

Kaspersky Mobile Security 9
Microsoft Windows Mobile için

KASPERSKY **lab**

Kullanım Kılavuzu

PROGRAM SÜRÜMÜ: 9.0

Sevgili Kullanıcımız!

Ürünümüzü seçtiğiniz için teşekkür ederiz. Bu belgelerin size çalışmanıza yardımcı olacağını ve bu yazılım ürünüyle ilgili ihtiyacınız olan cevapları sunacağını umuyoruz.

Dikkat! Bu belge Kaspersky Lab ZAO firmasına (burada Kaspersky Lab olarak anılacaktır) aittir; belgenin tüm hakları, Rusya Federasyonu yasaları ve uluslararası anlaşmalar uyarınca saklıdır. Bu belgenin veya parçalarının hukuka aykırı olarak çoğaltılması ve dağıtılması, yürürlükteki yasalar uyarınca hukuki, idari veya adli yaptırıma tabidir.

Herhangi bir belgenin, tercümelemleri de dahil olmak üzere herhangi bir şekilde çoğaltılması ve dağıtımı, sadece Kaspersky Lab Ltd'nin yazılı izniyle mümkündür.

Bu belge ve bu belgeyle ilgili grafik görüntüler, sadece bilgilendirme amacıyla; ticari olmayan ve kişisel amaçlarla kullanılabilir.

Kaspersky Lab ayrıca herhangi bir bildirimde bulunmadan bu belgede değişiklik yapma hakkını saklı tutar. Bu belgenin en son sürümünü <http://www.kaspersky.com/docs> adresindeki Kaspersky Lab web sitesinde bulabilirsiniz.

Kaspersky Lab Ltd. bu belgede kullanılan ve hakları üçüncü kişilere ait olan malzemelerin içeriği, kalitesi, geçerliliği veya doğruluğu ve bu malzemelerin kullanımıyla ilişkili muhtemel zararlar konusunda hiçbir sorumluluk kabul etmemektedir.

Bu belgedeki tescilli markalar ve hizmet ticari markaları ilgili hak sahiplerinin mülkiyetindedir.

Değişiklik tarihi: 20.01.2011

© 1997-2011 Kaspersky Lab ZAO. Tüm Hakları Saklıdır.

<http://www.kaspersky.com.tr/>
<http://support.kaspersky.com>

KASPERSKY LAB SON KULLANICI LİSANS ANLAŞMASI

TÜM KULLANICILAR İÇİN ÖNEMLİ YASAL BİLDİRİM: YAZILIMI KULLANMAYA BAŞLAMADAN ÖNCE AŞAĞIDAKİ YASAL ANLAŞMAYI DİKKATLİCE OKUYUNUZ.

LİSANS ANLAŞMASI PENCERESİNDEKİ KABUL TUŞUNU TIKLADIĞINIZDA VEYA KARŞILIK GELEN SİMGEYİ (SİMGELERİ) GİRDİĞİNİZDE, BU ANLAŞMANIN HÜKÜM VE KOŞULLARINI KABUL ETMİŞ SAYILIRSINIZ. **BU İŞLEM İMZANIZIN YERİNE GEÇER VE BU ANLAŞMANIN BİR TARAFI OLARAK SİZİN İÇİN BAĞLAYICI OLDUĞUNU VE BU ANLAŞMANIN TARAFINIZDAN İMZALANMIŞ HERHANGİ BİR YAZILI ANLAŞMA GİBİ UYGULANABİLİR OLDUĞUNU KABUL EDERSİNİZ.** BU ANLAŞMANIN BÜTÜN HÜKÜM VE KOŞULLARINI KABUL ETMİYORSANIZ, YAZILIMIN KURULUMUNU İPTAL EDİN VE YAZILIMI KURMAYIN.

LİSANS ANLAŞMASI PENCERESİNDEKİ KABUL TUŞUNU TIKLADIĞINIZDA VEYA KARŞILIK GELEN SİMGEYİ (SİMGELERİ) GİRDİĞİNİZDE, YAZILIMI BU ANLAŞMANIN HÜKÜM VE KOŞULLARINA UYGUN OLARAK KULLANMA HAKKINA SAHİP OLURSUNUZ.

1. Tanımlar

- 1.1. **Yazılım**, Güncellemeler ve ilgili materyalleri içeren yazılım anlamındadır.
- 1.2. **Hak Sahibi** (Yazılımla ilgili münhasır veya diğer tüm hakların sahibi) Rusya Federasyonu kanunlarına göre kurulmuş bir şirket olan Kaspersky Lab ZAO anlamındadır.
- 1.3. **Bilgisayar(lar)** kişisel bilgisayarlar, dizüstü bilgisayarlar, iş istasyonları, kişisel dijital yardımcılar, "akıllı telefonlar", elde taşınan cihazlar veya Yazılımın bunlara yönelik tasarlandığı diğer elektronik cihazlar gibi Yazılımın kurulacağı ve/veya kullanılacağı donanım(lar) anlamındadır.
- 1.4. **Son Kullanıcı (Siz/Sizin)** kendi adına Yazılımı kuran veya kullanan ya da Yazılımın bir kopyasını yasal olarak kullanan ya da Yazılım bir kuruluş adına yükleniyor veya kuruluyorsa işveren gibi kişi(ler) anlamındadır, "Siz" ayrıca Yazılımın yüklendiği veya kurulduğu kuruluş anlamına gelir ve kuruluş bu anlaşmayı kabul eden kişiye bu işlem için yetki verdiğini beyan eder. Bu belge bağlamında, "kuruluş", terimi her türlü ortaklık, sınırlı sorumlu şirket, anonim şirket, birlik, işletme, tröst, ortak girişim, işçi örgütü, şirket halinde kurulmamış örgüt veya resmi kurumları içerir.
- 1.5. **Ortak(lar)** Hak Sahibi ile yapılan bir anlaşma ve lisansa dayanarak Yazılımın dağıtımını gerçekleştiren kuruluşlar veya kişi(ler) anlamındadır.
- 1.6. **Güncelleme(ler)** her türlü yükseltme, revizyon, her türlü yükseltme, revizyon, tadilat, kopya veya bakım paketleri, vb. anlamındadır.
- 1.7. **Kullanım Kılavuzu**, kullanım kılavuzu, yönetici kılavuzu, başvuru kitabı ve ilgili açıklayıcı veya diğer nitelikte materyaller anlamındadır.

2. Lisansın Verilmesi

- 2.1. Hak Sahibi, Yazılımın yüklendiği Bilgisayarınızın Kullanım Kılavuzunda açıklanan tehditlerden korunmasında yardımcı olmak amacıyla Yazılımın belirli sayıda Bilgisayarda Kullanım Kılavuzunda açıklanan tüm teknik gerekliliklere ve bu Anlaşmanın hüküm ve koşullarına uygun olarak depolanması, yüklenmesi, kurulması, yürütülmesi ve gösterilmesi ("kullanım") için münhasır olmayan bir lisansı ("Lisans") Size verir ve Siz de bu Lisansı kabul edersiniz:
Deneme Sürümü. Yazılımın deneme sürümünü aldıysanız, karşıdan yüklediyseniz ve/veya kurduysanız ve Yazılım için değerlendirme lisansı aldıysanız, Yazılımı sadece değerlendirme amacıyla ve aksi belirtilmedikçe ilk kurulum tarihinden itibaren sadece tek bir değerlendirme dönemi boyunca kullanabilirsiniz. Yazılımın başka amaçlarla veya geçerli değerlendirme döneminin bitmesinden sonra kullanılması kesinlikle yasaktır.
Çoklu Ortam Yazılımı; Çoklu Dil Yazılımı; Çift Araçlı Yazılım; Çoklu Kopyalar; Paketler. Yazılımın farklı sürümlerini veya farklı dildeki baskılarını kullanıyorsanız, Yazılımı çoklu araçlarda alırsanız, başka şekilde Yazılımın birden fazla kopyasını alırsanız veya Yazılımı başka yazılımlarla paket halinde aldıysanız, Yazılımın tüm sürümlerinin kurulduğu izin verilen toplam Bilgisayar sayısı Hak Sahibinden aldığınız lisanslarda belirtilen bilgisayar sayısı ile aynı olmalıdır *ancak* lisans hükümlerinde aksi belirtilmedikçe, edinilen her lisans Yazılımı Madde 2.2 ve 2.3'te belirtilen sayıda Bilgisayara kurma ve kullanma hakkını kazandırır.
- 2.2. Yazılım fiziksel bir ortam üzerinde edinilmişse, Yazılımı, Yazılım paketinde veya ek anlaşmada belirtilen sayıda Bilgisayarın korunması amacıyla kullanma hakkınız vardır.
- 2.3. Yazılım İnternet üzerinden edinilmişse, Yazılımı, Yazılım için Lisansı edindiğinizde belirtilen veya ek anlaşmada belirtilen sayıda Bilgisayarın korunması amacıyla kullanma hakkınız vardır.
- 2.4. Yazılımın, sadece yedekleme amacıyla ve yasal olarak sahip olunan kopyanın kaybolması, bozulması veya kullanılamaz olması halinde bunun yerine kullanmak amacıyla bir kopyasını alma hakkınız vardır. Bu yedek kopya başka amaçlarla kullanılamaz ve Yazılımı kullanma hakkınız sona erdiğinde veya lisansınızın süresi dolduğunda veya ikamet ettiğiniz ülkede ya da Yazılımı kullanmakta olduğunuz ülkede geçerli mevzuata göre başka herhangi bir nedenle feshedildiğinde imha edilmelidir.
- 2.5. Yazılımın etkin hale getirildiği andan itibaren veya lisans anahtarı dosyası kurulumundan sonra (Yazılımın deneme sürümü hariç olmak üzere) Yazılım paketinde belirtilen (Yazılım bir fiziksel ortamda edinilmişse) veya

edinme sırasında belirtilen (Yazılım İnternet üzerinden edinilmişse) belirli bir süre boyunca aşağıdaki hizmetleri alma hakkınız vardır:

- Hak Sahibi web sitesinde yayınladığında veya başka çevrimiçi servisler yoluyla İnternet üzerinden Yazılım Güncellemeleri. Yaptığınız her türlü Güncelleme bu Yazılımın bir parçası haline gelir ve bu Anlaşmanın hüküm ve koşulları aynen geçerlidir;
- İnternet üzerinden Teknik Destek ve Teknik Destek telefon yardım hattı.

3. Etkinleştirme ve Süre

- 3.1. Bilgisayarınızda değişiklik yaparsanız veya Bilgisayarınızda kurulu başka yazılımlarda değişiklik yaparsanız, Hak Sahibi tarafından Yazılımı tekrar etkinleştirmeniz veya lisans anahtarı dosyası kurulmasını yinelemeniz talep edilebilir. Hak Sahibi, Bilgisayarınızda kurulu ve/veya Bilgisayarınızda kullanılan Yazılım Lisansının geçerliliğini ve/veya Yazılım kopyasının yasallığını doğrulamak için her türlü aracı ve doğrulama prosedürünü kullanma hakkını saklı tutar.
- 3.2. Yazılım bir fiziksel ortamda edinilmişse, bu Anlaşmayı kabul ettiğiniz andan itibaren başlamak üzere paketin üzerinde belirtilen veya ek anlaşmada belirtilen süre boyunca kullanılabilir.
- 3.3. Yazılım İnternet üzerinden edinilmişse, bu Anlaşmayı kabul ettiğiniz andan itibaren edinme sırasında belirtilen veya ek anlaşmada belirtilen süre boyunca kullanılabilir.
- 3.4. Bu Anlaşmaya göre Yazılımın etkinleştirme zamanından itibaren tek bir değerlendirme süresi (7 gün) boyunca Yazılım deneme sürümünü ücretsiz olarak Madde 2.1'de öngörülen koşullar çerçevesinde kullanma hakkınız vardır, *ancak* deneme sürümü boyunca Güncelleme ve İnternet üzerinden Teknik Destek ile Teknik destek telefon yardım hattı yoluyla yardım alamazsınız. Hak Sahibi tek bir değerlendirme süresi için başka bir süre belirlerse bildirim yoluyla Bilgilendirileceksiniz.
- 3.5. Yazılımı Kullanma Lisansınız Madde 3.2 veya 3.3'te (duruma göre) belirtilen süre ile sınırlıdır ve kalan süre Kullanım Kılavuzunda açıklanan yollarla görülebilir.
- 3.6. Yazılımı birden fazla bilgisayarda kullanmak üzere edindiyseniz, Yazılımı Kullanma Lisansınızın süresi, Yazılımın etkinleştirildiği tarihten veya lisans anahtarı dosyası kurulmasının ilk bilgisayarda yapıldığı tarihten başlayarak hesaplanır.
- 3.7. Hak Sahibinin hukuken veya hakkaniyet esasına göre sahip olabileceği diğer çözüm yolları saklı kalmak üzere, bu Anlaşmanın herhangi bir hükmü ve koşulunu ihlal etmeniz halinde, Hak Sahibi satın alma fiyatını veya bunun herhangi bir bölümünü iade etmeksizin Yazılımı kullanma Lisansını ihbarsız olarak herhangi bir zamanda feshetme hakkına sahiptir.
- 3.8. Yazılımı kullanırken veya bu Yazılımı kullanma sonucunda ortaya çıkabilecek herhangi bir rapor veya bilgiyi kullanırken, kişisel gizlilik, telif hakkı, ihracat denetimi ve müstehcenlik kanunu dâhil olmak üzere bütün geçerli uluslararası, ulusal, eyalet, bölgesel ve yerel kanun ve düzenlemelere uyacağınızı kabul edersiniz.
- 3.9. Burada aksi özellikle belirtilmediği sürece, bu Anlaşma kapsamında size verilen hakları veya bu Anlaşma kapsamındaki yükümlülüklerinizi devir veya ferağ edemezsiniz.
- 3.10. Yazılımı, Yazılımın Hak Sahibi veya Ortaklarından edinildiği bir bölgenin dil yerelleştirmesi için geçerli olan bir aktivasyon kodu ile edindiyseniz, Yazılımı başka bir dil yerelleştirmesi için tasarlanmış olan aktivasyon kodunu kullanarak aktif hale getiremezsiniz.
- 3.11. Belirli bir telekomünikasyon operatörü ile çalışmak için tasarlanmış olan bir Yazılım edindiyseniz, bu Yazılım sadece edinme esnasında belirtilmiş olan operatör ile kullanılabilir.
- 3.12. Madde 3.10 ve 3.11'da belirtilmiş olan kısıtlamaların olması halinde, bu kısıtlamalarla ilgili bilgi paketin üzerinde ve/veya Hak Sahibi ve/veya Ortaklarının web sayfasında bulunmaktadır.

4. Teknik Destek

Bu Anlaşmanın Madde 2.6 hükmünde açıklanan Teknik Destek, Yazılımın en son Güncellemesi yüklendiğinde (Yazılımın deneme sürümü hariç) Size sağlanır.

Teknik destek hizmeti: <http://support.kaspersky.com>

5. Sınırlamalar

- 5.1. Geçerli mevzuat uyarınca Size feragat edilemez bir hak verilen durumlar haricinde, Yazılımı taklit edemez, çoğaltamaz, kiralayamaz, ödünç veremez, kiraya veremez, satamaz, değiştiremez veya tersine mühendislik uygulayamazsınız ya da Yazılımı parçalarına ayıramaz veya buna dayanarak türevsel çalışmalar yaratamazsınız ve geçerli kanun uyarınca böyle bir kısıtlama yasaklanmadığı sürece başka şekilde Yazılımın herhangi bir parçasını insanlarca okunabilir biçime dönüştüremez veya lisanslı Yazılımı veya herhangi bir alt kümesini devredemez ve herhangi bir üçüncü tarafın bunları yapmasına izin veremezsiniz. Yazılımın tescilli ikili kodu veya kaynağı, program algoritmasını yeniden oluşturmak amacıyla kullanılamaz veya bunlara tersine mühendislik uygulanamaz. Burada açıkça verildiği belirtilmeyen bütün haklar Hak Sahibi ve/veya tedarikçileri tarafından saklı tutulur. Yazılımın bu şekilde yetkisiz kullanımı, bu Anlaşmanın ve bu kapsamda verilen Lisansın derhal ve otomatik olarak feshine neden olur ve Size karşı cezai ve/veya hukuki işlemlerin başlatılmasına yol açabilir.

- 5.2. Ek anlaşmada öngörülen haller dışında, Yazılımı kullanma haklarını herhangi bir üçüncü tarafa devredemezsiniz.
- 5.3. Aktivasyon kodu ve/veya lisans şifresi dosyasını üçüncü taraflara veremezsiniz veya üçüncü tarafların Hak Sahibinin gizli verileri olarak kabul edilen aktivasyon kodu ve/veya lisans şifresine erişimine izin veremezsiniz ve aktivasyon kodu ve/veya lisans şifresini gizli biçimde korumak için makul özen ve dikkati göstermelisiniz. İstisna olarak, aktivasyon kodu ve/veya lisans şifresini ek anlaşmada öngörülen üçüncü taraflara devredebilirsiniz.
- 5.4. Yazılımı herhangi bir üçüncü tarafa kiraya veremez, kiralayamaz veya ödünç veremezsiniz.
- 5.5. Yazılımı, Kullanım Kılavuzunda tanımlanan tehditlerin tespiti, engellenmesi veya bunlarla ilgili işlem yapılması için kullanılan veri veya yazılımların oluşturulması amacıyla kullanamazsınız.
- 5.6. Bu Anlaşmanın hüküm ve koşullarından herhangi birini ihlal etmeniz halinde, Hak Sahibi ücretini iade etmeksizin şifre dosyasını bloke etme veya Yazılımı kullanma Lisansınızı sonlandırma hakkına sahiptir.
- 5.7. Yazılımın deneme sürümünü kullanıyorsanız, bu Anlaşmanın Madde 4 hükmünde belirtilen Teknik Desteği alma hakkınız ve Yazılımı kullanma lisansı veya haklarınızı herhangi bir üçüncü tarafa devretme hakkınız yoktur.

6. **Sınırlı Garanti ve Feragat**

- 6.1. Hak Sahibi, Yazılımın büyük oranda Kullanım Kılavuzunda öngörülen özellikler ve açıklamalara göre performans göstereceğini garanti eder, *ancak* bu sınırlı garanti aşağıdaki durumlar için geçerli değildir: (w) Hak Sahibinin garanti sorumluluğundan açıkça feragat ettiği Bilgisayarınızdan kaynaklanan aksaklıklar ve ilgili ihlaller; (x) hatalı kullanım, suiistimal, kaza, ihmal, yanlış kurulum, işletim veya bakım, hırsızlık, vandalizm, doğal afetler, terör olayları, elektrik kesintileri veya dalgalanmaları, zayıf, Hak Sahibi dışındaki herhangi bir tarafça yapılan yetkisiz tadilat, değişiklik ve onarımlar veya başka üçüncü tarafların veya Sizin eylemlerinizi ya da Hak Sahibinin makul kontrolü dışında gelişen sebeplerden kaynaklanan arızalar, kusurlar veya bozukluklar; (y) ilk ortaya çıktığında Sizin tarafınızdan Hak Sahibine mümkün olan en kısa zamanda bildirilmeyen her türlü kusur; ve (z) Bilgisayarınıza kurulan donanım ve/veya yazılım bileşenlerinden kaynaklanan uyumsuzluk.
- 6.2. Hiçbir yazılımın hatasız olmadığını kabul ve beyan ederek, Bilgisayarınızı Sizin için uygun aralıklarla yedeklemeyi kabul edersiniz.
- 6.3. Hak Sahibinin Sizin tarafınızdan yetki verilen veri silme işlemlerinden sorumlu veya yükümlü olmadığını kabul, beyan ve taahhüt edersiniz.
- 6.4. Hak Sahibi, Kullanım Kılavuzunda veya bu Anlaşmada açıklanan koşulların ihlali halinde Yazılımın doğru biçimde çalışacağına dair herhangi bir garanti vermez.
- 6.5. Hak Sahibi, bu Anlaşmanın Madde 2.5 hükmünde belirtilen Güncellemeleri düzenli olarak karşıdan yüklememeniz halinde Yazılımın doğru biçimde çalışacağını garanti etmez.
- 6.6. Hak Sahibi, bu Anlaşmanın Madde 3.2 veya 3.3. hükümlerinde belirtilen dönemin sona ermesinden veya Yazılımı kullanma Lisansının herhangi bir nedenle sonlandırılmasından sonra, Kullanım Kılavuzunda açıklanan tehditlerden koruma sağlanacağını garanti etmez.
- 6.7. YAZILIM "OLDUĞU GİBİ" TEMİN EDİLMİŞTİR VE HAK SAHİBİ YAZILIMIN KULLANIMI VEYA PERFORMANSI İLE İLGİLİ HERHANGİ BİR GARANTİ VEYA TAAHHÜTTE BULUNMAZ. GEÇERLİ KANUN UYARINCA KAPSAM DIŞI BIRAKILAMAYAN VEYA SINIRLANDIRILAMAYAN HERHANGİ BİR GARANTİ, KOŞUL, TAAHHÜT VEYA HÜKÜM HARİCİNDE, HAK SAHİBİ VE ORTAKLARI ÜÇÜNCÜ TARAF HAKLARININ İHLAL EDİLMEMESİ, TİCARETE ELVERİŞLİLİK, TATMINKÂR KALİTE, ENTEGRASYON VEYA BELİRLİ BİR AMACA UYGUNLUK GİBİ KONULARDA AÇIK VEYA ZİMNİ HERHANGİ BİR GARANTİ, KOŞUL, TAAHHÜT VEYA HÜKÜMDE BULUNMAZ (HUKUKEN, ÖRF, ADET VE GELENEKLERE DAYANARAK VEYA BAŞKA ŞEKİLDE). PERFORMANS VE İSTENEN SONUÇLARI ELDE EDECEK YAZILIMI SEÇME SORUMLULUĞU İLE İLGİLİ VE YAZILIMIN KURULUMU, KULLANIMI VE YAZILIMDAN ALINAN SONUÇLARLA İLGİLİ BÜTÜN RİSKİ VE HATALARI ÜSTLENİRSİNİZ YUKARIDAKİ HÜKÜMLERE SINIRLAMA GETİRMEKSİZİN, HAK SAHİBİ YAZILIMIN HATASIZ OLACAĞI VEYA KESİNTİ VE ARIZALARIN OLMAYACAĞI YA DA YAZILIMIN HAK SAHİBİNE BİLDİRİLMİŞ VEYA BİLDİRİLMEMİŞ BÜTÜN ŞARTLARI YERİNE GETİRECEĞİ KONUSUNDA HERHANGİ BİR GARANTİ VERMEZ VE TAAHHÜTTE BULUNMAZ.

7. **Hariç Tutma ve Sorumluluğun Sınırlandırılması**

GEÇERLİ KANUN KAPSAMINDA İZİN VERİLEN AZAMI ÖLÇÜDE, HAK SAHİBİ VEYA ORTAKLARI, SÖZ KONUSU ZARAR OLASILIĞI İLE İLGİLİ KENDİLERİNE ÖNCEDEN HABER VERİLMİŞ OLSA DAHİ, HİÇBİR ŞEKİLDE YAZILIMIN KULLANILMASI VEYA YAZILIMIN KULLANILAMAMASI, DESTEK VE BAŞKA HİZMETLER, BİLGİLER, YAZILIMLAR VEYA YAZILIMLA İLGİLİ İÇERİKLERİN SAĞLANMASI VEYA SAĞLANAMAMASINDAN YA DA BAŞKA ŞEKİLDE YAZILIMIN KULLANIMINDAN KAYNAKLANAN YA DA BAŞKA ŞEKİLDE BU ANLAŞMANIN HERHANGİ BİR HÜKMÜ KAPSAMINDA VEYA BUNUNLA İLGİLİ OLARAK YA DA SÖZLEŞME İHLALİ VEYA HAKSIZ FİİL (İHMAL, YALAN BEYAN, KATI SORUMLULUK, YÜKÜMLÜLÜK VEYA GÖREV DÂHİL) YA DA YASAL GÖREVIN İHLALİ YA DA HAK SAHİBİNİN VEYA ORTAKLARINDAN HERHANGİ BİRİNİN GARANTİSİNİN İHLALİNDEN KAYNAKLANAN ÖZEL, ARIZİ, CEZAI, DOLAYLI VEYA SONUÇTA ORTAYA ÇIKAN ZARARLARDAN DOLAYI SORUMLU TUTULAMAZ (KAR MAHRUMİYETİ, GİZLİ VEYA BAŞKA BİLGİLERİN KAYBEDİLMESİ, İŞLERİN KESİNTİYE UĞRAMASI, KİŞİSEL GİZLİLİK KAYBI, VERİ VEYA PROGRAMLARIN BOZULMASI, ZARAR GÖRMESİ VEYA KAYBOLMASI, YASAL GÖREV, İYİ NİYETLİ GÖREV VEYA MAKUL DİKKAT GÖREVİ GİBİ HERHANGİ BİR GÖREVİ YERİNE GETİREMEME, İHMAL, EKONOMİK ZARAR VE BAŞKA HER TÜRLÜ PARASAL VEYA DİĞER KAYIPLARLA İLGİLİ ZARAR VE TAZMİNATLAR DAHİL).

HAK SAHİBİ VE/VEYA ORTAKLARININ SORUMLU BULUNMASI HALİNDE, HAK SAHİBİ VE/VEYA ORTAKLARININ SORUMLULUĞUNUN YAZILIM MALİYETLERİ İLE SINIRLI OLACAĞINI KABUL EDERSİNİZ. HAK SAHİBİ VE/VEYA ORTAKLARININ YÜKÜMLÜLÜĞÜ HİÇBİR ŞEKİLDE YAZILIM İÇİN HAK SAHİBİ VE/VEYA ORTAKLARINA (DURUMA GÖRE) ÖDENEN ÜCRETLERDEN FAZLA OLAMAZ.

BU ANLAŞMANIN HİÇBİR HÜKMÜ ÖLÜM VEYA YARALANMA İLE İLGİLİ HERHANGİ BİR HAK TALEBİNİ HARIÇ TUTAMAZ VEYA SINIRLANDIRAMAZ. AYRICA BU ANLAŞMADAKİ HERHANGİ BİR FERAGAT, HARIÇ TUTMA VEYA SINIRLANDIRMANIN GEÇERLİ KANUN UYARINCA HARIÇ TUTULAMAMASI VEYA SINIRLANDIRILAMAMASI HALİNDE, SADECE SÖZ KONUSU FERAGAT, HARIÇ TUTMA VEYA SINIRLANDIRMA SİZE UYGULANMAZ FAKAT KALAN BÜTÜN FERAGAT, HARIÇ TUTUMA VE SINIRLANDIRMALAR GEÇERLİ OLMAYA DEVAM EDER.

8. GNU ve Diğer Üçüncü Taraf Lisansları

Yazılım, GNU Genel Kamu Lisansı (GPL) veya kullanıcının belirli programları kopyalaması, değiştirmesi ve yeniden dağıtmasına ve kaynak koda erişmesine izin veren başka benzer ücretsiz yazılım ("Açık Kaynaklı Yazılım") lisansları kapsamında kullanıcıya lisanslanan (veya alt-lisanslanan) bazı yazılım programları içerebilir. Bu lisanslarda, yürütülebilir ikili formatta bir kimseye dağıtılan yazılımlar için kaynak kodun da bu kullanıcılara sağlanması öngörülürse, kaynak kodun temin edilmesi için source@kaspersky.com adresine talep gönderilmelidir veya kaynak kodu Yazılımla birlikte verilir. Açık Kaynaklı Yazılım lisansları, Hak Sahibinin bir Açık Kaynaklı Yazılım programının kullanımı, kopyalanması veya değiştirilmesi ile ilgili olarak bu Anlaşmada verilen haklardan daha geniş kapsamlı haklar vermesini öngörürse, söz konusu haklar burada belirtilen haklar ve kısıtlamalara göre öncelikli olarak geçerlidir.

9. Fikri Mülkiyet Hakları

- 9.1 Yazılım ve Yazılımla birlikte verilen yazılar, sistemler, fikirler, işletim yöntemleri, dokümantasyon ve diğer bilgilerin Hak Sahibi ve/veya ortaklarının özel fikri mülkiyeti ve/veya değerli ticari sırları olduğunu ve Hak Sahibi ve ortaklarının Rusya Federasyonu, Avrupa Birliği ve Amerika Birleşik Devletleri ile diğer ülkelerin medeni hukuku ve ceza hukuku ile telif hakkı, ticari sırlar, ticari marka ve patent kanunları ve uluslararası antlaşmaları yoluyla korunduğunu kabul edersiniz. Bu Anlaşma Size Hak Sahibi ve/veya ortaklarının Ticari Markaları veya Hizmet Markaları ("Ticari Markalar") gibi fikri mülkiyetleri ile ilgili herhangi bir hak vermez. Ticari Markaları kabul görmüş ticari marka uygulamalarına uygun olarak sadece Ticari Marka sahibinin adını belirlemek dâhil olmak üzere Yazılım tarafından üretilen basılı çıktıları tespit etmek için kullanabilirsiniz. Herhangi bir Ticari Markanın bu şekilde kullanılması, size söz konusu Ticari Markanın mülkiyet haklarını vermez. Yazılımla ilgili bütün hak, tasarruf hakkı ve menfaatler Hak Sahibi ve/veya ortaklarına aittir. Hak Sahibi veya başka bir üçüncü tarafça yapılan Yazılımla ilgili hata düzeltmeleri, güçlendirmeler, Güncellemeler veya diğer değişiklikler ile bunlara ilişkin bütün telif hakları, patentler, ticari sır hakları, ticari markalar ve diğer fikri mülkiyet hakları da buna dâhildir. Yazılım elinizde bulunduranız, kurmanız veya kullanmanız Yazılımla ilgili fikri mülkiyet tasarruf haklarının size devredildiği anlamına gelmez ve bu Anlaşmada açıkça belirtilenler dışında Yazılımla ilgili hiçbir hakkınız olmayacaktır. Bu Anlaşma kapsamında yapılan bütün Yazılım kopyaları, Yazılımın üstünde ve içinde görünen aynı mülkiyet bildirimlerini içermelidir. Burada belirtilenler haricinde, bu Anlaşma size Yazılımla ilgili fikri mülkiyet hakları vermez ve bu Anlaşma kapsamında verilen Lisansın (burada tanımlandığı üzere) size sadece bu Anlaşmanın hüküm ve koşulları kapsamında bir sınırlı kullanım hakkı verdiğini kabul ve beyan edersiniz. Hak sahibi, bu Anlaşmada size açıkça verilmeyen bütün hakları saklı tutar.
- 9.2 Yazılımla ilgili kaynak kodu, aktivasyon kodu ve/veya lisans şifresi dosyasının Hak Sahibinin malı olduğunu ve Hak Sahibinin ticari sırları olduğunu kabul edersiniz. Yazılımın kaynak kodunu değiştirmeme, uyarlamama, çevirmeme, tersine mühendislik uygulamama, kaynak koda dönüştürmeme, parçalarına ayırmama veya başka şekilde keşfetmeye çalışmamayı kabul edersiniz.
- 9.3 Yazılımı hiçbir şekilde değiştirmeme veya tahrif etmemeyi kabul edersiniz. Yazılımın kopyaları üzerinde bulunan telif hakkı bildirimleri veya diğer mülkiyet bildirimlerini çıkaramaz veya değiştiremezsiniz.

10. Geçerli Hukuk; Tahkim

Bu Anlaşma, kanunlar ihtilafı kural ve ilkeleri hesaba katılmaksızın Rusya Federasyonu kanunlarına uygun olarak yürütülecek ve yorumlanacaktır. Bu Anlaşma Malların Uluslararası Satışına dair Birleşmiş Milletler Konvansiyonu hükümlerine tabi değildir ve bu hükümlerin uygulanması açıkça hariç tutulmuştur. Bu Anlaşmanın hükümlerinin yorumlanması veya uygulanmasından ya da ihlalinden kaynaklanan herhangi bir ihtilaf, doğrudan görüşme yoluyla çözülememesi halinde, Rusya Federasyonu'nun Moskova şehrinde bulunan Rusya Federasyonu Ticaret ve Sanayi Odası Uluslararası Ticari Tahkim Mahkemesi tarafından nihai çözüme kavuşturulur. Tahkim mahkemesi tarafından verilen her türlü karar, taraflar için nihai ve bağlayıcıdır ve söz konusu tahkim kararı ile ilgili olarak yetkili mahkemeler yoluyla yürütme yapılabilir. Bu 10. Bölüm hükümleri, bir Tarafın tahkim işlemleri öncesinde, sırasında veya sonrasında yetkili bir mahkeme yoluyla hakkını aramasına engel teşkil etmez.

11. Dava Açma Süresi.

Bu Anlaşma kapsamındaki işlemlerden kaynaklanan davalar, şekli ne olursa olsun, taraflarca dava sebebinin ortaya çıkmasından veya ortaya çıktığının tespit edilmesinden itibaren en geç bir (1) yıl içinde açılmalıdır, ancak istisna olarak fikri mülkiyet haklarının ihlali ile ilgili davalar yasal olarak geçerli azami dönem içinde açılabilir.

12. Anlaşmanın Bütünü; Bölünebilirlik; Feragat Yasağı.

Bu Anlaşma, Siz ve Hak Sahibi arasındaki anlaşmanın bütünüdür ve Yazılımla ilgili veya bu Anlaşmanın konusuyla ilgili olarak daha önce düzenlenmiş yazılı ve sözlü bütün anlaşmalar, teklifler, iletişimler veya duyuruları geçersiz kılarak bunların yerine geçer. Bu Anlaşmayı okuduğunuzu, anladığınızı ve koşullarına bağlı kalacağınızı kabul edersiniz. Bu Anlaşmanın herhangi bir hükmü yetkili bir mahkeme tarafından herhangi bir sebeple tamamen veya kısmen geçersiz, yasadışı veya uygulanamaz bulunursa, söz konusu hüküm yasal ve uygulanabilir olacak şekilde daha dar kapsamlı olarak yorumlanacak, Anlaşmanın tamamı bundan etkilenmeyecek ve Anlaşmanın geri kalanının mümkün olduğu ölçüde esas şekil ve içeriğini koruyarak kanunen izin verilen azami çerçevede geçerli ve yürürlükte olmaya devam edecektir. Herhangi bir hüküm veya koşul ile ilgili feragatin geçerli olabilmesi için, yazılı olarak düzenlenmeli ve siz ve Hak Sahibinin yetkili temsilcisi tarafından imzalanmalıdır, ancak şöyle ki bu Anlaşmanın herhangi bir hükmünün ihlali ile ilgili feragat daha önceki, eş zamanlı veya daha sonraki bir ihlalden de feragat edildiği anlamına gelmez. Hak Sahibinin bu Anlaşmanın herhangi bir hükmü veya herhangi bir hakkın katı biçimde uygulanmasında ısrarcı olmaması, söz konusu hüküm veya haktan feragat edildiği şeklinde yorumlanamaz.

13. Hak Sahibi İletişim Bilgileri.

Bu Anlaşma ile ilgili herhangi bir sorunuz varsa veya herhangi bir nedenle Hak Sahibi ile irtibat kurmak isterseniz, lütfen Müşteri Hizmetleri Bölümümüz ile irtibata geçiniz:

Kaspersky Lab ZAO, 10 build.1, 1st Volokolamsky Proezd
Moskova, 123060
Rusya Federasyonu
Tel: +7-495-797-8700
Faks: +7-495-645-7939
E-posta: info@kaspersky.com
Web sitesi: www.kaspersky.com

© 2004-2011 Kaspersky Lab ZAO. Tüm Hakları Saklıdır. Yazılım ve yanında verilen dokümantasyon teklif hakkına tabidir ve telif hakkı kanunları, uluslararası telif hakkı antlaşmaları ve diğer fikri mülkiyet kanunları ve antlaşmaları ile korunmaktadır.

İÇİNDEKİLER

BU KILAVUZ HAKKINDA	12
Bu belgede.....	12
Belge kuralları.....	15
EK VERİ KAYNAKLARI.....	16
Daha fazla araştırma için bilgi.....	16
Satış Departmanı ile iletişim kuma	17
Web forumunda Kaspersky Lab uygulamalarını tartışma	17
Belgelendirme Gelişim Grubu ile İletişim Kuma.....	17
KASPERSKY MOBİLE SECURITY 9	18
Kaspersky Mobile Security 9'daki yenilikler	19
Dağıtım kiti.....	19
Donanım ve yazılım gerekleri	19
KASPERSKY MOBİLE SECURITY 9'UN KURULUMU	20
UYGULAMANIN KALDIRILMASI	20
UYGULAMAYI GÜNCELLEME	22
BAŞLARKEN.....	24
Uygulamayı etkinleştirme.....	24
Ticari sürümü etkinleştirme	25
Kaspersky Mobile Security 9 aboneliğini etkinleştirme.....	26
Etkinleştirme kodunu çevrimiçi satın alma	27
Deneme sürümünü etkinleştirme	27
Gizli kodu belirleme	28
Gizli kodun kaldırılması seçeneğini etkinleştirme	29
Gizli kodun kaldırılması	29
Uygulamayı başlatma	30
Uygulamanın veritabanlarını güncelleme.....	30
Aygıtı virüslere karşı tarama	31
Uygulama hakkındaki bilgileri görüntüleme	31
LİSANS YÖNETİMİ	32
Lisans sözleşmesi hakkında	32
Kaspersky Mobile Security 9 lisansları hakkında	32
Lisans Bilgilerini Görüntüleme	34
Lisansı yenileme	34
Lisansı etkinleştirme koduyla yenileme	35
Lisansı çevrimiçi yenileme	36
Lisansı aboneliği etkinleştirerek yenileme	37
Aboneliği kaldırma	38
Aboneliği yenileme	39
UYGULAMA ARAYÜZÜ	39
Koruma durumu penceresi	40
Uygulama menüsü.....	41

DOSYA SİSTEMİ KORUMASI	43
Koruma hakkında.....	43
Korumayı etkinleştirme ve devre dışı bırakma	43
Seçilen nesnelere uygulanacak işlemin seçilmesi	45
AYGITI TARAMA.....	47
Tespit edilen nesnelere uygulanacak eylemi seçme.....	47
Bir taramayı elle başlatma	48
Zamanlanmış taramayı başlatma.....	49
Taranacak nesne türünü seçme	50
Arşiv taramalarını yapılandırma.....	51
Seçilen nesnelere uygulanacak işlemin seçilmesi	52
KÖTÜ AMAÇLI NESNELERİN KARANTİNAYA ALINMASI	54
Karantina hakkında.....	54
Karantinaya alınan nesnelere görüntüleme	54
Nesneleri Karantinadan geri yükleme	55
Karantinadaki nesnelere silme.....	56
GELEN ARAMALARI VE SMS'LERİ FİLTRELEME	57
Arama/SMS Filtresi Hakkında.....	57
Arama/SMS Filtresi modları hakkında	58
Arama/SMS Filtresi modunun değiştirilmesi	58
Kara Liste oluşturma.....	59
Kara listeye giriş ekleme	60
Kara Listedeki girişleri düzenleme	61
Kara Listedeki girişleri silme.....	62
Beyaz Liste oluşturma	62
Beyaz Listeye giriş ekleme.....	63
Beyaz Listedeki girişleri düzenleme	64
Beyaz Listedeki girişleri silme	65
Telefon defterinde olmayan kişilerden gelen SMS mesajlarını ve aramaları yanıtlama.....	66
Sayısal olmayan numaralardan gelen SMS mesajlarını yanıtlama	67
Gelen SMS'ler için bir yanıt seçme	68
Gelen aramalar için bir yanıt seçme	69
GİDEN ARAMALARI VE SMS MESAJLARINI SINIRLAMA. EBEVEYN DENETİMİ	69
Ebeveyn Denetimi hakkında	70
Ebeveyn Denetimi modları.....	70
Ebeveyn Denetiminin Etkinleştirilmesi/Devre Dışı Bırakılması.....	71
Kara Liste oluşturma.....	71
Kara listeye giriş ekleme	72
Kara Listedeki girişleri düzenleme	73
Kara Listedeki girişleri silme.....	74
Beyaz Liste oluşturma	74
Beyaz Listeye giriş ekleme.....	75
Beyaz Listedeki girişleri düzenleme	76
Beyaz Listedeki girişleri silme	77
AYGITIN KAYBOLMASI VEYA ÇALINMASI DURUMUNDA VERİ KORUMASI	78
Hırsızlığa Karşı Koruma hakkında	78
Aygıtı engelleme	79

Kişisel Veri Silme	81
Silinecek nesnelere listesi oluşturma	83
Aygıttaki SIM kartının değiştirilmesini izleme	84
Aygıtın coğrafi koordinatlarını belirleme	85
Hırsızlığa Karşı Koruma işlevlerini uzaktan başlatma	87
GİZLİLİK KORUMASI	89
Gizlilik Koruması	89
Gizlilik Koruması modları	89
Gizlilik Korumasını Etkinleştirme/Devre Dışı Bırakma	90
Gizlilik Korumasını otomatik olarak etkinleştirme	91
Gizlilik Korumasını uzaktan etkinleştirme	92
Özel numaralar listesi oluşturma	94
Özel numaralar listesine numara ekleme	95
Özel kişiler listesinde bir numarayı düzenleme	96
Özel kişiler listesinde bir numarayı silme	96
Gizlenecek verileri seçme: Gizlilik Koruması	97
AĞ ETKİNLİĞİNİ FİLTRELEME, GÜVENLİK DUVARI	98
Güvenlik Duvarı hakkında	99
Güvenlik Duvarını etkinleştirme/devre dışı bırakma	99
Güvenlik Duvarı güvenlik düzeyini seçme	99
Engelleme bildirimleri	100
KİŞİSEL VERİLERİ ŞİFRELEME	102
Şifreleme hakkında	102
Verileri şifreleme	102
Verilerin şifresini çözme	104
Şifreli verilere erişimi engelleme	105
UYGULAMANIN VERİTABANLARINI GÜNCELLEME	107
Uygulamanın veritabanlarını güncelleme hakkında	107
Veritabanı bilgilerini görüntüleme	108
Elle güncelleme	108
Zamanlanmış güncelleme	109
Dolaşımdayken güncelleme	110
UYGULAMA GÜNLÜKLERİ	112
Günlükler hakkında	112
Günlük kayıtlarını görüntüleme	112
Günlük kayıtlarını silme	113
EK AYARLARI YAPILANDIRMA	113
Gizli kodu değiştirme	114
Uyarıları görüntüleme	114
Sesli bildirimleri yapılandırma	115
TEKNİK DESTEK HİZMETİ İLE İLETİŞİME GEÇME	116
SÖZLÜK	117
KASPERSKY LAB	120
ÜÇÜNCÜ TARAF KODLAR HAKKINDA BİLGİ	121
Dağıtılmış program kodu	121

Diğer bilgiler.....	121
İNDEKS.....	122

BU KILAVUZ HAKKINDA

Bu Kılavuz, Kaspersky Mobile Security 9'un kurulumu, yapılandırılması ve kullanımı konusunda bilgi veren bir belgedir. Bu belge, geniş kullanıcı kitlesi düşünülerek hazırlanmıştır.

Belgenin amaçları:

- kullanıcının uygulamayı, bir mobil aygıtta kendi başına kurmasına, etkinleştirmesine ve kendi gereksinimlerine uygun olarak ayarlamasına yardımcı olmak;
- uygulamayla ilgili sorunlar hakkında hızlı bilgi aramalarına olanak sağlamak;
- uygulama hakkında alternatif bilgi kaynakları ve teknik destek alma olanakları ile ilgili bilgi vermek.

BU BÖLÜMDE

Bu belgede	12
Belge kuralları	15

BU BELGEDE

Bu belgede aşağıdaki bölümler bulunmaktadır:

Ek veri kaynakları

Bu bölümde, uygulama ve kullanıcıların uygulamayı tartışabilecekleri, sorular sorabilecekleri ve yanıtlar alabilecekleri İnternet kaynakları ile ilgili ek bilgi kaynaklarını açıklanmaktadır.

Kaspersky Mobile Security 9

Bu bölümde, uygulamanın özellikleri açıklanmakta, bileşenleri ve ana işlevleri hakkında özet bilgi verilmektedir. Bu bölümde, dağıtım kitinin amacı hakkında bilgi verilmektedir. Bu bölümde, Kaspersky Mobile Security 9'un yüklenebilmesi için bir mobil aygıtın karşılaması gereken donanım ve yazılım gereksinimleri liste halinde verilmektedir.

Kaspersky Mobile Security 9'un kurulumu

Bu bölümde, uygulamayı bir mobil aygıtta kurmanıza yardımcı olacak talimatlar bulunmaktadır.

Uygulamayı kaldırma

Bu bölümde, uygulamayı bir mobil aygıttan kaldırmanıza yardımcı olacak talimatlar bulunmaktadır.

Uygulamayı güncelleme

Bu bölümde, uygulamanın önceki sürümlerini güncellemenize yardımcı olacak talimatlar bulunmaktadır.

Başlarken

Bu bölümde; uygulamanın etkinleştirilmesi, uygulama için gizli bir kod belirlenmesi, gizli kodu kurtarma seçeneğinin etkinleştirilmesi, gizli kodun kurtarılması, uygulamanın başlatılması, anti-virüs veritabanlarının güncellenmesi ve bir aygıtta virüs taramasının yapılması dahil olmak üzere, Kaspersky Mobile Security 9'u nasıl kullanmaya başlayabileceğinizle ilgili bilgiler verilmektedir.

Lisans yönetimi

Bu bölümde, uygulamanın lisanslanması çerçevesinde sık kullanılan terimlerle ilgili bilgiler bulunmaktadır. Ayrıca Kaspersky Mobile Security 9 lisansı ve geçerlilik süresinin uzatılmasına ilişkin bilgilerin nasıl bulunacağı da bu bölümde anlatılmaktadır.

Uygulama arayüzü

Bu bölümde, Kaspersky Mobile Security 9 arabiriminin ana unsurları hakkında bilgi verilmektedir.

Dosya sistemi koruması

Bu bölüm, aygıtınızın dosya sistemine virüslerin bulaşmasından sakınmayı sağlayan Koruma bileşeni hakkında bilgiler vermektedir. Aynı zamanda Korumanın nasıl etkinleştirileceği / durdurulacağı ve çalıştırma ayarlarının nasıl yapılacağı da bu bölümde anlatılmaktadır.

Aygıt tarama

Bu bölümde, aygıtınızdaki tehditlerin algılanması ve temizlenmesi işlevini gerçekleştiren, aygıtta isteğe bağlı olarak tarama yapma işlemi hakkında bilgi verilmektedir. Bu bölümde, aygıtta tarama başlatma, otomatik programlı dosya sistemi taraması ayarlama, taranacak dosyaları seçme ve kötü amaçlı bir nesne tespit edildiğinde uygulamanın yapacağı işlemi belirleme gibi konular da anlatılmaktadır.

Kötü amaçlı nesnelere karantina alma

Bu bölümde potansiyel olarak kötü amaçlı nesnelere yerleştirildiği özel bir dizin olan *karantina* hakkında bilgiler verilmektedir. Bu bölümde, dizinde bulunan zararlı nesnelere nasıl görüntüleneceği, geri yükleneceği ya da silineceği hakkında bilgiler verilmektedir.

Gelen aramaları ve SMS'leri filtreleme

Bu bölüm, oluşturduğunuz Kara ve Beyaz Listelere uygun olarak istenmeyen aramaları ve SMS'leri engelleyen Arama/SMS Filtresi hakkında bilgi vermektedir. Bu bölümde ayrıca Arama/SMS Filtresinin gelen aramaları ve SMS'leri tarayacağı modun nasıl seçileceği, gelen SMS ve aramalar için ek filtreleme ayarlarının nasıl yapılandırılacağı ve ayrıca Kara ve Beyaz Listelerin nasıl oluşturulacağı açıklanmaktadır.

Giden aramaları ve SMS mesajlarını sınırlama. Ebeveyn Denetimi

Bu bölüm, belirtilen numaralara giden aramaların ve SMS mesajlarının sınırlanmasını sağlayan Ebeveyn denetimi bileşeni hakkında bilgiler verir. Bölüm ayrıca izin verilen ve yasaklı numaralar listesinin nasıl oluşturulacağını ve Ebeveyn Denetimi ayarlarının nasıl yapılacağını açıklar.

Aygıtın kaybolması veya çalınması durumunda veri koruması

Bu bölümde, aygıtın çalınması ya da kaybolması durumunda, mobil aygıtta kayıtlı bilgilere izinsiz erişimi engelleyen ve aygıtın bulunmasını kolaylaştıran Hırsızlığa Karşı Koruma sistemi hakkında bilgiler verilmektedir.

Ayrıca Hırsızlığa Karşı Koruma'nın nasıl etkinleştirileceği/devre dışı bırakılacağı, çalışma parametrelerinin nasıl belirleneceği ve Hırsızlığa Karşı Koruma'nın başka bir mobil cihaz üzerinden uzaktan nasıl başlatılacağı da bu bölümde anlatılmaktadır.

Gizlilik Koruması

Bu bölümde, kullanıcının gizli bilgilerini saklayabilen Gizlilik Koruması hakkında bilgiler verilmektedir.

Ağ etkinliğini filtreleme. Güvenlik Duvarı

Bu bölümde, aygıtınızdaki ağ bağlantılarını kontrol eden Güvenlik Duvarı ile ilgili bilgiler verilmektedir. Bu bölümde Güvenlik Duvarı'nın nasıl etkinleştirileceği/devre dışı bırakılacağı ve istenen modun nasıl seçileceği açıklanmaktadır.

Kişisel verileri şifreleme

Bu bölümde, aygıtınızdaki dizinleri şifreleyebilecek olan Şifreleme hakkında bilgiler verilmektedir. Aynı zamanda seçilmiş dizinlerin nasıl şifreleneceği ve şifrelerinin nasıl çözüleceğini de açıklamaktadır.

Uygulamanın veritabanlarını güncelleme

Bu bölüm, aygıtınızın korumasının güncel olmasını sağlayan uygulama veritabanlarını güncelleme hakkında bilgi verir. Ayrıca, yüklü anti-virüs veritabanlarındaki bilgilerin nasıl görüntüleneceği, güncellemenin nasıl elle başlatılacağı ve anti-virüs veritabanlarının otomatik güncellemelerinin nasıl yapılandırılacağı da bu bölümde açıklanmaktadır.

Uygulama günlükleri

Bu bölümde, her bileşenin işlemlerini ve her görevin gerçekleştirilmesini (ör. uygulama veritabanı güncellemeleri, virüs taramaları) kaydeden günlüklerle ilgili bilgiler verilmektedir.

Ek ayarları yapılandırma

Bu bölüm Kaspersky Mobile Security 9 uygulamasının ek seçenekleri hakkında bilgi verir: Uygulamanın sesli bildirimini ve ekran arka ışığının yönetimi, ipuçlarını, koruma simgesini ve koruma durumu penceresini etkinleştirme / devre dışı bırakma.

Teknik Destek Hizmeti ile İletişime Geçme

Bu bölümde, Teknik Destek Servisi web sitesi ya da telefonla Kişisel Kabin'inizden yardım almak için Kaspersky Lab ile görüşmenize yardımcı olacak öneriler verilmektedir.

Sözlük

Bu bölümde, belgede kullanılan terimleri ve tanımlarını içeren bir liste bulunmaktadır.

Kaspersky Lab

Bu bölümde, Kaspersky Lab ZAO hakkında bilgiler bulunmaktadır.

Üçüncü taraf kodlar hakkında bilgi

Bu bölümde, uygulamada kullanılan, başka firmalarca sağlanan kodlar hakkında bilgiler verilmektedir.

İndeks

Bu bölüm, belgede istediğiniz bilgileri çabucak bulmanızı sağlamaktadır.

BELGE KURALLARI

Bu belgede, aşağıdaki tabloda gösterilen kurallar açıklanmıştır.

Table 1. Belge kuralları

ÖRNEK METİN	BELGE KURALLARI AÇIKLAMASI
Unutmayın...	Uyarılar, kırmızı renkte vurgulanmıştır ve çerçeve içine alınmıştır. Uyarılar'da, örneğin güvenlik açısından kritik bilgisayar işlemleri gibi önemli bilgiler yer alır.
Kullanılması önerilir...	Notlar, çerçeve içine alınmıştır. Notlar, daha fazla ve referans amaçlı bilgiler içerir.
Örnek: ...	Örnekler bölüme göre, sarı bir arka plan üzerinde ve "Örnek" başlığı altında verilmektedir.
Güncelle'nin anlamı...	Yeni terimler, yatık harflerle belirtilmektedir.
ALT+F4	Klavye tuşlarının adları, kalın yazı tipiyle ve büyük harflerle gösterilmektedir. Tuş adının arkasından gelen "artı" işareti, gösterilen tuşlara birlikte basılacağını gösterir.
Etkinleştir	Giriş alanları, menü komutları, düğmeler, vs. gibi arabirim unsurlarının adları kalın yazı tipi ile gösterilmektedir.
► Bir görev programını yapılandırmak için:	Talimat tanıtım ibareleri italik yazı tipi ile işaretlenmiştir.
yardım	Ekranında gösterilen komut satırındaki metinler ya da mesaj metinleri için özel bir yazı tipi kullanılmaktadır.
<Bilgisayarınızın IP adresi>	Değişkenler köşeli parantezler içinde verilmektedir. Her durum için değişkenler yerine ilgili değerler yerleştirilir (köşeli parantezler kaldırılır).

EK VERİ KAYNAKLARI

Kaspersky Mobile Security 9'un kurulması ya da kullanılmasıyla ilgili sorularınızın yanıtlarını, çeşitli bilgi kaynaklarını kullanarak bulabilirsiniz. İsteğinizin ne kadar önemli ya da acil olduğuna bağlı olarak en uygun kaynağı seçebilirsiniz.

BU BÖLÜMDE

Daha fazla araştırma için bilgi	16
Satış Departmanı ile iletişim kurma	17
Web forumunda Kaspersky Lab uygulamalarını tartışma	17
Belgelendirme Gelişim Grubu ile İletişim Kurma	17

DAHA FAZLA ARAŞTIRMA İÇİN BİLGİ

Uygulama ile ilgili olarak aşağıdaki bilgi kaynaklarına başvurabilirsiniz:

- Kaspersky Lab uygulama web sitesi
- Teknik Destek Hizmeti web sitesindeki uygulamanın Bilgi Tabanı sayfası
- Yüklü yardım sistemi ve ipuçları
- Yüklü uygulama belgeleri.

Kaspersky Lab web sitesindeki sayfa

http://www.kaspersky.com.tr/kaspersky_mobile_security

Bu sayfada, Kaspersky Mobile Security 9 ile özellikleri ve seçenekleri hakkında genel bilgiler verilmektedir. Kaspersky Mobile Security 9 ürününü E-Mağazamızdan satın alabilirsiniz.

Teknik Destek Hizmeti web sitesindeki uygulama sayfası (Bilgi Tabanı)

<http://support.kaspersky.com>

Bu sayfada Teknik Destek Hizmeti uzmanları tarafından yazılan makaleler bulunur.

Bu makalelerde Kaspersky Mobile Security 9'un satın alınması, kurulması ve kullanılmasıyla ilgili yararlı bilgiler, öneriler ve Sıkça Sorulan Sorular (SSS'ler) yer almaktadır. "Veritabanı güncellemeleri" ve "Sorun giderme" gibi başlıklar halinde düzenlenmişlerdir. Bu makalelerde, Kaspersky Mobile Security 9'un yanı sıra diğer Kaspersky Lab ürünleriyle ilgili sorular da yanıtlanmaktadır. Ayrıca Teknik Destek Hizmeti haberlerini içerebilir.

Yüklü Yardım sistemi

Eğer Kaspersky Mobile Security 9'daki belirli bir pencere ya da sekme ile ilgili sorunuz varsa, içerik yardımına bakabilirsiniz.

İçerik yardımını açmak için istediğiniz ekranı açın ve **Yardım** ögesini seçin.

Yüklü Belgeler

Kullanım Kılavuzu, uygulamanın işlevleri ve Kaspersky Mobile Security 9'un nasıl kullanılacağı hakkında ayrıntılı bilgiler içerirken, yapılandırılması ile ilgili tavsiye ve öneriler de sunar.

Belgeler Kaspersky Mobile Security 9 dağıtım paketinde PDF dosyası biçiminde bulunur.

Bu belgeleri Kaspersky Lab'ın web sitesinden elektronik dosya biçiminde de indirebilirsiniz.

SATIŞ DEPARTMANIYLA İLETİŞİM KURMA

Kaspersky Mobile Security'yi seçme ya da satın almayla veya lisansınızın süresini uzatmayla ilgili sorularınız varsa lütfen aşağıdaki telefonları arayarak Moskova'daki Merkez Ofisimizde bulunan Satış Departmanı'ndaki uzmanlarla görüşün:

+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00

Bu hizmet Rusça veya İngilizce olarak sağlanır.

Satış Departmanına sorularınızı sales@kaspersky.com adresine e-postayla da gönderebilirsiniz.

WEB FORUMUNDA KASPERSKY LAB UYGULAMALARINI TARTIŞMA

Sorunuz acil bir yanıt gerektirmiyorsa, <http://forum.kaspersky.com> adresinde bulunan forumumuzda Kaspersky Lab uzmanları ve diğer Kaspersky Lab anti-virüs kullanıcılarıyla sorunuzu tartışabilirsiniz.

Bu forumda var olan tartışmaları görebilir, yorumlarınızı bırakabilir, yeni konular oluşturabilir ve belli sorgular için arama motorunu kullanabilirsiniz.

BELGELENDİRME GELİŞİM GRUBUYLA İLETİŞİM KURMA

Belgelerle ilgili herhangi bir sorunuz varsa, belgelerde herhangi bir hata bulursanız ya da bir yorum yapmak isterseniz, lütfen Kullanıcı belgeleri gelişim grubuyla iletişim kurun. Belgelendirme Gelişim Grubuyla iletişim kurmak için docfeedback@kaspersky.com adresine e-posta atın. Bu konu satırını kullanın: "Kaspersky Help Feedback: Kaspersky Mobile Security 9".

KASPERSKY MOBILE SECURITY 9

Kaspersky Mobile Security 9, Microsoft Mobile işletim sistemi ile çalışan mobil aygıtları (bundan böyle "aygıtlar" olarak anılacaktır) korur. Uygulama, aygıt üzerindeki bilgileri bilinen tehditlere karşı koruyabilir, istenmeyen SMS mesajlarını ve aramaları engelleyebilir, aygıttaki ağ bağlantısını kontrol edebilir, bilgileri şifreleyebilir, gizli kişiler listesi için gizleyebilir ve ayrıca aygıtın kaybolması veya çalınması durumunda da bilgileri koruyabilir. Her türden tehdit programın ayrı bileşenleri tarafından işlenir. Bu da uygulama ayarlarının esnek yapılandırmasını etkinleştirir.

Kaspersky Mobile Security 9, aşağıdaki koruma bileşenlerinden oluşur:

- **Anti-Virüs** dizini. Mobil aygıtın dosya sistemini virüslerden ve diğer kötü niyetli uygulamalardan korur. Anti-Virüs, aygıtınız üzerindeki kötü niyetli nesnelere tespit edip etkisizleştirebilir ve uygulamanızın anti-virüs uygulamalarını günceller.
- **Arama/SMS Filtresi**. Gelen tüm SMS mesajlarını ve aramaları istenmeyen mesajlara karşı tarar. Bu bileşen, istenmeyen olarak değerlendirilen mesajların ve aramaların esnek biçimde engellenmesini sağlar.
- **Hırsızlığa Karşı Koruma**. Bu özellik, aygıt kaybolduğunda ya da çalındığında, aygıttaki bilgileri izinsiz erişimlere karşı korur ve aygıtın bulunmasını kolaylaştırır. Hırsızlığa Karşı Koruma, diğer bir aygıttan gönderilen SMS komutları ile aygıtınızı uzaktan kilitlemenize, depolanan herhangi bir bilgiyi silmenize ve (mobil aygıtınızın bir GPS alıcısı varsa) coğrafi konumunuzu belirlemenize olanak tanır. Hırsızlığa Karşı Koruma, SIM kartı değiştirilmişse veya aygıt bir SIM kartı olmadan etkinleştirilmişse aygıtınızı kilitlemenize imkan verir.
- **Ebeveyn Denetimi**. Tüm giden SMS mesajları ve aramalar kontrol edilir. Bileşen, giden SMS mesajlarının ve aramaların filtrelenmesinin esnek yapılandırmasına olanak tanır.
- **Gizlilik Koruması**. Kişi listesindeki gizli numaralara ilişkin bilgileri gizler. Gizlilik Koruması, bu numaralar ile ilgili olarak Kişi Listesindeki girişleri, arama günlüğündeki SMS mesajlarını ve alınan yeni mesajlar ile gelen aramaları gizler.
- **Güvenlik Duvarı**. Mobil aygıtınızın ağ bağlantılarını kontrol eder. Güvenlik duvarı, izin verilecek veya yasaklanacak bağlantıları belirler.
- **Şifreleme**. Bilgileri şifreli modda korur. Bileşen, aygıt belleğinde veya depolama kartlarındaki tüm sistem dışı dizinleri şifreler. Şifreli dizinlerden dosyalara erişim, yalnızca gizli uygulama kodu girildikten sonra mümkün olur.

Ayrıca uygulamanın güncelliğini korumasını sağlayan, uygulamanın kullanımı sırasında seçenekleri arttıran ve uygulamayı kullanımınızda sizi destekleyen bir dizi hizmet fonksiyonu bulunmaktadır:

- **Koruma durumu**. Program bileşenlerinin durumu ekranda görüntülenir. Verilen bilgilere göre, aygıtınızda mevcut bilgi koruma durumunu değerlendirebilirsiniz.
- **Uygulamanın anti-virüs veri tabanlarının güncellenmesi**. Bu işlev Kaspersky Mobile Security 9 anti-virüs veritabanlarını güncel tutar.
- **Olay günlüğü**. Uygulama bileşenlerinin her birinin bileşenin işleyişi (örneğin, tamamlanmış işlem, engellenen nesnedeki veriler, tarama raporu, güncellemeler) hakkında bilgileri içeren kendi olay günlüğü vardır.
- **Lisans**. Kaspersky Mobile Security 9 uygulamasını satın aldığınızda, sizinle Kaspersky Lab arasında bir lisans sözleşmesi yapılır ve bu sözleşmeye göre, belirli bir süre boyunca uygulamayı kullanabilir ve anti-virüs veri tabanı güncellemelerine ve Teknik Destek Hizmetine erişebilirsiniz. Lisans süresi ve uygulamanın tam işlevsel modda çalışması için gerekli olan diğer bilgiler lisansta belirtilir.

Lisans seçeneğini kullanarak geçerli lisans hakkında ayrıntılı bir rapor almanın yanında lisansı yenileyebilirsiniz.

Kaspersky Mobile Security 9 yedekleme ve geri yükleme işlemleri için kullanılamaz.

BU BÖLÜMDE

Kaspersky Mobile Security 9'daki yenilikler.....	19
Dağıtım kiti	19
Donanım ve yazılım gerekleri.....	19

KASPERSKY MOBILE SECURITY 9'DAKİ YENİLİKLER

Kaspersky Mobile Security 9'daki yeniliklerin ayrıntılarını aşağıda görebilirsiniz.

Kaspersky Mobile Security 9 aşağıdaki yeni seçenekleri içermektedir:

- Uygulamaya erişim gizli bir kod tarafından korunur.
- Gizlilik Koruması bileşeni, Kişi listesindeki gizli kişilerin şu bilgilerini gizlemenizi sağlar: Kişi listesindeki girişler, SMS mesajları, arama günlüğü, yeni gelen SMS mesajları ve gelen aramalar. Gizli bilgiler görülebilmeleri için erişilebilir durumdadır; gizleme görünümü devre dışı bırakılmıştır.
- Şifreleme, aygıt belleğinde veya bir bellek kartında kaydedilen dizinlerin şifrlenmesini sağlar. Bileşen, gizli verileri şifrelenmiş moda korur ve gizli bilgilere yalnızca uygulama gizli kodu girildiğinde erişim izni verir.
- Uyarıları görüntüleme adında yeni bir hizmet işlevi eklenmiştir: Akıllı telefona yönelik Kaspersky Mobile Security 9, bileşen ayarlarının yapılandırılmasından önce bileşenin kısa bir tanımını verir.
- Etkileştirme kodu satın alabilir veya lisansınızın geçerlilik süresini abonelik seçeneği ile veya çevrimiçi olarak doğrudan mobil aygıtınızdan uzatabilirsiniz.

DAĞITIM KİTİ

Kaspersky Mobile Security 9 ürününü çevrimiçi satın alabilirsiniz, bu durumda uygulamanın dağıtım kiti ve belgeler elektronik biçimde sağlanır. Kaspersky Mobile Security 9 telefon ve teknoloji ürünleri satan tüm büyük mağazalardan da satın alınabilir. Uygulamayı satın alma ve dağıtım kitini alma hakkında ayrıntılı bilgi için lütfen sales@kaspersky.com adresinden satış departmanımız ile iletişim kurun.

DONANIM VE YAZILIM GEREKLERİ

Kaspersky Mobile Security 9 aşağıdaki işletim sistemlerinden biri ile çalışan mobil aygıtlara kurulmak üzere tasarlanmıştır:

- Microsoft Windows Mobile 5.0;
- Microsoft Windows Mobile 6.0, 6.1, 6.5.

KASPERSKY MOBILE SECURITY 9'UN KURULUMU

Uygulama mobil aygıtta birkaç adımda kurulur.

Kuruluma başlamadan önce çalışan diğer tüm uygulamaları kapatmanız önerilir.

➔ *Kaspersky Mobile Security 9 uygulamasını kurmak için:*

1. Microsoft ActiveSync uygulamasını kullanarak mobil aygıtı bilgisayara bağlayın.
2. Aşağıdaki işlemlerden birini gerçekleştirin:
 - Programı CD'de satın aldıysanız, satın alınan CD'deki Kaspersky Mobile Security 9 otomatik kurulumunu çalıştırın.
 - Dağıtım paketini İnternet üzerinden satın aldıysanız, aşağıdaki yöntemlerden birini kullanarak mobil aygıtta kopyalayın:
 - Kaspersky Lab web sitesinden;
 - Microsoft ActiveSync uygulamasını kullanarak
 - bir bellek kartı kullanarak.

Mobil aygıtınızdaki dağıtım paketini içeren cab arşivini açarak kurulumu çalıştırın.
3. Sizinle Kaspersky Lab arasındaki Lisans Sözleşmesinin metnini okuyun. Sözleşmenin tüm şartlarını kabul ediyorsanız, **Tamam** düğmesine basın. Kaspersky Mobile Security 9 uygulaması aygıtta kurulacaktır. Lisans Sözleşmesinin şartlarını kabul etmiyorsanız, **İptal** düğmesine basın.
4. Kaspersky Mobile Security 9 için arabirim dilini seçin ve **Tamam** düğmesine basın.
5. Kurulumu tamamlamak için aygıtı yeniden başlatın. Bunun için, **Yeniden başlat** düğmesine basın.

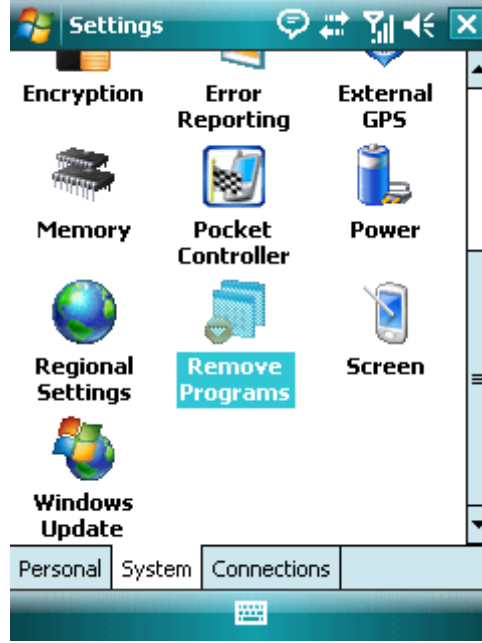
Uygulama Kaspersky Lab uzmanları tarafından önerilen parametrelerle kurulur.

UYGULAMANIN KALDIRILMASI

➔ *Kaspersky Mobile Security 9 uygulamasını kaldırmak için:*

1. Aygıtınızdaki verilerin şifresini çözün Kaspersky Mobile Security 9 ile şifrelenmiş ise (bkz. "Verilerin şifresini çözme" bölümü sayfa [104](#)).
2. Gizlilik Korumasını devre dışı bırakın (bkz. "Gizlilik Korumasını etkinleştirme/devre dışı bırakma" bölümü, sayfa [90](#)).
3. Kaspersky Mobile Security 9 uygulamasını kapatın. Bunun için, **Menü** → **Çıkış** düğmesine basın.
4. Kaspersky Mobile Security 9 uygulamasını kaldırın. Bunun için aşağıdaki işlemleri gerçekleştirin:
 - a. **Başlat** → **Ayarlar** düğmesine basın.

- b. **Sistem** sekmesindeki **Program Kaldır** ögesini seçin (bkz. aşağıdaki Şekil).



Şekil 1: **Sistem** sekmesi

- c. Kurulu programlar listesinden **Kaspersky Mobile Security** programını seçerek **Kaldır** düğmesine basın (bkz. aşağıdaki Şekil).



Şekil 2: **Kaldırılacak uygulamayı seçme**

- d. Açılan pencerede **Evet** seçeneğine tıklayarak uygulamanın silinmesini onaylayın.
- e. Gizli kodu girin ve **Tamam** düğmesine basın.

- f. Program ayarlarının ve karantinadaki nesnelerin korunup korunmayacağını belirtin (bkz. aşağıdaki Şekil):
- Uygulama ayarlarını ve karantinadaki nesnelere korumak istiyorsanız, **Sakla** düğmesine basın (bkz. aşağıdaki Şekil).
 - Uygulamayı tümüyle kaldırmak için **Sil** düğmesine basın.



KMS 9 kaldırılıyor

Uygulama ayarlarını ve Karantinadaki bütün dosyaları silmek istiyor musunuz?



Şekil 3: Uygulamayı ayarlarını kaldırma

5. Uygulamanın kaldırılmasını tamamlamak için aygıtı yeniden başlatın.

UYGULAMAYI GÜNCELLEME

Uygulamanın bu nesildeki en son sürümünü kurarak (örneğin 9.0 sürümünü 9.2 sürümüne güncelleyerek) Kaspersky Mobile Security 9'u güncelleyebilirsiniz.

Kaspersky Mobile Security 8.0'ı kullanıyorsanız, Kaspersky Mobile Security 9'a geçebilirsiniz.

► *Programın sürümünü güncellemek için:*

1. Şifrelemeyi Devre Dışı Bırakın – tüm verileri çöz (bkz. "Veri Şifresinin Çözülmesi" bölümü, sayfa [104](#)).
2. Gizlilik Koruması bileşenini devre dışı bırakın (bkz. "Gizlilik Koruma bileşenini etkinleştirme/devre dışı bırakma" bölümü, sayfa [90](#)).
3. Kaspersky Mobile Security'nin geçerli sürümünü kapatın. Bunun için, **Menü** → **Çıkış** düğmesine basın.
4. Uygulamanın dağıtım paketini aşağıdaki yöntemlerden birini kullanarak aygıtınıza kopyalayın:
 - Kaspersky Lab web sitesinden;
 - Microsoft ActiveSync uygulamasını kullanarak
 - bir bellek genişletme kartı kullanarak.
5. Aygıttaki Kaspersky Mobile Security 9 dağıtım paketini başlatın.

6. Lisans sözleşmesini dikkatle okuyun. Şartlarını kabul ediyorsanız, **Tamam** düğmesine basın. Sizden ilk önce geçerli uygulama sürümünü kaldırmanız istenecektir.
 7. Uygulamanın önceki sürümünü kaldırılmasını **Tamam** düğmesine basarak onaylayın.
 8. Gizli kodu girin.
 9. Uygulama ayarları ve Karantinadaki nesnelerin korunup korunmayacağını belirtin:
 - Uygulama ayarlarını ve karantinadaki nesnelere korumak istiyorsanız, **Sakla** düğmesine basın (bkz. aşağıdaki Şekil).
 - Uygulamayı tümüyle kaldırmak için **Kaldır** düğmesine basın.
 10. Kaldırma işlemi tamamlamak için aygıtı yeniden başlatın. Bunun için, **Yeniden başlat** düğmesine basın.
 11. Aygıtı yeniden başlattıktan sonra Kaspersky Mobile Security 9 kurulumunu çalıştırın (bkz. "Kaspersky Mobile Security 9'un kurulumu" bölümü, sayfa [20](#)).
- Mevcut lisans hala geçerliyse, uygulama otomatik olarak etkinleştirilecektir. Lisansın süresi sona ermişse, uygulamayı etkinleştirme işlemi gerçekleştirin (bkz. "Uygulamayı etkinleştirme" bölümü, sayfa [24](#)).

➔ *Kaspersky Mobile Security 8.0 sürümünden 9 sürümüne geçmek için:*

1. Kaspersky Mobile Security 8.0'ı kullanarak şifrelenmişlerse, tüm verilerin şifrelerini çözün.
2. Kaspersky Mobile Security 9 uygulamasını kapatın. Bunun için, **Menü** → **Çıkış** düğmesine basın.
3. Kaspersky Mobile Security 9 uygulamasını kaldırın. Bunun için aşağıdaki işlemleri gerçekleştirin:
 - a. **Başlat** → **Ayarlar** düğmesine basın.
 - b. **Sistem** sekmesindeki **Program Kaldır** öğesini seçin
 - c. Kurulu programlar listesinden **Kaspersky Mobile Security** programını seçerek **Kaldır** düğmesine basın.
 - d. Açılan pencerede **Evet** seçeneğine tıklayarak uygulamanın silinmesini onaylayın.
 - e. Uygulamanın önceki sürümünde ayarlanan gizli kodu girin ve **Tamam** düğmesine basın.
 - f. Kaspersky Mobile Security 8.0'in ayarlarını tümüyle silin çünkü bunlar 9 sürümünün ayarlarıyla uyumsuzdur. Bunun için, **Sil** düğmesine basın.
4. Kaspersky Mobile Security 8.0'ın kaldırma işlemi tamamlamak için aygıtı yeniden başlatın.
5. Kaspersky Mobile Security 9'un kurulumunu başlatın (bkz. "Kaspersky Mobile Security 9'un kurulumu" bölümü, sayfa [20](#)).
6. Uygulamayı etkinleştirmeyi başlatın (bkz. "Uygulamayı etkinleştirme" bölümü, sayfa [24](#)).

Kaspersky Mobile Security 8.0 lisansının geçerlilik süresi sona ermemişse, 8.0 sürümünün etkinleştirme kodunu kullanarak programın 9 sürümünü etkinleştirin.

BAŞLARKEN

Bu bölümde; uygulamanın etkinleştirilmesi, uygulama için gizli bir kod belirlenmesi, gizli kodu kurtarma seçeneğinin etkinleştirilmesi, gizli kodun kurtarılması, uygulamanın başlatılması, anti-virüs veritabanlarının güncellenmesi ve bir aygıtta virüs taramasının yapılması dahil olmak üzere, Kaspersky Mobile Security 9'u nasıl kullanmaya başlayabileceğinizle ilgili bilgiler verilmektedir.

BU BÖLÜMDE

Uygulamayı etkinleştirme	24
Gizli kodu belirleme	28
Gizli kodun kurtarılması seçeneğini etkinleştirme.....	28
Gizli kodun kurtarılması	29
Uygulamanın başlatılması	30
Uygulamanın veritabanlarını güncelleme	30
Aygıt virüslere karşı tarama.....	30
Uygulama hakkındaki bilgileri görüntüleme	31

UYGULAMAYI ETKİNLEŞTİRME

Kaspersky Mobile Security 9'u kullanmaya başlamadan önce etkinleştirilmesi gerekmektedir.

Kaspersky Mobile Security 9 uygulamasını etkinleştirmek için, yapılandırılmış bir İnternet bağlantınızın olması gerekir.

Uygulamayı etkinleştirmeden önce aygıtın sistem tarih ve saat ayarlarının doğru olduğundan emin olun.

Uygulamayı aşağıdaki yollardan etkinleştirebilirsiniz:

- **Deneme lisansını etkinleştir.** Deneme sürümünü etkinleştirdiğinizde, uygulama bir ücretsiz deneme lisansı alır. Deneme lisansının geçerlilik süresi etkinleştirme tamamlandıktan sonra ekranda görüntülenir. Deneme lisansının geçerlilik süresi sona erdiğinde uygulamanın işlevleri sınırlanacaktır. Yalnızca aşağıdaki özellikler kullanılabilir:
 - Uygulamayı etkinleştirme;
 - Uygulama lisansını yönetme;
 - Kaspersky Mobile Security 9 Yardım sistemi;
 - Şifrelemeyi devre dışı bırakma;
 - Gizlilik Korumasını devre dışı bırakma.

Bir deneme sürümünü yeniden etkinleştirmek olanaksızdır.

- **Ticari lisansı etkinleştir.** Uygulamanın ticari sürümünü etkinleştirmek için, uygulamayı satın aldığınızda verilen etkinleştirme kodunu kullanmalısınız. Ticari sürümü etkinleştirirken, uygulama size tüm işlevlerine erişim veren bir ticari lisans alır. Lisans geçerlilik süresi aygıtın ekranında görüntülenecektir. Deneme lisansının geçerlilik süresi sona erdiğinde uygulamanın işlevleri sınırlanacaktır ve güncellenemez.

Etkinleştirme kodunu aşağıdaki yollardan edebilirsiniz:

- Kaspersky Mobile Security 9 uygulamasından mobil aygıtlara özel Kaspersky Lab web sitesine giderek çevrimiçi
- Kaspersky Lab eStore'dan (<http://www.kaspersky.com/globalstore>);
- Kaspersky Lab distribütörlerinden
- **Aboneliği etkinleştir.** Aboneliği etkinleştirirken, uygulama abonelik ile bir ticari lisans alır. Abonelik ile ticari lisansın geçerlilik süresi 30 gün ile sınırlıdır. Abonelik etkinleştirildiğinde uygulama lisansı her 30 günde bir yeniler. Lisans yenilediğinde uygulamanın kullanımı için aboneliğin etkinleştirilmesinde belirtilen sabit bir ödeme kişisel hesabınızdan kesilir. Ödenebilir bir SMS mesajı gönderilerek bu tutar borç kaydedilir. Bu tutar borç olarak kaydedildiğinde, uygulama size tüm işlevlerine erişim veren abonelik ile yeni bir lisansı uygulama sunucusundan alır. Kaspersky Mobile Security 9 aboneliğini iptal edebilirsiniz. Bu durumda, geçerli lisansın süresi sona erdiğinde uygulamanın işlevselliği sınırlanacak ve uygulamanın veritabanları artık güncellenmeyecektir.

BU BÖLÜMDE

Ticari sürümü etkinleştirme	25
Kaspersky Mobile Security 9 aboneliğini etkinleştirme	26
Etkinleştirme kodunu çevrimiçi satın alma.....	27
Deneme sürümünü etkinleştirme.....	27

TİCARİ SÜRÜMÜ ETKİNLEŞTİRME

► *Uygulamanın ticari sürümünü etkinleştirme koduyla etkinleştirmek için:*

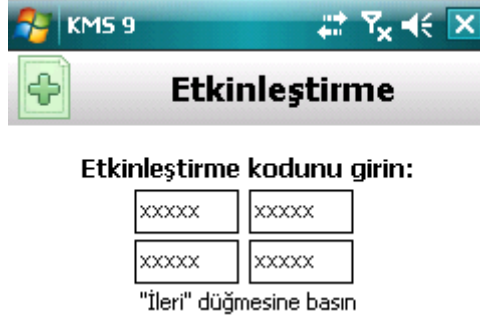
1. **Başlat** → **Uygulamalar** ögesini seçin.
2. Kaleminizi veya kumanda kolunuzun orta düğmesini kullanarak **KMS 9**'u seçin ve uygulamayı başlatın.

Etkinleştirme penceresi açılacaktır.

3. **Kodu gir** ögesini seçin.

Kaspersky Mobile Security 9 etkinleştirme penceresi açılacaktır (bkz. aşağıdaki Şekil).

4. Edinilen etkinleřtirme kodunu drtl alana girin ve ardından **İleri** dğmesini seřin.



řekil 4: Ticari srm etkinleřtirme

5. İnternet baėlantısını **Evet** dğmesine basarak doėrulayın.

Uygulama Kaspersky Lab'ın etkinleřtirme sunucusuna bir istek gnderecek ve bir lisans alacaktır. Lisans bařarıyla alındıėında ekranda lisans hakkında bilgiler grntlenir.

Girdiėiniz etkinleřtirme kodu herhangi bir nedenle geęersizse, ekranda bununla ilgili bir mesaj grntlenir. Bu durumda girilen etkinleřtirme kodunun doėru olduėunun kontrol edilmesini ve Kaspersky Mobile Security 9 rnn satın aldıėınız yazılım tedarikçisiyle iletiřim kumanızı neririz.

Sunucuya baėlanırken hatalar oluřmuřsa ve hiębir lisans alınmamıřsa, etkinleřtirme iptal edilir. Bu durumda İnternete baėlanma parametrelerinin doėrulanması nerilir. Hataları dzeltmek mmkn deėilse, Teknik Destekle iletiřime geęin.

6. Uygulama gizli kodunu oluřturma adımına gidin (bkz. "Gizli kodu oluřturma" blm, sayfa [28](#)).

KASPERSKY MOBILE SECURITY 9 ABONELİĐİNİ ETKİNLEŐTİRME

Aboneliėi etkinleřtirmek ięin aygıtta bir İnternet baėlantısı yapılandırılmıř olmalıdır.

► *Kaspersky Mobile Security 9 aboneliėini etkinleřtirmek ięin:*

1. **Bařlat** → **Uygulamalar** ėesini seřin.
2. Kaleminizi veya kumanda kolunuzun orta dğmesini kullanarak **KMS 9**'u seřin ve uygulamayı bařlatın.
Etkinleřtirme penceresi aęılacaktır.
3. **Tek Tıklamayla Satın Al** ėesini seřin.
4. İnternet baėlantısını **Evet** dğmesine basarak doėrulayın.

Uygulama kullandığınız abonelik hizmetinin mobil hizmet sağlayıcısında erişilebilir olup olmadığını kontrol eder. Abonelik hizmetine erişilebiliyorsa, aboneliğin şartları hakkındaki bilgiler ekranda görüntüleyen **Etkinleştirme** ekranı açılır.

Abonelik hizmeti verilemiyorsa, uygulama bunu size bildirecek ve uygulamayı etkinleştirmek için başka bir yolu seçebileceğiniz ekrana geri döner.

5. Abonelik şartlarını okuyun ve ardından **İleri** düğmesine basarak Kaspersky Mobile Security 9 aboneliğini etkinleştirmeyi onaylayın.

Uygulama bir ödeme SMS'i gönderecek ve Kaspersky Lab'ın etkinleştirme sunucusundan bir lisansı alacaktır. Abonelik etkinleştirilmişse, Mobile Security 9 bunu size bildirecektir.

Bakiyeniz ödeme SMS mesajını göndermek için yeterli değilse, aboneliğin etkinleştirilmesi iptal edilecektir.

Sunucuya bağlanırken hatalar oluşmuşsa ve hiçbir lisans alınmamışsa, etkinleştirme iptal edilir. Bu durumda İnternete bağlanma parametrelerinin doğrulanması önerilir. Hataları düzeltmek mümkün değilse, Teknik Destekle iletişime geçin.

Abonelik şartlarını kabul etmiyorsanız, **İptal** düğmesine basın. Bu durumda, uygulama aboneliğin etkinleştirilmesini iptal eder ve uygulamayı etkinleştirmek için başka bir yolu seçebileceğiniz ekrana geri döner.

6. Gizli kodun girilmesine gidin (bkz: "Gizli kodun ayarlanması" bölümü, sayfa [28](#)).

ETKİNLEŞTİRME KODUNU ÇEVİRİMİÇİ SATIN ALMA

► *Uygulamanın etkinleştirme kodunu çevrimiçi satın almak için aşağıdaki adımları uygulayın:*

1. **Başlat** → **Uygulamalar** ögesini seçin.

2. Kaleminizi veya kumanda kolunuzun orta düğmesini kullanarak **KMS 9**'u seçin ve uygulamayı başlatın.

Etkinleştirme penceresi açılacaktır.

3. **Çevrimiçi satın al** ögesini seçin.

Çevrimiçi satın al penceresi açılacaktır.

4. **Aç** düğmesine basın.

Lisansın süresi sona ermişse, lisansı yenileme siparişi verebileceğiniz özel bir mobil aygıtlar için Kaspersky Lab web sitesi açılır.

5. Yönergeleri adım adım izleyin.

6. Etkinleştirme kodunu satın alma işlemi tamamlandıktan sonra, uygulamanın ticari sürümünün etkinleştirilmesi adımına geçin (bkz. "Ticari sürümün etkinleştirilmesi" bölümü, sayfa [25](#)).

DENEME SÜRÜMÜNÜ ETKİNLEŞTİRME

► *Kaspersky Mobile Security 9'un deneme sürümünü etkinleştirmek için:*

1. **Başlat** → **Uygulamalar** ögesini seçin.

2. Kaleminizi veya kumanda kolunuzun orta düğmesini kullanarak **KMS 9**'u seçin ve uygulamayı başlatın.

Etkinleştirme penceresi açılacaktır.

3. **Deneme sürümü** ögesini seçin.

4. İnternet bağlantısını **Evet** düğmesine basarak doğrulayın.

Uygulama Kaspersky Lab'ın etkinleştirme sunucusuna bir istek gönderecek ve bir lisans alacaktır.

Sunucuya bağlanırken hatalar oluşmuşsa ve hiçbir lisans alınmamışsa, etkinleştirme iptal edilir. Bu durumda İnternete bağlanma parametrelerinin doğrulanması önerilir. Hataları düzeltmek mümkün değilse, Teknik Destekle iletişime geçin.

5. Uygulamanın gizli kodunu girmeye başlayın (bkz. "Gizli kodu oluşturma" bölümü, sayfa [28](#)).

GİZLİ KODU BELİRLEME

Uygulamayı başlattıktan sonra uygulamanın gizli kodunu girmeniz istenecektir. *Uygulama gizli kodu*, uygulama ayarlarına yetkisiz erişilmesini engeller.

Yüklenen gizli kodu daha sonra değiştirebilirsiniz.

Kaspersky Mobile Security 9, aşağıdaki durumlarda gizli kodu sorar:

- uygulamaya erişim için;
- Şifreli dizinlere erişim için;
- Aşağıdaki işlevleri uzaktaki diğer bir aygıttan başlatmak için bir SMS komutu gönderirken: Engelle, Veri Silme, SIM Gözcüsü, GPS Bul, Gizlilik Koruması.
- uygulamayı kaldırırken.

Gizli kod rakamlardan oluşur. En az dört karakter içermelidir.

Eğer uygulama gizli kodunu unutursanız, geri yükleyebilirsiniz (bkz. "Gizli kodu kurtarma" bölümü, sayfa [29](#)). Bu amaçla, daha önceden Gizli kodun kurtarılması seçeneğinin etkinleştirilmesi olması gerekmektedir(bkz. "Gizli kodun kurtarılması seçeneğini etkinleştirme" bölümü, sayfa [28](#)).

► *Gizli kodu kurmak için:*

1. Uygulamayı etkinleştirdikten sonra **Bir kod ayarlayın** giriş alanına kodun karakterlerini girin
2. Aynı kodu, **Onayla** alanına tekrar girin.

Girilen kod otomatik olarak onaylanacaktır.

3. Onaylamanın sonuçlarına göre kod geçersiz sayılırsa, bir uyarı mesajı görüntülenecek ve uygulama doğrulama isteyecektir. Kodu kullanmak için **TAMAM** ögesine basın. Yeni bir kod oluşturmak için **Hayır** düğmesine basın.
4. **Tamam** düğmesine basın.

GİZLİ KODUN KURTARILMASI SEÇENEĞİNİ ETKİNLEŞTİRME

Uygulamanın ilk etkinleştirilmesinden sonra, gizli kodun kurtarılması seçeneğini etkinleştirebilirsiniz. Daha sonra, unutulursa gizli kodu kurtarabilirsiniz.

Uygulamanın ilk etkinleştirilmesi sırasında bu seçeneği iptal ettiyseniz, aygıtta Kaspersky Mobile Security 9'u tekrar kurduktan sonra etkinleştirebilirsiniz.

Yalnızca gizli kodun kurtarılması seçeneği etkinse uygulama gizli kodunu kurtarabilirsiniz (bkz. "Gizli kodu kurtarma" bölümü, sayfa 29). Şifreyi unutursanız ve gizli kodu kurtarma seçeneği devre dışı bırakılmış ise Kaspersky Mobile Security 9 işlevleri yönetilemez, erişim dosyalarına erişilemez veya uygulama kaldırılamaz.

► *Gizli kod seçeneğinin kurtarılmasını etkinleştirmek için:*

1. Uygulama için gizli kodu yükledikten sonra, **Evet** ögesine tıklayarak gizli kodu kurtarma seçeneğinin etkinleştirilmesini onaylayın.
2. E-posta adresinizi **E-posta adresiniz** alanına girin ve **İleri** ögesine basın.

Verdiğiniz e-posta adresi, gizli kodun kurtarılması sırasında kullanılacaktır.

Uygulama, gizli kod kurtarma sunucusuyla bir İnternet bağlantısı kuracak, girdiğiniz bilgileri gönderecek ve gizli kod seçeneğinin kurtarılmasını etkinleştirecektir.

GİZLİ KODUN KURTARILMASI

Gizli kodu yalnızca daha önceden Gizli kodun kurtarılması seçeneğini etkinleştirerek kurtarabilirsiniz (bkz. "Gizli kodun kurtarılması seçeneğini etkinleştirme" bölümü, sayfa 28).

► *Uygulamanın gizli kodunu kurtarmak için:*

1. **Başlat** → **Uygulamalar** ögesini seçin.
2. Kaleminizi veya kumanda kolunuzun orta düğmesini kullanarak **KMS 9**'u seçin ve uygulamayı başlatın.

Gizli kodu gime ekranı açılır.

3. **İptal** düğmesine basın.
4. **Evet** ögesine tıklayarak gizli kod kurtarmaya gidin.

Gizli kod kurtarma ekranında, aşağıdaki bilgiler görüntülenecektir

- Gizli kodun kurtarılması için Kaspersky Lab web sitesi;
- aygıt tanımlama kodu.

5. Gizli kodu kurtarmak için <http://mobile.kaspersky.com/recover-code> web sitesine gidin.

6. Uygun alanlara aşağıdaki bilgileri girin:

- gizli kodun kurtarılması için daha önce verdiğiniz e-posta adresi;

- aygıt tanımlama kodu.

Sonuç olarak gizli kod, belirtmiş olduğunuz e-posta adresine gönderilecektir.

7. **Gizli kod kurtarma** ekranında **Devam** et tuşuna basın ve aldığınız kurtarma kodunu girin.
8. Yeni uygulama gizli kodunu girin. Bunu yapmak için **Bir kod ayarlayın** ve **Onayla** alanına yeni bir uygulama kodu girin.
9. **Tamam** düğmesine basın.

UYGULAMAYI BAŞLATMA

► *Kaspersky Mobile Security 9 uygulamasını başlatmak için:*

1. **Başlat** → **Uygulamalar** ögesini seçin.
2. Kalemizi veya kumanda kolunuzun orta düğmesini kullanarak **KMS 9**'u seçin ve uygulamayı başlatın.
3. Uygulamanın gizli kodunu girin ve **Tamam** düğmesine basın.

Uygulama Kaspersky Mobile Security 9'un geçerli durumunu gösteren bir pencere görüntüleyecektir (bkz. "Koruma durumu penceresi" bölümü, sayfa [39](#)). Uygulama işlevlerine gitmek için, **Menü** düğmesine basın.

UYGULAMANIN VERİTABANLARINI GÜNCELLEME

Kaspersky Mobile Security 9, bilinen tüm kötü amaçlı programların açıklamalarını, etkisiz hale getirme yöntemlerini ve diğer istenmeyen nesnelerin açıklamalarını içeren uygulama veritabanlarını temel olarak tehditlere karşı tarama yapmaktadır. Kurulum anında Kaspersky Mobile Security 9 yükleme paketine dahil olan Anti-Virüs veritabanlarının tarihi geçmiş olabilir.

Uygulama kurulumundan hemen sonra Anti-Virüs veritabanlarını güncellenizi öneririz.

Uygulamanın Anti-Virüs veritabanlarını güncellemek için, mobil aygıtınızda yapılandırılmış bir İnternet bağlantınızın olması gerekir.

► *Anti-virüs veritabanının güncelleme işlemini başlatmak için:*

1. **Menü** → **Anti-Virüs** ögesini seçin.
Anti-Virüs penceresi açılacaktır.
2. **Güncelle** ögesini seçin.
Bu, **Güncelle** penceresini açacaktır.
3. **Güncelle** ögesini seçin.

Uygulama Kaspersky Lab sunucusundan veritabanlarını güncelleme işlemini başlatır. Güncelleme işlemi bilgileri ekranda görüntülenir.

AYGITI VİRÜSLERE KARŞI TARAMA

Uygulamayı kurduktan sonra, mobil aygıtınızda kötü amaçlı nesnelere karşı bir taramayı hemen çalıştırmanız önerilir.

İlk tarama Kaspersky Lab uzmanları tarafından önceden yapılmış ayarlarla gerçekleştirilecektir.

► *Aygıtın tam taramasını çalıştırmak için:*

1. **Menü** → **Anti-Virüs** öğesini seçin.

Anti-Virüs penceresi açılacaktır.

2. **Tara** öğesini seçin.

Anti-Virüs penceresi açılacaktır.

3. **Tam Tara** öğesini seçin.

UYGULAMA HAKKINDAKİ BİLGİLERİ GÖRÜNTÜLEME

Kaspersky Mobile Security 9 ve sürümü hakkında genel bilgileri görebilirsiniz.

► *Lisans bilgilerini görüntülemek için:*

1. **Menü** → **Ek** öğesini seçin.

Ek penceresi açılacaktır.

2. **Hakkında** sekmesini seçin.

LİSANS YÖNETİMİ

Kaspersky Lab uygulamalarının lisansının alınması bağlamında aşağıdaki üç terimi bilmek önemlidir:

- Lisans Sözleşmesi;
- Lisans.

Bu terimler birbirleriyle ayrılmaz biçimde bağlantılıdır ve tek bir lisans verme modelini oluştururlar. Her bir terime yakından bakalım.

Ayrıca Kaspersky Mobile Security 9 lisansı ve geçerlilik süresinin uzatılmasına ilişkin bilgilerin nasıl bulunacağı da bu bölümde anlatılmaktadır.

BU BÖLÜMDE

Lisans sözleşmesi hakkında.....	32
Kaspersky Mobile Security 9 lisansları hakkında.....	32
Lisans Bilgilerini Gör.....	33
Lisansı yenileme.....	34

LİSANS SÖZLEŞMESİ HAKKINDA

Lisans Sözleşmesi Kaspersky Mobile Security 9'un bir kopyasına yasal olarak sahip olan bir özel veya tüzel kişi ile Kaspersky Lab arasındaki bir sözleşmedir. Sözleşme her Kaspersky Lab uygulamasında bulunur. Sözleşme, Kaspersky Mobile Security uygulamasını kullanma hakları ve sınırlamaları hakkında ayrıntılı bilgiler verir.

Bir Kaspersky Lab uygulamasını satın alırken ve kurarken, Lisans Sözleşmesine uygun olarak, uygulamanın bir kopyasına sahip olma sınırsız hakkını elde edersiniz.

Kaspersky Lab size aşağıdaki ek hizmetleri de vermektedir:

- Teknik destek
- Kaspersky Mobile Security 9 anti-virüs veritabanlarının güncelleştirilmesi;
- Kaspersky Mobile Security 9 program modüllerinin güncellenmesi.

Bunlardan yararlanmak için bir lisans satın alarak etkinleştirmelisiniz (bkz. "Kaspersky Mobile Security 9 lisansları hakkında " bölümü, sayfa [32](#)).

KASPERSKY MOBILE SECURITY 9 LİSANSLARI HAKKINDA

Lisans Kaspersky Mobile Security 9 ve Kaspersky Lab veya iş ortakları tarafından sağlandığı şekliyle ilişkili ek hizmetleri kullanma hakkıdır (bkz. "Lisans Sözleşmesi Hakkında" bölümü, sayfa [32](#)).

Her lisansın bir geçerlilik süresi ve türü vardır.

Lisans süresi – ek hizmetlerin sunulduğu süre:

- Teknik destek
- Kaspersky Mobile Security 9 anti-virüs veritabanlarının güncelleştirilmesi;
- Kaspersky Mobile Security 9 program modüllerinin güncellenmesi.

Sağlanan hizmetlerin kapsamı lisansın türüne bağlıdır.

Aşağıdaki lisans türleri mevcuttur:

- *Deneme* – 30 gün gibi sınırlı bir geçerlilik süresine sahip, Kaspersky Mobile Security 9'un tanınması için verilen ücretsiz bir lisans.

Deneme lisansı yalnızca bir kez kullanılabilir.

Deneme lisansınız varsa, Teknik Destek Hizmetiyle yalnızca uygulamayı etkinleştirmek veya bir ticari lisans satın almak için iletişim kurulabilir. Kaspersky Mobile Security 9'un deneme lisansı süresi dolduğunda, tüm özellikler devre dışı kalır. Uygulamayı sürdürmek için etkinleştirmelisiniz (bkz. "Ticari sürümü etkinleştirme" bölümü, sayfa [25](#)).

- *Ticari* – Kaspersky Mobile Security 9 satın alındığında verilen, sınırlı bir geçerlilik süresine (örneğin, bir yıl) sahip ticari lisans.

Ticari lisans etkinleştirilmişse, tüm uygulama özellikleri ve ek hizmetler kullanılabilir.

Ticari lisansın geçerlilik süresi sona erdiğinde, Kaspersky Mobile Security 9'un bazı işlevlerine ulaşılamaz ve uygulama veritabanları güncelleştirilmez. Sona erme tarihinden bir hafta önce lisansı yenileyebilmeniz için uygulama bu durumu size bildirir.

- *Abonelik ile ticari* – otomatik veya elle modunda yenileme seçeneğiyle ödemeli lisans. Abonelik ile lisans hizmet sağlayıcılar tarafından dağıtılmaktadır.

Abonelik sınırlı bir süreyle (30 gün) geçerlidir. Abonelik sona erdikten sonra elle veya otomatik olarak yenilenebilir. Aboneliğin yenilenme yöntemi mevzuata ve mobil hizmet sağlayıcıya bağlıdır. Aboneliğin yenilenmesi sağlayıcıya vaktinde peşin ödeme yapılmasına bağlıdır.

Bu durumda abonelik şartlarında belirtilen sabit tutar kişisel hesabınızdan kesilir. Hizmet sağlayıcının numarasına bir ödeme SMS'i göndermeniz ardından bu tutar kişisel hesabınızdan kesilir.

Abonelik yenilenmezse, Kaspersky Mobile Security 9 uygulama anti-virüs veritabanlarını güncellemeyi durdurur, uygulamanın işlevselliği sınırlanır.

Aboneliği kullanırken ticari lisansı etkinleştirme koduyla etkinleştirebilirsiniz. Bu durumda abonelik otomatik olarak iptal edilecektir.

Ticari lisans kullanırken aboneliği etkinleştirebilirsiniz. Abonelik etkinleştirilmesi sırasında sınırlı süreye sahip bir lisansı zaten etkinleştirmişseniz, bunun yerini abonelik lisansı alır.

LİSANS BİLGİLERİNİ GÖRÜNTÜLEME

Aşağıdaki lisans bilgilerini görebilirsiniz: lisans numarası, türü, sona ermeye kadar geçen gün sayısı, etkinleştirme tarihi ve aygıt seri numarası.

► *Lisans bilgilerini görüntülemek için:*

1. **Menü** → **Ek** ögesini seçin.

Ek penceresi açılacaktır.

2. **Lisans** ögesini seçin.

Lisans penceresi açılacaktır.

3. **Lisans** hakkında ögesini seçin.

LİSANSI YENİLEME

Kaspersky Mobile Security 9 uygulamanın lisansını yenilemenize olanak tanır.

Lisans aşağıdaki yollardan biri kullanılarak uzatılabilir:

- Etkinleştirme kodunu girin – uygulamayı etkinleştirme koduyla etkinleştirin. Etkinleştirme kodunu <http://www.kaspersky.com/globalstore> web sitesinden veya yerel Kaspersky Lab distribütörünüzden satın alabilirsiniz.
- Etkinleştirme kodunu çevrimiçi satın alın – mobil aygıtınız tarafından ziyaret edilen web sitesine gidin ve bir etkinleştirme kodunu çevrimiçi satın alın.
- Kaspersky Mobile Security 9'a abone olun – lisansı her 30 günde bir otomatik olarak yenilemek için aboneliğini etkinleştirin.

Mobil aygıtınızdaki uygulamayı etkinleştirmek için, yapılandırılmış bir İnternet bağlantınızın olması gerekir.

BU BÖLÜMDE

Lisansı etkinleştirme koduyla yenileme	34
Lisansı çevrimiçi yenileme.....	36
Lisansı aboneliği etkinleştirerek yenileme	36
Aboneliği kaldırma.....	38
Aboneliği yenileme	39

LİSANSI ETKİNLEŞTİRME KODUYLA YENİLEME

► *Lisansı etkinleştirme koduyla yenilemek için:*

1. **Menü** → **Ek** ögesini seçin.

Ek penceresi açılacaktır.

2. **Lisans** ögesini seçin.

Lisans penceresi açılacaktır.

3. **Yenile** ögesini seçin.

Yenile penceresi açılacaktır.

4. Edinilen etkinleştirme kodunu dördü alana girin ve ardından **İleri** düğmesini seçin (bkz. aşağıdaki Şekil).



Şekil 5: Lisansı etkinleştirme koduyla yenileme

5. İnternet bağlantısını **Evet** düğmesine basarak doğrulayın.

Uygulama Kaspersky Lab'ın etkinleştirme sunucusuna bir istek gönderecek ve bir lisans alacaktır. Lisans başarıyla alındığında ekranda lisans hakkında bilgiler görüntülenir.

Girdiğiniz etkinleştirme kodu herhangi bir nedenle geçersizse, ekranda bununla ilgili bir mesaj görüntülenir. Bu durumda girilen etkinleştirme kodunun doğru olduğunun kontrol edilmesini ve Kaspersky Mobile Security 9 ürününü satın aldığınız yazılım tedarikçisiyle iletişim kurmanızı öneririz.

Sunucuya bağlanırken hatalar oluşmuşsa ve hiçbir lisans alınmamışsa, etkinleştirme iptal edilir. Bu durumda İnternete bağlanma parametrelerinin doğrulanması önerilir. Hataları düzeltmek mümkün değilse, Teknik Destekle iletişime geçin.

6. Tamamlandığında **Tamam** düğmesine basın.

LİSANSI ÇEVİRİMİÇİ YENİLEME

► *Lisansı çevrimiçi yenilemek için:*

1. **Menü** → **Ek** öğesini seçin.

Ek penceresi açılacaktır.

2. **Lisans** öğesini seçin.

Lisans penceresi açılacaktır.

3. **Çevrimiçi yenile** öğesini seçin. Geçerlilik süresi sona ermişse, menü öğesi **Çevrimiçi satın al** olarak değişir.

Çevrimiçi yenile penceresi açılır.

4. **Aç** düğmesine basın (bkz. aşağıdaki Şekil).



Şekil 6: Lisansı çevrimiçi yenileme

Lisansı yenileme siparişi verebileceğiniz bir web sitesi açılır.

Lisansın süresi sona ermişse, bir etkinleştirme kodunu çevrimiçi satın alabileceğiniz mobil aygıtlar için Kaspersky Lab web sitesi açılır.

5. Yönergeleri adım adım izleyin.
6. Lisans yenileme siparişi tamamlandığında, aldığınız etkinleştirme kodunu girin (bkz. "Lisansı etkinleştirme koduyla yenileme" bölümü, sayfa [34](#)).

LİSANSI ABONELİĞİ ETKİNLEŞTİREREK YENİLEME

Ek menüsünde Kaspersky Mobile Security 9 için aboneliği etkinleştirerek lisansın geçerlilik süresini uzatabilirsiniz (bkz. "Kaspersky Mobile Security 9 lisansları hakkında" bölümü, sayfa 32). Abonelik etkinleştirildiğinde Kaspersky Mobile Security 9 lisansı her 30 günde bir yeniler. Lisans her yenilediğinde, abonelik şartlarında belirtilen sabit tutar kişisel hesabınızdan kesilir.

Kaspersky Mobile Security 9 uygulamasını etkinleştirmek için bir İnternet bağlantısının kurulmuş olması gerekir.

► *Kaspersky Mobile Security 9 aboneliğini etkinleştirmek için:*

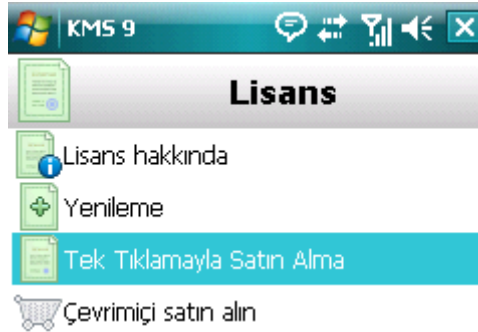
1. **Menü** → **Ek** ögesini seçin.

Ek penceresi açılacaktır.

2. **Lisans** ögesini seçin.

Lisans penceresi açılacaktır.

Tek Tıklamayla Satın al sekmesini seçin (aşağıdaki şekle bakınız).



Şekil 7: Aboneliği etkinleştirme

3. İnternet bağlantısını **Evet** düğmesine basarak doğrulayın.

Uygulama kullandığınız abonelik hizmetinin mobil hizmet sağlayıcısında erişilebilir olup olmadığını kontrol eder.

Abonelik hizmetine erişilebiliyorsa, aboneliğin şartları hakkındaki bilgiler ekranda görüntüleyen **Etkinleştirme** ekranı açılır.

Abonelik hizmeti verilemiyorsa, uygulama bu olay hakkında sizi bilgilendirecek ve lisansı yenilemek için başka bir yolu seçebileceğiniz ekrana geri dönecektir. Aboneliğin etkinleştirilmesi iptal edilecektir.

4. Abonelik şartlarını okuyun ve ardından **İleri** düğmesine basarak Kaspersky Mobile Security 9 aboneliğini etkinleştirmeyi onaylayın.

Uygulama bir ödeme SMS'i gönderecek ve Kaspersky Lab'in etkinleştirme sunucusundan bir lisansı alacaktır. Abonelik etkinleştirilmişse, Mobile Security 9 bunu size bildirecektir.

Bakiyeniz ödeme SMS mesajını göndermek için yeterli değilse, aboneliğin etkinleştirilmesi iptal edilecektir.

Sunucuya bağlanırken hatalar oluşmuşsa ve hiçbir lisans alınmamışsa, etkinleştirme iptal edilir. Bu durumda İnternete bağlanma parametrelerinin doğrulanması önerilir. Hataları düzeltmek mümkün değilse, Teknik Destekle iletişime geçin.

Abonelik şartlarını kabul etmiyorsanız, **İptal** düğmesine basın. Bu durumda, uygulama aboneliğin etkinleştirilmesini iptal edecek ve lisansı yenilemek için başka bir yolu seçebileceğiniz ekrana geri dönecektir.

5. Tamamlandığında **Tamam** düğmesine basın.

ABONELİĞİ KALDIRMA

Kaspersky Mobile Security 9 aboneliğini iptal edebilirsiniz. Bu durumda, Kaspersky Mobile Security 9 lisansı her 30 günde bir yenilemeyecektir. Geçerli lisansın süresi sona erdiğinde uygulamanın işlevselliği sınırlanacak ve uygulama veritabanları artık güncellenmeyecektir.

Aboneliğinizi iptal ettiyseniz, onu devam ettirebilirsiniz (bkz. "Aboneliği Yenileme" bölümü, sayfa [39](#)).

► *Kaspersky Mobile Security 9 aboneliğini iptal etmek için:*

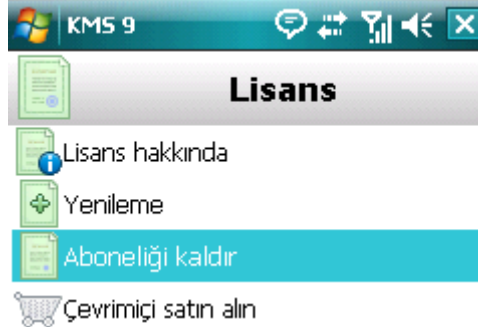
1. **Menü** → **Ek** ögesini seçin.

Ek penceresi açılacaktır.

2. **Lisans** ögesini seçin.

Lisans penceresi açılacaktır.

3. **Aboneliği kaldır** ögesini seçin (bkz. aşağıdaki şekil).



Şekil 8: Aboneliği kaldırma

- Aboneliğin iptal edildiğini **Evet** düğmesine basarak doğrulayın.

Kaspersky Mobile Security 9 aboneliğin iptal edildiğini size bildirecektir.

ABONELİĞİ YENİLEME

Aboneliği iptal ettiyseniz, onu yeniden başlatabilirsiniz (bkz. "Aboneliği Yenileme" bölümü, sayfa [38](#)). Bu durumda, Kaspersky Mobile Security 9 lisansı her 30 günde bir yenileyecektir.

Aboneliği yeniden başlatırken, geçerli lisansın süresi üç günden daha kısa bir süre içinde sona erecekse, bedeli kişisel hesabınızdan kesilecektir.

► Aboneliği yeniden başlatmak için:

- Menü** → **Ek** öğesini seçin.

Ek penceresi açılacaktır.

- Lisans** öğesini seçin.

Lisans penceresi açılacaktır.

- Tek Tıklatmayla Satın Al** sekmesini seçin.

Geçerli lisansınızın süresi sona ermişse, Kaspersky Mobile Security 9 aboneliği yeniden etkinleştirme olanağını sunacaktır (bkz. "Lisansı yenileme" bölümü, sayfa [34](#)).

Geçerli lisansın süresi henüz sona ermemişse, Kaspersky Mobile Security 9 aboneliği yeniden başlatır ve geçerli lisansın süresi sona erdikten sonra her 30 günde bir aboneliği yeniler.

UYGULAMA ARAYÜZÜ

Bu bölümde, Kaspersky Mobile Security 9 arabiriminin ana unsurları hakkında bilgi verilmektedir.

BU BÖLÜMDE

Koruma durumu penceresi	39
Uygulama menüsü	41

KORUMA DURUMU PENCERESİ

Uygulamanın ana bileşenlerinin durumu geçerli durum penceresinde görüntülenir.

Her bileşen için, her biri trafik ışıkları koduna benzer özel spesifik bir renkle görüntülenen üç olası durum vardır. Yeşil ışık aygıtınızın korumasının gerekli düzeyde sağlandığı anlamına gelir. Sarı ve kırmızı, çeşitli tehdit türlerini belirtmektedir. Tehditler yalnızca tarihi geçmiş Anti-Virüs uygulaması veritabanlarını içermekle kalmamakta, aynı zamanda örneğin devre dışı bırakılmış koruma bileşenleri ve minimum uygulama işlem ayarlarını da içermektedir.

Uygulama başlatıldıktan sonra durum penceresine hemen erişilebilir ve pencerede aşağıdaki bilgiler bulunur:

- **Koruma** gerçek zamanlı koruma modundaki koruma durumudur (bkz. "Dosya sistemi koruması" bölümü, sayfa [43](#)).

Yeşil durum simgesi, korumanın etkin ve doğru seviyede ayarlanmış olduğunu ve uygulamanın Anti-Virüs veritabanlarının güncel olduğunu göstermektedir.

Sarı simge veritabanlarının birkaç gündür güncellenmediğini belirtir.

Kırmızı simge rengi bilgi kaybıyla veya aygıtı virüs bulaşmasıyla sonuçlanabilecek sorunlar olduğunu belirtir. Örneğin, koruma kapatılmıştır. Uygulamanın veritabanları 15 günden daha uzun bir süre boyunca güncellenmemiş olabilir.

- **Güvenlik Duvarı** aygıtın istenmeyen ağ etkinliğinden korunma düzeyidir (bkz. "Ağ etkinliğini filtreleme. Güvenlik Duvarı" bölümü, sayfa [98](#)).

Yeşil durum simgesi bileşenin etkin olduğunu gösterir. Güvenlik Duvarının koruma düzeyi seçilmiştir.

Kırmızı simge, ağ etkinliğinin filtrelenmediğini belirtir.

- **Hırsızlığa Karşı Koruma** - aygıtın kaybolması veya çalınması halinde veri koruması durumu (bkz. "Aygıtın kaybolması veya çalınması durumunda veri koruması" bölümü, sayfa [78](#)).

Yeşil durum simgesi Hırsızlığa Karşı Koruma bileşenini etkin olduğu anlamına gelir; adı bileşenin durumunun altında görüntülenir.

Kırmızı simge, Hırsızlığa Karşı Korumanın tüm işlevlerinin devre dışı bırakıldığını gösterir.

- **Gizlilik Koruması** gizli verilerin korunma durumudur (bkz. "Kişisel verileri gizleme" bölümü, sayfa [89](#)).

Yeşil durum simgesi bileşenin etkin olduğunu gösterir. Gizli veriler gizlenir.

Sarı renkli durum simgesi bileşenin devre dışı bırakıldığını gösterir. Kişisel veriler görüntülenir ve görüntülenmek üzere erişilebilirler.

- **Lisans**, lisansın geçerlilik süresidir (bkz. "Lisans yönetimi" bölümü, sayfa [32](#)).

Yeşil durum simgesi lisansın geçerlilik süresinin 14 günden daha uzun bir süre sonra sona ereceği anlamına gelir.

Sarı durum simgesi lisansın geçerlilik süresinin 14 günden daha kısa bir süre sonra sona ereceği anlamına gelir.

Kırmızı simge lisansınızın sona erdiği anlamına gelir.



Şekil 9: Uygulama bileşeni durum penceresi

Durum penceresine **Menü** → **Koruma durumu** öğesini seçerek de gidebilirsiniz.

UYGULAMA MENÜSÜ

Uygulama bileşenleri mantıksal olarak gruplandırılır ve uygulama menüsünden erişilebilir. Her menü öğesi seçilen bileşenin ve koruma görevlerinin parametrelerine gidilmesini sağlar (bkz. aşağıdaki Şekil).



Şekil 10: Uygulama menüsü

Kaspersky Mobile Security 9 menüsünde aşağıdaki öğeler bulunur:

- **Anti-Virüs:** Virüslere karşı dosya sisteminin korunması, istek üzerine tarama ve uygulamanın anti-virüs veritabanlarını güncelleme.
- **Hırsızlığa Karşı Koruma:** Kaybolur veya çalınırsa aygıtı bloke etme ve içindeki bilgileri silme.
- **Gizlilik Koruması:** Aygıttaki gizli verileri gizleme.
- **Şifreleme:** Şifrelemeyi kullanarak aygıttaki bilgileri koruma.
- **Arama/SMS Filtresi:** İstenmeyen gelen aramaları ve SMS'leri filtreleme.
- **Ebeveyn Denetimi:** Giden aramaların ve SMS mesajlarının denetimi.
- **Güvenlik Duvarı:** Ağa bağlandığında aygıtı koruma.
- **Ek:** genel uygulama ayarları, uygulama hakkında bilgiler, kullanımdaki veritabanları ve lisans.
- **Koruma durumu:** Aygıtın koruma durumu hakkında bilgi.
- **Çıkış:** Uygulamadan çıkış.

➤ *Uygulama menüsünü açmak için:*

Menü ögesini seçin.

Uygulama menüsünde gezinmek için aygıtın kumanda kolunu veya kalemi kullanın.

➤ *Uygulamaya geri dönmek için:*

Menü → **Koruma durumu** ögesini seçin.

➤ *Uygulamadan çıkmak için:*

Menü → **Çık** ögesini seçin.

DOSYA SİSTEMİ KORUMASI

Bu bölüm, aygıtınızın dosya sistemine virüslerin bulaşmasından sakınmayı sağlayan Koruma bileşeni hakkında bilgiler vermektedir. Aynı zamanda Korumanın nasıl etkinleştirileceği / durdurulacağı ve çalışma ayarlarının nasıl yapılacağı da bu bölümde anlatılmaktadır.

BU BÖLÜMDE

Koruma hakkında	43
Korumayı etkinleştirme ve devre dışı bırakma.....	43
Seçilen nesnelere uygulanacak işlemin seçilmesi	45

KORUMA HAKKINDA

Koruma, işletim sistemi başladığında başlamakta ve her zaman aygıt belleğinde bulunmaktadır. Koruma, açılan, kaydedilen ya da çalıştırılan tüm dosyaları taramaktadır. Dosyalar aşağıdaki algoritmaya göre taranır:

1. Koruma, kullanıcı değerlendirdiğinde tüm dosyaları taramaktadır.
2. Koruma, kötü amaçlı nesnelere varlığına karşı dosyayı analiz etmektedir. Kötü amaçlı nesnelere, uygulamanın Anti-Virüs veritabanları tarafından karşılaştırma ile tespit edilmektedir. Anti-Virüs veritabanları, halihazırda bilinen tüm zararlı nesnelere açıklamalarını ve bunların etkisiz hale getirilmesi yöntemlerini içermektedir.
3. Analiz sonuçlarına göre aşağıdaki Koruma türleri mümkündür:
 - Dosyada kötü amaçlı kod tespit edilirse, Koruma bu dosyaya erişimi engeller ve ayarlarda belirtilen işlemi uygular.

Dosyada hiçbir kötü amaçlı kod bulunmazsa, hemen geri yüklenecektir. Tarama sonuçlarına ilişkin bilgiler uygulamanın günlüğüne kaydedilir (bkz. "Uygulama günlükleri" bölümü, sayfa [112](#)).

KORUMAYI ETKİNLEŞTİRME VE DEVRE DIŞI BIRAKMA

Koruma etkinleştirildiğinde sistemdeki tüm işlemler kalıcı bir denetim altına alınır.

Aygıt kaynakları, virüslere ve diğer tehditlere karşı korumanın sağlanması için kullanılmaktadır. Aygıtın yükünü azaltmak için, bazı görevleri yürütürken Korumayı geçici olarak durdurabilirsiniz.

Kaspersky Lab uzmanları bilgisayarınıza virüs bulaşmasına ve veri kaybına neden olabileceği için, korumayı devre dışı bırakmamanızı önerir.

Korumanın Devre Dışı Bırakılması, virüs taraması görevlerinin yürütülmesini ve uygulama Anti-Virüs veritabanlarının güncellenmesini etkilememektedir.

Geçerli Koruma durumu **Anti-Virüs** penceresinde **Koruma** öğesinin yanında görüntülenir.

Korumayı aşağıdaki yollardan etkinleştirebilirsiniz:

- Bileşen ayarları menüsünden;
- **Anti-Virüs** menüsünden.

Ayarların değerlerini değiştirmek için, aygıtın kumanda kolunu veya kalemı kullanın.

► *Korumayı etkinleştirmek için:*

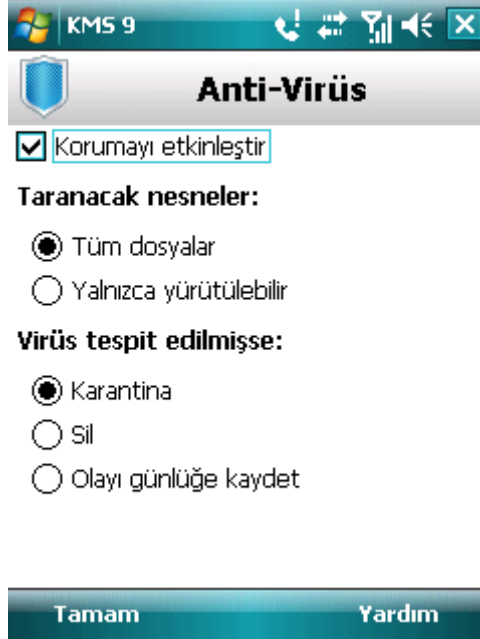
1. **Menü** → **Anti-Virüs** ögesini seçin.

Anti-Virüs penceresi açılacaktır.

2. **Koruma** ögesini seçin.

Ayarlar penceresi açılacaktır.

3. **Korumayı etkinleştir** kutusunu işaretleyin (bkz. aşağıdaki Şekil).



Şekil 11: Korumayı etkinleştirme

4. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

► *Korumayı devre dışı bırakmak için:*

1. **Menü** → **Anti-Virüs** ögesini seçin.

Anti-Virüs penceresi açılacaktır.

2. **Koruma** ögesini seçin.

Ayarlar penceresi açılacaktır.

3. **Korumayı etkinleştir** kutusunun işaretini kaldırın.

4. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

➔ *Gizlilik Korumasını hızlı etkinleştirmek / devre dışı bırakmak için:*

1. **Menü** → Anti-Virüs ögesini seçin.
2. **Anti-Virüs** penceresi açılacaktır.
3. **Etkinleştir / Kapat** bırak düğmesine basın. Korumanın geçerli durumuna bağlı olarak düğmenin adı aksiyile değişecektir.

SEÇİLEN NESNELERDE UYGULANACAK İŞLEMİN SEÇİLMESİ

Kaspersky Mobile Security 9 bulunan kötü amaçlı nesnelere varsayılan olarak karantinaya yerleştirir. Kaspersky Mobile Security 9'un kötü amaçlı bir nesne tespit ettiğinde gerçekleştirdiği işlemi seçebilirsiniz.

Ayarların değerlerini değiştirmek için, aygıtın kumanda kolunu veya kalemi kullanın.

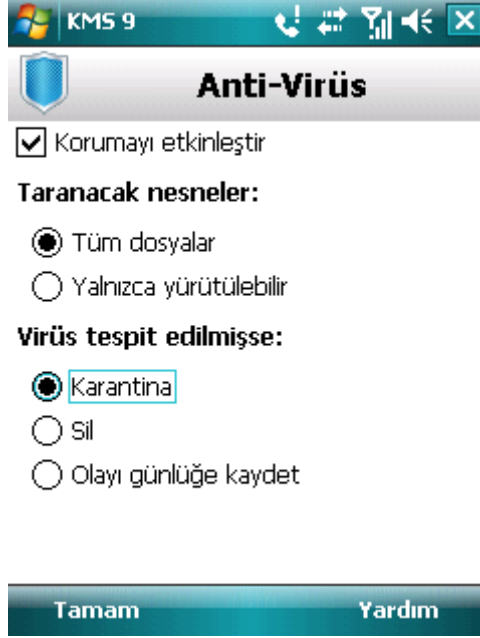
Koruma ayarlarının değerlerini değiştirmek için, etkinleştirildiğinden emin olun.

➔ *Programın kötü amaçlı bir nesne tespit ettiğinde vereceği yanıtı yapılandırmak için:*

1. **Menü** → **Anti-Virüs** ögesini seçin.
Anti-Virüs penceresi açılacaktır.
2. **Koruma** ögesini seçin.
Ayarlar penceresi açılacaktır.

3. Uygulamanın kötü amaçlı bir nesne bulduğunda yapacağı işlemi ayarlayın. Bunun için, **Virüs tespit edilmişse** ayarı için bir değer seçin (bkz. aşağıdaki Şekil):
- **Karantina:** Kötü amaçlı nesnelere karantinaya alır.
 - **Sil:** Kötü amaçlı nesnelere kullanıcıya bildirmeden siler.

Olayı günlüğe kaydet: kötü amaçlı nesnelere işlemez ve bunların tespit edilmeleriyle ilgili bilgileri uygulamanın günlüğüne kaydeder; kullanma (örneğin, kopyalama veya açma) girişiminde bulunulduğunda engeller.



Şekil 12: Kötü amaçlı nesnelere uygulanacak işlemi seçme

4. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

AYGITI TARAMA

Bu bölümde, aygıtınızdaki tehditlerin algılanması ve temizlenmesi işlevini gerçekleştiren, aygıtta isteğe bağlı olarak tarama yapma işlemi hakkında bilgi verilmektedir. Bu bölümde, aygıtta tarama başlatma, otomatik programlı dosya sistemi taraması ayarlama, taranacak dosyaları seçme ve kötü amaçlı bir nesne tespit edildiğinde uygulamanın yapacağı işlemi belirleme gibi konular da anlatılmaktadır.

BU BÖLÜMDE

Tespit edilen nesnelere uygulanacak eylemi seçme	47
Bir taramayı elle başlatma	48
Zamanlanmış taramayı başlatma	49
Taranacak nesne türünü seçme	50
Arşiv taramalarını yapılandırma	51
Seçilen nesnelere uygulanacak işlemin seçilmesi	52

TESPİT EDİLEN NESNELERE UYGULANACAK EYLEMİ SEÇME

İstek üzerine tarama hakkında, Kaspersky Mobile Security 9 aygıtın dosya sisteminin tamamen ya da kısmen - yani yalnızca aygıtın entegre belleğinin ya da spesifik bir dizininin (bellek kartındakiler dahil) içeriğinin taranması - taramasının gerçekleşmesini sağlar.

Aygıt, aşağıdaki şekilde taranmaktadır.

1. Kaspersky Mobile Security 9 belirlenen dosya türlerini tarar (bkz. "Taranacak nesne türlerini seçme" bölümü, sayfa [50](#)).
2. Her dosya, kötü amaçlı nesnelere (kötü amaçlı yazılımlar) varlığına karşı taranır. Kötü amaçlı nesnelere, uygulamanın Anti-Virüs veritabanları tarafından karşılaştırma ile tespit edilmektedir. Anti-Virüs veritabanları, bilinen tüm zararlı nesnelere açıklamalarını ve bunların etkisiz hale getirilmesi yöntemlerini içermektedir.

Analiz sonrasında Kaspersky Mobile Security 9, aşağıdaki adımları atmaktadır.

- Dosyada zararlı kod tespit edilmesi durumunda, Kaspersky Mobile Security 9 dosyaya erişimi önler ve ayarlarda belirtilen işlemi gerçekleştirir (bkz: "Nesnelere gerçekleştirilecek adımların seçilmesi" bölümü - sayfa [52](#)).
- Dosyada kötü amaçlı kod tespit edilmezse, dosya anında işlem için erişilebilir hale gelir.

Bir tarama görevi elle veya önceden ayarlanan çizelgeye göre otomatik olarak başlatılır (bkz. "Zamanlanmış bir görevi başlatma" bölümü, sayfa [49](#)).

İstek üzerine tarama sonuçlarına ilişkin bilgiler uygulamanın günlüğüne kaydedilir (bkz. "Uygulama günlükleri" bölümü, sayfa [112](#)).

BİR TARAMAYI ELLE BAŞLATMA

İstek üzerine taramayı istediğiniz zaman elle başlatabilirsiniz: Bunun için en iyi zaman aygıtın işlemcisinin başka görevleri yerine getirmekle meşgul olmadığı zamandır.

► *Anti-virüs taramasını elle başlatmak için:*

1. **Menü** → **Anti-Virüs** ögesini seçin.

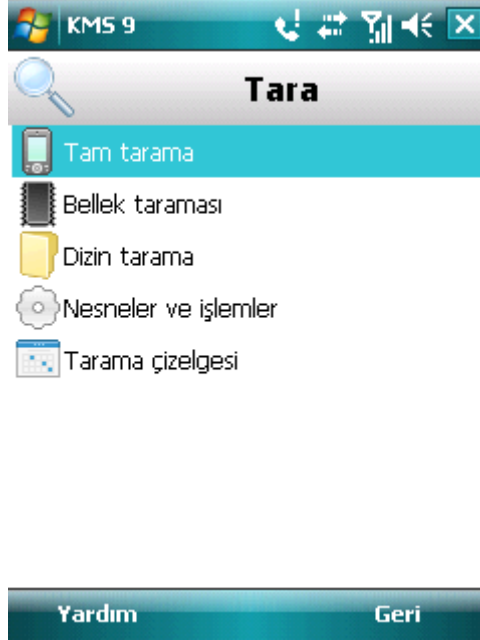
Anti-Virüs penceresi açılacaktır.

2. **Tara** ögesini seçin.

Anti-Virüs penceresi açılacaktır.

3. Aygıt tarama alanını seçin (bkz. aşağıdaki şekil).

- **Tam tarama:** Aygıtın dosya sisteminin tümü taranır. Aşağıdaki nesnelere varsayılan olarak taranır: Aygıt belleği ve depolama kartı.
- **Bellek tarama:** sistem belleğinde başlatılan işlemler ve ilgili dosyalar taranır.
- **Dizin tarama:** Aygıtın dosya sisteminde veya bellek kartında bulunan ayrı bir nesne taranır. **Dizin tarama** ögesi seçildiğinde, aygıtın dosya sistemini gösteren bir pencere açılır. Dosya sistemi içinde gezinmek için kumanda kolu düğmelerini veya kalem kullanın. Dizin taramayı başlatmak için, gerekli dizini ve **Tara** ögesini seçin.



Şekil 13: Tarama alanını seçme

Tarama başlatıldığında tarama işlemi penceresi açılır ve taranan nesnelere sayısı, o sırada taranan nesnenin yolu ve taramanın tamamlanma yüzdesini veren bir göstereyi içeren taramanın durumu görüntülenir.

Kaspersky Mobile Security 9 virüs bulaşmış bir nesneyi tespit ederse, ayarlanan tarama parametrelerine göre bir eylem gerçekleştirir (bkz. "Nesnelere uygulanacak eylemi seçme" bölümü, sayfa [52](#)).

Varsayılan olarak, Kaspersky Mobile Security 9 bir tehdit tespit ederse, onu karantinaya alır.

Tarama tamamlandığında aşağıdaki bilgilerle birlikte toplam istatistikler ekranda görüntülenir:

- Taranmış nesne sayısı
 - Tespit edilen, karantinaya alınan veya silinen virüslerin sayısı
 - geçen nesnelerin sayısı (örneğin, işletim sistemi tarafından bir dosya engellendiğinde veya yalnızca yürütülebilir program dosyaları taranırken, bir dosya yürütülemez ise)
 - tarama süresi.
4. Tamamlandığında **Tamam** düğmesine basın.

ZAMANLANMIŞ TARAMAYI BAŞLATMA

Kaspersky Mobile Security 9 taramaların otomatik olarak başlatılacağı zamanların bir çizelgesinin oluşturulmasına olanak verir. Taramalar arka plan modunda gerçekleştirilir. Virüslü bir nesne tespit edildiğinde, tarama ayarlarında seçilen eylem uygulanır (bkz. "Nesnelere uygulanacak işlemi seçme" bölümü, sayfa [52](#)).

Zamanlanmış taramalar varsayılan olarak devre dışı bırakılmıştır.

► Zamanlanmış bir taramayı yapılandırmak için

1. **Menü** → **Anti-Virüs** ögesini seçin.
Anti-Virüs penceresi açılacaktır.
2. **Tara** ögesini seçin.
Anti-Virüs penceresi açılacaktır.
3. **Tarama çizelgesi** ögesini seçin.
Çizelge ekranı açılacaktır.
4. **Çizelgeye göre** tara ögesini işaretleyin (bkz. aşağıdaki Şekil).
5. **Sıklık** ayarı için değerlerden birini seçin:
 - **Günlük:** Tarama her gün gerçekleştirilir. Taramanın başlatılacağı saati ayarlamak için giriş alanında **Zaman** değerini belirtin.

- **Haftalık:** tarama haftada bir gerçekleştirilir. Specify the **Time** and **Day of the week**.

Şekil 14: Bir otomatik tarama planı yapılandırma

6. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

TARANACAK NESNE TÜRÜNÜ SEÇME

Kötü amaçlı koda karşı hangi nesne türlerinin taranacağını belirtebilirsiniz.

Ayarların değerlerini değiştirmek için, aygıtın kumanda kolunu veya kalem kullanın.

➔ *Taranacak nesnelere seçim için:*

1. **Menü** → **Anti-Virüs** öğesini seçin.

Anti-Virüs penceresi açılacaktır.

2. **Tara** öğesini seçin.

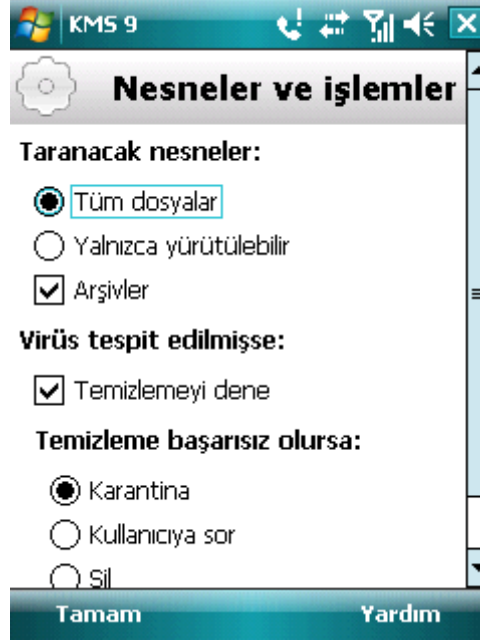
Anti-Virüs penceresi açılacaktır.

3. **Nesneler ve eylemler** öğesini seçin.

Nesneler ve işlemler penceresi açılacaktır.

4. Taranacak nesneleri **Taranacak nesneler** bloğunda seçin (bkz. aşağıdaki Şekil).

- **Tüm dosyalar** - tüm dosya türlerini tara.
- **Yalnızca Yürütülebilirler** – yalnızca aşağıdaki biçimler için yürütülebilir uygulama dosyalarını kontrol eder: EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS.



Şekil 15: Koruma nesnelerini seçme

5. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

ARŞİV TARAMALARINI YAPILANDIRMA

Virüsler genellikle arşivlerde saklanır. Program, şu arşiv formatlarını tarar: ZIP, JAR, JAD ve CAB. Arşivler, İstek üzerine Tarama hızını önemli ölçüde azaltabilecek tarama sırasında açılmaktadır.

İstek üzerine Tarama sırasında kötü amaçlı kod arşivi taramasını etkinleştirebilir / devre dışı bırakabilirsiniz.

Ayarların değerlerini değiştirmek için, aygıtın kumanda kolunu veya kalemi kullanın.

► **Arşiv taramasını etkinleştirmek için:**

1. **Menü** → **Anti-Virüs** ögesini seçin.

Anti-Virüs penceresi açılacaktır.

2. **Tara** ögesini seçin.

Anti-Virüs penceresi açılacaktır.

3. **Nesneler ve eylemler** ögesini seçin.

Nesneler ve işlemler penceresi açılacaktır.

4. **Taranacak nesnelere** bloğunda **Arşivler** kutusunun işaretini kaldırın.
5. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

SEÇİLEN NESNELERDE UYGULANACAK İŞLEMİN SEÇİLMESİ

Varsayılan olarak, Kaspersky Mobile Security 9 virüslü nesnelere karantinaya yerleştirir. Kötü amaçlı bir nesne tespit edildiğinde uygulamanın gerçekleştireceği eylemi değiştirebilirsiniz.

Ayarların değerlerini değiştirmek için, aygıtın kumanda kolunu veya kalem kullanın.

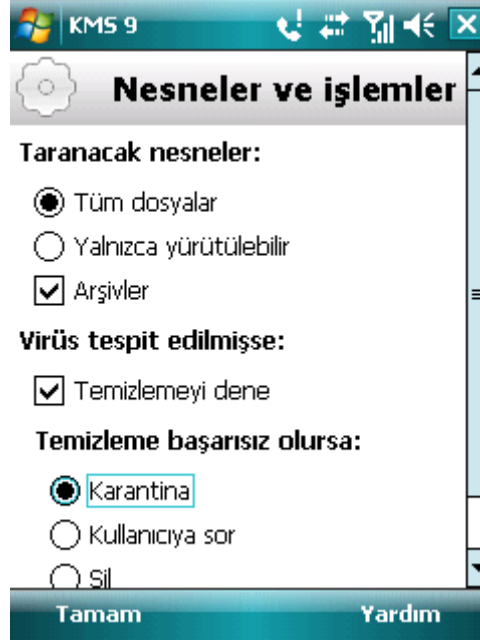
► *Programın kötü amaçlı bir nesne tespit ettiğinde vereceği yanıtı yapılandırmak için:*

1. **Menü** → **Anti-Virüs** ögesini seçin.
Anti-Virüs penceresi açılacaktır.
2. **Tara** ögesini seçin.
Anti-Virüs penceresi açılacaktır.
3. **Nesneler ve eylemler** ögesini seçin.
Nesneler ve işlemler penceresi açılacaktır.
4. Uygulamanın virüslü bir nesneyi temizlemeyi denemesini istiyorsanız, **Virüs tespit edilmişse** ayarının yanındaki **Temizlemeyi dene** kutusunu işaretleyin.
5. Tespit edilen kötü amaçlı nesneye ilişkin bir eylem ayarlayın. Bunun için, **İşlemi uygula** ayarı için bir değer seçin:

Eğer **Temizlemeyi dene** kutusu önceden işaretlenmişse, bu ayarın başlığı **Temizleme başarısız olursa** haline gelir. Nesnenin düzeltilmesi başarılı olmasa bile bu ayar programın eylemini belirler.

- **Karantina:** nesnelere karantinaya alır.
- **Kullanıcıya sor:** kötü amaçlı bir nesne tespit edildiğinde işlemleri kullanıcıya sorar.
- **Sil:** Kötü amaçlı nesnelere kullanıcıya bildirmeden siler.

- **Olayı günlüğe kaydet:** kötü amaçlı nesnelere işlemez ve bunların tespit edilmeleriyle ilgili bilgileri uygulamanın günlüğüne kaydeder; kullanma (örneğin, kopyalama veya açma) girişiminde bulunulduğunda engeller.



Şekil 16: Kötü amaçlı nesnelere uygulanacak işlemi seçme

6. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

KÖTÜ AMAÇLI NESNELERİN KARANTİNAYA ALINMASI

Bu bölümde potansiyel olarak kötü amaçlı nesnelere yerleştirildiği özel bir dizin olan *karantina* hakkında bilgiler verilmektedir. Bu bölümde, dizinde bulunan zararlı nesnelere nasıl görüntüleneceği, geri yükleneceği ya da silineceği hakkında bilgiler verilmektedir.

BU BÖLÜMDE

Karantina hakkında	54
Karantinaya alınan nesnelere görüntüleme	54
Nesnelere Karantinadan geri yükleme.....	55
Karantinadaki nesnelere silme	56

KARANTİNA HAKKINDA

Bir aygıt taranırken veya Koruma etkinleştirilmişse, uygulama tespit edilen kötü amaçlı nesnelere özel bir izole dizin olan *karantinaya* yerleştirir. Karantinaya alınan nesnelere, bu nesnelere etkinliğini engelleyen bir paketleme biçiminde depolanır ve dolayısıyla bu nesnelere aygıt için herhangi bir tehdit oluşturmaz.

Karantinaya alınan dosyaları görebilir, silebilir veya geri yükleyebilirsiniz.

KARANTİNAYA ALINAN NESNELERİ GÖRÜNTÜLEME

Uygulamanın Karantinaya taşıdığı nesnelere listesini görüntüleyebilirsiniz. Her nesne için tam adı ve tespit edilme tarihi listede belirtilir.

Seçtiğiniz virüslü nesne hakkında aşağıdaki ek bilgileri de görüntüleyebilirsiniz: Uygulama tarafından Karantinaya taşınmadan önce nesnenin aygıttaki yolu ve tehdidin adı.

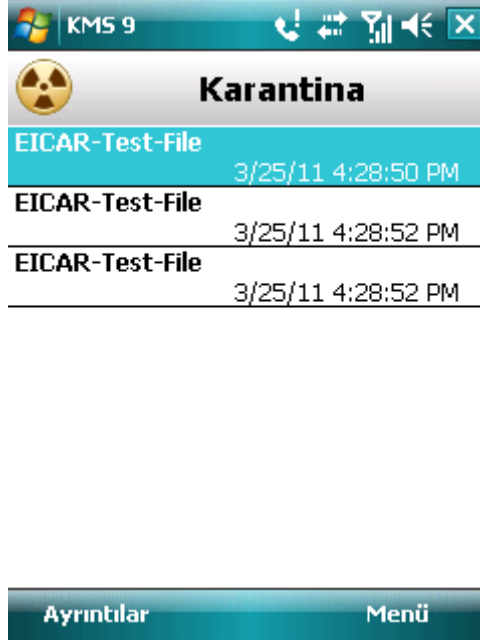
► *Karantinaya alınan nesnelere listesini görüntülemek için:*

1. **Menü** → **Anti-Virüs** öğesini seçin.

Anti-Virüs penceresi açılacaktır.

2. **Karantina** ögesini seçin.

Karantina ekranı, Karantinaya taşınan nesnelerin listesini açar (bkz. aşağıdaki şekil).



Şekil 17: Karantinadaki nesnelerin listesi

► **Virüslü nesne hakkındaki bilgileri görüntülemek için,**

Ayrıntılar ögesine basın.

Ayrıntılar ekranında nesne ile ilgili aşağıdaki bilgiler görüntülenecektir: uygulamanın aygıtta tespit ettiği dosyanın yolu ve virüsün adı.

Ayrıntılar ekranı açılır.

NESNELERİ KARANTINADAN GERİ YÜKLEME

Nesnenin aygıtta bir tehdit oluşturmadığından eminseniz, nesneyi karantinadan geri yükleyebilirsiniz. Geri yüklenen nesne orijinal dizinine yerleştirilir.

► **Karantinadaki bir nesneyi geri yüklemek için:**

1. **Menü** → **Anti-Virüs** ögesini seçin.

Anti-Virüs penceresi açılacaktır.

2. **Karantina** ögesini seçin.

Karantina penceresi açılacaktır.

3. Geri yüklenecek bir nesne seçin ve daha sonra **Menü** → **Geri Yükle** ögesini seçin.

Seçilen nesne Karantinadan orijinal dizinine geri yüklenecektir.

KARANTİNADAKİ NESNELERİ SİLME

Karantinadaki tek bir nesneyi veya tüm nesnelere silebilirsiniz.

► *Karantinadaki bir nesneyi silmek için:*

1. **Menü** → **Anti-Virüs** öğesini seçin.
Anti-Virüs penceresi açılacaktır.
2. **Karantina** öğesini seçin.
Karantina penceresi açılacaktır.
3. Silinecek bir nesneyi seçin ve daha sonra **Menü** → **Sil** öğesine basın.

Seçilen nesne Karantinadan silinecektir.

► *Karantinaya alınmış tüm nesnelere silmek için:*

1. **Menü** → **Anti-Virüs** öğesini seçin.
Anti-Virüs penceresi açılacaktır.
2. **Karantina** öğesini seçin.
Karantina penceresi açılacaktır.
3. **Menü** → **Tümünü sil**'e basın.

Karantinadaki tüm nesnelere silinecektir.

GELEN ARAMALARI VE SMS'LERİ FİLTRELEME

Bu bölüm, oluşturduğunuz Kara ve Beyaz Listelere uygun olarak istenmeyen aramaları ve SMS'leri engelleyen Arama/SMS Filtresi hakkında bilgi vermektedir. Bu bölümde ayrıca Arama/SMS Filtresinin gelen aramaları ve SMS'leri tarayacağı modun nasıl seçileceği, gelen SMS ve aramalar için ek filtreleme ayarlarının nasıl yapılandırılacağı ve ayrıca Kara ve Beyaz Listelerin nasıl oluşturulacağı açıklanmaktadır.

BU BÖLÜMDE

Arama/SMS Filtresi Hakkında	57
Arama/SMS Filtresi modları hakkında	58
Arama/SMS Filtresi modunun değiştirilmesi.....	58
Kara Liste oluşturma	59
Beyaz Liste oluşturma	62
Telefon defterinde olmayan kişilerden gelen SMS mesajlarını ve aramaları yanıtlama.....	65
Sayısal olmayan numaralardan gelen SMS mesajlarını yanıtlama.....	67
Gelen SMS'ler için bir yanıt seçme.....	68
Gelen aramalar için bir yanıt seçme.....	68

ARAMA/SMS FİLTRESİ HAKKINDA

Arama/SMS Filtresi, oluşturmuş olduğunuz Kara Liste ve Beyaz Liste temel alınarak iletilecek olan istenmeyen aramaları ve SMS'leri engeller.

Listeler girişlerden oluşur. Listelerden birindeki bir giriş, aşağıdaki bilgileri içerir:

- Arama/SMS Filtresinin, eğer numara Kara Liste içindeyse, hakkındaki her türlü bilgiyi gizlediği ve eğer numara Beyaz Liste içindeyse de hakkındaki her türlü bilgiyi gösterdiği telefon numarası.
- Arama/SMS Filtresinin eğer Beyaz Liste içindeyse engellediği ve eğer Kara Liste içindeyse de gösterdiği olay türü. Aşağıdaki iletişim türleri mevcut durumdadır: aramalar ve SMS, sadece aramalar ve sadece SMS.
- İstenen ve istenmeyen SMS'leri tanımlamak için Arama/SMS Filtresinin kullandığı anahtar ifade. Kara Liste için, Arama/SMS Filtresi bu ifadenin bulunmadığı SMS'leri ulaştırırken, bu ifadenin bulunduğu SMS'leri engeller. Beyaz Liste için, Arama/SMS Filtresi bu ifadenin bulunmadığı SMS'leri engellerken, bu ifadenin bulunduğu SMS'leri ulaştırır.

Arama/SMS Filtresi, seçilen mod ile öngörüldüğü şekilde gelen SMS'leri ve aramaları filtreler (bkz. "Arama/SMS Filtresi modları hakkında" bölümü, sayfa [58](#)). Arama/SMS Filtresi gelen her SMS veya aramayı tarar ve bu SMS veya aramanın istenen veya istenmeyen (spam) SMS veya arama olduğunu belirler. Arama/SMS Filtresi, SMS'e veya aramaya istenen veya istenmeyen durumu atar, tarama sonlandırılır.

Engellenen SMS ve aramalarla ilgili bilgiler uygulama günlüğüne kaydedilir (bkz. "Uygulama günlükleri" bölümü, sayfa [112](#)).

ARAMA/SMS FİLTRESİ MODLARI HAKKINDA

Mod, kuralları Arama/SMS Filtresinin aramaları ve SMS'leri filtrelemede kullandığı kuralları tanımlar.

Aşağıdaki Arama/SMS Filtresi modları mevcuttur:

- **Kapalı** - tüm gelen arama ve SMS'lere izin verilir.
- **Beyaz Listeye İzin Ver** – sadece Beyaz Liste içinde bulunan numaralardan gelen aramalara ve SMS'lere izin verilir.
- **Kara Listeyi Engelle** – Kara Listedeki numaralardan gelenler hariç bütün aramalara ve SMS'lere izin verilir.
- **Her iki liste** – Beyaz Listedeki gelen aramalara ve SMS'lere izin verilirken Kara Listedeki numaralardan gelenler engellenir. Her iki listede de olmayan bir numarayla konuşmanın veya bu numaradan gelen SMS mesajının okunmasının ardından Arama/SMS Filtresi numarayı iki listeden birine girmenizi isteyecektir.

Arama/SMS Filtresi modunu değiştirebilirsiniz (bkz. "Arama/SMS Filtresi modunun değiştirilmesi" bölümü, sayfa [58](#)). Geçerli Arama/SMS Filtresi modu **Arama/SMS Filtresi** ekranında **Mod** menü öğesinin yanında görüntülenir.

ARAMA/SMS FİLTRESİ MODUNUN DEĞİŞTİRİLMESİ

➔ *Arama/SMS Filtresi modunun değiştirmek için:*

1. **Menü** → **Arama/SMS Filtresi** öğesini seçin.

Arama/SMS Filtresi açılır.

2. **Mod** öğesini seçin.

Mod penceresi açılacaktır.

3. **Arama/SMS Filtresi modu** ayarlamak için değer seçin (bkz. aşağıdaki şekil).



Şekil 18: Arama/SMS Filtresi modunu değiştirme

4. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

KARA LİSTE OLUŞTURMA

Kara Liste yasaklanan numaraların girişlerini içerir, örn: Arama/SMS Filtresinin gelen aramaları ve SMS'leri engellediği numaralar. Her giriş aşağıdaki bilgileri içerir:

- Arama/SMS Filtresinin gelen aramaları ve / veya SMS'leri engellediği telefon numarası.
- Arama/SMS Filtresinin bu numaradan gelen aramaları ve SMS'leri engellediği olayların türleri. Aşağıdaki olay türleri mevcuttur: aramalar ve SMS, sadece arama ve sadece SMS.
- Arama/SMS Filtresinin SMS'leri istenmeyen (spam) olarak sınıflandırmak için kullandığı anahtar ifade. Arama/SMS Filtresi anahtar ifadeyi içeren SMS'leri engellerken diğer tüm SMS'leri iletir.

Arama/SMS Filtresi, Kara Liste içindeki bir girişin bütün kriterlerine uyan aramaları ve SMS'leri engeller. Kara Liste içindeki bir girişin kriterlerinden bir tanesiyle bile uymayan Aramalara ve SMS'lere, Arama/SMS Filtresi tarafından izin verilecektir.

Aynı filtreleme kriterlerine sahip bir telefon numarasını hem Kara Listeye hem de Beyaz Listeye ekleyemezsiniz.

Engellenen SMS ve aramalarla ilgili bilgiler uygulama günlüğüne kaydedilir (bkz. "Uygulama günlükleri" bölümü, sayfa [112](#)).

BU BÖLÜMDE

Kara listeye giriş ekleme	60
Kara Listedeki girişleri düzenleme.....	61
Kara Listedeki girişleri silme.....	62

KARA LİSTEYE GİRİŞ EKLEME

Aynı filtreleme kriterlerine sahip aynı numaranın Arama/SMS Filtresi numaralarının hem Kara listesinde hem de Beyaz listesinde aynı anda olamayacağını unutmayın. Böyle filtreleme kriterlerine sahip bir numara bu listelerden birinde zaten kayıtlıysa, Kaspersky Mobile Security 9 bunu size bildirecek ve ilgili mesaj ekranda görünecektir.

➔ *Arama/SMS Filtresi Kara Listesi'ne bir giriş eklemek için:*

1. **Menü** → **Arama/SMS Filtresi** ögesini seçin.

Arama/SMS Filtresi açılır.

2. **Kara Liste** ögesini seçin.

Kara Liste penceresi açılacaktır.

3. **Menü** → **Ekle** ögesini seçin.

Bu işlem, **Yeni giriş** penceresini açacaktır.

4. Aşağıdaki ayarlar için değerleri belirleyin (bkz. Aşağıdaki Şekil).

- **Geleni engelle** : Arama/SMS Filtresinin engelleyeceği bir telefon numarasından gelen olayın türü
 - **Aramalar ve SMS**: Gelen aramaları ve SMS mesajlarını engeller.
 - **Yalnızca aramalar**: yalnızca gelen aramaları engeller.
 - **Yalnızca SMS**: yalnızca gelen SMS mesajlarını engeller.
- **Telefon numarası**: Arama/SMS Filtresinin gelen bilgileri engellediği telefon numarası. Telefon numarası yalnızca alfanümerik karakterler içerebilir; bir rakam veya harfle başlayabilir veya başına "+" simgesi gelebilir. Numara olarak "*" veya "?" gibi maskeler de kullanmak mümkündür. (burada "*" herhangi bir sayıda simgeyi ve "?" herhangi bir simgeyi ifade eder). Örneğin *1234? Kara Listedir. Arama/SMS Filtresi 1234 rakamını bir simgenin izlediği aramaları veya SMS'leri engeller.
- **İçerdiği metin** – alınan SMS mesajının istenmeyen mesaj (spam) olduğunu gösteren anahtar ifade. Arama/SMS Filtresi anahtar ifadeyi içeren SMS'leri engellerken diğer tüm SMS'leri iletir.

Kara Listedeki belirli bir numaradan gelen tüm SMS'lerin engellenmesini istiyorsanız, bu girişin **İçerdiği metin** alanını boş bırakın.

Şekil 19: Giriş ayarları

Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

KARA LİSTEDEKİ GİRİŞLERİ DÜZENLEME

Yasaklanan numaraların Kara listesindeki bir girişin tüm ayarlarının değerlerini değiştirebilirsiniz.

► *Arama/SMS Filtresi Kara Listesi'ndeki bir girişi düzenlemek için:*

1. **Menü** → **Arama/SMS Filtresi** ögesini seçin.

Arama/SMS Filtresi açılır.

2. **Kara Liste** ögesini seçin.

Kara Liste penceresi açılacaktır.

3. Düzenlemek istediğiniz öğeyi listeden seçin ve daha sonra **Menü** → **Düzenle** ögesini seçin.

Düzenle penceresi açılacaktır.

4. Gerekli ayarları değiştirin:

- **Geleni engelle:** Arama/SMS Filtresinin engelleyeceği bir telefon numarasından gelen olayın türü
 - **Aramalar ve SMS:** Gelen aramaları ve SMS mesajlarını engeller.
 - **Yalnızca aramalar:** yalnızca gelen aramaları engeller.
 - **Yalnızca SMS:** yalnızca gelen SMS mesajlarını engeller.
- **Telefon numarası:** Arama/SMS Filtresinin gelen bilgileri engellediği telefon numarası. Telefon numarası yalnızca alfanümerik karakterler içerebilir; bir rakam veya harfle başlayabilir veya başına "+" simgesi

gelebilir. Numara olarak "*" veya "?" gibi maskeler de kullanmak mümkündür. (burada "*" herhangi bir sayıda simgeyi ve "?" herhangi bir simgeyi ifade eder). Örneğin *1234? Kara Listedir. Arama/SMS Filtresi 1234 rakamını bir simgenin izlediği aramaları veya SMS'leri engeller.

- **İçerdiği metin** – alınan SMS mesajının istenmeyen mesaj (spam) olduğunu gösteren anahtar ifade. Arama/SMS Filtresi anahtar ifadeyi içeren SMS'leri engellerken diğer tüm SMS'leri iletir.

Kara Listedeki belirli bir numaradan gelen tüm SMS'lerin engellenmesini istiyorsanız, bu girişin İçerdiği metin alanını boş bırakın.

5. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

KARA LİSTEDEKİ GİRİŞLERİ SİLME

Kara Liste'den bir numarayı silebilirsiniz. Ayrıca tüm girişleri kaldırarak Arama/SMS Filtresi Kara Listesini tamamen temizleyebilirsiniz.

➔ *Arama/SMS Filtresi Kara Listesi'nden bir giriş silmek için:*

1. **Menü** → **Arama/SMS Filtresi** ögesini seçin.
Arama/SMS Filtresi açılır.
2. **Kara Liste** ögesini seçin.
Kara Liste penceresi açılacaktır.
3. Listeden silinecek bir giriş seçin ve daha sonra **Menü** → **Sil** ögesini seçin.
4. Girişin silinmesini onaylayın. Bunun için, **Evet** düğmesine basın.

➔ *Arama/SMS Filtresi Kara Listesi'ni temizlemek için:*

1. **Menü** → **Arama/SMS Filtresi** ögesini seçin.
Arama/SMS Filtresi açılır.
2. **Kara Liste** ögesini seçin.
Kara Liste penceresi açılacaktır.
3. **Menü** → **Tümünü sil**'i seçin.

Liste boşaltılır.

BEYAZ LİSTE OLUŞTURMA

Beyaz Liste, izin verilen numaraların girişlerini içerir, örn: Arama/SMS Filtresinin gelen aramaları ve SMS'leri kullanıcıya ilettiği numaralar. Her giriş aşağıdaki bilgileri içerir:

- Arama/SMS Filtresinin gelen aramaları ve / veya SMS'leri ilettiği telefon numarası.
- Arama&SMS Filtresinin bu numaradan gelen aramaları ve SMS'leri ilettiği olayların türleri. Aşağıdaki olay türleri mevcuttur: aramalar ve SMS, sadece arama ve sadece SMS.
- Bir SMS'i istenmeyen (spam değil) olarak sınıflandırmak için Arama&SMS Filtresi tarafından kullanılan anahtar sözcük. Arama/SMS Filtresi anahtar ifadeyi içeren SMS'leri iletirken diğer tüm SMS'leri engeller.

Arama/SMS Filtresi yalnızca Beyaz Liste içindeki bir girişin bütün kriterlerine uyan aramalara ve SMS'lere izin verir. Beyaz Liste içindeki bir girişin kriterlerinden bir tanesine bile uymayan Aramalar ve SMS'ler, Arama/SMS Filtresi tarafından engellenecektir.

BU BÖLÜMDE

Beyaz Listeye giriş ekleme.....	63
Beyaz Listedeki girişleri düzenleme	64
Beyaz Listedeki girişleri silme.....	65

BEYAZ LİSTEYE GİRİŞ EKLEME

Aynı filtreleme kriterlerine sahip aynı numaranın Arama/SMS Filtresi numaralarının hem Kara listesinde hem de Beyaz listesinde aynı anda olamayacağını unutmayın. Böyle filtreleme kriterlerine sahip bir numara bu listelerden birinde zaten kayıtlıysa, Kaspersky Mobile Security 9 bunu size bildirecek ve ilgili mesaj ekranda görünecektir.

➔ *Arama/SMS Filtresi Beyaz Listesi'ne bir giriş eklemek için:*

1. **Menü** → **Arama/SMS Filtresi** ögesini seçin.

Arama/SMS Filtresi açılır.

2. **Beyaz Liste** ögesini seçin.

Beyaz Liste penceresi açılacaktır.

3. **Menü** → **Ekle** ögesini seçin.

Bu işlem, **Yeni giriş** penceresini açacaktır.

4. Aşağıdaki ayarlar için değerleri belirleyin (bkz. Aşağıdaki Şekil).

- **Geleni engelle:** Arama/SMS Filtresinin izin verdiği bir telefon numarasından gelen olayın türü
 - **Aramalar ve SMS:** Gelen aramalara ve SMS mesajlarına izin verir.
 - **Yalnızca aramalar:** Yalnızca gelen aramalara izin verir.
 - **Yalnızca SMS:** Yalnızca gelen SMS mesajlarına izin verir.
- **Telefon numarası:** Arama/SMS Filtresinin gelen bilgileri engellediği telefon numarası. Telefon numarası yalnızca alfanümerik karakterler içerebilir; bir rakam veya harfle başlayabilir veya başına "+" simgesi gelebilir. Numara olarak "*" veya "?" gibi maskeler de kullanmak mümkündür. (burada "*" herhangi bir sayıda simgeyi ve "?" herhangi bir simgeyi ifade eder). Örneğin *1234? Beyaz Listede. Arama/SMS Filtresi 1234 rakamını bir simgenin izlediği aramaları veya SMS'leri iletir.
- **İçerdiği metin** – alınan SMS mesajının istenen mesaj olduğunu gösteren anahtar ifade. Beyaz Listedeki numaralar için, Arama/SMS Filtresi yalnızca anahtar ifadeyi içeren SMS mesajlarını iletirken diğer SMS mesajlarını engeller.

Beyaz Listedeki belirli bir numaradan gelen tüm SMS'lerin iletilmesini istiyorsanız, bu girişin **İçerdiği metin** alanını boş bırakın.

KMS 9

Düzenle

Gelene izin ver:

Aramalar ve SMS

Yalnızca aramalar

Yalnızca SMS

Telefon numarası:

+321654987

İçerdiği metin:

Ödeme

Tamam Menü

Şekil 20: Giriş ayarları

5. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

BEYAZ LİSTEDEKİ GİRİŞLERİ DÜZENLEME

İzin verilen numaraların Beyaz listesindeki bir girişin tüm ayarlarının değerlerini değiştirebilirsiniz.

► *Arama/SMS Filtresi Beyaz Listesi'ndeki bir girişi düzenlemek için:*

1. **Menü** → **Arama/SMS Filtresi** ögesini seçin.

Arama/SMS Filtresi açılır.

2. **Beyaz Liste** ögesini seçin.

Beyaz Liste penceresi açılacaktır.

3. Düzenlemek istediğiniz öğeyi listeden seçin ve daha sonra **Menü** → **Düzenle** ögesini seçin.

Düzenle penceresi açılacaktır.

4. Gerekli ayarları değiştirin:

- **Geleni engelle:** Arama/SMS Filtresinin izin verdiği bir telefon numarasından gelen olayın türü
 - **Aramalar ve SMS:** Gelen aramalara ve SMS mesajlarına izin verir.
 - **Yalnızca aramalar:** Yalnızca gelen aramalara izin verir.
 - **Yalnızca SMS:** Yalnızca gelen SMS mesajlarına izin verir.

- **Telefon numarası:** Arama/SMS Filtresinin gelen bilgileri engellediği telefon numarası. Telefon numarası yalnızca alfanümerik karakterler içerebilir; bir rakam veya harfle başlayabilir veya başına "+" simgesi gelebilir. Numara olarak "*" veya "?" gibi maskeler de kullanmak mümkündür. (burada "*" herhangi bir sayıda simgeyi ve "?" herhangi bir simgeyi ifade eder). Örneğin *1234? Beyaz Listede. Arama/SMS Filtresi 1234 rakamını bir simgenin izlediği aramaları veya SMS'leri iletir.
- **İçerdiği metin** – alınan SMS mesajının istenen mesaj olduğunu gösteren anahtar ifade. Beyaz Listedeki numaralar için, Arama/SMS Filtresi yalnızca anahtar ifadeyi içeren SMS mesajlarını iletirken diğer SMS mesajlarını engeller.

Beyaz Listedeki belirli bir numaradan gelen tüm SMS'lerin iletilmesini istiyorsanız, bu girişin **İçerdiği metin** alanını boş bırakın.

5. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

BEYAZ LİSTEDEKİ GİRİŞLERİ SİLME

Beyaz Listesi'nden bir girişi silebileceğiniz gibi listedeki tüm girişleri de silebilirsiniz.

➔ *Arama&SMS Filtresi Beyaz Listesi'nden bir giriş silmek için:*

1. **Menü** → **Arama/SMS Filtresi** ögesini seçin.
Arama/SMS Filtresi açılır.
2. **Beyaz Liste** ögesini seçin.
Beyaz Liste penceresi açılacaktır.
3. Listedeki silinecek bir giriş seçin ve daha sonra **Menü** → **Sil** ögesini seçin.
4. Girişin silinmesini onaylayın. Bunun için, **Evet** düğmesine basın.

➔ *Arama/SMS Filtresi Beyaz Listesi'ni temizlemek için:*

1. **Menü** → **Arama/SMS Filtresi** ögesini seçin.
Arama/SMS Filtresi açılır.
2. **Beyaz Liste** ögesini seçin.
Beyaz Liste penceresi açılacaktır.
3. **Menü** → **Tümünü sil** ögesini seçin.

Liste boşaltılır.

TELEFON DEFTERİNDE OLMAYAN KİŞİLERDEN GELEN SMS MESAJLARINI VE ARAMALARI YANITLAMA

Arama/SMS Filtresi için **Her iki liste** veya **Beyaz Liste** modları seçilmişse (bkz. "**Arama/SMS Filtresi modları hakkında**" bölümü, sayfa 58) numarası Kişiler'de kayıtlı olmayan abonelerden gelen Aramalara/SMS'lere ayrıca bir yanıt ayarlayabilirsiniz. Arama/SMS Filtresi, kişiler listesinden numaralar eklenerek Beyaz Listenin genişletilmesine olanak verir.

Ayarların değerlerini değiştirmek için, aygıtın kumanda kolunu veya kalemı kullanın.

► *Arama/SMS Filtresinin telefon rehberinde bulunmayan bir numaraya yanıtını seçmek için:*

1. **Menü** → **Arama/SMS Filtresi** ögesini seçin.

Arama/SMS Filtresi açılır.

2. **Mod** ögesini seçin.

3. **Mod** penceresi açılacaktır.

4. **Kişilere izin ver** ayarı için istediğiniz değeri seçin (aşağıdaki Şekil'e bakın):

- Arama/SMS Filtresinin telefon defterindeki numaraları ek bir Beyaz Liste olarak görmesi ve telefon defterinde olmayan göndericilerden SMS ve aramaların alınmasını engellemesi için **Kişilere İzin Ver** kutusunu işaretleyin.
- Arama/SMS Filtresinin ayarlanan Arama/SMS Filtresi moduna göre SMS mesajlarını ve aramaları filtrelemesi için **Kişilere izin ver** kutusunun işaretini kaldırın.



Şekil 21: Arama/SMS Filtresinin aygıtın telefon rehberinde bulunmayan numaralara yanıtı

5. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

SAYISAL OLMAYAN NUMARALARDAN GELEN SMS MESAJLARINI YANITLAMA

Arama/SMS Filtresi Modu **Her iki liste** veya **Kara Liste** is seçili ise (bkz. "**Arama/SMS Filtresi modunu değiştirme**" bölümü, sayfa 58), tüm sayısal olmayan (harf içeren) numaraları ekleyerek Kara Listeyi büyütebilirsiniz. Daha sonra Arama/SMS Filtresi sayısal olmayan numaralardan gelen SMS'leri engelleyecektir.

Ayarların değerlerini değiştirmek için, aygıtın kumanda kolunu veya kalemli kullanın.

► *Arama/SMS Filtresi'nin sayısal olmayan numaralardan mesajlar aldığınızdaki yanıtını ayarlamak için:*

1. **Menü** → **Arama/SMS Filtresi** ögesini seçin.

Arama/SMS Filtresi açılır.

2. **Mod** ögesini seçin.

Mod penceresi açılacaktır.

3. **Sayısal olmayan numaraları engelle** ayarı için bir değer seçin (bkz. aşağıdaki Şekil):

- Arama/SMS Filtresinin sayısal olmayan numaralardan gelen mesajları otomatik olarak silmesi için, **Sayısal olmayan numaraları engelle** kutusunu işaretleyin;
- Arama/SMS Filtresinin sayısal olmayan numaralardan gelen SMS mesajlarını yalnızca ayarlanan Anti-Spam moduna göre filtrelemesi için **Sayısal olmayan numaraları engelle** kutusunun işaretini kaldırın.



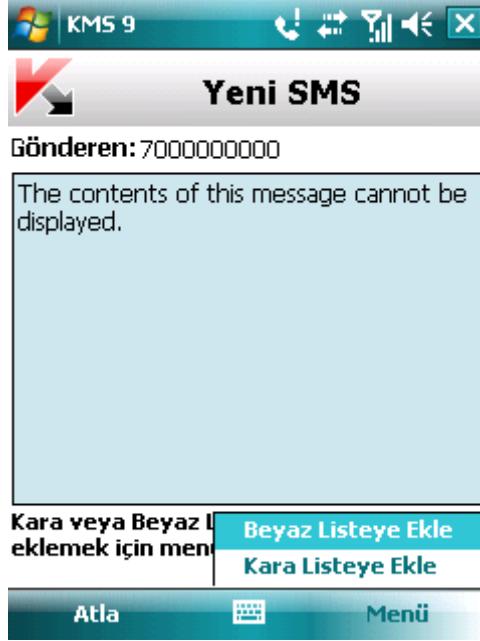
Şekil 22: Arama/SMS Filtresinin sayısal olmayan numaralardan gelen SMS'ler için eylemini yapılandırma

4. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

GELEN SMS'LER İÇİN BİR YANIT SEÇME

Her iki liste modunda (bkz. "Arama/SMS Filtresi modları hakkında" bölümü, sayfa 58), Arama/SMS Filtresi gelen SMS'i Kara ve Beyaz listelerle karşılaştırır.

Gönderenin numarası Kara veya Beyaz listede bulunmuyorsa, Arama/SMS Filtresi bunu size bildirir . Gelen SMS mesajı ile ilgili olarak Arama/SMS Filtresi eylemlerinden birini seçmeniz istenir (bkz. aşağıdaki şekil).



Şekil 23: Mesaj alındığına dair Arama/SMS Filtresi bildirimi

SMS ile ilgili olarak aşağıdaki işlemlerden birini seçebilirsiniz:

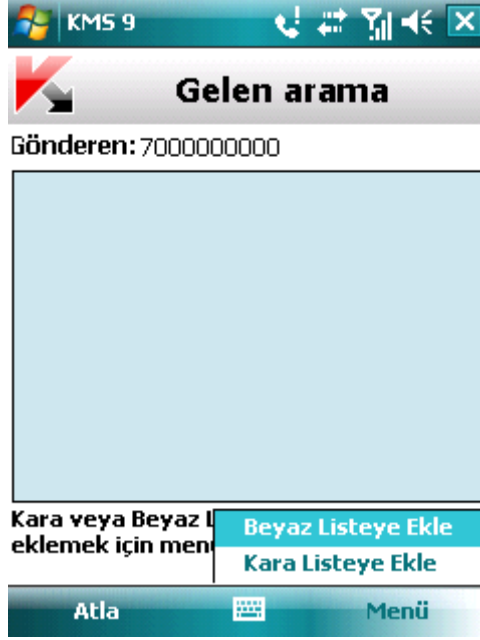
- Bir SMS mesajını engellemek ve gönderenin telefon numarasını Kara Listeye eklemek için **Menü** → **Kara Listeye ekle** öğesini seçin.
- Bir SMS mesajını iletme ve gönderenin telefon numarasını Beyaz Listeye eklemek için **Menü** → **Beyaz Listeye ekle** öğesini seçin.
- SMS mesajını, gönderenin telefon numarasını herhangi bir listeye eklemeyen iletme için **Atla** düğmesine basın.

Engellenen SMS mesajları ile ilgili bilgiler uygulama günlüğüne kaydedilir (bkz. "Uygulama günlükleri" bölümü, sayfa 112).

GELEN ARAMALAR İÇİN BİR YANIT SEÇME

Her iki liste modunda (bkz. "Arama/SMS Filtresi modları hakkında" bölümü, sayfa 58), Arama/SMS Filtresi gelen aramaları Kara ve Beyaz listelere göre kontrol eder.

Gönderenin numarası Kara veya Beyaz listede bulunmuyorsa, Arama/SMS Filtresi taramayı bitirdikten sonra bunu size bildirir ve gelen aramaya ilişkin bir eylem belirlemenizi ister (bkz. Aşağıdaki şekil).



Şekil 24: Kabul edilen bir arama ile ilgili Arama/SMS Filtresi bildirimi

Aramanın yapıldığı numaraya uygulanması için aşağıdaki işlemlerden birini seçebilirsiniz:

- Arayanın telefon numarasını Kara Listeye eklemek için **Menü** → **Kara Listeye ekle** öğesini seçin.
- Arayanın telefon numarasını Beyaz Listeye eklemek için **Menü** → **Beyaz Listeye ekle** öğesini seçin.
- arayanın telefon numarasını iki listeye de eklememek için **Atla** düğmesine basın.

Engellenen aramalarla ilgili bilgiler uygulama günlüğüne kaydedilir.

GİDEN ARAMALARI VE SMS MESAJLARINI SINIRLAMA. EBEVEYN DENETİMİ

Bu bölüm, belirtilen telefon numaralara giden aramaların ve SMS mesajlarının sınırlandırmasını sağlayan Ebeveyn denetimi bileşeni hakkında bilgiler sağlar. Bölüm ayrıca izin verilen ve yasaklı numaralar listesinin nasıl oluşturulacağını ve Ebeveyn Denetimi ayarlarının nasıl yapılacağını açıklar.

BU BÖLÜMDE

Ebeveyn Denetimi hakkında.....	70
Ebeveyn Denetimi modları	70
Ebeveyn Denetiminin Etkinleştirilmesi/Devre Dışı Bırakılması	70
Kara Liste oluşturma	71
Beyaz Liste oluşturma.....	74

EBEVEYN DENETİMİ HAKKINDA

Ebeveyn Denetimi abone numaralarının Kara ve Beyaz listelerini kullanarak giden SMS mesajlarının ve aramaların denetlenmesini etkinleştirir. Bileşenin çalışması mod tarafından yönetilir.

Kara Liste modunda, Ebeveyn Denetimi Kara Listedeki numaralara giden SMS ve aramaları engellerken diğer tüm numaralara giden SMS ve aramalara izin verir. **Beyaz Liste** modunda, Ebeveyn Denetimi yalnızca Beyaz Listedeki numaralara giden SMS ve aramalara izin verirken diğer tüm numaralara giden SMS ve aramaları engeller. **Kapalı** modunda, Ebeveyn Denetimi giden SMS mesajlarını ve aramaları izlemez.

Ebeveyn Denetimi, yalnızca aygıtın standart araçlarını kullanarak gönderilen giden SMS mesajlarını engeller. Ebeveyn Denetimi, üçüncü taraf uygulamaları kullanılarak gönderilen giden SMS mesajlarına izin verir.

Bileşenin işleyişiyle ilgili bilgiler uygulama günlüğüne girilir (bkz. "Uygulama Günlükleri" bölümü, sayfa [112](#)).

EBEVEYN DENETİMİ MODLARI

Ebeveyn Denetimi modu giden SMS ve aramaların denetlenmesini tanımlayan kuralı belirler.

Aşağıdaki Ebeveyn Denetimi modları mevcuttur:

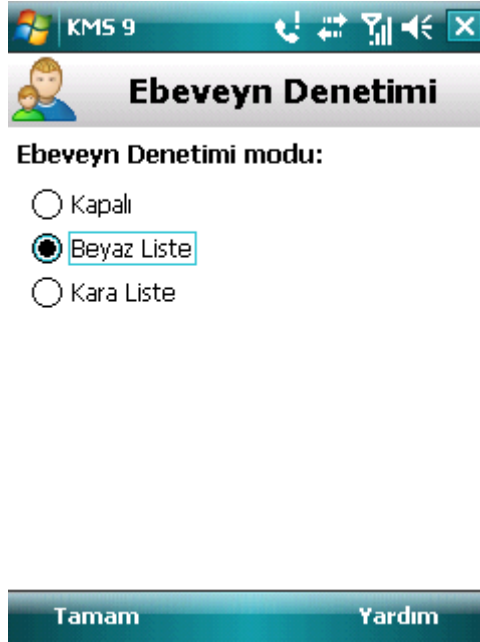
- **Kapalı:** Ebeveyn Denetimini devre dışı bırakır. Giden SMS mesajları ve aramalar denetlenmez.
Bu mod varsayılan olarak seçilidir.
- **Beyaz Liste:** Yalnızca Beyaz Listedeki numaralara SMS gönderilmesine ve / veya arama yapılmasına izin verir. (bkz. "Beyaz Liste Oluşturma" bölümü, sayfa [74](#)). Diğer tüm mesajlar ve aramalar engellenir.
- **Kara Liste:** Yalnızca Kara Listedeki numaralara SMS gönderilmesini ve / veya arama yapılmasını engeller. (bkz. "Kara Liste Oluşturma" bölümü, sayfa [71](#)). Diğer tüm mesajlara ve aramalara izin verilir.

Ebeveyn Denetim modunudeğiştirebilirsiniz (bkz. "Ebeveyn Denetiminin Etkinleştirilmesi/devre dışı bırakılması" bölümü, sayfa [70](#)). Geçerli Ebeveyn Denetimi modu **Ebeveyn Denetimi** penceresinde **Mod** öğesinin yanında görüntülenir.

EBEVEYN DENETİMİNİN ETKİNLEŞTİRİLMESİ/DEVRE DIŞI BIRAKILMASI

➔ *Ebeveyn Denetimi modunu değiştirmek için:*

1. **Menü** → **Ebeveyn Denetimi** ögesini seçin.
2. **Ebeveyn Denetimi** penceresi açılacaktır.
3. **Mod** ögesini seçin.
Mod penceresi açılacaktır.
4. Önerilen Ebeveyn Denetimi modlarından birini seçin (bkz. Aşağıdaki Şekil).



Şekil 25: Ebeveyn Denetimi modunu değiştirme

5. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

KARA LİSTE OLUŞTURMA

Ebeveyn Denetiminin giden SMS mesajlarını ve aramaları engellemek için kullanacağı bir Kara Liste oluşturmalısınız. Liste, SMS göndermenin veya arama yapılmasının engelli olmadığı telefon numaralarını içerir.

Engellenen SMS mesajları ve aramalar ile ilgili bilgiler uygulama günlüğüne kaydedilir (bkz. "Uygulama günlükleri" bölümü, sayfa [112](#)).

BU BÖLÜMDE

Kara listeye giriş ekleme	72
Kara Listedeki girişleri düzenleme.....	73
Kara Listedeki girişleri silme.....	74

KARA LİSTEYE GİRİŞ EKLEME

Aynı filtreleme kriterlerine sahip aynı numaranın Ebeveyn Denetimi numaralarının hem Kara listesinde hem de Beyaz listesinde aynı anda olamayacağını aklınızda tutun. Böyle kriterlere sahip bir numara bu listelerden birinde zaten kayıtlıysa, Kaspersky Mobile Security 9 bunu size bildirecek ve ilgili mesaj ekranda görünecektir.

► *Ebeveyn Denetimi Kara Listesine bir giriş eklemek için:*

1. **Menü** → **Ebeveyn Denetimi** öğesini seçin.
2. **Ebeveyn Denetimi** penceresi açılacaktır.
3. **Kara Liste** öğesini seçin.

Kara Liste penceresi açılacaktır.

4. **Menü** → **Ekle**'yi seçin.

Bu işlem, **Yeni giriş** penceresini açacaktır.

5. Aşağıdaki ayarlar için değerleri belirleyin (bkz. Aşağıdaki Şekil).

- **Gideni engelle:** Ebeveyn Denetiminin engellediği bir abone numarasına giden bilginin türü:
 - **SMS ve aramalar:** Giden aramaları ve SMS mesajlarını engeller.
 - **Yalnızca aramalar:** Yalnızca giden aramaları engeller.
 - **Yalnızca SMS:** Yalnızca giden SMS mesajlarını engeller.

- **Telefon numarası:** Giden SMS ve/veya aramalar için engellenecek olan telefon numarası. Telefon numarası yalnızca alfanümerik karakterler içerebilir; bir rakam veya harfle başlayabilir veya başına "+" simgesi gelebilir. Numara olarak "*" veya "?" gibi maskeler de kullanmak mümkündür. (burada "*" herhangi bir sayıda simgeyi ve "?" herhangi bir simgeyi ifade eder).

Şekil 26: Giriş ayarları

6. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

KARA LİSTEDEKİ GİRİŞLERİ DÜZENLEME

Yasaklanan numaraların Kara listesindeki bir girişin tüm ayarlarının değerlerini değiştirebilirsiniz.

- **Ebeveyn Denetimi Kara listesindeki bir girişi düzenlemek için:**

1. **Menü** → **Ebeveyn Denetimi** ögesini seçin.
2. **Ebeveyn Denetimi** penceresi açılacaktır.
3. **Kara Liste** ögesini seçin.

Kara Liste penceresi açılacaktır.

4. Düzenlemek istediğiniz ögeyi listeden seçin ve **Menü** → **Düzenle**'yi seçin.

Düzenle penceresi açılacaktır.

5. Gerekli ayarları değiştirin:

- **Gideni engelle:** Ebeveyn Denetiminin engellediği bir abone numarasına giden bilginin türü:
 - **SMS ve aramalar:** Giden aramaları ve SMS mesajlarını engeller.
 - **Yalnızca aramalar:** Yalnızca giden aramaları engeller.
 - **Yalnızca SMS:** Yalnızca giden SMS mesajlarını engeller.

- **Telefon numarası:** Giden SMS ve/veya aramalar için engellenecek olan telefon numarası. Telefon numarası yalnızca alfanümerik karakterler içerebilir; bir rakam veya harfle başlayabilir veya başına "+" simgesi gelebilir. Numara olarak "*" veya "?" gibi maskeler de kullanmak mümkündür. (burada "*" herhangi bir sayıda simgeyi ve "?" herhangi bir simgeyi ifade eder).

6. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

KARA LİSTEDEKİ GİRİŞLERİ SİLME

Bir numaranın engellenen numaralar listesinin Kara listesine yanlışlıkla eklenmesi mümkündür. Böyle bir numarayı listeden silebilirsiniz. Ayrıca tüm girişleri kaldırarak Ebeveyn Denetimi Kara Listesini tamamen temizleyebilirsiniz.

► *Ebeveyn Denetimi Beyaz Listesindeki bir girişi silmek için aşağıdaki işlemleri gerçekleştirin:*

1. **Menü** → **Ebeveyn Denetimi** ögesini seçin.
2. **Ebeveyn Denetimi** penceresi açılacaktır.
3. **Kara Liste** ögesini seçin.
Kara Liste penceresi açılacaktır.
4. Listedeki silinecek bir giriş seçin ve daha sonra **Menü** → **Sil** ögesini seçin.
5. Silme işlemini onaylayın. Bunun için, **Evet** düğmesine basın.

► *Ebeveyn Denetimi Kara Listesi'ni temizlemek için*

1. **Menü** → **Ebeveyn Denetimi** ögesini seçin.
2. **Ebeveyn Denetimi** penceresi açılacaktır.
3. **Kara Liste** ögesini seçin.
Kara Liste penceresi açılacaktır.
4. **Menü** → **Tümünü sil**'i seçin.

Liste boşaltılır.

BEYAZ LİSTE OLUŞTURMA

Arama/SMS Filtresinin gelen aramalara ve SMS mesajlarına izin verirken kullanması gereken bir Beyaz Liste oluşturun.

BU BÖLÜMDE

Beyaz Listeye giriş ekleme.....	75
Beyaz Listedeki girişleri düzenleme	76
Beyaz Listedeki girişleri silme.....	77

BEYAZ LİSTEYE GİRİŞ EKLEME

Aynı filtreleme kriterlerine sahip aynı numaranın Ebeveyn Denetimi numaralarının hem Kara listesinde hem de Beyaz listesinde aynı anda olamayacağını aklınızda tutun. Böyle kriterlere sahip bir numara bu listelerden birinde zaten kayıtlıysa, Kaspersky Mobile Security 9 bunu size bildirecek ve ilgili mesaj ekranda görünecektir.

➔ *Ebeveyn Denetimi Beyaz Listesine bir giriş eklemek için:*

1. **Menü** → **Ebeveyn Denetimi** ögesini seçin.
2. **Ebeveyn Denetimi** penceresi açılacaktır.
3. **Beyaz Liste** ögesini seçin.
4. **Beyaz Liste** penceresi açılacaktır.
5. **Menü** → **Ekle**'yi seçin.

Bu işlem, **Yeni giriş** penceresini açacaktır.

6. Aşağıdaki ayarlar için değerleri belirleyin (bkz. Aşağıdaki Şekil).
 - **Gidene izin ver:** Ebeveyn Denetiminin bir abone numarasına gönderilmesine izin verdiği giden bilgilerin türü:
 - **SMS ve aramalar:** Giden aramalara ve SMS mesajlarına izin verir.
 - **Yalnızca aramalar:** Yalnızca giden aramalara izin verir.
 - **Yalnızca SMS:** Yalnızca giden SMS mesajlarına izin verir.

- **Telefon numarası:** Ebeveyn Denetiminin SMS mesajı gönderilmesine ve/veya arama yapılmasına izin verdiği telefon numarası. Telefon numarası yalnızca alfanümerik karakterler içerebilir; bir rakam veya harfle başlayabilir veya başına "+" simgesi gelebilir. Numara olarak "*" veya "?" gibi maskeler de kullanmak mümkündür. (burada "*" herhangi bir sayıda simgeyi ve "?" herhangi bir simgeyi ifade eder).

Şekil 27: Giriş ayarları

7. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

BEYAZ LİSTEDEKİ GİRİŞLERİ DÜZENLEME

İzin verilen numaraların Beyaz listesindeki bir girişin tüm ayarlarının değerlerini değiştirebilirsiniz.

- *Ebeveyn Denetimi Beyaz Listesindeki bir girişi düzenlemek için:*

1. **Menü** → **Ebeveyn Denetimi** ögesini seçin.
2. **Ebeveyn Denetimi** penceresi açılacaktır.
3. **Beyaz Liste** ögesini seçin.
4. **Beyaz Liste** penceresi açılacaktır.
5. Düzenlemek istediğiniz öğeyi listeden seçin ve **Menü** → **Düzenle**'yi seçin.

Düzenle penceresi açılacaktır.

6. Gerekli ayarları değiştirin:

- **Gidene izin ver:** Ebeveyn Denetiminin bir abone numarasına gönderilmesine izin verdiği giden bilgilerin türü:
 - **SMS ve aramalar:** Giden aramalara ve SMS mesajlarına izin verir.
 - **Yalnızca aramalar:** Yalnızca giden aramalara izin verir.
 - **Yalnızca SMS:** Yalnızca giden SMS mesajlarına izin verir.

- **Telefon numarası:** Ebeveyn Denetiminin SMS mesajı gönderilmesine ve/veya arama yapılmasına izin verdiği telefon numarası. Telefon numarası yalnızca alfanümerik karakterler içerebilir; bir rakam veya harfle başlayabilir veya başına "+" simgesi gelebilir. Numara olarak "*" veya "?" gibi maskeler de kullanmak mümkündür. (burada "*" herhangi bir sayıda simgeyi ve "?" herhangi bir simgeyi ifade eder).

7. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

BEYAZ LİSTEDEKİ GİRİŞLERİ SİLME

Bir girişi silebilir veya Beyaz Listeyi tamamen temizleyebilirsiniz.

► *Ebeveyn Denetimi Beyaz Listesi'nden bir giriş silmek için:*

1. **Menü** → **Ebeveyn Denetimi** ögesini seçin.
2. **Ebeveyn Denetimi** penceresi açılacaktır.
3. **Beyaz Liste** ögesini seçin.
4. **Beyaz Liste** penceresi açılacaktır.
5. Listeden silinecek bir giriş seçin ve daha sonra **Menü** → **Sil** ögesini seçin.
6. Silme işlemini onaylayın. Bunun için, **Evet** düğmesine basın.

► *Ebeveyn Denetimi Beyaz Listesi'ni temizlemek için:*

1. **Menü** → **Ebeveyn Denetimi** ögesini seçin.
2. **Ebeveyn Denetimi** penceresi açılacaktır.
3. **Beyaz Liste** ögesini seçin.
4. **Beyaz Liste** penceresi açılacaktır.
5. **Menü** → **Tümünü sil** ögesini seçin.

Liste boşaltılır.

AYGITIN KAYBOLMASI VEYA ÇALINMASI DURUMUNDA VERİ KORUMASI

Bu bölümde, aygıtın çalınması ya da kaybolması durumunda, mobil aygıtta kayıtlı bilgilere izinsiz erişimi engelleyen ve aygıtın bulunmasını kolaylaştıran Hırsızlığa Karşı Koruma sistemi hakkında bilgiler verilmektedir.

Ayrıca Hırsızlığa Karşı Koruma'nın nasıl etkinleştirileceği/devre dışı bırakılacağı, çalışma parametrelerinin nasıl belirleneceği ve Hırsızlığa Karşı Koruma'nın başka bir mobil cihaz üzerinden uzaktan nasıl başlatılacağı da bu bölümde anlatılmaktadır.

BU BÖLÜMDE

Hırsızlığa Karşı Koruma hakkında.....	78
Aygıtı engelleme.....	79
Kişisel Verileri Silme.....	81
Silinecek nesnelere listesi oluşturma.....	83
Aygıtta SIM kart değişikliğinin izlenmesi.....	84
Aygıtın coğrafi koordinatlarını belirleme	85
Hırsızlığa Karşı Koruma işlevlerini uzaktan başlatma.....	87

HIRSIZLIĞA KARŞI KORUMA HAKKINDA

Hırsızlığa Karşı Koruma, mobil aygıtınızda depolanan bilgileri yetkisiz erişime karşı korur.

Hırsızlığa Karşı Koruma, aşağıdaki işlevleri içerir:

- **Engelle** – aygıtın uzaktan engellenmesini sağlar ve engellenen aygıtın ekranında gösterilen metni verir.
- **Veri Silme** – aygıtta yer alan kullanıcının kişisel verilerini (Kişiler'deki kayıtlar, SMS, resim galerisi, takvim, günlükler, İnternet bağlantısı ayarları) ve bellek kartları, silme listelerindeki dizinlerde bulunan bilgileri uzaktan silebilir.
- **SIM Gözcüsü**, SIM kartının değiştirilmesi durumunda güncel telefon numarasının alınmasına ve SIM kartının değiştirilmesi ve aygıtın bir SIM kart olmadan etkinleştirilmesi durumunda aygıtı kilitlemesini sağlar. Yeni telefon numarası hakkındaki bilgiler, telefon numarasına bir mesaj olarak ve/veya belirtmiş olduğunuz e-posta adresine gönderilir.
- **GPS Bul** işlevi, aygıtınızın yerini bulmanızı sağlar. Aygıtın coğrafi koordinatları, özel bir SMS komutunun gönderildiği telefon numarasına ve bir e-posta adresine gönderilir.

Kaspersky Mobile Security 9 kurulduktan sonra tüm Hırsızlığa Karşı Koruma işlevleri devre dışı bırakılır.

Kaspersky Mobile Security 9 başka bir mobil aygıttan SMS komutlarının gönderilmesi ile Hırsızlığa Karşı Koruma işlevini uzaktan başlatabilir (bkz. "Hırsızlığa Karşı Koruma işlevlerinin uzaktan başlatılması" bölümü, sayfa [87](#)).

Hırsızlığa Karşı Korumayı uzaktan başlatmak için Kaspersky Mobile Security 9 ilk başlatıldığında ayarlanan gizli kodu bilmeniz gerekir.

Her işlevin geçerli durumu **Hırsızlığa Karşı Koruma** ekranındaki her işlevin adının yanında görüntülenir.

Bileşenin işleyişiyle ilgili bilgiler uygulama günlüğüne girilir (bkz. "Uygulama Günlükleri" bölümü, sayfa [112](#)).

AYGITI ENGELLEME

Özel bir SMS komutu alınmışsa, engelleme işlevi aygıtın uzaktan engellenmesine ve aygıttaki verilerin engellenmesine olanak tanır. Aygıtın engellenmesini ancak gizli kodu girerek kaldırabilirsiniz.

Bu işlev aygıtı engellemez, yalnızca aygıtın uzaktan engellenmesi seçeneği etkinleştirir.

► *Engelleme işlevini etkinleştirmek için:*

1. **Menü** → **Hırsızlığa Karşı Koruma** ögesini seçin.

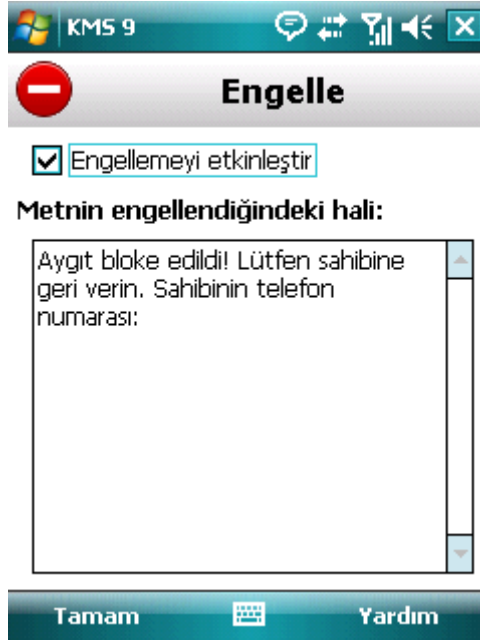
Hırsızlığa Karşı Koruma penceresi açılacaktır.

2. **Bloke et** ögesini seçin.

Engelle penceresi açılacaktır.

3. **Engellemeyi Etkinleştir** kutusunu işaretleyin.

4. Aygıtın ekranında gösterilecek mesajı **Metnin engellendiğindeki hali** alanına girin (aşağıdaki Şekil'e bakın). Mesajda, varsayılan olarak aygıt sahibinin telefonunu ekleyebileceğiniz standart bir metin kullanılır.



Şekil 28: Engelleme işlevi ayarları

5. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

Engelleme işlevi başka bir aygıtta etkinleştirilmişse, aygıtı aşağıdaki yöntemlerle engelleyebilirsiniz:

- Aygıtınıza bir SMS komutu göndermek için başka bir aygıttaki, Kaspersky Mobile Security 9 gibi bir Kaspersky Lab mobil uygulamasını kullanın. Özel bir SMS komutu oluşturmak için **Komut gönder** işlevini kullanın. Sonuç olarak, aygıtınız gizli bir SMS alacak ve aygıt engellenecektir.

- Başka bir mobil aygıtta özel metni ve alıcı aygıt için daha önce ayarlanmış gizli kodu içeren bir SMS oluşturun ve gönderin. Sonuç olarak, aygıtınız gizli bir SMS alacak ve aygıt engellenecektir.

Giden SMS mesajları diğer mobil aygıtın hizmet sağlayıcısının koyduğu ücretler üzerinden faturalanacaktır.

Aygıtı tamamen engellemek için bir Komut gönderme işlevinin kullanıldığı güvenli yöntemi tercih etmeniz önerilmektedir. Bu durumda uygulamanın gizli kodu şifreli biçimde gönderilir.

Aygıtı uzaktan bloke etmek için, komut Gönderme işlevi ile güvenli yöntemi kullanmanız tavsiye edilir. Burada komut ve gizli kod şifreleme ile gönderilir.

► **Komut gönder işlevini kullanarak başka bir aygıtta bir SMS komutu göndermek için:**

1. **Menü** → **Ek** ögesini seçin.

Ek penceresi açılacaktır.

2. **Komut gönder** ögesini seçin.

Bu işlem **Komut gönder** penceresini açacaktır.

3. **SMS komutu** seçeneği için **Bloke Et** değerini seçin (bkz. aşağıdaki şekil).

4. **Telefon numarası** alanına SMS komutunu alan cihazın telefon numarasını girin.

5. **Uzak aygıtın kodu** alanına SMS komutunu alan aygıtta ayarlanan gizli kodu girin.

Şekil 29: Aygıtı uzaktan bloke etmeye başlamae

6. **Gönder** düğmesine basın.

► **Telefonun standart SMS oluşturma işlevleri ile bir SMS mesajı oluşturmak için,**

bloke etmek istediğiniz aygıtta bir SMS mesajı göndermek için. SMS mesajı şu metni içermelidir `block:<kod>`, burada `<kod>`, bloke edilecek aygıt üzerinde belirlenen gizli koddur. Bu mesaj büyük/küçük harf duyarlı değildir ve iki nokta üst üste işaretinden önceki ve sonraki boşluklar yok sayılır.

KİŞİSEL VERİ SİLMEME

Özel bir SMS komutu alındıktan sonra Veri Silme işlevi aygıtta depolanan aşağıdaki bilgileri uzaktan silmenize olanak tanır:

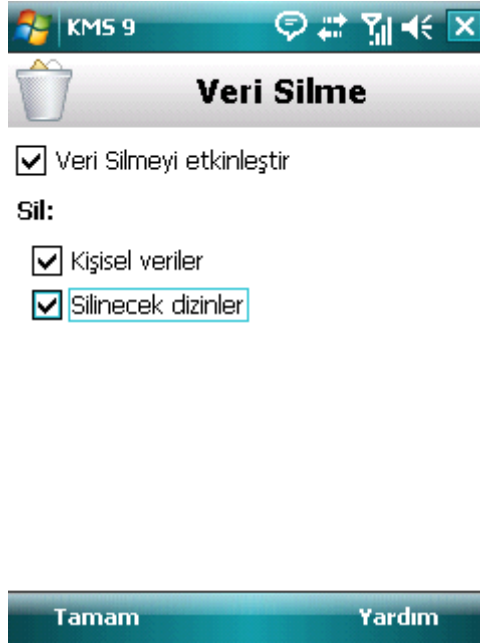
- kullanıcının kişisel verileri (Kişi listesindeki ve SIM Kartındaki girişler, SMS mesajları, galeri, takvim, internet bağlantı ayarları);
- bellek kartındaki bilgiler;
- **Belgelerim** dizinindeki dosyalar ve **Silinecek dizinler** listesindeki diğer dizinler.

Bu işlev, aygıtta kayıtlı verileri silmez ancak silme seçeneği içerir.

► *Veri Silme işlevini etkinleştirmek için:*

1. **Menü** → **Hırsızlığa Karşı Koruma** öğesini seçin.
Hırsızlığa Karşı Koruma penceresi açılacaktır.
2. **Verileri Silme** öğesini seçin.
Veri Silme ekranı açılacaktır.
3. **Mod** öğesini seçin.
Veri Silme ekranı açılacaktır.
4. **Veri Silmeyi etkinleştir** kutusunu işaretleyin.
5. Silmek istediğiniz bilgileri seçin. Bunu yapmak için **Sil** bölümündeki gerekli ayarların yanındaki kutuları işaretleyin (bkz. aşağıdaki şekil).
 - kişisel verileri silmek için **Kişisel veriler** kutusunu işaretleyin;

- **Belgelerim** dizininden ve **Silinecek dizinler** listesinden dosyaları silmek için **Dizinler** kutusunu işaretleyin.



Şekil 30: Silinecek verilerin türünün seçilmesi

6. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.
7. **Silinecek dizinler** listesini oluşturmaya devam edin (bkz. "**Silinecek dizinler listesi oluşturma**" bölümü, sayfa [83](#)).

Aygıttaki kişisel verileri aşağıdaki yöntemlerle etkinleştirilen işlevi kullanarak silebilirsiniz:

- Aygıtınıza bir SMS komutu göndermek için başka bir aygıttaki, Kaspersky Mobile Security 9 gibi bir Kaspersky Lab mobil uygulamasını kullanın. Özel bir SMS komutu oluşturmak için Komut gönderme işlevini kullanın. Sonuç olarak, aygıtınız gizli bir SMS alacak ve bilgiler silinecektir.
- Başka bir mobil aygıtta özel metni ve alıcı aygıt için daha önce ayarlanmış gizli kodu içeren bir SMS oluşturun ve gönderin.

Aygıttaki bilgileri uzaktan silmek için Komut gönderme işlevi ile birlikte güvenli yöntemi kullanmanız tavsiye edilir. Burada komut ve gizli kod şifreleme ile gönderilir.

► **Başka bir aygıtta komut göndermek için:**

1. **Menü** → **Ek** ögesini seçin.
Ek penceresi açılacaktır.
2. **Komut gönder** ögesini seçin.
Bu işlem **Komut gönder** penceresini açacaktır.
3. **SMS komutu** ayarı için **Verileri Silme** değerini seçin (bkz. aşağıdaki şekil).
4. **Telefon numarası** alanına SMS komutunu alan cihazın telefon numarasını girin.

5. **Uzaktaki aygıt için kod** alanına SMS komutunu alan aygıtta ayarlanan gizli kodu girin.

KMS 9

Komut gönder

SMS komutu seçin:

Engelle

Veri Silme

GPS Bulma

Gizlilik Koruması

Telefon numarası:

+123456789

Uzaktaki aygıt için kod:

Gönder Menü

Şekil 31: Kişisel verilerin silinmesini uzaktan başlatma

6. **Gönder** düğmesine basın.

► *Telefonun standart SMS oluşturma işlevleri ile bir SMS mesajı oluşturmak için,*

başka bir aygıtta standart bir SMS gönderin; SMS şu metni içermelidir `wipe:<kod> burada <kod>`, diğer aygıt üzerinde ayarlanan uygulamanın gizli kodudur. Bu mesaj büyük/küçük harf duyarlı değildir ve iki nokta üst üste işaretinden önceki ve sonraki boşluklar yok sayılır.

SİLİNECEK NESNELER LİSTESİ OLUŞTURMA

Verileri Sil işlevi özel bir SMS komutu alındıktan sonra silinecek dizinlerin listesini oluşturmaya olanak verir.

Hırsızlığa Karşı Korumanın özel bir SMS komutu aldıktan sonra listedeki tüm dizinleri silmesini etkinleştirmek için, **Mod** menüsünde **Dizinler** kutusunun işaretlendiğinden emin olun.

► *Bir dizini silinecek dizinler listesine eklemek için:*

1. **Menü** → **Hırsızlığa Karşı Koruma** öğesini seçin.

Hırsızlığa Karşı Koruma penceresi açılacaktır.

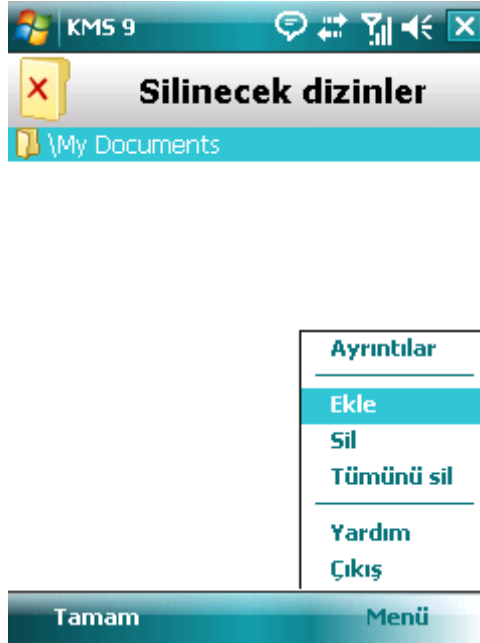
2. **Verileri Sil** öğesini seçin.

Veri Silme ekranı açılacaktır.

3. **Silinecek dizinler** öğesini seçin.

Silinecek dizinler ekranı açılacaktır.

4. **Menü** → **Dizin ekle** öğesini seçin (aşağıdaki Şekil'e bakın).



Şekil 32: Silenecek dizinlerin seçilmesi

5. Dizin ağacından istediğiniz dizini seçin ve ardından **Seç** düğmesine basın.

Dizin listeye eklenir.

► *Dizini listeden kaldırmak için:*

1. **Menü** → **Hırsızlığa Karşı Koruma** öğesini seçin.
Hırsızlığa Karşı Koruma penceresi açılacaktır.
2. **Verileri Sil** öğesini seçin.
Veri Silme ekranı açılacaktır.
3. **Silenecek dizinler** öğesini seçin.
Silenecek dizinler ekranı açılacaktır.
4. Listedenden bir dizin seçin ve **Menü** → **Sil** düğmesine basın.

AYGITTAKİ SIM KARTININ DEĞİŞTİRİLMESİNİ İZLEME

SIM kartı değiştirilirse, SIM Gözcüsü yeni numarayı içeren bir SMS'i telefon numaranıza ve / veya e-postanıza göndermenize veya aygıtı kilitlemenize olanak tanır.

► *SIM Gözcüsü işlevini etkinleştirmek ve SIM kartının değiştirilmesini izlemek için:*

1. **Menü** → **Hırsızlığa Karşı Koruma** öğesini seçin.
Hırsızlığa Karşı Koruma penceresi açılacaktır.
2. **SIM Gözcüsü** öğesini seçin.

Bu işlem **SIM Gözcüsü** penceresini açar.

3. **SIM Gözcüsünü Etkinleştir** kutusunu işaretleyin.

4. Aygıtta SIM kartın değiştirilmesini denetlemek için aşağıdaki ayarları yapın (aşağıdaki Şekil'e bakın):

- Yeni telefon numarası ile ilgili otomatik olarak mesaj göndermek için **Telefon numarasını gönder** bloğundaki **Telefon numarası** alanına mesajın gönderildiği telefon numarasını girin.

Telefon numarası bir rakam veya "+" ile başlayabilir ve yalnızca rakamlardan oluşmak zorundadır.

- Telefonunuzun yeni numarası ile ilgili bir e-posta mesajı almak için **Telefon numarasını gönder** bölümündeki **E-postaya mesaj** alanına bir e-posta adresi girin.
- SIM kartı değiştirildiğinde veya aygıt kartsız olarak açıldığında aygıtı bloke etmek için, **Ek** ayarı için **Aygıtı bloke et** kutusunu işaretleyin. Aygıtın engellenmesini ancak gizli kodu girerek kaldırabilirsiniz.
- engelleme modunda ekranda bir mesaj görüntülemek için **Metnin engellendiğindeki hali** alanına girin. Mesajda, varsayılan olarak aygıt sahibinin numarasını ekleyebileceğiniz standart bir metin kullanılır.



Şekil 33: SIM Gözcüsü işlevi ayarları

5. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

AYGITIN COĞRAFİ KOORDİNATLARINI BELİRLEME

Özel bir SMS komutu aldıktan sonra, GPS Bul aygıtın coğrafi koordinatlarının belirlenmesini ve isteyen aygıtta ve bir e-posta adresine SMS ve e-posta ile gönderilmesini sağlar.

Giden SMS mesajları, mobil hizmet sağlayıcının güncel tarifesi üzerinden faturalandırılır.

Bu işlem yalnızca yerleşik GPS alıcısına sahip aygıtlarda çalışır. GPS alıcı aygıt özel bir SMS mesajını aldıktan sonra otomatik olarak etkinleşir. Eğer aygıt, uyduların ulaşabileceği bir aladaysa GPS Bul işlevi aygıtın coğrafi koordinatlarını alır ve gönderir. Eğer sorgu sırasında uydular kullanılmıyorsa GPS Bul, bunları bulmak ve aygıtın konum sonuçlarını göndermek için düzenli olarak tekrar denemelerde bulunacaktır.

➔ *GPS Bul işlevini etkinleştirmek için:*

1. **Menü** → **Hırsızlığa Karşı Koruma** ögesini seçin.

Hırsızlığa Karşı Koruma penceresi açılacaktır.

2. **GPS Bul** ögesini seçin.

Bu işlem **GPS Bul** penceresini açar.

3. **GPS Bul'u etkinleştir** kutusunu işaretleyin.

Varsayılan olarak Kaspersky Mobile Security 9, aygıtın koordinatlarını SMS mesajı olarak gönderir.

4. Aygıtın koordinatlarını e-posta olarak da almak için **Aygıt koordinatlarını gönder** ayarına e-posta adresi girin (bkz. Aşağıdaki şekil).

Şekil 34: GPS Bul işlevi ayarları

5. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

GPS Bul işlevi etkinleştirilmiş bir aygıtın koordinatlarını aşağıdaki yöntemlerle isteyebilirsiniz:

- Aygıtınıza bir SMS komutu göndermek için başka bir aygıttaki, Kaspersky Mobile Security 9 gibi bir Kaspersky Lab mobil uygulamasını kullanın. Sonuç olarak, aygıtınız gizli bir SMS alacak ve uygulama aygıtın koordinatlarını gönderecektir. Özel bir SMS komutu oluşturmak için Komut gönderme işlevini kullanın.
- Başka bir mobil aygıtta özel metni ve alıcı aygıt için daha önce ayarlanmış gizli kodu içeren bir SMS oluşturun ve gönderin. Sonuç olarak, aygıtınız gizli bir SMS alacak ve uygulama aygıtın koordinatlarını gönderecektir.

Giden SMS mesajları diğer mobil aygıtın hizmet sağlayıcısının koyduğu ücretler üzerinden faturalanacaktır.

Aygıtın konumunu almak için, Komut gönderme işlevinin kullanıldığı güvenli yöntemi tercih etmeniz önerilmektedir. Bu durumda uygulamanın gizli kodu şifreli modda gönderilir.

Aygıtın konumunu uzaktan belirlemek için Komut gönder işlevi ile güvenli yöntemi kullanmanız önerilir. Burada komut ve gizli kod şifreleme ile gönderilir.

► *Başka bir aygıtta komut göndermek için:*

1. **Menü** → **Ek** ögesini seçin.

Ek penceresi açılacaktır.

2. **Komut gönder** ögesini seçin.

Bu işlem **Komut gönder** penceresini açacaktır.

3. **SMS komutu** ayarı için **GPS-Bul** değerini seçin (bkz. aşağıdaki şekil).

4. **Telefon numarası** alanına SMS komutunu alan cihazın telefon numarasını girin.

5. **Uzaktaki aygıt için kod** alanına SMS komutunu alan aygıtta ayarlanan gizli kodu girin.

Şekil 35: Aygıtın yerini belirleme

6. **Gönder** düğmesine basın.

► *Telefonun standart SMS oluşturma işlevleri ile bir SMS mesajı oluşturmak için,*

başka bir aygıtta standart bir SMS gönderin; SMS'de şu metin olmalıdır `find:<kod> burada <kod>`, diğer aygıt üzerinde ayarlanan gizli koddur. Bu mesaj büyük/küçük harf duyarlı değildir ve iki nokta üst üste işaretinden önceki ve sonraki boşluklar yok sayılır.

SMS komutunun gönderildiği telefon numarasına ve GPS Bul seçeneklerinde önceden belirttiyseniz bir e-posta adresine aygıtın koordinatlarını içeren bir SMS gönderilecektir.

HIRSIZLIĞA KARŞI KORUMA İŞLEVLERİNİ UZAKTAN BAŞLATMA

Uygulama Hırsızlığa Karşı Koruma işlevlerini Kaspersky Mobile Security kurulu başka bir aygıttan uzaktan çalıştırmak için özel bir SMS komutu gönderilmesine olanak tanır. Şifrelenmiş bir SMS olarak bir SMS komutu gönderilir ve diğer aygıtta ayarlanmış olan uygulama gizli kodunu içerir. SMS komutunun alındığı bildirilmeyecektir.

SMS, mobil servis sağlayıcınızın geçerli ücreti üzerinden faturalanır.

► Başka bir aygıtta komut göndermek için:

1. **Menü** → **Ek** ögesini seçin.

Ek penceresi açılacaktır.

2. **Komut gönder** ögesini seçin.

3. Bu işlem **Komut gönder** penceresini açacaktır.

4. **SMS komutu** ayarı için mevcut değerlerden birini seçin (bkz. aşağıdaki Şekil):

- **Bloke Et.**
- **Verileri Sil.**
- **GPS-Bul.**
- **Gizlilik Koruması** (bkz. "**Kişisel verileri gizleme**" bölümü, sayfa [89](#)).

5. **Telefon numarası** alanına SMS komutunu alan cihazın telefon numarasını girin.

6. **Uzaktaki aygıt için kod** alanına SMS komutunu alan aygıtta ayarlanan gizli kodu girin.

Şekil 36: Hırsızlığa Karşı Koruma işlevlerini uzaktan başlatma

7. **Gönder** düğmesine basın.

GİZLİLİK KORUMASI

Bu bölümde, kullanıcının gizli bilgilerini saklayabilen Gizlilik Koruması hakkında bilgiler verilmektedir.

BU BÖLÜMDE

Gizlilik Koruması.....	89
Gizlilik Koruması modları.....	89
Gizlilik Korumasını Etkinleştirme/Devre Dışı Bırakma	90
Gizlilik Korumasını otomatik olarak etkinleştirme	91
Gizlilik Korumasını uzaktan etkinleştirme	92
Özel numaralar listesi oluşturma	94
Gizlenecek verileri seçme Gizlilik Koruması.....	97

GİZLİLİK KORUMASI

Gizlilik Koruması, özel numaraların listelendiği Kişi Listenize göre özel verileri gizler. Gizlilik Koruması, gizli numaralar için Kişiler girişlerini, gelenleri, taslakları, gönderilen SMS'leri ve arama geçmişi girişlerini gizler. Gizlilik Koruması, yeni SMS sinyali bastırır ve gelen kutusunda mesajın kendisini gizler. Gizlilik Koruması, özel numaralardan gelen aramaları engeller ve arama bilgilerini ekranda görüntülemeyi engeller. Sonuç olarak, arayan meşgul sinyali alacaktır. Gizlilik Korumasının etkinleştirildiği süre için gelen arama ve SMS'leri görmek için Gizlilik Korumasını devre dışı bırakın. Gizlilik Koruması yeniden etkinleştirildiğinde bilgiler görüntülenmez.

Gizlilik Korumasını Kaspersky Mobile Security 9'dan ya da uzaktaki diğer bir mobil aygıttan etkinleştirebilirsiniz. Ancak Gizlilik Korumasının devre dışı bırakılması yalnızca uygulama dahilinde gerçekleştirilir.

Gizlilik Korumasının işleyişiyle ilgili bilgiler uygulama günlüğüne depolanır (bkz. "Uygulama günlükleri" bölümü, sayfa [112](#)).

GİZLİLİK KORUMASI MODLARI

Gizlilik Korumasının çalışma modunu yönetebilirsiniz. Mod Gizlilik Korumasının etkin mi yoksa devre dışı mı olduğunu tanımlar.

Varsayılan olarak, Gizlilik Koruması devre dışıdır.

Aşağıdaki Gizlilik Koruması modları mevcuttur:

- **Normal** – özel veriler görüntülenir. Değiştirmek için Gizlilik Koruması ayarlarına erişilebilir.
- **Gizli** – özel veriler gizlenir. Gizlilik Koruması ayarları değiştirilemez.

Gizlilik Korumasını otomatik başlayacak şekilde (bkz. "Gizlilik Korumasının otomatik etkinleştirilmesi" bölümü, sayfa [91](#)) ayarlayabilirsiniz veya başka bir aygıttan uzaktan başlatabilirsiniz (bkz. bölüm "Gizlilik Korumasının uzaktan etkinleştirilmesi" bölümü, sayfa [92](#)).

Bileşenin geçerli durumu **Mod** ögesinin yanındaki **Gizlilik Koruması** sekmesinde görüntülenir.

Gizlilik Korumasının modunun değiştirilmesi biraz zaman alabilir.

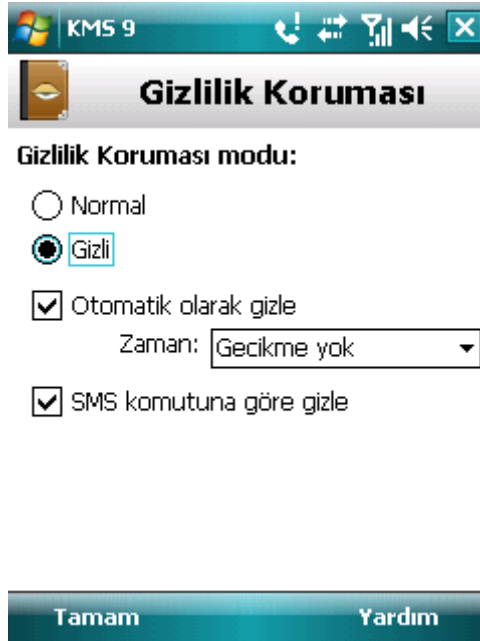
GİZLİLİK KORUMASINI ETKİNLEŞTİRME/DEVRE DIŞI BIRAKMA

Gizlilik Koruması modu aşağıdaki şekilde değiştirilebilir:

- Bileşen ayarları menüsünden;
- **Gizlilik Koruması** menüsünden.

➔ *Gizlilik Koruması modunu değiştirmek için:*

1. **Menü** → **Gizlilik Koruması** ögesini seçin.
Gizlilik Koruması penceresi açılacaktır.
2. **Mod** ögesini seçin.
Mod penceresi açılacaktır.
3. **Mod** ayarı için bir değer seçin (bkz. aşağıdaki Şekil).
4. **Tamam** düğmesine basın.



Şekil 37: Gizlilik Koruması modunu değiştirme

5. Gizlilik Koruması modu değişikliğini onaylayın. Bunun için, **Evet** düğmesine basın.

➔ *Gizlilik Koruması modunu hızlı değiştirmek için:*

1. **Menü** → **Gizlilik Koruması** ögesini seçin.

Gizlilik Koruması penceresi açılacaktır.

2. **Gizli / Normal** düğmesine basın. Gizlilik Korumasının geçerli durumuna bağlı olarak düğmenin adı aksiyle değişecektir.
3. Gizlilik Koruması modu değişikliğini onaylayın. Bunun için, **Evet** düğmesine basın.

GİZLİLİK KORUMASINI OTOMATİK OLARAK ETKİNLEŞTİRME

Belirtilen zaman aralığı geçtikten sonra gizli bilgilerin gizlenmesi işlevinin otomatik olarak etkinleştirilmesini yapılandırabilirsiniz. Aygıt güç tasarrufu moduna geçtikten sonra bu işlev etkinleştirilir.

Gizlilik Koruması ayarlarını düzenlemeden önce Gizlilik Korumasını devre dışı bırakın.

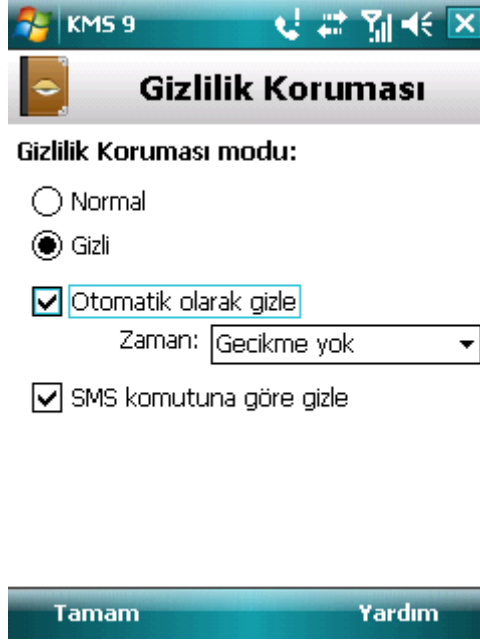
➔ *Belirtilen zaman aralığı geçtikten sonra Gizlilik Korumasını otomatik olarak etkinleştirmek için:*

1. **Menü** → **Gizlilik Koruması** ögesini seçin.

Gizlilik Koruması penceresi açılacaktır.

2. **Mod** ögesini seçin.
3. **Mod** penceresi açılacaktır.
4. **Erişimi engelle** kutusunu işaretleyin (bkz. aşağıdaki şekil).
5. Geçtiğinde Gizlilik Korumasının etkinleştirileceği zaman aralığı için bir değer belirtin. Bunun için **Zaman** ayarının mevcut değerlerinden birini seçin:
 - **Hemen.**
 - **1 dakika sonra.**
 - **5 dakika sonra.**

- 15 dakika sonra.
- 1 saat sonra.



Şekil 38: Gizlilik Korumasını otomatik başlatma

6. **Tamam** düğmesine basın.

GİZLİLİK KORUMASINI UZAKTAN ETKİNLEŞTİRME

Kaspersky Mobile Security 9 Gizlilik Korumasını başka bir mobil aygıttan uzaktan etkinleştirmenize olanak verir. Bunun için öncelikle aygıtınızdaki SMS komutu ile Gizle seçeneğini etkinleştirin.

► *Gizlilik Korumasını uzaktan etkinleştirmek için:*

1. **Menü** → **Gizlilik Koruması** öğesini seçin.

Gizlilik Koruması penceresi açılacaktır.

2. **Mod** öğesini seçin.

Mod penceresi açılacaktır.

3. **SMS komutu ile gizle** kutusunu işaretleyin (bkz. aşağıdaki şekil).



Şekil 39: Gizlilik Korumasını uzaktan etkinleştirme ayarları

4. **Tamam** düğmesine basın.

Aşağıdaki yöntemlerden herhangi birini kullanarak Gizlilik Korumasını uzaktan etkinleştirebilirsiniz:

- Aygıtınıza bir SMS komutu göndermek için başka bir aygıttaki, Kaspersky Mobile Security 9 gibi bir Kaspersky Lab mobil uygulamasını kullanın. Sonuç olarak aygıtınız dikkat çekmeden bir SMS alır ve gizli bilgiler gizlenir. Özel bir SMS komutu oluşturmak için Komut gönderme işlevini kullanın.
- Başka bir mobil aygıtta özel bir metin ve aygıtınızda belirtilen uygulamanın gizli kodunu içeren bir SMS iletisini oluşturun ve gönderin. Sonuç olarak aygıtınız bir SMS alır ve gizli bilgiler gizlenir.

Giden SMS, SMS komutunun geldiği telefonun mobil sağlayıcısı tarafından belirlenen fiyatlar üzerinden faturalandırılacaktır.

► Özel bir SMS komutu kullanarak Gizlilik Korumasını uzaktan etkinleştirmek için:

1. **Menü** → **Ek** ögesini seçin.

Ek penceresi açılacaktır.

2. **Komut gönder** ögesini seçin.

Bu işlem **Komut gönder** penceresini açacaktır.

3. **SMS komutu** ayarı için **Gizlilik Koruması** değerini seçin (bkz. aşağıdaki şekil).

4. **Telefon numarası** alanına SMS komutunu alan cihazın telefon numarasını girin.

5. **Uzak aygıtın kodu** alanına SMS komutunu alan aygıtta ayarlanan gizli kodu girin.



Şekil 40: Gizlilik Korumasını uzaktan başlatma

6. **Gönder** düğmesine basın.

Aygıt SMS komutunu aldığı anda Gizlilik Korumasını otomatik olarak etkinleştirir.

► *Telefonun SMS oluşturmaya yönelik standart araçlarını kullanarak Gizlilik Korumasını uzaktan etkinleştirmek için:*

kilitlemek istediğiniz aygıtta bir SMS gönderin; mesaj şu metni içermelidir: `hide:<kod>`, burada `<kod>` diğer aygıtta belirlenen uygulamanın gizli kodudur. Bu mesaj büyük/küçük harf duyarlı değildir ve iki nokta üst üste işaretinden önceki ve sonraki boşluklar yok sayılır.

ÖZEL NUMARALAR LİSTESİ OLUŞTURMA

Kişi listesi Gizlilik Koruması bileşeninin bilgilerini ve olaylarını gizlediği özel numaraları içerir. Listeyi bir numarayı elle ekleyerek veya Kişiler ve SIM kartından içe aktararak genişletebilirsiniz.

Kişi Listesi yapmadan önce gizli bilgileri gizleme işlevini devre dışı bırakın.

BU BÖLÜMDE

Özel numaralar listesine numara ekleme	94
Özel kişiler listesinde bir numarayı düzenleme.....	96
Özel kişiler listesinde bir numarayı silme.....	96

ÖZEL NUMARALAR LİSTESİNE NUMARA EKLEME

Manüel olarak bir numara ekleyebilir (örnek, +12345678), Kişi Listesinden veya SIM karttan bir numarayı içeri aktarabilirsiniz.

Gizlilik Koruması ayarlarını düzenlemeden önce Gizlilik Korumasını devre dışı bırakın.

► Kişi listesine bir telefon numarası eklemek için:

1. **Menü** → **Gizlilik Koruması** ögesini seçin.

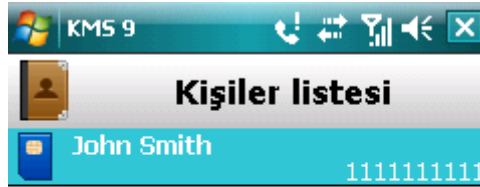
Gizlilik Koruması penceresi açılacaktır.

2. **Kişi Listesi** ögesini seçin.

Kişi listesi penceresi açılacaktır.

3. Aşağıdaki işlemlerden birini gerçekleştirin (bkz. aşağıdaki Şekil):

- Kişiler'den bir numara eklemek için, **Menü** → **Ekle** → **Outlook kişisi** ögesini seçin. Açılan **Outlook kişisi** ekranında istenen girişi belirtin ve daha sonra **Seç** düğmesine basın.
- SIM kartına kaydedilen bir numarayı eklemek için **Menü** → **Ekle** → **SIM'den gelen Kişi** ögesini seçin. Açılan **SIM'den gelen kişi** penceresinde, gereken girişi seçin ve **Tamam** ögesine basın.
- Numara eklemek için **Menü** → **Ekle** → **Numara** ögesini seçin. Açılan **Giriş ekle** penceresinde **Telefon numarası** alanını doldurun ve **Tamam**'a basın.



Şekil 41: Korunan kişiler listesine giriş ekleme

Numara Kişi listesine eklenir.

ÖZEL KİŞİLER LİSTESİNDE BİR NUMARAYI DÜZENLEME

Kişi Listesi yapmadan önce gizli bilgileri gizleme işlevini devre dışı bırakın.

Elle eklenen telefon numaraları yalnızca Kişiler listesini düzenlemek için kullanılabilir. Telefon rehberinden veya SIM kartındaki numaralar listesinden seçilen numaraları düzenlemek mümkün değildir.

► *Kişiler listesindeki bir telefon numarasını düzenlemek için:*

1. **Menü** → **Gizlilik Koruması** ögesini seçin.
Gizlilik Koruması penceresi açılacaktır.
2. **Kişi Listesi** ögesini seçin.
Kişi listesi penceresi açılacaktır.
3. Kişi listesinde düzenlenecek bir numara seçin ve daha sonra **Menü** → **Düzenle** ögesini seçin.
Düzenle ekranı açılır.
4. **Telefon numarası** alanındaki verileri değiştirin.
5. Düzenleme tamamlandığında **Tamam** düğmesine basın.

Numara değiştirilir.

ÖZEL KİŞİLER LİSTESİNDE BİR NUMARAYI SİLME

Kişi listesinde bir numarayı veya listenin tamamını silebilirsiniz.

Kişi Listesi yapmadan önce gizli bilgileri gizleme işlevini devre dışı bırakın.

► *Bir numarayı Kişi listesinden kaldırmak için:*

1. **Menü** → **Gizlilik Koruması** ögesini seçin.
Gizlilik Koruması penceresi açılacaktır.
2. **Kişi Listesi** ögesini seçin.
Kişi listesi penceresi açılacaktır.
3. Silinecek bir numara seçin ve daha sonra **Menü** → **Sil** ögesini seçin.
4. Silme işlemini onaylayın. Bunun için, **Evet** düğmesine basın.

► *Kişi Listesini temizlemek için:*

1. **Menü** → **Gizlilik Koruması** ögesini seçin.
Gizlilik Koruması penceresi açılacaktır.
2. **Kişi Listesi** ögesini seçin.
Kişi listesi penceresi açılacaktır.

3. **Menü** → **Tümünü sil**'i seçin.
4. Silme işlemini onaylayın. Bunun için, **Evet** düğmesine basın.

Kişi listesi boşaltılır.

GİZLENECEK VERİLERİ SEÇME: GİZLİLİK KORUMASI

Gizlilik Koruması, Kişi Listesinde aşağıda belirtilen bilgileri gizleyebilir: kişiler, SMS yazışmaları, arama günlüğü girişleri, gelen aramaları ve SMS mesajları. Gizlilik Korumasının özel numaralar için gizlemesi gereken bilgileri ve olayları seçebilirsiniz.

Gizlilik Koruması ayarlarını düzenlemeden önce Gizlilik Korumasını devre dışı bırakın.

► *Gizlilik Korumasının özel numaralar için gizlemesi gereken bilgileri ve olayları seçmek için:*

1. **Menü** → **Gizlilik Koruması** ögesini seçin.

Gizlilik Koruması penceresi açılacaktır.

2. **Gizli nesnelere** ögesini seçin.

Gizli nesnelere penceresi açılır (bkz. aşağıdaki şekil).

3. **Girişleri gizle** bölümünde özel numaralar için gizlenmesi gereken bilgileri seçin. Aşağıdaki ayarlar bulunur:

- **Kişiler** – Kişiler listesindeki tüm gizli numaralar ile ilgili bilgileri gizler.
- **SMS** – gizli numaralar için **Gelen**, **Giden** ve **Gönderilmiş** dizinlerindeki SMS mesajlarını gizler.
- **Aramalar** – gizli numaralardan gelen aramaları kabul ederken arayanın numarasını belirlemez ve aramalar listesinde gizli numaralar ile ilgili bilgi görüntülenmez (gelen, giden ve cevapsız).

4. **Olayları gizle** bölümünde özel numaralar için gizlenmesi gereken olayları seçin. Aşağıdaki ayarlar bulunur:

- **Gelen SMS** – gelen SMS mesajlarının teslim edildiğini görüntülenmez (gizli numaradan yeni bir SMS mesajı alındığına ilişkin ekranda hiçbir mesaj görüntülenmez). Özel numaralardan alınan tüm SMS mesajları Gizlilik Koruması devre dışı bırakıldığında görülecek şekilde görüntülenir.

- **Gelen aramalar** – özel numaralardan gelen aramaları engeller (bu durumda arayan meşgul sesi duyacaktır). Gizlilik Koruması devre dışı bırakıldığında gelen arama hakkındaki bilgiler görüntülenecektir.



Şekil 42: Gizli nesnelere seçme

5. **Tamam** düğmesine basın.

AĞ ETKİNLİĞİNİ FİLTRELEME. GÜVENLİK DUVARI

Bu bölümde, aygıtınızdaki ağ bağlantılarını kontrol eden Güvenlik Duvarı ile ilgili bilgiler verilmektedir. Bu bölümde Güvenlik Duvarı'nın nasıl etkinleştirileceği/devre dışı bırakılacağı ve istenen modun nasıl seçileceği açıklanmaktadır.

BU BÖLÜMDE

Güvenlik Duvarı hakkında	98
Güvenlik Duvarını etkinleştirme/devre dışı bırakma	99
Güvenlik Duvarı güvenlik düzeyini seçme	99
Engelleme bildirimleri	100

GÜVENLİK DUVARI HAKKINDA

Güvenlik Duvarı, seçilmiş olan mod temel alınarak aygıtınızın ağ bağlantılarını izler. Güvenlik duvarı, izin verilen bağlantıları (örn: uzaktan yönetim sistemi ile senkronizasyon kumak) ve engellenen bağlantıları (örn: internette arama, dosya indirme) belirlemenize olanak sağlar.

Kurulumdan sonra Kaspersky Mobile Security 9 Güvenlik Duvarı devre dışı bırakılır.

Güvenlik duvarı, engellenen bağlantılar ile ilgili bildirimler ayarını etkinleştirir (bkz. "Güvenlik Duvarını etkinleştirme/devre dışı bırakma" bölümü, sayfa [99](#)).

Güvenlik duvarının işleyişiyle ilgili bilgiler uygulama günlüğüne girilir (bkz. "Uygulama Günlükleri" bölümü, sayfa [112](#)).

GÜVENLİK DUVARINI ETKİNLEŞTİRME/DEVRE DIŞI BIRAKMA

Güvenlik Duvarının belirlediği izin verilen ve engellenen bağlantılara göre modu seçebilirsiniz. Aşağıdaki Güvenlik Duvarı modları kullanılabilir:

- **Kapalı** Tüm ağ etkinliklerine izin verilir. Bu güvenlik düzeyi, varsayılan olarak seçilmiştir.
- **Minimum koruma:** yalnızca gelen bağlantılar engellenir. Giden bağlantılara izin verilir.
- **Maksimum koruma:** tüm gelen bağlantılar engellenir. E-postaları denetleme, web sitelerini görüntüleme ve dosyaları karşıdan yüklemeye erişilebilir. Giden bağlantılar yalnızca SSH, HTTP, HTTPS, IMAP, SMTP, POP3 bağlantı noktaları kullanılarak kurulabilir.
- **Tümünü engelle:** Uygulamanın veritabanlarının güncellenmesi ve lisansının yenilenmesi dışında tüm ağ etkinliklerini engeller.

Güvenlik duvarının güvenlik düzeyini değiştirebilirsiniz (bkz. "Güvenlik duvarı güvenlik düzeyini seçme" bölümü, sayfa [99](#)). Geçerli mod, **Mod** menü öğesinin yanındaki **Güvenlik duvarı** penceresinde görüntülenir.

GÜVENLİK DUVARI GÜVENLİK DÜZEYİNİ SEÇME

Ayarların değerlerini değiştirmek için, aygıtın kumanda kolunu veya kalemı kullanın.

➔ *Güvenlik Duvarı güvenlik düzeyini ayarlamak için:*

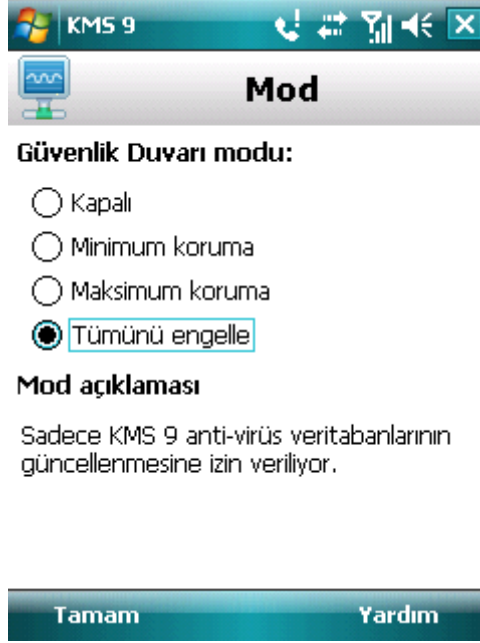
1. **Menü** → **Güvenlik duvarı** öğesini seçin.

Güvenlik duvarı penceresi açılacaktır.

2. **Mod** öğesini seçin.

Ayarlar penceresi açılacaktır.

3. Önerilen güvenlik düzeylerinden birini seçin (bkz. aşağıdaki Şekil).



Şekil 43: Güvenlik Duvarı güvenlik düzeyi seçimi

4. **Tamam** düğmesine basın.

ENGELLEME BİLDİRİMLERİ

Güvenlik duvarı engellenen bağlantıların bildirimlerinin alınmasına izin verir. Güvenlik duvarı bildirimlerini yönetebilirsiniz.

Varsayılan olarak bildirimlerin engellenmesi devre dışı bırakılır.

► *Engelleme bildirimlerini yönetmek için:*

1. **Menü** → **Güvenlik duvarı** ögesini seçin.

Güvenlik duvarı penceresi açılacaktır.

2. **Bildirimler** ögesini seçin.

Bildirimler ekranı açılır (bkz. aşağıdaki şekil).



Şekil 44: Engelleme bildirimlerinin iletiminin yapılandırılması

3. **Bildirimleri engelleme** bölümünde, mevcut eylemlerden birini seçin:
 - **Göster** – bildirimlerin iletimini etkinleştirir. Güvenlik duvarı, engellenen bir bağlantıyı bildirir.
 - **Gösterme** – bildirimlerin iletimini devre dışı bırakır. Güvenlik duvarı, engellenen bir bağlantıyı size bildirmez.
4. **Tamam** düğmesine basın.

KİŞİSEL VERİLERİ ŞİFRELEME

Bu bölümde, aygıtınızdaki dizinleri şifreleyebilecek olan Şifreleme hakkında bilgiler verilmektedir. Aynı zamanda seçilmiş dizinlerin nasıl şifreleneceği ve şifrelerinin nasıl çözüleceğini de açıklamaktadır.

BU BÖLÜMDE

Şifreleme hakkında.....	102
Verileri şifreleme.....	102
Verilerin şifresini çözme	104
Şifreli verilere erişimi engelleme.....	105

ŞİFRELEME HAKKINDA

Şifreleme, şifrelenecek dizinler listesindeki verileri şifreler. Şifreleme işlevinin çalışma şekli, aygıtınızın işletim sistemi içinde yerleşik olan aynı isimli işlevin çalışma şeklini esas alır. Şifreleme işlevi, sistem dizinleri dışında herhangi bir tür dizinin şifrlenmesini sağlar. Şifrelenecek olan dizinleri, aygıtın belleğinden veya depolama kartı üzerinden seçebilirsiniz. Şifrelenmiş verilere erişim sağlamak için, uygulama ilk kez çalıştırıldığı zaman ayarlanmış olan uygulama PIN kodunu girin.

Yürütülebilen dosyaları şifrelenmiş dizinin dışında çalıştırmak için, önce dizinin şifresini çözmeniz gerekir. Bunun için öncelikle uygulama PIN kodunun girilmesi gerekir.

Şifreli dizinlere erişmek için uygulama gizli kodunu girin (bkz. "Gizli kodu ayarlama" bölümü, sayfa 28). Aygıt, enerji tasarrufu moduna geçtikten sonra ayarlanan süre sona erdiğinde (bkz. "Şifreli verilere erişimin korunması" bölümü, sayfa 105), verilere erişim otomatik olarak engellenir.

Dizindeki dosyalar, **Şifrele** komutu verildiğinde şifrelenecektir. Sonrasında, dosyalar şifrenir ve dizine taşındığında, dizinden çıkarıldığında veya dosyalara erişildiğinde anında şifreleri çözülür.

Yürütülebilen dosyaları şifrelenmiş dizinin dışında çalıştırmak için, önce dizinin şifresini çözmeniz gerekir.

Kurulumdan sonra Kaspersky Mobile Security 9 Şifreleme bileşeni devre dışı bırakılır.

Bileşenin işleyişiyle ilgili bilgiler uygulama günlüğüne girilir(bkz. "Uygulama Günlükleri" bölümü, sayfa 112).

VERİLERİ ŞİFRELEME

Şifreleme, sistem dizinleri dışında, aygıtın belleğinde veya depolama kartındaki dizinlerdeki tüm verilerin şifrlenmesine olanak verir.

Önceden şifrelenmiş ve şifresi çözülmüş tüm dosyaların listesine **Şifreleme** pencresindeki dizin listesi öğesinden erişilebilir.

Ayrıca dizinler listesindeki bir dizini veya tüm dizinleri anında şifreleyebilirsiniz.

► Verileri şifrelemek için:

1. **Menü** → **Şifreleme** ögesini seçin.

Şifreleme penceresi açılacaktır.

2. **Dizin Listesi** ögesini seçin.

Dizin listesi penceresi açılacaktır.

3. **Menü** → **Dizin ekle** düğmesine basın.

Aygıtınızın sistem dosyaları ağacını gösteren bir ekran açılacaktır.

4. Şifrelenecek dizini seçin ve **Şifrele** düğmesine basın (bkz. aşağıdaki şekil).

Dosya sisteminde dolaşmak için, aygıtın kalemını veya kumanda kolu düğmelerini kullanın.



Şekil 45: Veri şifreleme

Şifreleme işlemi tamamlandığında, Kaspersky Mobile Security 9 bunu size bildirir. Bildirim penceresi açılır.

5. **Tamam** düğmesine basın.

Şifreli bir dizin için, **Şifrele** ögesinin **menüde** adı **Şifreyi Çöz** olarak değişir.

Şifreleme işleminden sonra şifreli dizindeki verilerle çalışırken, şifreli dizinden taşırken veya daha sonra yeni dizine yeni veriler eklediğinizde, veriler otomatik olarak şifrelenir ve şifresi çözülür.

► *Listedeki tüm dizinleri aynı anda şifrelemek için aşağıdaki adımları uygulayın:*

1. **Menü** → **Şifreleme** ögesini seçin.

Şifreleme penceresi açılacaktır.

2. **Dizin Listesi** ögesini seçin.

Dizin listesi penceresi açılacaktır.

3. **Menü** → **Eklenen işlemler** → **Tümünü şifrele** öğesini seçin.

Şifreleme işlemi tamamlandığında, Kaspersky Mobile Security 9 bunu size bildirir. Bildirim penceresi açılır.

4. **Tamam** düğmesine basın.

VERİLERİN ŞİFRESİNİ ÇÖZME

Önceden şifrelenmiş verilerin şifresini tamamen çözebilirsiniz (bkz. "Veri şifreleme" bölümü, sayfa [102](#)). Aygıt üzerinde önceden şifrelediğiniz bir dizinin veya tüm dizinlerin şifrelerini çözebilirsiniz.

► **Önceden şifrelenmiş bir dizinin şifresini çözmek için:**

1. **Menü** → **Şifreleme** öğesini seçin.

Şifreleme penceresi açılacaktır.

2. **Dizin Listesi** öğesini seçin.

Önceden şifresi çözülmüş ve şifrelenmiş dizinlerin listesini içeren **Dizin listesi** penceresi açılacaktır.

3. Şifrelenmiş dizini listeden seçin ve **Menü** → **Şifre Çöz** düğmesine basın (bkz. aşağıdaki şekil).



Şekil 46: SWEçeneği etkinleştirme

Şifre çözme işlemi tamamlandığında, Kaspersky Mobile Security 9 bunu size bildirir. Bildirim penceresi açılır.

4. **Tamam** düğmesine basın.

Şifresi çözülmüş bir dizin için **Şifre çöz** öğesi **Menüde Şifrele** olarak değişir. Veri şifrelemeyi yeniden kullanabilirsiniz (bkz. "Veri Şifreleme" bölümü, sayfa [102](#)).

► *Listedeki tüm izinleri aynı anda çözmek için aşağıdaki adımları uygulayın:*

1. **Menü** → **Şifreleme** ögesini seçin.

Şifreleme penceresi açılacaktır.

2. **Dizin Listesi** ögesini seçin.

Dizin listesi penceresi açılacaktır.

3. **Menü** → **Eklene işlemler** → **Tümünün şifresini çöz** ögesini seçin.

Şifre çözme işlemi tamamlandığında, Kaspersky Mobile Security 9 bunu size bildirir. Bildirim penceresi açılır.

4. **Tamam** düğmesine basın.

ŞİFRELİ VERİLERE ERİŞİMİ ENGELLEME

Şifreleme, şifreli dizinlere erişimin engellenmesinin başlayacağı zamanı ayarlayabilir. Bu işlem, aygıtınız güç tasarrufu moduna geçtiği anda etkinleştirilir. Şifrelenmiş verileri değiştirmek için, uygulama PIN kodunu girin. Gizli kod şifreli verilerle çalışmaya devam etmek için girilmelidir (bkz. "Gizli kodu ayarlama" bölümü, sayfa [28](#)).

Şifreli verilere erişimi anlık olarak da engelleyebilir ve gizli kod istemini etkinleştirebilirsiniz.

► *Dizine belli bir süre sonra erişimi engellemek için aşağıdaki görevleri gerçekleştirin:*

1. **Menü** → **Şifreleme** ögesini seçin.

Şifreleme penceresi açılacaktır.

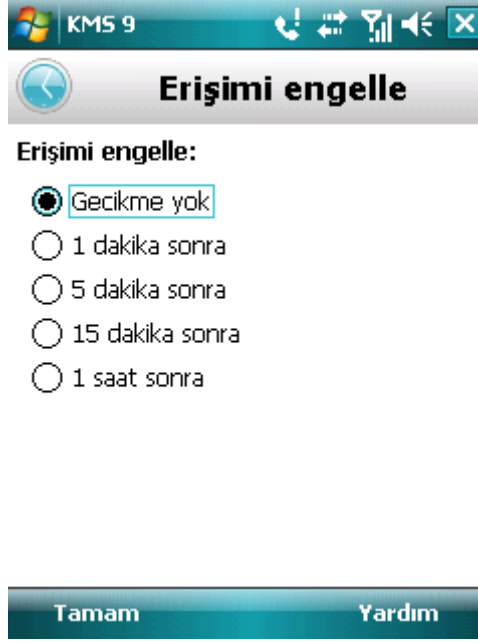
2. **Erişimi engelle** ögesini seçin.

Erişimi engelle penceresi açılacaktır.

3. Aygıt boşa moduna geçtikten sonra verilerin erişebilir olacağı süreyi girin. **Erişimi engelle** ayarı için önerilen değerlerden birini seçin {bkz. aşağıdaki şekil}:

- **Hemen.**
- **1 dakika sonra.**
- **5 dakika sonra.**

- 15 dakika sonra.
- 1 saat sonra.



Şekil 47: Şifreli verilere erişimi engelleme

4. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

► Bir dizine erişimi hemen engellemek için,

aygıt bildirim alanındaki Kaspersky Mobile Security 9 simgesine basın ve **Verileri kilitle** öğesini seçin (bkz. aşağıdaki şekil).



Şekil 48: Aygıt bildirim alanındaki uygulama içerik menüsü

UYGULAMANIN VERİTABANLARINI GÜNCELLEME

Bu bölüm, aygıtınızın korumasının güncel olmasını sağlayan uygulama veritabanlarını güncelleme hakkında bilgi verir. Ayrıca, yüklü anti-virüs veritabanlarındaki bilgilerin nasıl görüntüleneceği, güncellenmenin nasıl elle başlatılacağı ve anti-virüs veritabanlarının otomatik güncellemelerinin nasıl yapılandırılacağı da bu bölümde açıklanmaktadır.

BU BÖLÜMDE

Uygulamanın veritabanlarını güncelleme hakkında.....	107
Veritabanı bilgilerini görüntüleme	108
Elle güncelleme	108
Çizelge ile güncelleme	109
Dolaşımdayken güncelleme	110

UYGULAMANIN VERİTABANLARINI GÜNCELLEME HAKKINDA

Uygulama o sırada bilinen tüm kötü amaçlı yazılımlar ve diğer istenmeyen programlar ve bunların temizlenme yöntemlerinin yanı sıra diğer istenmeyen nesnelere hakkında açıklamalar içeren uygulama anti-virüs veritabanlarını kullanarak aygıtı kötü amaçlı programlara karşı tarar. Anti-virüs veritabanlarınızı güncel tutmanız son derece önemlidir.

Uygulama veri tabanlarının düzenli olarak güncellenmesi önerilir. Son güncellemeden bu yana 15 günden daha uzun bir süre geçmişse, veritabanlarının son kullanma tarihleri geçmiş sayılır. Koruma daha az güvenilir olur.

Kaspersky Mobile Security 9, uygulama anti-virüs veritabanı güncellemelerini Kaspersky Lab güncelleme sunucularından gerçekleştirir. Bunlar Kaspersky Lab ürünlerinin tümünün veritabanlarının güncellemelerini içeren özel internet siteleridir.

Uygulamanın Anti-Virüs veritabanlarını güncellemek için, mobil aygıtınızda yapılandırılmış bir İnternet bağlantınızın olması gerekir.

Uygulamanın anti-virüs veritabanları aşağıdaki algoritmaya göre güncellenir:

1. Uygulamanın mobil aygıtınızda yüklü olan veritabanları Kaspersky Lab'ın özel güncelleme sunucusunda bulunan veritabanlarıyla karşılaştırılır.
2. Kaspersky Mobile Security 9 aşağıdaki işlemlerden birini gerçekleştirir:
 - En son anti-virüs veritabanları yüklüyse, ekranda bir bilgilendirme mesajı görüntülenir.
 - Yüklü anti-virüs veritabanları farklıysa, yeni bir güncelleme paketi karşıdan yüklenir.

Güncelleme işlemi tamamlandığında, bağlantı otomatik olarak kesilir. Bağlantı güncelleme başlatılmadan önce kurulmuşsa, kullanılması için açık kalır.

Güncelleme görevini, aygıt başka görevlerle meşgul değilken elle başlatabilir veya otomatik güncellemeleri zamanlayabilirsiniz.

Kullanılan anti-virüs veritabanları hakkındaki bilgilerin ayrıntıları **Veritabanı bilgisine** menü ögesindeki **Ek** penceresinden ulaşılabilir.

Anti-virüs veritabanlarının güncellemeleri ile ilgili bilgiler uygulamanın günlüğünde kayıtlıdır (bkz. "Uygulama günlükleri" bölümü, sayfa [112](#)).

VERİTABANI BİLGİLERİNİ GÖRÜNTÜLEME

Uygulamanın yükü olan anti-virüs veritabanları ile ilgili aşağıdaki bilgileri görebilirsiniz: son güncelleme, veritabanının yayın tarihi, veri tabanı boyutu ve veritabanındaki girişlerin sayısı.

► *Veritabanları hakkındaki bilgileri görmek için:*

1. **Menü** → **Ek** ögesini seçin.

Ek penceresi açılacaktır.

2. **Veritabanı bilgileri** sekmesini seçin.

Veritabanı bilgisi penceresi, kurulu programın anti-virüs veritabanları ile ilgili bilgilerle açılır.

ELLE GÜNCELLEME

Anti-virüs Veritabanlarını güncelleme işlemi elle başlatabilirsiniz.

► *Veritabanı güncelleme işlemi başlatmak için:*

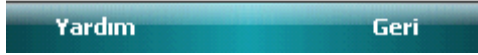
1. **Menü** → **Anti-Virüs** ögesini seçin.

Anti-Virüs penceresi açılacaktır.

2. **Güncelle** ögesini seçin.

Bu, **Güncelle** penceresini açacaktır.

3. **Güncelle** ögesini seçin (bkz. aşağıdaki Şekil).



Şekil 49: Güncelleme: elle başlatma

Uygulama Kaspersky Lab sunucusundan veritabanlarını güncelleme işlemini başlatır. Güncelleme işlemi bilgileri ekranda görüntülenir.

ZAMANLANMIŞ GÜNCELLEME

Düzenli güncellemeler aygıtınızın kötü amaçlı nesnelere karşı etkin bir şekilde korunmasının önkoşuludur. Size kolaylık sağlaması için otomatik anti-virüs veritabanı güncellemelerini yapılandırabilirsiniz.

► *Uygulamanın anti-virüs veritabanlarının otomatik güncellenmesini yapılandırmak için:*

1. **Menü** → **Anti-Virüs** ögesini seçin.

Anti-Virüs penceresi açılacaktır.

2. **Güncelle** ögesini seçin.

Bu, **Güncelle** penceresini açacaktır.

3. **Güncelleme çizelgesi** ögesini seçin.

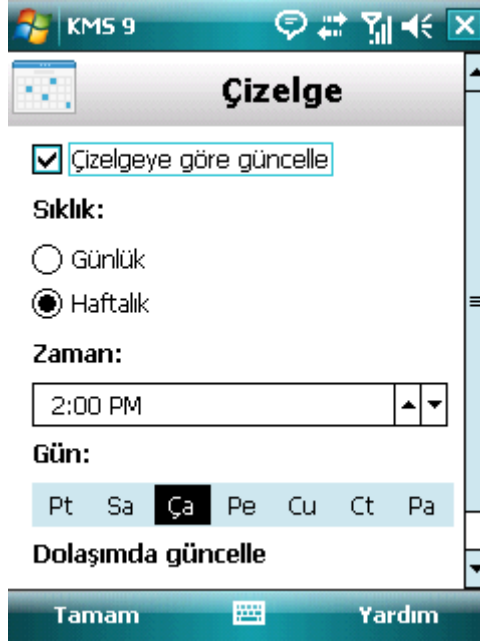
Çizelge ekranı açılacaktır.

4. **Çizelgeye göre güncelle** kutusunu seçin (bkz. Aşağıdaki şekil).

5. Güncellemeleri başlatmak için bir çizelge oluşturun. Bunun için, **Sıklık** ayarı için bir değer seçin:

- **Günlük** - anti-virüs veritabanları her gün güncellenir. Ardından **Saat** ayarı için değer girin.

- **Haftalık** - Uygulamanın anti-virüs veritabanları haftada bir güncellenir. Daha sonra **Saat** ve **Haftanın günü** ayarları için değer seçin.



Şekil 50: Otomatik güncelleme ayarları

6. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

DOLAŞIMDAYKEN GÜNCELLEME

Dolaşım bölgesindeyken zamanlanmış anti-virüs veritabanı güncellemelerine izin verebilir / bu güncellemeleri engelleyebilirsiniz. Dolaşırken güncelleme engellenmiş ise elle güncellemeye standart modda erişilebilir.

- *Dolaşım bölgesindeyken zamanlanmış anti-virüs veri tabanı güncellemelerine izin vermek için aşağıdaki işlemleri gerçekleştirin:*

1. **Menü** → **Anti-Virüs** ögesini seçin.

Anti-Virüs penceresi açılacaktır.

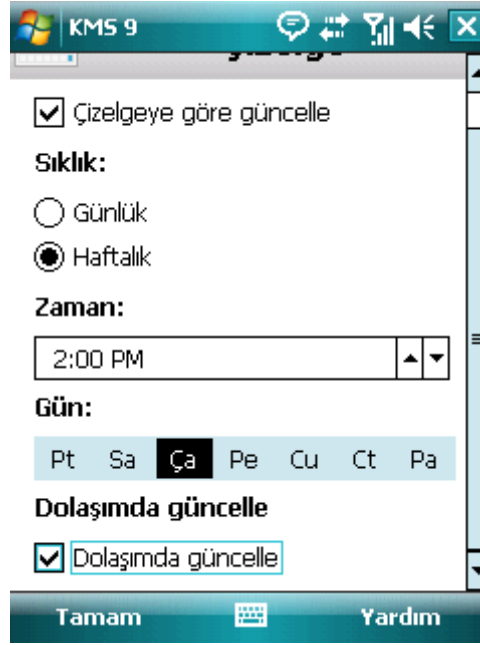
2. **Güncelle** ögesini seçin.

Bu, **Güncelle** penceresini açacaktır.

3. **Güncelleme çizelgesi** ögesini seçin.

Çizelge ekranı açılacaktır.

4. **Dolaşımda güncelleme** bloğudna **Dolaşımda güncelle** kutusunu işaretleyin.



Şekil 51: Dolaşım modunda güncellemeleri yapılandırma

5. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

UYGULAMA GÜNLÜKLERİ

Bu bölümde, her bileşenin işlemlerini ve her görevin gerçekleştirilmesini (ör. uygulama veritabanı güncellemeleri, virüs taramaları) kaydeden günlüklerle ilgili bilgiler verilmektedir.

BU BÖLÜMDE

Günlükler hakkında	112
Günlük kayıtlarını görüntüleme.....	112
Günlük kayıtlarını silme	112

GÜNLÜKLER HAKKINDA

Uygulamanın günlükleri Kaspersky Mobile Security 9'un işleyişi sırasında oluşan olaylar hakkındaki kayıtları depolar. Girişler en yeni olaydan başlayarak olayın zamanına göre sıralanır.

Her bileşen için ayrı bir olay günlüğü kullanılır.

GÜNLÜK KAYITLARINI GÖRÜNTÜLEME

► *Günlükte depolanan tüm kayıtları görüntülemek için:*

1. **Menü** → **Ek** öğesini seçin.
Ek penceresi açılacaktır.
2. **Günlükler** öğesini seçin.
Günlükler penceresi açılacaktır.
3. Olaylar günlüğünü görmek istediğiniz bir bileşeni seçin.

Seçilen bileşenin olaylar günlüğü açılır.

► *Ayrıntılı günlük kaydı bilgilerini görüntülemek için,*

istenen kaydı seçin ve **Ayrıntılar** düğmesine basın.

Ayrıntılar ekranı uygulamanın eylemi ve ayrıntıları hakkında bilgi görüntüler. Örneğin "Karantinaya alınmış nesne" eylemi için virüslü dosyaya giden yol da görüntülenir.

► *Günlüklere geri dönmek için:*

Menü → **Geri** düğmesine basın.

GÜNLÜK KAYITLARINI SİLME

Tüm günlükleri temizleyebilirsiniz. Kaspersky Mobile Security 9'un tüm bileşenlerinin işleyişi hakkındaki bilgiler silinecektir.

► Tüm günlükleri silmek için:

1. **Menü** → **Ek** ögesini seçin.
Ek penceresi açılacaktır.
2. **Günlükler** ögesini seçin.
Günlük penceresi açılacaktır.
3. Herhangi bir bileşenin günlüğünü açın.
4. **Menü** → **Tümünü sil** ögesini seçin (bkz. aşağıdaki şekil).



Şekil 52: Kayıtları silme

5. **Evet** düğmesine basarak kaldırmayı onaylayabilirsiniz.

Tüm bileşen günlüklerindeki tüm kayıtlar silinir.

EK AYARLARI YAPILANDIRMA

Bu bölüm Kaspersky Mobile Security 9 uygulamasının ek seçenekleri hakkında bilgi vermektedir: uygulamanın sesli bildirimini ve ekran arka ışığının yönetimi, ipuçlarını, koruma simgesini ve koruma durumu penceresini etkinleştirme / devre dışı bırakma.

BU BÖLÜMDE

Gizli kodu değiştirme.....	114
Uyarıları görüntüleme.....	114
Sesli bildirimleri yapılandırma.....	115

GİZLİ KODU DEĞİŞTİRME

Uygulamanın etkinleştirildikten sonra ayarlanan gizli kodunu değiştirebilirsiniz.

► *Gizli kodu değiştirmek için:*

1. **Menü** → **Ek** ögesini seçin.
Ek penceresi açılacaktır.
2. **Ayarlar** ögesini seçin.
Ayarlar penceresi açılacaktır.
3. **Kod değişikliği** ögesini seçin.
4. **Gizli kodu girin**, Kodu gir alanına girin.
5. **Bir kod ayarlayın** alanına yeni kodu girin ve **Onayla**, daha sonra değişiklikleri kaydetmek için **Tamam** düğmesine basın.

UYARILARI GÖRÜNTÜLEME

Bileşenin ayarlarını yapılandırırken, Kaspersky Mobile Security 9 varsayılan olarak, seçilen işlevin kısa açıklamasıyla birlikte bir uyarı görüntüler. Kaspersky Mobile Security 9 ipuçlarının görüntülenmesi yapılandırabilirsiniz.

► *İpuçlarının görüntülenmesini yapılandırmak için aşağıdaki işlemleri gerçekleştirin:*

1. **Menü** → **Ek** ögesini seçin.
Ek penceresi açılacaktır.
2. **Ayarlar** ögesini seçin.
Ayarlar penceresi açılacaktır.
3. **İpuçları** ögesini seçin.
İpuçları penceresi açılacaktır.
4. **İpuçları** ayarı için önerilen değerlerden birini seçin:
 - **Göster:** Seçilen işlevin ayarlarını yapılandırmadan önce ipuçlarını görüntüler.
 - **Gizle:** İpuçlarını görüntülemez.
5. **Tamam** düğmesine basın.

SESLİ BİLDİRİMLERİ YAPILANDIRMA

Uygulamanın çalışmasının sonucunda belirli olaylar oluşur: Örneğin virüslü bir nesne veya bir virüs bulunabilir, lisans geçerlilik süresi sona eriyordur. Uygulamanın böyle her olayı size bildirmesi için gerçekleşen olayın sesli bildirimini etkinleştirebilirsiniz.

Kaspersky Mobile Security 9 varsayılan olarak, sesli bildirim yalnızca aygıtın ayarlanmış moduna göre içerir.

Ayarların değerlerini değiştirmek için, aygıtın kumanda kolunu veya kalemi kullanın.

► *Uygulamanın sesli bildirimini yönetmek için aşağıdaki işlemleri gerçekleştirin:*

1. **Menü** → **Ek** ögesini seçin.
Ek penceresi açılacaktır.
2. **Ayarlar** ögesini seçin.
Ayarlar penceresi açılacaktır.
3. **Ses** ögesini seçin.
Ses penceresi açılacaktır.
4. **Sesli bildirimler** ayarının değerlerinden birini seçin (bkz. aşağıdaki Şekil):
 - **Etkinleştir:** Aygıtın seçili profiline bakılmaksızın, bildirim sesli yapılır.
 - **Kapat:** Sesli bildirim kullanılmaz.
5. Değişiklikleri kaydetmek için **Tamam** düğmesine basın.

TEKNİK DESTEK HİZMETİ İLE İLETİŞİME GEÇME

Eğer zaten Kaspersky Internet Security'yi satın aldıysanız, telefon ya da Internet üzerinden Teknik Destek Servisi ile görüşerek ürün hakkında bilgi alabilirsiniz.

Teknik Destek Servisi uzmanları, uygulamanın kurulması ve kullanılmasıyla ilgili tüm sorularınızı yanıtlayacaklardır. Aynı zamanda, aygıtınıza zararlı uygulama bulaştığında, bu zararlı uygulamanın sonuçlarını ortadan kaldırmanıza da yardımcı olacaklardır.

Teknik destek servisi ile görüşmeden önce Kaspersky Lab'ın ürünleri için Destek kuralları'nı okuyun (<http://support.kaspersky.com/support/rules>).

Sorunuzu Teknik Destek Servisi'ne e-posta ile gönderme

Sorunuzu, <http://support.kaspersky.com/helpdesk.html> adresindeki Yardım masası web formuna girerek Teknik Destek Servisi uzmanlarına gönderebilirsiniz.

Sorunuzu, Rusça, İngilizce, Almanca, Fransızca ya da İspanyolca yazabilirsiniz.

Sorunuzu içeren bir e-posta mesajı göndermek için Teknik Destek Servisi'nin web sitesine kayıt olurken aldığınız **Müşteri Kodu** ve **parola**'yı eklemeniz gerekir.

Eğer Kaspersky Lab'ın uygulamalarının kayıtlı kullanıcısı değilseniz bir kayıt formu doldurabilirsiniz (<https://support.kaspersky.com/personalcabinet/registration/form/>). Kayıt sırasında uygulamanız için *etkinleştirme kodunu* ya da *anahtar dosya adını* girin.

Teknik Destek Servisi isteğinize Kişisel Kabininizde (<https://support.kaspersky.com/PersonalCabinet>) ve sorunuzda belirttiğiniz e-posta adresine e-posta göndererek yanıtlayacaktır.

Sorunuzda lütfen karşılaştığınız sorunu yazın. Aşağıdaki zorunlu alanları belirtin:

- **İstek türü.** Ortaya çıkan soruna en yakın konuyu seçin, örneğin "Ürün Kurulumu/Kaldırması Sorunu" ya da "Anti-Virüs tarama/virüs temizleme sorunu". Eğer ilgili bir konu bulamıyorsanız, "Genel soru"yu seçin.
- **Uygulama adı ve sürüm numarası.**
- **İstek metni.** Karşılaştığınız sorunu, mümkün olduğunca çok bilgi vererek açıklayın.
- **Müşteri Kodu ve parola.** Teknik Destek Servisi'nin web sitesine kayıt olurken aldığınız Müşteri Kodu ve parola'yı girin.
- **E-posta adresi.** Teknik Destek Servisi, sorunuzu bu e-posta adresine mesaj göndererek yanıtlayacaktır.

Telefonla teknik destek

Eğer acil bir sorunuz varsa, Teknik Destek Servisi'ni arayabilirsiniz. Yerel (http://support.kaspersky.com/support/support_local) ya da uluslararası (<http://support.kaspersky.com/support/international>) Teknik Destek Servisi ile görüşmeden önce lütfen aygıtınız ve yüklü anti-virüs uygulamasıyla ilgili gerekli bilgileri (<http://support.kaspersky.com/support/details>) hazırlayın. Bu sayede uzmanlarımız size daha çabuk yardımcı olabileceklerdir.

SÖZLÜK

A

ANTI-VİRÜS VERİ TABANLARI

Kaspersky Lab uzmanları tarafından oluşturulan ve bilgisayar güvenliğine ilişkin tüm mevcut tehditlerin yanı sıra bunların saptanmasına ve temizlenmesine ilişkin ayrıntılı açıklamaları içeren veritabanları. Bu veritabanları yeni tehditler ortaya çıktıkça Kaspersky Lab tarafından güncellenir.

ARŞİV

Arşiv olabilecek bir veya birkaç nesne "içeren" dosya.

B

BEYAZ LİSTE

Bu listedeki girişler, aşağıdaki bilgileri içerirler:

- Arama/SMS Filtresinin gelen aramaları ve / veya SMS'leri ilettiği telefon numarası.
- Arama/SMS Filtresinin bu numaradan gelen aramaları ve SMS'leri ilettiği olayların türleri. Aşağıdaki olay türleri mevcuttur: aramalar ve SMS, sadece arama ve sadece SMS.
- Bir SMS'i istenmeyen (spam değil) olarak sınıflandırmak için Arama&SMS Filtresi tarafından kullanılan anahtar sözcük. Arama/SMS Filtresi anahtar ifadeyi içeren SMS'leri iletirken diğer tüm SMS'leri engeller.

BİR NESNENİN ENGELLENMESİ

Harici uygulamalardan gelen bir nesneye erişimi engeller. Engellenen bir nesne okunamaz, yürütülemez, değiştirilemez veya silinemez.

BİR NESNENİN SİLİNMESİ

Orijinal konumundan fiziksel olarak silerek bir nesnenin işlenmesi yöntemi. Bu işlemi, temizlenemeyen tüm kötü niyetli nesnelere uygulamanız önerilir.

D

DOSYA MASKELEME

Joker karakterler kullanarak bir dosya adının ve uzantısının gösterilmesi. Dosya maskelemede kullanılan iki temel joker karakter "*" ve "?"'dir, burada "*" herhangi bir sayıyı veya karakteri temsil ederken "?" herhangi bir tek karakteri simgeler. Bu joker karakterleri kullanarak herhangi bir dosyayı temsil edebilirsiniz. Dosya adının ve dosya uzantısının her zaman ayrılması gerektiğini unutmayın.

İ

İSTEK ÜZERİNE TARAMALAR

Kaspersky Lab uygulamasının kullanıcı tarafından başlatılan ve herhangi bir dosyanın taranması amacıyla kullanılan bir işletim modu.

K

KARA LİSTE

Bu listedeki girişler, aşağıdaki bilgileri içerirler:

- Arama/SMS Filtresinin gelen aramaları ve / veya SMS'leri engellediği telefon numarası.
- Arama/SMS Filtresinin bu numaradan gelen aramaları ve SMS'leri engellediği olayların türleri. Aşağıdaki olay türleri mevcuttur: aramalar ve SMS, sadece arama ve sadece SMS.
- Arama/SMS Filtresinin SMS'leri istenmeyen (spam) olarak sınıflandırmak için kullandığı anahtar ifade. Arama/SMS Filtresi anahtar ifadeyi içeren SMS'leri engellerken diğer tüm SMS'leri iletir.

KARANTİNA

Aygıt taramaları veya Koruma işlemi ile tespit edilen tüm olası virüslü nesnelere depolamak için kullanılan dizin.

L

LİSANS SÜRESİ

Kaspersky Lab uygulamanızın tüm özelliklerini kullanabileceğiniz zaman dilimi. Lisansın süresi sona erdiğinde uygulama sınırlı işlevsellik moduna geçer. Bu moda, uygulamada bulunan aşağıdaki işlemler kullanılabilir:

- tüm bileşenlerin devre dışı bırakılması;
- bir veya birkaç dizinin şifrelenmesi;
- kişisel verilerin gizlenmesinin devre dışı bırakılması;
- gizli bilgilerin otomatik gizlenmesinin engellenmesi;
- uygulamanın yardım sisteminin görüntülenmesi.

N

NESNELERİN KARANTİNAYA ALINMASI

Virüs bulaşma olasılığı olan bir nesneye erişimin engellenerek ve orijinal konumunun Karantina dizinine taşınarak işlenmesinde kullanılan yöntem. Karantinede nesne şifreli bir biçimde depolanır, bu da aygıtta virüs bulaştırmalarını engeller.

NESNELERİN TEMİZLENMESİ

Virüs bulaşmış nesnelere işlemek için kullanılan, verilerin tamamen veya kısmen kurtarılması ile sonuçlanan veya nesnelere temizlenemeyeceği kararının verildiği bir yöntem. Nesnelere temizlenmesi uygulama veritabanına göre gerçekleştirilir. Bir dosyanın uygun verileri temizleme işlemi sırasında kaybolabilir.

NESNENİN GERİ YÜKLENMESİ

Bir nesnenin Karantineden orijinal dizinine (karantinaya alınmadan, temizlenmeden veya silinmeden önce depolandığı dizin) veya başka bir kullanıcı tanımlı dizine taşınması.

S

SMS MESAJLARINI SİLME

SPAM özellikleri içeren SMS mesajlarının silinmesi yoluyla işleme yöntemi. Bu yöntemi, kesinlikle spam içerdiğini bildiğiniz SMS mesajları için uygulamanız önerilmektedir.

SAYISAL OLMAYAN NUMARA

Harfler içeren ya da yalnızca harflerden oluşan bir telefon numarası.

U**UYGULAMA GİZLİ KODU**

Gizli kod uygulama ayarlarına ve aygıttaki engellenmiş bilgilere yetkisiz erişilmesini engeller. Kullanıcı en az dört karakterden oluşan bu kodu ilk başlattığında ayarlar. Aşağıdaki durumlarda gizli kod istenir:

- uygulama ayarlarına erişim için;
- Şifreli dizinlere erişim için;
- aşağıdaki işlevleri uzaktaki diğer bir aygıttan başlatmak için bir SMS komutu gönderirken: Engelle, Veri Silme, SIM Gözcüsü, GPS Bul, Gizlilik Koruması;
- uygulamayı kaldırırken.

UYGULAMAYI ETKİNLEŞTİRME

Uygulamayı tam işlev moduna geçirme. Uygulamayı etkinleştirmek için kullanıcının lisansa sahip olması gerekmektedir.

V**VERİ TABANLARININ GÜNCELLENMESİ**

Kaspersky Lab uygulamasının, korumayı güncel tutan işlevlerinden biri. Anti-virüs veritabanları Kaspersky Lab güncelleme sunucularından aygıtta kopyalanır ve uygulama otomatik olarak bu veritabanlarına bağlanır.

VİRÜSLÜ NESNE

Kötü amaçlı kod içeren nesne. Uygulama, ikili kodlarını tarayarak ve nesne kodunun bir bölümünün bilinen tehlike kodunun bir bölümü ile aynı olduğunu tespit ederek virüslü nesnelere saptamıştır. Kaspersky Lab uzmanları, aygıtınıza virüs bulaşmasına neden olabileceğinden bu tür nesnelere kullanmanızı tavsiye etmez.

KASPERSKY LAB

Kaspersky Lab, 1997 yılında kurulmuştur. Günümüzde, anti-virüs, anti-spam ve bilgisayar korsanlığı önleme dahil olmak üzere çok çeşitli yüksek performanslı bilgi güvenliği ürünleri alanında öncü geliştiricilerden biridir.

Kaspersky Lab, uluslararası bir şirkettir. Merkezi Rusya Federasyonu'nda bulunan şirket İngiltere, Fransa, Almanya, Japonya, Benelüks ülkeleri, Çin, Polonya, Romanya ve ABD'de (Kaliforniya) ofislere sahiptir. Kısa bir süre önce Fransa'da şirketin yeni bir bölümü olan European Anti-Virus Research Centre kuruldu. Kaspersky Lab'ın iş ortağı ağında, dünyanın çeşitli yerlerinde faaliyet gösteren 500'ü aşkın şirket bulunmaktadır.

Kaspersky Lab şu anda, aralarından 10 tanesi MBA ve 16 tanesi PhD dereceli olmak üzere konusunda uzman binlerce kişi istihdam etmektedir. Kaspersky Lab'ın tüm üst düzey anti-virüs uzmanları Computer Anti-Virus Researchers Organization'a (CARO) üyedir.

Kaspersky Lab, 14 yıl boyunca bilgisayar virüsleriyle mücadele alanında edindiği müthiş deneyim ve bilgi seviyesini temel alan, sınıfının en iyisi güvenlik çözümleri sunmaktadır. Bilgisayar virüsü etkinliklerinin ayrıntılı biçimde analizi, şirketteki uzmanların zararlı uygulamaların geliştirilmesindeki eğilimleri öngörmesini ve kullanıcılara yeni saldırı türlerine karşı zamanında koruma sunmalarını sağlamaktadır. Bu avantaj, Kaspersky Lab ürünleri ve hizmetlerinin temelini oluşturmaktadır. Şirketin ürünleri, tüm ev ve iş kullanıcıları için geniş anti-virüs kapsamı sağlamada diğer sağlayıcıların birçoğuna kıyasla bir adım önde kalmaktadır.

Uzun yıllar süren zorlu çalışmalar, şirketin anti-virüs yazılımı geliştiricileri arasında üst sıralarda yer bulmasını sağlamıştır. Kaspersky Lab, anti-virüs yazılımları için birçok modern standardın geliştirilmesinde öncü olmuştur. Şirketin ana ürünü olan Kaspersky Anti-Virus, iş istasyonları, dosya sunucuları, posta sistemleri, güvenlik duvarları, İnternet ağ geçitleri ve elde taşınabilir bilgisayarlar dahil olmak üzere tüm bilgisayar sistemlerini güvenilir biçimde korur. Kaspersky Lab'ın müşterileri, şirketin ürünlerinin kararlı çalışmasını sağlarken aynı zamanda işletmelere özgü gereksinimlere uyum sağlayan çok çeşitli ek hizmetlerden yararlanmaktadır. Ürünlerinde Kaspersky Anti-Virus ® çekirdeğini kullanan tanınmış üreticiler arasında şunlar gösterilebilir: Nokia ICG (ABD), Aladdin (İsrail), Sybari (ABD), G Data (Almanya), Deerfield (ABD), Alt-N (ABD), Microworld (Hindistan) ve BorderWare (Kanada).

Kaspersky Lab'ın müşterileri, şirketin ürünlerinin kararlı çalışmasını sağlarken aynı zamanda müşterilerin kendi işletmelerine özgü gereksinimlerine tam uyum sağlayan çok çeşitli ek hizmetlerden yararlanmaktadır. Kurumsal anti-virüs uygulama grupları planlıyoruz, kuruyoruz ve bunları destekliyoruz. Kaspersky Lab'ın anti-virüs veritabanı saatte bir güncellenmektedir. Şirket müşterilerine, birçok dilde 24 saat teknik destek sağlamaktadır.

Herhangi bir sorunuz, yorumunuz ya da öneriniz varsa, bayilerimiz aracılığıyla ya da doğrudan Kaspersky Lab ile görüşebilirsiniz. Telefon ya da e-posta ile ayrıntılı bilgi verilmektedir. Her türlü sorunuz ayrıntılı biçimde yanıtlanacaktır.

Kaspersky Lab web sitesi <http://www.kaspersky.com.tr/>

Virüs Ansiklopedisi: <http://www.securelist.com/>

Anti-virüs laboratuvarı: newvirus@kaspersky.com
(yalnızca arşivlere kuşkulu nesnelere göndermek için)
<http://support.kaspersky.com/virlab/helpdesk.html>
(virüs analistlerine istekler göndermek için)

Kaspersky Lab web forumu: <http://forum.kaspersky.com>

ÜÇÜNCÜ TARAF KODLAR HAKKINDA BİLGİ

Uygulamanın oluşturulmasında başka firmaların sağladığı kodlar kullanılmaktadır.

BU BÖLÜMDE

Dağıtılmış program kodu	121
Diğer bilgiler	121

DAĞITILMIŞ PROGRAM KODU

Uygulama içinde, bağımsız bir başka firma tarafından sağlanan program kodu, hiçbir değişiklik yapılmadan kaynak ya da ikili (binary) biçimde dağıtılmaktadır.

DİĞER BİLGİLER

Başka firmalarca sağlanan kodlar hakkında ek bilgiler.

Dijital imzaları oluşturmak ve doğrulamak için Kaspersky Internet Security, CryptoEx LLC tarafından sağlanan Crypto C veri güvenliği yazılım kütüphanesini kullanılmaktadır.

CryptoEx LLC kurumsal web sitesi <http://www.cryptoex.ru>

İNDEKS

A

Arama/SMS Filtresi	57
arama ile ilgili eylem	69
Beyaz Liste:	62
Kara Liste:.....	59
Kişiler Listesinin dışındaki numaraları.....	66
modlar.....	58
sayısal olmayan numaralar	67
SMS ile ilgili eylem.....	68
Arşivler	
İstek üzerine taramalar	50, 51

B

Başlatma	
Güncelleme.....	108
İstek üzerine taramalar	48
uygulama	30
Beyaz Liste	
Arama/SMS Filtresi.....	62
Ebeveyn Denetimi.....	74

Ç

Çizelge	
Güncelleme.....	109
İstek üzerine taramalar	49

D

Devre dışı bırakma	
Arama/SMS Filtresi.....	58
Güvenlik duvarı.....	99
Şifreleme	104
Devre Dışı Bırakma	
Ebeveyn Denetimi.....	70, 71
Gizlilik Koruması	89, 90
Düzenle	
Arama/SMS Filtresi Beyaz Listesi	64
Düzenleme	
Arama/SMS Filtresi Kara Listesi	61
Ebeveyn Denetimi Beyaz Listesi.....	76
Ebeveyn Denetimi Kara Listesi	73
kişiye özel Gizlilik Koruması kişileri listesi.....	96

E

Ebeveyn Denetimi	
Beyaz Liste	74
Kara Liste	71
modlar.....	70
Ekleme	
Arama/SMS Filtresi Beyaz Listesi	63
Arama/SMS Filtresi Kara Listesi	60
Ebeveyn Denetimi Beyaz Listesi.....	75
Ebeveyn Denetimi Kara Listesi	72
Gizli Gizlilik Koruması numaraları listesi	95
Ekran	
Koruma durumu penceresi	40

Engelleme	
ağ bağlantıları.....	99
bilgilerin şifrelenmesi	105
gelen aramalar.....	59, 62
gelen SMS	59
giden aramalar.....	71, 72
giden SMS mesajları.....	71, 72
Etkinleştirme	
Arama/SMS Filtresi.....	58
Ebeveyn Denetimi.....	70, 71
Gizlilik Koruması	90
Güvenlik duvarı.....	99
Şifreleme	102
F	
FİLTRELEME	
GELEN ARAMALAR.....	57
GELEN SMS.....	57
G	
Giriş	
Arama/SMS Filtresi Beyaz Listesi	63
Arama/SMS Filtresi Kara Listesi	60
Ebeveyn Denetimi Beyaz Listesi.....	75
Gizlilik Koruması.....	89
gizlenecek bilgileri ve olayları seçme.....	97
gizli kişiler listesi	94
modlar.....	89
otomatik başlatma.....	91
Güncelle	
elle başlatma.....	108
Güncelleme	
zamanlanmış başlatma.....	109
GÜNCELLEME	
UYGULAMA SÜRÜMÜ.....	22
Güvenlik düzeyi	
Güvenlik duvarı.....	99
H	
Hırsızlığa Karşı Koruma	78
Engelleme.....	79
GPS Bul.....	85
SIM Gözcüsü	84
Veri Silme	81
I	
İşlemler	
İstek üzerine taramalar	52
İstek üzerine taramalar	
arşivler	51
Nesneler üzerinde gerçekleştirilecek işlemler	52
taranacak nesneler	50
zamanlanmış başlangıç	49
İzin ver	
gelen aramalar.....	63
gelen SMS	63
İzin verme	
ağ bağlantıları.....	99
giden aramalar.....	74
giden SMS mesajları.....	74

K

KALDIRMA	
UYGULAMA.....	20
Kara Liste	
Arama/SMS Filtresi.....	59
Ebeveyn Denetimi.....	71
Karantina	
bir nesneyi silme.....	56
nesneleri görüntüleme.....	54
nesnenin geri yüklenmesi.....	55
KARANTINA.....	54
Kod	
etkinleştirme kodu.....	24, 25, 27
uygulamanın gizli kodu.....	28
Koruma durumu.....	40

L

Lisans.....	32
bilgiler.....	34
Lisans Sözleşmesi.....	32
uygulamanın etkinleştirilmesi.....	24
yenileme.....	34
Lisans Sözleşmesi.....	32
Lisansı yenileme.....	34

M

Modlar	
Arama/SMS Filtresi.....	58
Ebeveyn Denetimi.....	70
Gizlilik Koruması.....	89, 90

N

Nesnelerle ilgili işlemler.....	45, 52
Nesnenin geri yüklenmesi.....	55

O

Olay günlüğü.....	112
girişleri görüntüleme.....	112
girişleri silme.....	113

S

Şifreleme	
erişimin otomatik engellenmesi.....	105
verileri şifreleme.....	102
verilerin şifresini çözmeye.....	104
Şifreli verilere erişimi engelleme.....	105
Sil	
Arama/SMS Filtresi Beyaz Listesi.....	65
Arama/SMS Filtresi Kara Listesi.....	62
Silme	
Ebeveyn Denetimi Beyaz Listesi.....	77
Ebeveyn Denetimi Kara Listesi.....	74
gizli Gizlilik Koruması kişileri listesi.....	96
Günlük kayıtları.....	113
Karantinadan nesne.....	56
SMS komutu gönderme.....	87

T

Taramayı elle başlatma	48
------------------------------	----

U

UYGULAMA ARAYÜZÜ	39
Uygulama gizli kodu	28, 29
Uygulama menüsü	41
Uygulamayı etkinleştirme	24
lisans	32
UYGULAMAYI KURMA	20

V

Veri	
Şifreleme	102
VERİ	
GİZLİ BİLGİLER	89
Veriler	
gizli koda erişim	105
Şifre çözme	104