Kara Liste

**Kara liste**, tüm iletileri engellenen telefon numaralarını içeren bir listedir. Bu listede yer alan girişler Antispam ayarlarındaki (**Ayarlar** sekmesi) tüm seçenekleri geçersiz kılar.

**Beyaz liste**, tüm iletileri kabul edilen telefon numaralarını içeren bir listedir. Bu listede yer alan girişler Antispam ayarlarındaki (**Ayarlar** sekmesi) tüm seçenekleri geçersiz kılar.



Kara liste

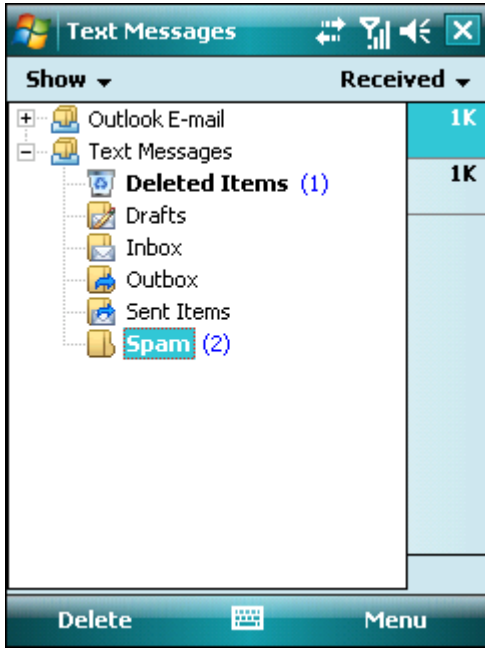
Beyaz liste'ye ya da Kara liste'ye yeni bir numara eklemek için, değişiklik yapmak istediğiniz listenin sekmesini seçip **Menü > Ekle** seçeneğine dokununuz. **Menü > Kişi ekle** yolunu izleyerek kişi listesinden bir numara ekleyebilirsiniz.

**Uyarı:** Kara listeye bir numara/kişi eklenmesi bu gönderenden gelen iletileri otomatik olarak ve sessizce **Spam** klasörüne taşır.

### 10.3 Spam iletilerini bulma

**Spam** klasörü, Antispam ayarlarına göre spam olarak sınıflandırılan engellenmiş iletileri saklamak için kullanılır. İlk spam iletileri alındığında klasör otomatik olarak oluşturulur. **Spam** klasörünü bulup engellenmiş iletileri gözden geçirmek için aşağıdaki adımları izleyin:

1. Aygıtınızın iletiler için kullandığı programı açın (örn. **Başlat** menüsünden **İletiler**),
2. **Metin İletileri** (ya da MMS İstenmeyen İletiler klasörünü bulmak istiyorsanız **MMS**) seçeneğine dokununuz,
3. **Menü > Git > Klasörler ...** yolunu izleyin (ya da akıllı telefonlarda **Menü > Klasörler**'e dokununuz),
4. **Spam** klasörünü seçin.

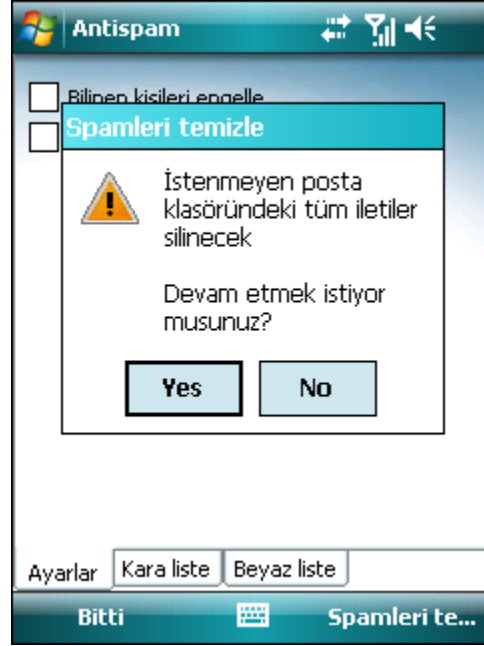


Spam klasörü

### 10.4 Spam iletilerini silme

Spam iletilerini mobil aygıtınızdan silmek için aşağıdaki adımları izleyin:

1. ESET Mobile Security ana penceresinden **Menü > Ayarlar > Antispam** yolunu izleyin,
2. **Spamleri temizle** seçeneğine dokununuz,
3. **Evet** seçeneğine dokunarak tüm spam iletilerinin silinmesini onaylayın.



Spam iletilerini silme

## 11. Uzaktan yönetim

ESET Remote Administrator (ERA), bir ağ ortamında doğrudan merkezi bir konumdan ESET Mobile Security uygulamasını yönetmenize olanak verir. ERA Server üzerinden aygıtınızı tarayabilir, güncelleme yükleyebilir, günlük dosyalarını denetleyebilir ve benzeri eylemi gerçekleştirebilirsiniz. ESET Mobile Security Kurumsal Sürüm, ESET Remote Administrator 4 ile uyumludur.

### 11.1 Ayarlar

Uzaktan yönetim ayarlarına **Menü > Ayarlar > Uzaktan yönetim** yolunu izleyerek erişebilirsiniz.

Uzaktan yönetim ayarları

**Uzak sunucu ve bağlantı noktası** alanına uzak sunucu adını girin. Bağlantı noktası alanı, ağ bağlantısı için kullanılan önceden tanımlanmış bir sunucu bağlantı noktası içerir. Varsayılan 2222 bağlantı noktası ayarını değiştirmemeniz önerilir.

ESET Remote Administrator parola kimlik doğrulaması gerektiriyorsa, **ERA Sunucusu parola gerektiriyor** seçeneğini işaretleyin ve **Parola** alanına parolayı girin.

**Bağlantı aralığı** seçeneği, ESET Mobile Security uygulamasının veri göndermek üzere ne sıklıkta ERA Server hedefine bağlanacağını belirtmenize olanak verir. Minimum bağlantı aralığı 1 saattir. ERA Server hedefine hemen bağlanmak isterseniz, ana ESET Mobile Security penceresinden **Eylem > ERA'ya bağlan** seçeneğine dokununuz.

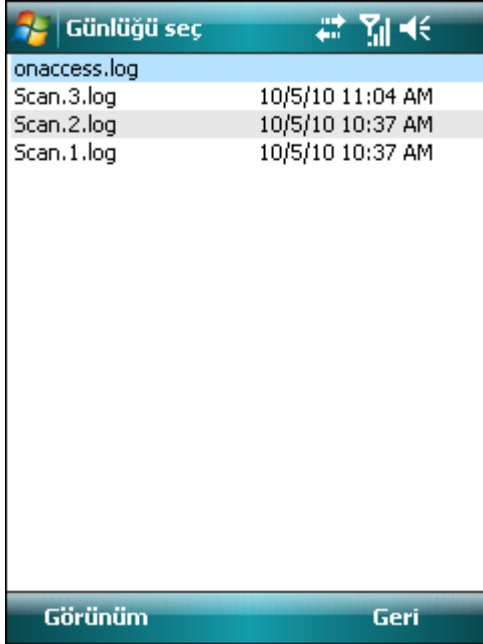
**NOT:** ESET Remote Administrator ile ağınızı nasıl yöneteceğinizi konusunda daha fazla yardım için, lütfen [ESET Uzaktan Yönetim Yükleme El Kitabı ve Kullanıcı Kılavuzu](#)'na bakınız.

## 12. Günlükleri ve istatistikleri görüntüleme

**Tarama günlüğü** bölümü (**Menü > Günlükler > Tarama**), tamamlanan tarama görevleri hakkında kapsamlı veri sağlayan günlükler içerir. Günlükler her başarılı işteğe bağlı tarama sonrasında ya da Aktif koruma tarafından bir sızıntı algılandığında oluşturulur. Tüm etkilenen dosyalar kırmızıyla vurgulanır. Her günlük girişinin sonunda dosyanın günlüğe eklenmesinin nedeni açıklanır.

**Tarama** günlükleri aşağıdaki öğeleri içerir:

- günlük dosyası adı (genellikle *Scan.Number.log* şeklinde),
- olayın tarihi ve saati,
- taranan dosyaların listesi,
- tarama sırasında gerçekleştirilen eylemler ya da karşılaşılan hatalar.



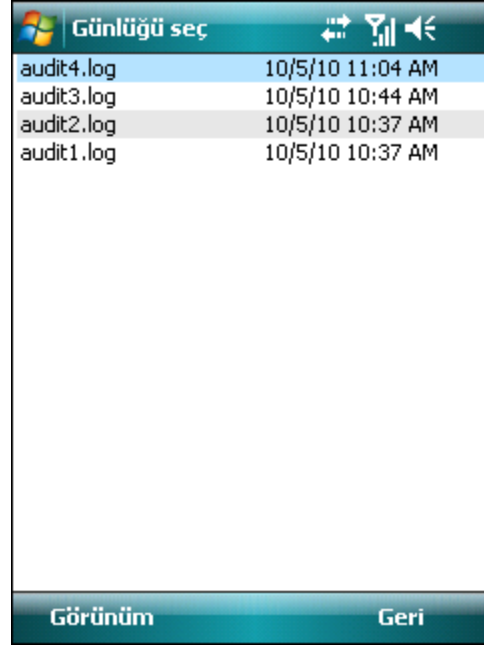
Günlüğü seç	
onaccess.log	
Scan.3.log	10/5/10 11:04 AM
Scan.2.log	10/5/10 10:37 AM
Scan.1.log	10/5/10 10:37 AM

Tarama günlüğü

**Güvenlik denetlemesi günlüğü** bölümü (**Menü > Günlükler > Güvenlik denetlemesi**) hem otomatik (zamanlanmış) hem de elle başlatılan denetlemelerin tüm güvenlik denetlemesi sonuçlarını depolar.

**Güvenlik denetlemesi** günlükleri aşağıdakileri içerir:

- günlük dosyası adı (*auditNumber.log* şeklinde),
- denetlemenin tarihi ve saati,
- ayrıntılı sonuçlar.



Günlüğü seç	
audit4.log	10/5/10 11:04 AM
audit3.log	10/5/10 10:44 AM
audit2.log	10/5/10 10:37 AM
audit1.log	10/5/10 10:37 AM

Güvenlik denetlemesi günlüğü

**Güvenlik duvarı günlüğü** (**Menü > Günlükler > Güvenlik duvarı**) ESET Mobile Security tarafından engellenen tüm güvenlik duvarı olayları hakkında bilgi içerir. Günlük, güvenlik duvarıyla gerçekleştirilen her iletişimden sonra güncellenir. Yeni olaylar günlüğün en üstünde görünür.

**Güvenlik duvarı günlüğü** aşağıdakileri içerir:

- olayın tarihi ve saati,
- kullanılan kuralın adı,
- gerçekleştirilen eylem (kural ayarlarına bağlı olarak),
- kaynak IP adresi,
- hedef IP adresi,
- kullanılan protokol.



Güvenlik duvarı günlüğü	
Tarih ve saat	05/10/2010 11:55:37
Kural adı	Blokavat All Incoming
Eylem	Paket bırakma
Kaynak IP	10.1.108.49
Hedef IP	255.255.255.255
Protokol	UDP
Tarih ve saat	05/10/2010 11:55:33
Kural adı	Blokavat All Incoming
Eylem	Paket bırakma
Kaynak IP	10.1.108.55
Hedef IP	10.1.108.255
Protokol	UDP
Tarih ve saat	05/10/2010 11:55:33
Kural adı	Blokavat All Incoming
Eylem	Paket bırakma
Kaynak IP	10.1.108.55
Hedef IP	255.255.255.255

Güvenlik duvarı günlüğü

**İstatistikler** ekranı (**Menü > Görünüm > İstatistikler**) aşağıdakilerin özetini görüntüler:

- Aktif korumanın taradığı dosyalar,



## 13. Sorun giderme ve destek

### 13.1 Sorun giderme

Bu bölüm ESET Mobile Security ile ilgili yaygın sorunlara çözümler sunar.

#### 13.1.1 Başarısız yükleme

Yükleme sırasında görüntülenen bir hata iletilisinin en yaygın nedeni, aygıtınıza ESET Mobile Security programının yanlış sürümünün yüklenmiş olmasıdır. Yükleme dosyasını [ESET web sitesinden](http://www.eset.com) yüklerken, lütfen aygıtınız için doğru ürün sürümünü karşıdan yüklediğinizden emin olun.

#### 13.1.2 Güncelleme başarısız oldu

Bu hata iletilisi, programın güncelleme sunucularıyla temasa geçememesi sonucunda, başarısız bir güncelleme girişiminden sonra görüntülenir.

Aşağıdaki çözümleri deneyin:

1. İnternet bağlantınızı kontrol edin - İnternet tarayıcınızda <http://www.eset.com> adresini açarak İnternet'e bağlı olduğunuzu doğrulayın.
2. Programın doğru güncelleme sunucusunu kullandığını doğrulayın. **Menü > Ayarlar > Güncelle** yolunu izlediğinizde, **Güncelleme sunucusu** alanında [updmobile.eset.com](http://updmobile.eset.com) adresini görmelisiniz.

#### 13.1.3 Dosya karşıdan yükleme zaman aşımına uğradı

Güncelleme sırasında İnternet bağlantısı beklenmeyen bir şekilde yavaşladı veya kesildi. Lütfen güncellemeyi daha sonra yeniden çalıştırmayı deneyin.

#### 13.1.4 Güncelleme dosyası eksik

Güncelleme dosyasından (*esetav\_wm.upd*) yeni virüs imza veritabanı yüklemeye çalışıyorsanız, dosyanın ESET Mobile Security yükleme klasöründe (*\Program Files\ESET\ESET Mobile Security*) var olması gerekir.

#### 13.1.5 Veritabanı dosyası bozuk

Virüs veritabanı güncelleme dosyası (*esetav\_wm.upd*) bozuk. Dosyayı değiştirmeniz ve güncellemeyi tekrar çalıştırmanız gerekir.

### 13.2 Teknik destek

ESET Mobile Security ya da herhangi bir ESET güvenlik ürünüyle ilgili idari yardım ya da teknik destek gerektiğinde, Müşteri Hizmetleri uzmanlarımız yardıma hazırdır. Teknik destek sorununuza bir çözüm bulmak için aşağıdaki seçeneklerden birini seçebilirsiniz:

En sık sorulan sorulara yanıtları bulmak için aşağıdaki adresten ESET Knowledgebase'e (ESET Bilgi Bankası) erişin:

<http://kb.eset.com>

Knowledgebase (Bilgi Bankası), kategorilerle ve gelişmiş arama olanağıyla en yaygın sorunları çözeniz için çok sayıda faydalı bilgi içerir.

ESET Müşteri Hizmetleri ile temasa geçmek için aşağıdaki adreste bulunan destek talebini kullanın: <http://www.eset.com/support/contact>