kaspersky

Kaspersky Endpoint Security 10 Service Pack 2 for Windows

İçindekiler

Kaspersky Endpoint Security 10 Service Pack 2 for Windows Hakkında
- Neler Yeni
- Dağıtım kiti
- Kaspersky Endpoint Security for Windows hakkında
- Donanım ve yazılım gereksinimleri

Uygulamayı yükleme ve kaldırma
- Uygulamayı yükleme
  - Uygulamayı yükleme yolları hakkında
  - Kurulum Sihirbazını kullanarak uygulamayı yükleme
    - 1. Adım. Bilgisayarınızın kurulum gereksinimlerini karşıladığını kontrol etme
    - 2. Adım. Yükleme prosedürünün hoş geldiniz sayfası
    - 3. Adım. Lisans Sözleşmesi'ni ve Gizlilik Bildirimi'ni görüntüleme
    - 4. Adım. Yükleme türünü seçme
    - 5. Adım. Yüklenecek uygulama bileşenlerini seçme
    - 6. Adım. Hedef klasörü seçme
    - 7. Adım. Tarama istisnaları ekleme
    - 8. Adım. Uygulamayı yüklemeye hazırlanma
    - 9. Adım. Uygulamayı yükleme
  - Komut satırından uygulamayı yükleme
  - Sistem Merkezi Yapılandırma Yöneticisi'ni kullanarak uygulamayı uzaktan yükleme
  - setup.ini dosyası yükleme ayarlarının açıklaması
  - İlk Yapılandırma Sihirbazı
    - Uygulamayı etkinleştirme
    - 2. Adım. Etkinleştirme koduyla etkinleştirme
    - Anahtar dosyasıyla etkinleştirme
    - Etkinleştirilecek işlevleri seçme
    - Etkinleştirmeyi tamamlama
    - İşletim sistemini analiz etme
    - Uygulamanın ilk yapılandırması sonlandırılıyor
    - Kaspersky Security Network Bildirimi
  - Eski bir uygulama sürümünü yükseltme yolları hakkında
- Uygulamayı kaldırma
  - Uygulamayı kaldırma yolları hakkında
  - Kurulum Sihirbazını kullanarak uygulamayı kaldırma
    - 1. Adım. Gelecekte kullanmak üzere uygulama verilerini kaydetme
    - 2. Adım. Uygulama kaldırmayı onaylama
    - 3. Adım. Uygulamayı kaldırma. Kaldırmayı tamamlama
  - Komut satırından uygulamayı kaldırma
  - Kimlik Doğrulama Aracısı'nın test çalışmasının ardından kalan nesneleri ve verileri kaldırma

Uygulama arabirimi
- Görev çubuğu bildirim alanındaki uygulama simgesi
- Uygulama simgesi içerik menüsü
- Ana uygulama penceresi
- Uygulama ayarları penceresi
- Uygulama Koruma ve Denetim sekmesi

Uygulama lisanslama

Son Kullanıcı Lisans Sözleşmesi Hakkında
Lisans hakkında
Lisans sertifikası hakkında
Abonelik hakkında
Etkinleştirme kodu hakkında
Anahtar hakkında
Anahtar dosyası hakkında
Veri sağlama hakkında
Lisans bilgilerini görüntüleme
Lisans satın alma
Lisansı yenileme
Aboneliği yenileme
Hizmet sağlayıcının web sitesini ziyaret etme
Uygulama etkinleştirme yöntemleri hakkında
Uygulamayı etkinleştirmek için Etkinleştirme Sihirbazını kullanma
Komut satırından uygulamayı etkinleştirme
Uygulamayı başlatma ve durdurma
Uygulamanın otomatik başlatılmasını etkinleştirme ve devre dışı bırakma
Uygulamayı elle başlatma ve durdurma
Bilgisayar korumasını ve denetimini duraklatma ve sürdürme
Bilgisayarın dosya sistemini koruma. Dosya Koruması
Dosya Koruması Hakkında
Dosya Tehdidi Koruması'nı etkinleştirme ve devre dışı bırakma
Dosya Tehdidi Koruması'nı otomatik olarak duraklatma
Dosya Koruması'nı Yapılandırma
Güvenlik düzeyini değiştirme
Virüslü dosyalara uygulanacak Dosya Koruması eylemini değiştirme
Dosya Koruması'nın koruma kapsamını düzenleme
Dosya Koruması ile Sezgisel Analiz'i Kullanma
Dosya Koruması'nın çalışmasında tarama teknolojilerini kullanma
Dosya taramasını optimize etme
Bileşik dosyaları tarama
Tarama modunu değiştirme
E-posta koruması. Posta Koruması
Posta Koruması Hakkında
Posta Tehdidi Koruması'nı etkinleştirme ve devre dışı bırakma
Posta Koruması'nı Yapılandırma
E-posta güvenlik düzeyini değiştirme
Virüslü e-posta mesajlarına uygulanacak eylemi değiştirme
Posta Koruması'nın koruma kapsamını düzenleme
E-posta mesajlarına eklenen bileşik dosyaları tarama
E-posta mesajı eklerini filtreleme
Microsoft Office Outlook'ta e-postaları tarama
Outlook'ta e-posta taramasını yapılandırma
Kaspersky Security Center'ı kullanarak e-posta taramayı yapılandırma
İnternet'te bilgisayar bağlantısı. İnternet Koruması
İnternet Koruması Hakkında
Web Tehdidi Koruması'nı etkinleştirme ve devre dışı bırakma

İnternet Koruması'nı Yapılandırma
İnternet trafiği güvenlik düzeyini değiştirme
Kötü amaçlı İnternet trafiği nesnelerinde uygulanacak eylemi değiştirme
İnternet Koruması tarafından URL'lerin e-dolandırıcılık ve kötü amaçlı İnternet adreslerinin veritabanlarında taranması
İnternet Koruması ile Sezgisel Analiz'i Kullanma
Güvenilir URL'lerin listesini düzenleme
Anlık ileti uygulamaları koruması. IM Koruması
IM Koruması Hakkında
IM Koruması'nı etkinleştirme ve devre dışı bırakma
IM Koruması'nı Yapılandırma
IM Koruması'nın koruma kapsamını oluşturma
IM Koruması ile URL'lerin kötü amaçlı ve e-dolandırıcılık URL'lerinin veritabanlarında taranması
Sistem İzleyici
Sistem İzleyici hakkında
Sistem İzleyici'nin etkinleştirilmesi ve devre dışı bırakılması
Sistem İzleyici'yi Yapılandırma
Sömürüden korumayı etkinleştir veya devre dışı bırak
Bir programda kötü amaçlı etkinlik tespit edilmesi durumunda eylemi seçin
Temizlik sırasında kötü amaçlı yazılım eylemlerini geri almayı etkinleştirme ve devre dışı bırakma
Güvenlik Duvarı
Güvenlik Duvarı Hakkında
Güvenlik Duvarı'nın etkinleştirilmesi veya devre dışı bırakılması
Ağ kuralları hakkında
Ağ bağlantısı durumu hakkında
Ağ bağlantısı durumunu değiştirme
Ağ paketi kurallarını yönetme
Ağ paketi kuralı oluşturma ve düzenleme
Ağ paketi kuralını etkinleştirme veya devre dışı bırakma
Ağ paketi kuralı için Güvenlik Duvarı eylemini değiştirme
Ağ paketi kuralının önceliğini değiştirme
Uygulama ağ kurallarını yönetme
Uygulama ağ kuralı oluşturma ve düzenleme
Uygulama ağ kuralını etkinleştirme veya devre dışı bırakma
Ağ kuralı için Güvenlik Duvarı eylemini değiştirme
Ağ kuralının önceliğini değiştirme
Ağ İzleyicisi
Ağ İzleyicisini Hakkında
Ağ İzleyicisini Başlatma
Ağ Saldırısı Engelleyici
Ağ Saldırısı Engelleyici Hakkında
Ağ Saldırısı Engelleyici'yi etkinleştirme ve devre dışı bırakma
Ağ Saldırısı Engelleyici ayarları
Saldıran bir bilgisayarı engellemek için kullanılan ayarları düzenleme
Engelleme istisnalarının adreslerini yapılandırma
BadUSB Saldırısı Önleme
BadUSB Saldırı Engelleme Hakkında
BadUSB Saldırı Engelleme bileşenini yükleme
BadUSB Saldırı Önleme'yi Etkinleştirme ve Devre Dışı Bırakma

Yetkilendirme için Ekran Klavyesi'nin kullanımına izin verme ve yasaklama
Klavye yetkilendirme
Uygulama Başlatma Denetimi
Uygulama Başlatma Denetimi Hakkında
Uygulama Denetimi'ni etkinleştirme ve devre dışı bırakma
Uygulama Başlatma Denetimi işlevselliği sınırlamaları
Uygulama Denetimi kuralları hakkında
Uygulama Başlatma Denetimi kurallarını yönetme
Uygulama Başlatma Denetimi kuralının eklenmesi ve düzenlenmesi
Uygulama Başlatma Denetimi kuralına tetikleme koşulu ekleme
Uygulama Başlatma Denetimi kuralının durumunu değiştirme
Uygulama Başlatma Denetimi kurallarını test etme
Uygulama Başlatma Denetimi mesaj şablonlarını düzenleme
Uygulama Başlatma Denetimi işletim modları hakkında
Uygulama Başlatma Denetimi modunu seçme
Kaspersky Security Center'ı kullanarak Uygulama Başlatma Denetimi kurallarını yönetme
Kullanıcı bilgisayarlarına yüklenen uygulamalar hakkında bilgi toplama
Uygulama kategorileri oluşturma
Kaspersky Security Center'ı kullanarak Uygulama Başlatma Denetimi kuralları oluşturma
Kaspersky Security Center'ı kullanarak Uygulama Başlatma Denetimi kuralının durumunu değiştirme
Uygulama Ayrıcalığı Denetimi
Uygulama Ayrıcalığı Denetimi Hakkında
Ses ve video aygıtı denetiminin sınırlamaları
Sunucu Yetkisiz Erişim Önleme'yi etkinleştirme ve devre dışı bırakma
Uygulama güven gruplarını yönetme
Güven gruplarına atanan uygulamalar için ayarları yapılandırma
Güven grubunu değiştirme
Kaspersky Endpoint Security'den önce başlatılan uygulamalar için bir güven grubu seçme
Uygulama denetimi kurallarını yönetme
Güven grupları ve uygulama grupları için uygulama denetimi kurallarını değiştirme
Uygulama denetimi kuralını düzenleme
Kaspersky Security Network veritabanından uygulama denetimi kurallarının indirilmesini ve güncellenmesini devre dışı bırakma
Üst işlemden sınırlamaları devralmayı devre dışı bırakma
Belirli uygulama eylemlerini uygulama denetimi kurallarının dışında tutma
Eski uygulama denetimi kurallarını kaldırma
İşletim sistemi kaynaklarını ve kimlik verilerini koruma
Korunan kaynaklar kategorisi ekleme
Korunan kaynak ekleme
Kaynak korumasını devre dışı bırakma
Zayıf Nokta İzleyicisi
Zayıf Nokta İzleyicisi Hakkında
Zayıf Nokta İzleyicisi'ni etkinleştirme ve devre dışı bırakma
Aygıt Denetimi
Aygıt Denetimi Hakkında
Aygıt Denetimini etkinleştirme ve devre dışı bırakma
Aygıtlar ve bağlantı veri yollarına erişim kuralları hakkında
Güvenilir aygıtlar hakkında

- Aygıtlara erişim hakkında standart kararlar
- Aygıt erişim kuralını düzenleme
- Olay günlüğüne kayıtları ekleme veya günlük dışında tutma
- Güvenilir listeye bir Wi-Fi ağı ekleme
- Bir bağlantı veri yolu erişim kuralını düzenleme
- Güvenilir aygıtlarla eylemler
  - Uygulama arabiriminden Güvenilir listesine aygıt ekleme
  - Aygıt modeli veya kimliğine göre aygıtları Güvenilir listesine ekleme
  - Aygıt kimliği maskesine göre aygıtları Güvenilir listesine ekleme
  - Güvenilir aygıta kullanıcı erişimini yapılandırma
  - Güvenilir aygıtlar listesinden bir aygıtı kaldırma
- Aygıt Denetimi mesajlarının şablonlarını düzenleme
- Engellenen bir aygıta erişim elde etme
- Kaspersky Security Center'ı kullanarak engellenen aygıt erişim anahtarı oluşturma

İnternet Denetimi
- İnternet Denetimi Hakkında
- İnternet Denetimi'ni etkinleştirme ve devre dışı bırakma
- İnternet kaynağı içerik kategorileri
- İnternet kaynağı erişim kuralları hakkında
- İnternet kaynağı erişim kurallarıyla ilgili eylemler
  - İnternet kaynağı erişim kuralı ekleme ve düzenleme
  - İnternet kaynağı erişim kurallarına öncelikler atama
  - İnternet kaynağı erişim kurallarını test etme
  - İnternet kaynağı erişim kuralını etkinleştirme ve devre dışı bırakma
- Uygulamanın önceki sürümlerinden İnternet kaynağı erişim kurallarını taşıma
- İnternet kaynağı adreslerinin listesini dışa aktarma ve içe aktarma
- İnternet kaynağı adreslerinin maskelerini düzenleme
- İnternet Denetimi mesajlarının şablonlarını düzenleme

KATA Endpoint Sensor
- KATA Endpoint Sensor hakkında
- KATA Endpoint Sensor bileşenini etkinleştirme veya devre dışı bırakma

Veri Şifreleme
- Kaspersky Security Center ilkesinde şifreleme ayarlarının görüntülenmesini etkinleştirme
- Veri şifreleme hakkında
- Şifreleme işlevi sınırlamaları
- Şifreleme algoritmasını değiştirme
- Tek Oturum Açma (SSO) teknolojisini kullanma
- Dosya şifreleme ile ilgili özel hususlar
- Yerel bilgisayar sürücülerindeki dosyaları şifreleme
  - Yerel bilgisayar sürücülerindeki dosyaları şifreleme
  - Uygulamalar için şifreli dosyaya erişim kuralları oluşturma
  - Belirli uygulamaların oluşturduğu veya değiştirdiği dosyaları şifreleme
  - Şifre çözme kuralı oluşturma
  - Yerel bilgisayar sürücülerindeki dosyaların şifresini çözme
  - Şifrelenmiş paketler oluşturma
  - Şifrelenmiş paketleri çıkarma
- Çıkarılabilir sürücülerin şifrelenmesi
  - Çıkarılabilir sürücülerin şifrelenmesini başlatma

Çıkarılabilir sürücülere şifreleme kuralı ekleme
Çıkarılabilir sürücülerin şifreleme kuralını düzenleme
Çıkarılabilir sürücülerdeki şifreli dosyalara erişim için taşınabilir modu etkinleştirme
Çıkarılabilir sürücülerin şifresini çözme
Sabit sürücülerin şifrelenmesi
Sabit sürücülerin şifrelenmesi hakkında
Kaspersky Disk Encryption teknolojisini kullanarak sabit sürücülerin şifrelenmesi
BitLocker Drive Encryption teknolojisini kullanarak sabit sürücüleri şifreleme
Şifreleme dışında tutulan sabit sürücülerin listesini oluşturma
Sabit sürücü şifresini çözme
Kimlik Doğrulama Aracısı'nı yönetme
Kimlik Doğrulama Aracısı ile belirteç ve akıllı kart kullanma
Kimlik Doğrulama Aracısı yardım mesajlarını düzenleme
Kimlik Doğrulama Aracısı yardım mesajlarında karakterler için sınırlı destek
Kimlik Doğrulama Aracısı izleme düzeyini seçme
Kimlik Doğrulama Aracısı hesaplarını yönetme
Kimlik Doğrulama Aracısı hesabı oluşturmak için komut ekleme
Kimlik Doğrulama Aracısı hesap düzenleme komutunu ekleme
Kimlik Doğrulama Aracısı hesabını silmek için komut ekleme
Kimlik Doğrulama Aracısı hesabı kimlik bilgilerini sıfırlama
Kimlik Doğrulama Aracısı hesap kimlik bilgilerini sıfırlama kullanıcı isteğine yanıt verme
Veri şifreleme ayrıntılarını görüntüleme
Şifreleme durumu hakkında
Şifreleme durumunu görüntüleme
Kaspersky Security Center'ın ayrıntılar bölmesindeki şifreleme istatistiklerini görüntüleme
Yerel bilgisayar sürücülerinde dosya şifreleme hatalarını görüntüleme
Veri şifreleme raporunu görüntüleme
Sınırlı dosya şifreleme işlevine sahip şifreli dosyaları yönetme
Kaspersky Security Center'a bağlantı olmadan şifrelenmiş dosyalara erişim
Kaspersky Security Center'a bağlantı olmadan şifrelenmiş dosyalara kullanıcı erişimi sağlama
Şifrelenmiş dosya erişim mesajlarının şablonlarını düzenleme
Şifrelenmiş aygıtlara erişim olmadığında şifrelenmiş aygıtlarla çalışma
Uygulama arayüzü üzerinden şifrelenmiş aygıtlara erişim sağlama
Şifrelenmiş aygıtlara kullanıcı erişimi sağlama
Kullanıcıya, BitLocker ile şifrelenmiş sabit sürücülerin kurtarma anahtarını sağlama
Geri Yükleme Yardımcı Programının yürütülebilir dosyasını oluşturma
Geri Yükleme Yardımcı Programını kullanarak şifreli aygıtlara erişimi geri yükleme
Şifrelenmiş aygıtlardaki verileri geri yüklemek için bir kullanıcı isteğine yanıtlama
İşletim sistemi hatasının ardından şifrelenmiş verilere yeniden erişim sağlama
İşletim sistemi kurtarma diskini oluşturma
Ağ Koruması
Ağ Koruması Hakkında
Ağ trafiğini izleme ayarlarını yapılandırma
Tüm ağ bağlantı noktalarını izlemeyi etkinleştirme
İzlenen ağ bağlantı noktalarının listesini oluşturma
Tüm ağ bağlantı noktalarının izlendiği uygulamaların listesini oluşturma
Veritabanlarını ve uygulama yazılım modüllerini güncelleme
Veritabanı ve uygulama modülü güncellemeleri hakkında

Güncelleme kaynakları hakkında
Güncelleme ayarları yapılandırması
Güncelleme kaynağı ekleme
Güncelleme sunucusu bölgesini seçme
Paylaşım klasöründen güncellemeleri yapılandırma
Güncelleme görevinin çalışma modunu seçme
Farklı bir kullanıcı hesabının hakları altında bir güncelleme görevi başlatma
Uygulama modülü güncellemelerini yapılandırma
Güncelleme görevini başlatma veya durdurma
Son güncellemeyi geri alma
Proxy sunucusu ayarlarını yapılandırma
Bilgisayarı tarama
Tarama görevleri hakkında
Tarama görevini başlatma veya durdurma
Tarama görevi ayarlarını yapılandırma
Güvenlik düzeyini değiştirme
Virüslü dosyalara uygulanacak eylemi değiştirme
Taranacak nesnelerin bir listesinin üretilmesi
Taranacak dosya türlerinin seçimi
Dosya taramasını optimize etme
Bileşik dosyaları tarama
Tarama yöntemlerini kullanma
Tarama teknolojilerini kullanma
Tarama görevinin çalışma modunu seçme
Farklı bir kullanıcı hesabıyla bir tarama görevi başlatma
Bilgisayara bağlandığında çıkarılabilir sürücüleri tarama
İşlenmemiş dosyaları yönetme
Korumasız dosyalar hakkında
İşlenmemiş dosyaların listesini yönetme
İşlenmemiş dosyalar için Özel Tarama görevini başlatma
İşlenmemiş dosyaların listesinden dosyaları silme
Zayıf Nokta Taraması
Çalışan uygulamaların zayıf noktaları hakkında bilgi görüntüleme
Zayıf Nokta Taraması görevi hakkında
Zayıf Nokta Taraması görevini başlatma veya durdurma
Zayıf Nokta taraması ayarlarını yapılandırma
Zayıf nokta taraması kapsamını oluşturma
Zayıf Nokta Taraması görevinin çalışma modunu seçme
Zayıf Nokta Taraması görevini farklı bir kullanıcı hesabının haklarını kullanarak başlatma
Zayıf nokta listesini yönetme
Zayıf noktaların listesi hakkında
Zayıf Nokta Taraması görevini yeniden başlatma
Zayıf noktayı düzeltme
Zayıf noktalar listesinde girişleri gizleme
Zayıf noktalar listesini önem düzeyine göre filtreleme
Zayıf noktaların listesini Düzeltildi ve Gizli durum değerlerine göre filtreleme
Uygulama modüllerinin bütünlüğünü kontrol etme
Bütünlük denetimi görevi hakkında

Bütünlük denetimi görevini başlatma veya durdurma
Bütünlük Denetimi görevi için çalışma modunu seçme
Raporları yönetme
Raporlar hakkında
Raporlar ayarlarını yapılandırma
Maksimum rapor depolama süresini yapılandırma
Rapor dosyasının maksimum boyutunu yapılandırma
Raporların görüntülenmesi
Olay bilgilerini raporda görüntüleme
Raporu dosya olarak kaydetme
Raporları temizleme
Bildirim hizmeti
Kaspersky Endpoint Security bildirimleri hakkında
Bildirim hizmetini yapılandırma
Olay günlüğü ayarlarını yapılandırma
Bildirimlerin görüntülenmesini ve iletilmesini yapılandırma
Bildirim alanında uygulama durumu hakkında uyarıların görüntülenmesini yapılandırma
Karantina ve Yedeklemeyi Yönetme
Karantina ve Yedekleme Hakkında
Karantina ve Yedekleme Ayarlarını Yapılandırma
Karantina'daki dosyalar ve Yedekleme konumundaki dosya kopyaları için maksimum depolama süresini yapılandırma
Karantina ve Yedekleme için maksimum boyutu yapılandırma
Karantinayı Yönetme
Güncellemenin ardından Karantina'daki dosyaların taranmasını etkinleştirme ve devre dışı bırakma
Karantina'daki dosyalar için Özel Tarama görevini başlatma
Karantina konumundan dosyaları geri yükleme
Karantina konumundan dosyaları silme
Yedeklemeyi Yönetme
Yedekleme konumundan dosyaları geri yükleme
Yedekleme konumundan dosyaların yedekleme kopyalarını silme
Gelişmiş uygulama ayarları
Yapılandırma dosyası oluşturma ve kullanma
Güvenilir bölge
Güvenilir bölge hakkında
Tarama istisnası oluşturma
Tarama istisnasını değiştirme
Tarama istisnasını silme
Tarama istisnasını etkinleştirme ve devre dışı bırakma
Güvenilir uygulamalar listesini düzenleme
Güvenilir uygulamalar listesindeki bir uygulamanın güvenilir bölge kurallarını etkinleştirme ve devre dışı bırakma
Güvenilir sistem sertifikası depolama alanını kullanma
Kaspersky Endpoint Security Kendini Koruma
Kaspersky Endpoint Security Kendini Koruma Hakkında
Kendini Korumayı etkinleştirme veya devre dışı bırakma
Uzaktan Denetim Korumasını etkinleştirme veya devre dışı bırakma
Uzaktan yönetim uygulamalarını destekleme
Kaspersky Endpoint Security'nin performansı ve diğer uygulamalarla uyumluluğu
Kaspersky Endpoint Security'nin performansı ve diğer uygulamalarla uyumluluğu hakkında

Tespit edilebilir nesne türlerini seçme
İş istasyonları için Gelişmiş Temizleme teknolojisini etkinleştirme veya devre dışı bırakma
Dosya sunucuları için Gelişmiş Temizleme teknolojisini etkinleştirme veya devre dışı bırakma
Enerji tasarrufu modunu etkinleştirme veya devre dışı bırakma
Diğer uygulamalar için kaynak yaratmayı etkinleştirme veya devre dışı bırakma
Parola koruması
Kaspersky Endpoint Security'ye erişimi kısıtlama hakkında
Parola korumasını etkinleştirme ve devre dışı bırakma
Kaspersky Endpoint Security erişim parolasını değiştirme
Geçici bir parolanın kullanılması hakkında
Kaspersky Security Center Yönetim Konsolunu kullanarak geçici bir şifre oluşturma
Kaspersky Endpoint Security arabiriminde geçici bir parola uygulama
Kaspersky Security Center vasıtasıyla uygulamanın uzaktan yönetimi
Kaspersky Security Center'dan uygulamanın yönetimi hakkında
Yönetim eklentilerinin farklı sürümleriyle çalışırken dikkat edilmesi gereken hususlar
İstemci bilgisayarda Kaspersky Endpoint Security'nin başlatılması ve durdurulması
Kaspersky Endpoint Security ayarlarını yapılandırma
Görevleri yönetme
Kaspersky Endpoint Security görevleri hakkında
Görev yönetimi modunu yapılandırma
Yerel görev oluşturma
Grup görevi oluşturma
Aygıt seçimi için bir görev oluşturma
Görevi başlatma, durdurma, askıya alma ve sürdürme
Görev ayarlarını düzenleme
İlkeleri yönetme
İlkeler hakkında
İlke oluşturma
İlke ayarlarını düzenleme
Kaspersky Security Center ilkesinde görüntülenecek ayarları seçme
Kaspersky Security Center sunucusuna kullanıcı mesajlarını gönderme
Kaspersky Security Center olay depolama alanında kullanıcı mesajlarını görüntüleme
Kaspersky Security Network'e katılım
Kaspersky Security Network'e katılım hakkında
Kaspersky Security Network'ün kullanımını etkinleştirme ve devre dışı bırakma
Kaspersky Security Network bağlantısını denetleme
Kaspersky Security Network'den bir dosyanın saygınlığını kontrol etme
Kaspersky Security Network ile gelişmiş koruma
Uygulama hakkında bilgi kaynakları
Teknik Destek ile irtibat kurma
Teknik destek nasıl alınır
Telefonla teknik destek
Kaspersky CompanyAccount üzerinden Teknik Destek
Teknik Destek için bilgi toplama
Uygulama izi dosyası oluşturma
İz dosyalarının içeriği ve depolanması
Döküm dosyalarının ve iz dosyalarının Kaspersky'ye aktarılmasını etkinleştirme veya devre dışı bırakma
Teknik Destek sunucusuna dosya gönderme

Döküm dosyalarının ve iz dosyalarının korumasını etkinleştirme veya devre dışı bırakma
Sözlük
Açık bırakıcılar
Adres kara listesi
Ağ Aracısı
Ağ Aracısı Bağlayıcısı
Ağ hizmeti
Aktif anahtar
Anti-virüs veritabanları
Arşiv
Bir web kaynağının adresinin normalleştirilmiş biçimi
Büyük olasılıkla virüslü dosya
Doğrulama Aracısı
Dosya maskesi
Dosyaları Karantinaya Taşıma.
E-dolandırıcılık
E-dolandırıcılık web adreslerinin veritabanı
Ek anahtar
Görev
Görev Ayarları
Güncelleme
Güvenilir Platform Modülü
İmza Analizi
Karantina
Koruma kapsamı
Lisans Sertifikası
OLE nesnesi
Sertifika
Sertifika konusu
Sertifika veren
Sezgisel Analiz
Tarama kapsamı
Taşınabilir Dosya Yöneticisi
Temizlik
Thumbprint sertifikası
Uygulama Ayarları
Uygulama modülleri
Virüs bulaşabilecek dosya
Virüslü dosya
Yama
Yanlış alarm
Yedekleme
Yönetim grubu
Yönetim Sunucusu
Zararlı web adreslerinin veritabanı
Üçüncü taraf kod hakkında bilgi
Ticari marka bildirimleri

Kaspersky Endpoint Security 10 Service Pack 2 for Windows Hakkında

Bu bölümde, Kaspersky Endpoint Security'nin işlevleri, bileşenleri ve dağıtım kiti açıklanmaktadır ve Kaspersky Endpoint Security'nin donanım ve yazılım gereksinimlerinin bir listesi sağlanmaktadır.

Neler Yeni

Kaspersky Endpoint Security 10 Service Pack 2 for Windows aşağıdaki özellikleri ve iyileştirmeleri sunar:

1. Uygulama Başlatma Denetimi:
    - Sunucu işletim sistemlerini destekler.
    - DLL modüllerinin ve sürücülerin indirilmesini denetler.
    - Envanter görevindeki (DLL modülleri ve komut dosyaları) nesnelerin listesini yönetir.
    - Yeni bir kritere dayalı olarak, dijital imza sertifikalarını özelliklerine göre nesneleri denetler.
    - Engellenen uygulamaların test amaçlı başlatılmasıyla ilgili rapor oluşturur.
    - Uygulama Başlatma Denetimi için iki işletim modunu destekler: "Kara Liste" ve "Beyaz Liste".
    - Nesnelerin kontrolü ve envanteri için SHA256 sağlaması kullanır.
    - PowerShell yorumlayıcıdan komut dizilerinin çalıştırılmasını kontrol eder.
    - Güvenilir sistem sertifikası depoalama alanını kullanır.
2. Microsoft BitLocker yönetimi, Microsoft'un BitLocker teknolojisinin yardımıyla sabit sürücülerin şifrelenmesini mümkün kılar.
    - Şifrelemeyi uzaktan yönetir.
    - Şifrelenmiş aygıtları göster.
    - Aygıt şifreleme raporları oluştur.
    - Şifrelenmiş aygıtlara erişimi geri yükler.
3. Kaspersky Disk Encryption:
    - Sanal klavye kullanılarak Kimlik Doğrulama Aracısı'nda önyükleme ortamına kimlik bilgilerinin girilmesini destekler.
    - Bir aygıtta yalnızca kullanılan alanı şifrelemek için şifreleme modu desteği.
    - Tabletlerde şifreleme desteği (MS Surface sürüm 3, 4).
4. Uygulama Ayrıcalığı Denetimi:
    - Uygulamaların video ve ses aygıtlarına erişimini kontrol eder.

5. İnternet Denetimi:

   - Ek web kaynakları kategorileri için web kaynak erişim kurallarını yapılandırır.

6. Aygıt Denetimi:

   - USB aygıtlara dosyaların kaydedilmesi ve silinmesiyle ilişkili olayları günlüğe kaydeder.
   - Aşağıdaki ayarlara dayalı olarak güvenilir Wi-Fi ağlarının listesini üretir: ad, şifreleme türü ve kimlik doğrulama türü.
   - CD/DVD disklerdeki dosya okuma ve yazma işlemlerinin kullanıcı erişim haklarını yönetir.

7. Posta Koruması:

   - Posta Koruması taraması için arşivler içindeki belirli dosya türlerini silme ve yeniden adlandırma kapasitesi.

8. Kaspersky Security Network:

   - Kaspersky Endpoint Security raporlarındaki ve Kaspersky Security Center raporlarındaki nesne işleme yöntemiyle ilgili bir karara neden olarak KSN'yi görüntüler.
   - Seçili bir dosyanın itibarıyla ilgili olarak KSN'ye bir sorgu gönderir.
   - Kaspersky Endpoint Security'nin yüklü olduğu istemci bilgisayarlar için KSN sunucularının kullanılabilirlik durumu gösterir.

Dağıtım kiti

Kaspersky Endpoint Security dağıtım kiti aşağıdaki dosyaları içerir:

- Kullanılabilir yöntemlerden herhangi birini kullanarak uygulamaları yüklemek için gereken dosyalar:
- Uygulamanın yüklenmesi sırasında kullanılan güncelleme paketleri.
- Kaspersky Security Center vasıtasıyla Kaspersky Endpoint Security yönetimini yüklemek için klcfginst.msi dosyası.
- Kaspersky Security Network'e katılım koşullarını görüntülemekte kullanabileceğiniz ksn_<language ID>.txt dosyası.
- Son Kullanıcı Lisans Sözleşmesi'ni görüntülemek için kullanabileceğiniz license.txt dosyası.
- Uyumlu yazılımların listesini içeren incompatible.txt dosyası.
- Dağıtım kitinin iç ayarlarını içeren installer.ini dosyası.

  Bu ayarların değerlerinin değiştirilmesi önerilmez. Yükleme seçeneklerini değiştirmek istiyorsanız, setup.ini dosyasını kullanın.

Dosyalara erişim için dağıtım kitinin paketini açmalısınız.

Kaspersky Endpoint Security for Windows hakkında

Kaspersky Endpoint Security for Windows (bundan sonra Kaspersky Endpoint Security olarak anılacaktır) çeşitli tehdit türleri ile ağ ve kimlik avı saldırılarına karşı kapsamlı bilgisayar koruması sağlar.

Her bir tehdit türü ayrı bir bileşen tarafından ele alınır. Bileşenler bağımsız olarak etkinleştirilebilir veya devre dışı bırakılabilir ve ayarları yapılandırılabilir.

Aşağıdaki uygulama bileşenleri, denetim bileşenleridir:

- **Uygulama Denetimi**. Bu bileşen, kullanıcının uygulamaları başlatma girişimlerini takip eder ve uygulamaların başlatılmasını düzenler.
- **Aygıt Denetimi**. Bu bileşen, veri depolama aygıtlarına (sabit sürücüler, çıkarılabilir sürücüler ve CD/DVD diskleri gibi), veri iletim ekipmanına (modemler gibi), bilgiyi dönüştüren ekipmana (yazıcılar gibi) veya aygıtları bilgisayarlara bağlamaya yönelik arabirimlere (USB ve Bluetooth gibi) erişimle ilgili esnek sınırlamalar yapılandırmanızı sağlar.
- **İnternet Denetimi**. Bu bileşen, farklı kullanıcı grupları için İnternet kaynaklarına erişimle ilgili esnek sınırlamalar getirmenize olanak tanır.
- **Uyarlamalı Anomali Denetimi**. Bu bileşen, korunan bilgisayarda tipik olarak görülmeyen potansiyel olarak zararlı işlemleri izler ve denetler.

Denetim bileşenlerinin çalışması aşağıdaki kurallara dayalıdır:

- Uygulama Denetimi, Uygulama Başlatma Denetimi kurallarını kullanır.
- Aygıt Denetimi, aygıt erişim kuralları ve bağlantı veri yolu erişim kurallarını kullanır.
- İnternet Denetimi, İnternet kaynağına erişim kurallarını kullanır.
- Uyarlamalı Anomali Denetimi, Uyarlamalı Anomali Denetimi kurallarını kullanır.

Aşağıdaki uygulama bileşenleri, koruma bileşenleridir:

- **Davranış Tespiti**. Bu bileşen, bilgisayarınızdaki uygulamaların eylemleri hakkında bilgi alır ve daha etkin koruma sağlamak için bu bilgileri diğer bileşenlere sağlar.
- **Exploit Önleme**. Bu bileşen hassas uygulamalar tarafından çalıştırılan yürütülebilir dosyaları izler. Yürütülebilir bir dosyanın hassas bir uygulama tarafından çalıştırılması girişimi kullanıcı tarafından başlatılmadıysa Kaspersky Endpoint Security, bu dosyanın çalıştırılmasını engeller.
- **Sunucu Yetkisiz Erişim Önleme**. Bu bileşen, işletim sistemindeki uygulamaların eylemlerini kaydeder ve belirli bir uygulamanın güven grubuna bağlı olarak uygulama etkinliğini düzenler. Her bir uygulama grubu için bir kural kümesi belirlenir. Bu kurallar, uygulamaların kullanıcı verilerine ve işletim sistemi kaynaklarına erişimini düzenler. Bu veriler, Belgelerim klasörü içindeki kullanıcı dosyalarını, çerezleri, kullanıcı etkinliği günlük dosyalarını ve en sık kullanılan uygulamaların ayarlarını ve önemli bilgilerini içeren dosyaları, klasörleri ve kayıt defteri anahtarlarını kapsar.
- **Düzeltme Altyapısı**. Bu bileşen, Kaspersky Endpoint Security'nin işletim sisteminde zararlı yazılımlar tarafından gerçekleştirilen eylemleri geri almasını sağlar.
- **Dosya Tehdidi Koruması**. Bu bileşen, bilgisayarın dosya sistemini virüslere karşı korur. Bileşen, Kaspersky Endpoint Security başlatıldıktan hemen sonra başlatılır; sürekli olarak bilgisayar RAM'inde kalarak bilgisayarda ve tüm bağlı depolama aygıtlarında açılan, kaydedilen veya başlatılan tüm dosyaları tarar. Bu bileşen, her bir dosya erişim denemesinin arasına girer ve dosyada virüs ve başka tehditler olup olmadığını tarar.

- **Web Tehdidi Koruması**. Bu bileşen, HTTP ve FTP iletişim kuralları üzerinden kullanıcı bilgisayarına gelen trafiği tarar ve İnternet adreslerinin zararlı veya kimlik avı amaçlı olup olmadığını denetler.

- **Posta Tehdidi Koruması**. Bu bileşen, gelen ve giden e-posta mesajlarında virüsleri ve diğer tehditleri tarar.

- **Ağ Tehdidi Koruması**. Bu bileşen, gelen ağ trafiğinde ağ saldırılarında tipik olarak görülen etkinliği denetler. Bilgisayarınızı hedefleyen ağ saldırısı denemesinin tespit edilmesinin ardından Kaspersky Endpoint Security, saldıran bilgisayardan tüm ağ etkinliğini engeller.

- **Güvenlik Duvarı**. Bu bileşen, bilgisayarda kayıtlı verileri korur ve bilgisayar İnternet'e veya yerel alan ağına bağlıyken işletim sistemiyle ilgili tüm olası tehditleri engeller. Bileşen tüm ağ etkinliğini iki tür kurala göre filtreler: uygulamaların ağ kuralları ve ağ paketi kuralları.

- **BadUSB Saldırısı Önleme**. Bu bileşen, klavyeyi taklit eden virüslü USB aygıtların bilgisayara bağlanmasını engeller.

- **AMSI Koruma Sağlayıcısı**. Bu bileşen, üçüncü taraf uygulamalardan gelen talep doğrultusunda nesneleri tarar ve talepte bulunan uygulamaya tarama sonuçlarını bildirir.

Uygulama bileşenlerinin sağladığı gerçek zamanlı korumaya ek olarak, bilgisayarda düzenli şekilde virüs ve diğer tehditler için *tarama* yapmanızı öneririz. Bu, örneğin düşük güvenlik düzeyi nedeniyle koruma bileşenleri tarafından tespit edilmeyen zararlı yazılımların yayılma olasılığını ortadan kaldırmaya yardımcı olur.

Bilgisayar korumasını güncel tutmak için uygulamanın kullandığı veritabanlarını ve modülleri *güncellemelisiniz*. Varsayılan olarak uygulama otomatik şekilde güncellenir ancak gerekirse veritabanları ve uygulama modüllerini elle güncelleyebilirsiniz.

Kaspersky Endpoint Security'de aşağıdaki görevler sağlanmaktadır:

- **Bütünlük Denetimi**. Kaspersky Endpoint Security, uygulama yükleme klasöründeki uygulama modüllerinde bozulma veya değişiklik olup olmadığını denetler. Bir uygulama modülünün yanlış bir dijital imzası varsa modül bozuk olarak değerlendirilir.

- **Tam Tarama**. Kaspersky Endpoint Security; çekirdek belleği, işletim sistemi başlangıcında yüklenen nesneler, disk önyükleme kesimleri, işletim sisteminin yedekleme deposu ile tüm sabit sürücüler ve çıkarılabilir sürücüler dahil olmak üzere işletim sistemini tarar.

- **Özel Tarama**. Kaspersky Endpoint Security kullanıcı tarafından seçilen nesneleri tarar.

- **Kritik Alanları Tarama**. Kaspersky Endpoint Security, çekirdek belleğini, işletim sistemi başlangıcında yüklenen nesneleri ve disk önyükleme kesimlerini tarar.

- **Güncelleme**. Kaspersky Endpoint Security, güncellenen veritabanlarını ve uygulama modüllerini indirir. Güncelleme işlemi bilgisayarı en güncel virüsler ve diğer tehditlere karşı korur.

- **Son güncellemeyi geri alma**. Kaspersky Endpoint Security, veritabanları ve modüllerin son güncellemesini geri alır. Bu, örneğin yeni veritabanı sürümünde Kaspersky Endpoint Security'nin güvenli bir uygulamayı engellemesine neden olan bir geçersiz imza bulunduğunda gerekirse veritabanlarını ve uygulama modüllerini önceki sürümlerine geri almanıza olanak tanır.

Kaspersky Security Center vasıtasıyla uzaktan yönetim

Kaspersky Security Center, istemci bilgisayarda Kaspersky Endpoint Security'yi uzaktan başlatıp durdurmaya, görevleri yönetmeye, uygulama ayarlarını yapılandırmaya ve dosya şifreleme ile tam disk şifreleme işlemlerini gerçekleştirmeye imkan tanır.

Dosya şifreleme işlevi, yerel bilgisayar sürücülerinde depolanan dosya ve klasörleri şifrelemenize olanak tanır. Tam disk şifreleme işlevselliği, sabit sürücüleri ve çıkarılabilir sürücüleri şifrelemeye olanak tanır.

Uygulamanın hizmet işlevleri

Kaspersky Endpoint Security bir dizi hizmet işlevini içerir. Hizmet işlevleri; uygulamayı güncel tutmak, işlevselliğini genişletmek ve kullanıcının uygulamayı kullanımına yardımcı olmak için sağlanır.

- **Raporlar**. Uygulama, çalışma sırasında her uygulama bileşeni için bir rapor tutar. Raporları, tamamlanan görevlerin sonuçlarını izlemek için de kullanabilirsiniz. Raporlar, Kaspersky Endpoint Security'nin çalışması sırasında meydana gelen olayların listelerini ve uygulamanın gerçekleştirdiği tüm işlemleri içerir. Bir olay durumunda raporları Kaspersky'ye gönderebilirsiniz ve Teknik Destek uzmanları daha ayrıntılı olarak sorunu ele alabilir.

- **Veri depolama**. Uygulama bilgisayarda virüs ve diğer tehditleri tararken virüslü dosyalar algılarsa bu dosyaları engeller. Kaspersky Endpoint Security, temizlenen ve silinen dosyaların kopyalarını *Yedekleme* konumunda depolar. Kaspersky Endpoint Security, herhangi bir nedenle işlenmeyen dosyaları *etkin tehditler listesine* taşır. Dosyaları tarayabilir, dosyaları orijinal klasörlerine geri yükleyebilir ve veri depolama alanını boşaltabilirsiniz.

- **Bildirim hizmeti**. Bildirim hizmeti, kullanıcının bilgisayar koruma durumunu ve Kaspersky Endpoint Security'nin çalışmasını etkileyen olayları izlemesine yardımcı olur. Bildirimler ekranda görüntülenebilir veya e-postayla gönderilebilir.

- **Kaspersky Security Network**. Kaspersky Security Network'e kullanıcı katılımı, dünya çapındaki kullanıcılardan alınan dosyaların, İnternet kaynaklarının ve yazılımın tanınırlığı hakkındaki bilgilerin gerçek zamanlı kullanımıyla bilgisayar korumasının etkinliğini artırır.

- **Lisans**. Bir lisans satın alındığında uygulama işlevi açılır, uygulama veritabanı ve modül güncellemelerine erişim sağlanır, uygulamanın yüklenmesi, yapılandırılması ve kullanımıyla ilgili konularda telefon veya e-posta ile destek alınabilir.

- **Destek**. Kaspersky Endpoint Security'nin tüm kayıtlı kullanıcıları yardım için Teknik Destek uzmanları ile irtibat kurabilir. Kaspersky Teknik Destek'e Kaspersky CompanyAccount portalı üzerinden bir istek gönderebilir veya Teknik Destek'i telefonla arayabilirsiniz.

Uygulama hata verirse veya işlem sırasında donarsa otomatik olarak yeniden başlatılabilir.

Uygulama çökmesine neden olan tekrarlanan hatalarla karşılaşırsa uygulama aşağıdaki işlemleri gerçekleştirir:

1. Denetim ve koruma işlevlerini devre dışı bırakır (şifreleme işlevi etkin kalmaya devam eder).

2. Kullanıcıya işlevlerin devre dışı bırakıldığını bildirir.

3. Anti-virüs veritabanlarını güncelledikten veya uygulama modülü güncellemelerini uyguladıktan sonra uygulamayı işlevsel duruma geri getirmeye çalışır.

Uygulama, Kaspersky uzmanlarının geliştirdiği özel amaçlı algoritmaları kullanarak yinelenen çökmeye yol açan hatalar hakkında bilgileri alır. Bu bilgiler, uygulama kurtarma işlemi için gereklidir.

Donanım ve yazılım gereksinimleri

Kaspersky Endpoint Security'nin doğru bir şekilde çalışmasını sağlamak için bilgisayarınız aşağıdaki gereksinimleri karşılamalıdır:

Minimum genel gereksinimler:

- Sabit sürücüde 2 GB kullanılabilir disk alanı
- 1 GHz saat hızında (SSE2 komut setini destekleyen) işlemci
- RAM:
  - 32 bit işletim sistemleri için 1 GB;
  - 64 bit işletim sistemleri için 2 GB.

Kişisel bilgisayarlar için desteklenen işletim sistemleri:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 veya üstü;
- Windows 8 Professional / Enterprise;
- Windows 8.1 Professional / Enterprise;
- Windows 10 Home / Pro / Education / Enterprise.

Microsoft Windows 10 işletim sistemi desteği hakkında ayrıntılar için lütfen Teknik Destek Bilgi Bankası'na bakın.

Dosya sunucuları için desteklenen işletim sistemleri:

- Windows Small Business Server 2008 Standard / Premium (64 bit);
- Windows Small Business Server 2011 Essentials / Standard (64 bit);
- Windows MultiPoint Server 2011 (64 bit);
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2 veya üstü;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 veya üstü;
- Microsoft Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Microsoft Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Microsoft Windows Server 2016 Essentials / Standard / Datacenter;
- Microsoft Windows Server 2019 Essentials / Standard / Datacenter.

Microsoft Windows Server 2016 ve Microsoft Windows Server 2019 işletim sistemleri desteği hakkındaki ayrıntılar için lütfen Teknik Destek Bilgi Bankası'na bakın.

Uygulamayı yükleme ve kaldırma

Bu bölüm, Kaspersky Endpoint Security'yi bilgisayarınıza yükleme, ilk yapılandırmayı tamamlama, uygulamanın önceki bir sürümünden yükseltme ve uygulamayı bilgisayardan kaldırma konusunda size kılavuzluk eder.

Uygulamayı yükleme

Bu bölümde, bilgisayarınıza Kaspersky Endpoint Security'nin nasıl yükleneceği ve uygulamanın ilk yapılandırmasının nasıl tamamlanacağı açıklanmaktadır.

Uygulamayı yükleme yolları hakkında

Kaspersky Endpoint Security 10 for Windows yerel olarak (doğrudan kullanıcının bilgisayarına) veya yöneticinin iş istasyonundan uzaktan yüklenebilir.

Kaspersky Endpoint Security 10 for Windows'un yerel yüklemesi aşağıdaki modlardan birinde gerçekleştirilebilir:

- Uygulama Kurulum Sihirbazı'nı kullanarak etkileşimli modda

  Etkileşimli mod, kurulum işlemine müdahalenizi gerektirir.

- Komut satırından sessiz modda.

  Sessiz modda yüklemenin başlatılmasının ardından yükleme işlemine müdahale etmeniz gerekmez.

Aşağıdaki ağ bilgisayarlarını kullanarak uygulama uzaktan yüklenebilir:

- Kaspersky Security Center yazılım paketi (*Kaspersky Security Center Uygulama Kılavuzu*'na bakınız).
- Microsoft Windows'un Grup İlkesi Düzenleyicisi (işletim sistemi yardım dosyalarına bakınız).
- Sistem Merkezi Yapılandırma Yöneticisi.

Kaspersky Endpoint Security yüklemesini başlatmadan önce (uzaktan yükleme dahil) çalışan tüm uygulamaları kapatmanızı öneririz.

Kurulum Sihirbazını kullanarak uygulamayı yükleme

Kurulum Sihirbazı uygulamasının arayüzü uygulama kurulum adımlarına karşılık gelen sayfa sıralamalarından meydana gelir. Kurulum Sihirbazı'nın sayfaları arasında **Geri** ve **İleri** düğmelerini kullanarak gezinebilirsiniz. Görevini tamamladıktan sonra Kurulum Sihirbazı'nı kapatmak için **Sonlandır** düğmesine tıklayın. Kurulum Sihirbazını herhangi bir aşamada durdurmak için **İptal** düğmesine tıklayın.

Kurulum Sihirbazı'nı kullanarak uygulamayı yüklemek veya uygulamayı daha eski bir sürümden yükseltmek için:

1. Dağıtım kiti içindeki setup.exe dosyasını çalıştırın.

   Kurulum Sihirbazı başlatılır.

2. Kurulum Sihirbazı talimatlarını uygulayın.

setup.exe dosyası çalıştırıldığında, Kaspersky Endpoint Security bilgisayarı herhangi bir uyumsuz yazılıma karşı kontrol eder. Varsayılan olarak, uyumsuz yazılımın algılanması üzerinde kurulum süreci iptal edilir ve Kaspersky Endpoint Security ile uyumsuz olan uygulamaların listesi ekranda görünür. Kuruluma devam etmek için bu uygulamaları bilgisayardan kaldırın.

1. Adım. Bilgisayarınızın kurulum gereksinimlerini karşıladığını kontrol etme

Kaspersky Endpoint Security'yi bir bilgisayara yüklemeden veya uygulamanın önceki bir sürümünden yükseltmeden önce aşağıdaki koşullar kontrol edilir:

- İşletim sistemi ve servis paketinin ürün kurulumu yazılım gereksinimlerini karşılayıp karşılamadığı.
- Donanım ve yazılım gereksinimlerinin karşılanıp karşılanmadığı.
- Kullanıcının yazılım ürününü yükleme haklarına sahip olup olmadığı.

Önceki gereksinimlerden herhangi biri karşılanmazsa, ekranda ilgili bildirim görüntülenir.

Bilgisayar belirtilen gereksinimleri karşılıyorsa Kurulum Sihirbazı, yüklenen uygulama ile birlikte aynı anda çalışırken çakışmaya neden olabilecek Kaspersky uygulamalarını arar. Bu uygulamalar bulunur bunları elle kaldırmanız istenir.

Algılanan uygulamalar Kaspersky Endpoint Security'nin önceki sürümlerini içeriyorsa geçiş yapabilen tüm veriler (etkinleştirme verileri ve uygulama ayarları gibi) korunur ve Kaspersky Endpoint Security 11.1.1 for Windows'un yüklenmesi sırasında kullanılır ve uygulamanın önceki sürümü otomatik olarak kaldırılır. Bu, aşağıdaki uygulama sürümleri için geçerlidir:

- Kaspersky Endpoint Security 10 Service Pack 1 for Windows (yapı 10.2.2.10535).
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows (yapı 10.2.4.674)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows (yapı 10.2.5.3201)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 for Windows (yapı 10.2.6.3733)
- Kaspersky Endpoint Security 10 Service Pack 2 for Windows (yapı 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 for Windows (yapı 10.3.0.6294)
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 for Windows (yapı 10.3.0.6294)
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 for Windows (yapı 10.3.3.275)
- Kaspersky Endpoint Security 11.0.0 for Windows (yapı 11.0.0.6499).
- Kaspersky Endpoint Security for Windows 11.0.1 (yapı 11.0.1.90).
- Kaspersky Endpoint Security for Windows 11.1.0 (yapı 11.1.0.15919).

2. Adım. Yükleme prosedürünün hoş geldiniz sayfası

Uygulama yüklemeyle ilgili tüm gereksinimler karşılanıyorsa yükleme paketi başlatıldıktan sonra bir hoş geldiniz sayfası görülür. Hoş geldiniz sayfası, bilgisayarda Kaspersky Endpoint Security yüklemesinin başladığını belirtir.

Kurulum Sihirbazına devam etmek için **İleri** düğmesine tıklayın.

3. Adım. Lisans Sözleşmesi'ni ve Gizlilik Bildirimi'ni görüntüleme

Kurulum Sihirbazı'nın bu adımında, siz ve Kaspersky arasında yapılacak Son Kullanıcı Lisans Sözleşmesi'ni ve Gizlilik İlkesi'ni okumanız gerekir.

Lütfen Son Kullanıcı Lisans Sözleşmesi'ni ve Gizlilik İlkesi'ni dikkatlice okuyun. Son Kullanıcı Lisans Sözleşmesi'nin ve Gizlilik İlkesi'nin tüm koşullarını kabul ediyorsanız **Aşağıdakilerin tamamını okuduğumu, anladığımı ve kabul ettiğimi onaylıyorum** bölümünde aşağıdaki onay kutularını işaretleyin:

- **bu EULA'nın hüküm ve koşulları**
- **verilerin işlenmesini tanımlayan Gizlilik İlkesi**

Her iki onay kutusunu işaretledikten sonra aygıtınızda uygulamanın yüklemesi devam eder.

Son Kullanıcı Lisans Sözleşmesi'ni ve Gizlilik İlkesi'ni kabul etmiyorsanız **İptal** düğmesine tıklayarak yüklemeyi iptal edin.

4. Adım. Yükleme türünü seçme

Bu adımda en uygun Kaspersky Endpoint Security kurulum türünü seçebilirsiniz:

- **Temel kurulum**. Bu yükleme türünü seçerseniz BadUSB Saldırısı Önleme bileşeni haricindeki tüm koruma bileşenleri, bilgisayara Kaspersky uzmanlarının önerdiği ayarlarla yüklenir.
- **Standart kurulum**. Bu yükleme türünü seçerseniz BadUSB Saldırısı Önleme bileşeni haricindeki tüm koruma ve denetim bileşenleri, bilgisayara Kaspersky uzmanlarının önerdiği ayarlarla yüklenir.
- **Özel kurulum**. Bu kurulum türünü seçerseniz, yüklenecek bileşenleri seçmeniz ve uygulamanın hedef klasörünü seçmeniz istenir.

  Bu kurulum türü, temel ve standart kurulumlara dahil edilmeyen bileşenleri yüklemenize olanak tanır.

Varsayılan olarak standart kurulum seçilidir.

Kurulum Sihirbazının önceki adımına dönmek için **Geri** düğmesine tıklayın. Kurulum Sihirbazına devam etmek için **İleri** düğmesine tıklayın. Kurulum Sihirbazını durdurmak için **İptal** düğmesine tıklayın.

5. Adım. Yüklenecek uygulama bileşenlerini seçme

Bu adım, uygulamanın *Özel kurulum* seçeneğini seçerseniz gerçekleştirilir.

Bu adımda, yüklemek istediğiniz Kaspersky Endpoint Security bileşenlerini seçebilirsiniz. Dosya Koruması, kurulum için zorunlu bir bileşendir. Yüklemesini iptal edemezsiniz.

Varsayılan olarak aşağıdaki bileşenler hariç tüm yükleme bileşenleri yüklenmek üzere seçilidir:

- BadUSB Saldırı Engelleme.
- Sürücü Şifreleme.
- Dosya Şifreleme.
- Microsoft BitLocker Manager.
- KATA Endpoint Sensor.

Microsoft BitLocker Manager aşağıdaki işlevleri gerçekleştirir:

- Windows işletim sistemine entegre BitLocker şifrelemesini yönetir.
- Şifreleme ilkesi ayarlarını yapılandırır ve yönetilen bilgisayara uygulanabilirliğini denetler.
- Şifreleme ve şifre çözme işlemlerini başlatır.
- Yönetilen bilgisayarda şifreleme durumunu izler.
- Kurtarma anahtarlarını Kaspersky Security Center Yönetim Sunucusu'nda merkezi olarak depolar.

KATA Endpoint Sensor, Kaspersky Anti Targeted Attack Platform'un bir bileşenidir. Bu çözüm, hedeflenen saldırılar gibi tehditlerin hızlı tespitine yöneliktir. Bu bileşen sürekli olarak işlemleri, etkin ağ bağlantılarını ve değiştirilmiş dosyaları izler ve bu bilgileri Kaspersky Anti Targeted Attack Platform'a aktarır.

Yüklenecek bir bileşen seçmek için bileşen adının karşısındaki simgeye tıklayarak içerik menüsünü açın ve **Özellik yerel sabit sürücüye yüklenecek** seçeneğini seçin. Seçilen bileşen tarafından hangi görevlerin gerçekleştirileceği ve bileşeni yüklemek için ne kadar disk alanı gerektiğiyle ilgili daha ayrıntılı bilgi için mevcut Kurulum Sihirbazı sayfasının alt kısmına bakınız.

Yerel sabit sürücülerdeki kullanılabilir alanla ilgili ayrıntılı bilgi görüntülemek için **Birim** düğmesine tıklayın. Açılan **Kullanılabilir disk alanı** penceresinde bilgi görüntülenir.

Bileşenin kurulumunu iptal etmek için içerik menüsünde **Bu özellik kullanılamaz olacak** seçeneğini seçin.

Varsayılan olarak yüklenen bileşenlerin listesine dönmek için **Sıfırla** düğmesine tıklayın.

Kurulum Sihirbazının önceki adımına dönmek için **Geri** düğmesine tıklayın. Kurulum Sihirbazına devam etmek için **İleri** düğmesine tıklayın. Kurulum Sihirbazını durdurmak için **İptal** düğmesine tıklayın.

6. Adım. Hedef klasörü seçme

Bu adım, uygulamanın *Özel kurulum* seçeneğini seçerseniz uygulanabilir.

Bu adımda, uygulamanın yükleneceği hedef klasörün yolunu belirleyebilirsiniz. Uygulamanın hedef klasörünü seçmek için **Gözat** düğmesine tıklayın.

Yerel sabit sürücülerdeki kullanılabilir alanla ilgili bilgi görüntülemek için **Birim** düğmesine tıklayın. Açılan **Disk alanı gereksinimi** penceresinde bilgi görüntülenir.

Kurulum Sihirbazının önceki adımına dönmek için **Geri** düğmesine tıklayın. Kurulum Sihirbazına devam etmek için **İleri** düğmesine tıklayın. Kurulum Sihirbazını durdurmak için **İptal** düğmesine tıklayın.

7. Adım. Tarama istisnaları ekleme

Bu adım, uygulamanın *Özel kurulum* seçeneğini seçerseniz uygulanabilir.

Bu adımda, uygulama ayarlarına eklemek istediğiniz tarama istisnalarını belirtebilirsiniz.

Microsoft tarafından önerilen alanları tarama kapsamının dışında tut / **Kaspersky tarafından önerilen alanları tarama kapsamının dışında tut** onay kutuları, Microsoft veya Kaspersky'nin önerdiği alanları güvenilir bölgeye ekler / güvenilir bölge dışında tutar.

Bu onay kutularından biri seçilirse Kaspersky Endpoint Security, Microsoft veya Kaspersky'nin önerdiği alanları güvenilir bölgeye ekler ya da kapsam dışında tutar. Kaspersky Endpoint Security bu alanlarda virüs ve diğer tehdit taramalarını gerçekleştirmez.

Microsoft tarafından önerilen alanları tarama kapsamının dışında tut onay kutusu, dosya sunucuları için Microsoft Windows çalıştıran bir bilgisayara Kaspersky Endpoint Security yüklendiğinde etkindir.

Kurulum Sihirbazının önceki adımına dönmek için **Geri** düğmesine tıklayın. Kurulum Sihirbazına devam etmek için **İleri** düğmesine tıklayın. Kurulum Sihirbazını durdurmak için **İptal** düğmesine tıklayın.

8. Adım. Uygulamayı yüklemeye hazırlanma

Bilgisayarınızda Kaspersky Endpoint Security 10 for Windows'un yüklenmesine engel olabilecek kötü amaçlı programlar varsa yükleme işleminin korunması önerilir.

Yükleme işlemi koruması varsayılan olarak etkindir.

Ancak uygulama yüklenemezse (örneğin Windows Uzak Masaüstü yardımıyla uzaktan yükleme gerçekleştirirken), yükleme işleminin korumasını devre dışı bırakmanız tavsiye edilir. Bu durumda yüklemeyi iptal edin ve Uygulama Kurulum Sihirbazını yeniden başlatın. "Uygulamayı yüklemeye hazırlanma" adımında, **Yükleme işlemini koru** onay kutusu işaretini kaldırın.

Citrix PVS ile uyumluluk sağla onay kutusu, Citrix PVS uyumluluk modunda sürücüleri yükleyen işlevi etkinleştirir / devre dışı bırakır.

Citrix Hazırlama Hizmetleri ile çalışıyorsanız bu onay kutusunu seçin.

avp.com dosyasının yolunu %PATH% sistem değişkenine ekle onay kutusu, avp.com dosyasının yolunu %PATH% sistem değişkenine ekleyen seçeneği etkinleştirir / devre dışı bırakır.

Onay kutusu seçildiğinde komut satırından Kaspersky Endpoint Security veya görevlerinden herhangi birinin başlatılması, yürütülebilir dosyanın yolunun girilmesini gerektirmez. Yürütülebilir dosyanın adının ve belirli görevi başlatma komutunun girilmesi yeterlidir.

Kurulum Sihirbazının önceki adımına dönmek için **Geri** düğmesine tıklayın. Programı yüklemek için **Yükle** düğmesine tıklayın. Kurulum Sihirbazını durdurmak için **İptal** düğmesine tıklayın.

Mevcut ağ bağlantıları, uygulama bilgisayara yüklenirken sonlandırılabilir. Çoğu sonlandırılan ağ bağlantısı, uygulama yüklemesinin tamamlanmasının ardından geri yüklenir.

9. Adım. Uygulamayı yükleme

Uygulamanın yüklenmesi biraz zaman alabilir. Tamamlanmasını bekleyin.

Uygulamanın önceki bir sürümünü güncelliyorsanız bu adım ayarların taşınmasını ve uygulamanın önceki sürümünün kaldırılmasını da kapsar.

Kaspersky Endpoint Security kurulumu tamamlandıktan sonra İlk Yapılandırma Sihirbazı başlatılır.

Komut satırından uygulamayı yükleme

Kaspersky Endpoint Security, komut satırından aşağıdaki modlardan birinde yüklenebilir:

- Uygulama Kurulum Sihirbazı'nı kullanarak etkileşimli modda.
- Sessiz modda. Sessiz modda yüklemenin başlatılmasının ardından yükleme işlemine müdahale etmeniz gerekmez. Sessiz modda uygulamayı yüklemek için `/s` ve `/qn` anahtarlarını kullanın.

Uygulamayı yüklemek veya uygulama sürümünü yükseltmek için:

1. Komut satırı yorumlayıcısını (cmd.exe) yönetici olarak çalıştırın.
2. Kaspersky Endpoint Security dağıtım paketinin bulunduğu klasöre gidin.
3. Aşağıdaki komutu çalıştırın:

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pALLOWREBOOT=1|0] [/pADDLOCAL=<bileşen>] [/pSKIPPRODUCTCHECK=1|0] [/pSKIPPRODUCTUNINSTALL=1|0] [/pKLLOGIN=<kullanıcı adı> /pKLPASSWD=<parola> /pKLPASSWDAREA=<parola kapsamı>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<izleme düzeyi>] /s
   ```

   veya

   ```
   msiexec /i <dağıtım kiti adı> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [ALLOWREBOOT=1|0] [ADDLOCAL=<bileşen>] [SKIPPRODUCTCHECK=1|0] [SKIPPRODUCTUNINSTALL=1|0] [KLLOGIN=<kullanıcı adı> KLPASSWD=<parola> KLPASSWDAREA=<parola kapsamı>] [ENABLETRACES=1|0 TRACESLEVEL=<izleme düzeyi>] /qn
   ```

`EULA`	Son Kullanıcı Lisans Sözleşmesi koşullarının kabul edilmesi veya reddedilmesi. Kullanılabilir değerler: • `1` – Son Kullanıcı Lisans Sözleşmesi koşullarının kabulü. • `0` – Son Kullanıcı Lisans Sözleşmesi koşullarının reddedilmesi. Lisans Sözleşmesi metni Kaspersky Endpoint Security'nin dağıtım kitinde yer alır. Uygulamayı yüklemek veya uygulama sürümünü yükseltmek için Son Kullanıcı Lisans Sözleşmesi'nin koşullarının kabul edilmesi gerekir.

PRIVACYPOLICY	Gizlilik İlkesi'nin kabul edilmesi veya reddedilmesi. Kullanılabilir değerler: • 1 – Gizlilik İlkesi'nin kabul edilmesi. • 0 – Gizlilik İlkesi'nin reddedilmesi. Gizlilik İlkesi metni Kaspersky Endpoint Security dağıtım kitinde bulunur. Uygulamayı yüklemek veya uygulama sürümünü yükseltmek için Gizlilik İlkesi'ni kabul etmelisiniz.
KSN	Kaspersky Security Network'e katılmayı kabul etme veya reddetme. Bu parametre için değer belirtilmezse Kaspersky Endpoint Security ilk başlatıldığında KSN'ye katılım izni veya reddinizi onaylamanızı ister. Kullanılabilir değerler: • 1 – KSN'ye katılmayı kabul etme. • 0 – KSN'ye katılmayı reddetme (varsayılan değer). Kaspersky Endpoint Security dağıtım paketi, Kaspersky Security Network ile kullanılmak üzere optimize edilmiştir. Kaspersky Security Network'e katılmamayı seçtiyseniz yükleme tamamlandıktan sonra Kaspersky Endpoint Security'yi güncellemeniz gerekir.
ALLOWREBOOT	Uygulamanın yüklenmesinin veya yükseltilmesinin ardından gerekirse bilgisayarın otomatik olarak yeniden başlatılması. Kullanılabilir değerler: • 1 – gerekirse bilgisayarın otomatik olarak yeniden başlatılması. • 0 – bilgisayarın otomatik olarak yeniden başlatılması engellenir (varsayılan değer). Kaspersky Endpoint Security'yi yüklerken yeniden başlatma gerekli değildir. Yalnızca kurulumdan önce uyumsuz uygulamaları kaldırmanız gerekirse yeniden başlatma gereklidir. Uygulama sürümünü güncellerken de yeniden başlatma gerekebilir.
ADDLOCAL	Kurulum için ek bileşenler seçin. Varsayılan olarak aşağıdaki bileşenler hariç tüm yükleme bileşenleri yüklenmek üzere seçilidir: BadUSB Saldırısı Önleme, Dosya Düzeyinde Şifreleme, Tam Disk Şifreleme, BitLocker Management ve KATA Endpoint Sensor. Kullanılabilir değerler: • MSBitLockerFeature. BitLocker Manager bileşeni yüklenir. • AntiAPTFeature. KATA Endpoint Sensor bileşeni yüklenir.
SKIPPRODUCTCHECK	Uyumsuz yazılım kontrolü. Uyumsuz yazılımların listesi dağıtım kitinde bulunan incompatible.txt dosyasında mevcuttur. Kullanılabilir değerler: • 1 – uyumsuz yazılım kontrolü etkin (varsayılan değer). • 0 – uyumsuz yazılım kontrolü devre dışı.
SKIPPRODUCTUNINSTALL	Tespit edilen uyumsuz yazılımın otomatik kaldırılması. Kullanılabilir değerler: • 1 – Kaspersky Endpoint Security, uyumsuz yazılımı kaldırmaya çalışır (varsayılan değer). • 0 – uyumsuz yazılımın otomatik olarak kaldırılması yasaktır.

KLLOGIN	Kaspersky Endpoint Security özelliklerine ve ayarlarına erişim için kullanıcı adını ayarlayın (Parola Koruması bileşeni). Kullanıcı adı, KLPASSWD ve KLPASSWDAREA parametreleriyle birlikte ayarlanır. Varsayılan kullanıcı adı KLAdmin'dir.
KLPASSWD	Kaspersky Endpoint Security özelliklerine ve ayarlarına erişim için bir parola belirtin (parola, KLLOGIN ve KLPASSWDAREA parametreleriyle birlikte belirtilir). Bir parola belirlediyseniz ancak KLLOGIN parametresine sahip bir kullanıcı adı belirlemediyseniz, varsayılan olarak KLAdmin kullanıcı adı kullanılır.
KLPASSWDAREA	Kaspersky Endpoint Security'ye erişim için parola kapsamını belirtin. Kullanıcı bu kapsamdaki bir eylemi gerçekleştirmeye çalıştığında Kaspersky Endpoint Security kullanıcının hesap bilgilerini sorar (KLLOGIN ve KLPASSWD parametreleri). Birden çok değer belirtmek için ";" karakterini kullanın. Kullanılabilir değerler: • SET – Uygulama ayarlarını değiştirme. • EXIT – Uygulamadan çıkma. • DISPROTECT – Koruma bileşenlerini devre dışı bırakma ve tarama görevlerini durdurma. • DISPOLICY – Kaspersky Security Center ilkesini devre dışı bırakma. • UNINST – Uygulamayı bilgisayardan kaldırma. • DISCTRL – Denetim bileşenlerini devre dışı bırakma. • REMOVELIC – anahtarın kaldırılması. • REPORTS – raporların görüntülenmesi.
ENABLETRACES	Uygulama izlerini etkinleştirme veya devre dışı bırakma. Kaspersky Endpoint Security başladıktan sonra, iz dosyalarını %ProgramData%/Kaspersky Lab klasörüne kaydeder. Kullanılabilir değerler: • 1 – izler etkin. • 0 – izler devre dışı (varsayılan değer).
TRACESLEVEL	İzlerin ayrıntı düzeyi. Kullanılabilir değerler: • 100 (kritik). Sadece kritik hata mesajları. • 200 (yüksek). Önemli hatalar dahil tüm hatalarla ilgili mesajlar. • 300 (tanısal). Tüm hatalarla ilgili mesajlar ve uyarıları içeren çeşitli mesajlar. • 400 (önemli). Sıradan ve kritik hatalarla ilgili tüm uyarılar ve mesajlar ve ek bilgiler içeren çeşitli mesajlar. • 500 (normal). Sıradan ve kritik hatalarla ilgili tüm uyarılar ve mesajlar ile normal modda uygulamanın çalışması hakkında ayrıntılı bilgi içeren mesajlar (varsayılan değer). • 600 (düşük). Tüm olası mesajlar.

Örnek:

```
setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pALLOWREBOOT=1 /s

msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1
KSN=1 KLLOGIN=Yönetici KLPASSWD=Parola
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn

setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

Uygulama yüklendikten sonra setup.ini dosyasındaki. etkinleştirme kodunu belirtmediyseniz Kaspersky Endpoint Security deneme lisansını etkinleştirir. Deneme lisansı genellikle kısa sürelidir. Deneme lisansının süresi sona erdiğinde tüm Kaspersky Endpoint Security özellikleri devre dışı bırakılır. Uygulamayı kullanmaya devam etmek için ticari lisansı etkinleştirmeniz gerekir.

Uygulamayı yüklerken veya uygulama sürümünü sessiz modda yükseltirken aşağıdaki dosyaların kullanımı desteklenir:

- setup.ini – genel uygulama kurulum ayarları
- install.cfg – Kaspersky Endpoint Security'nin yerel ayarları
- setup.reg – kayıt defteri anahtarları.

  setup.reg dosyasındaki kayıt defteri anahtarları, yalnızca setup.ini dosyasındaki `SetupReg` parametresi için `setup.reg` değeri ayarlanmışsa kayıt defterine yazılır. setup.reg dosyası Kaspersky uzmanları tarafından oluşturulur. Bu dosyanın içeriğinin değiştirilmesi önerilmez.

setup.ini, install.cfg ve setup.reg dosyalarından ayarları uygulamak için bu dosyaları, Kaspersky Endpoint Security dağıtım paketini içeren klasöre yerleştirin.

Sistem Merkezi Yapılandırma Yöneticisi'ni kullanarak uygulamayı uzaktan yükleme

Bu talimatlar Sistem Merkezi Yapılandırma Yöneticisi 2012 R2 için geçerlidir.

Sistem Merkezi Yapılandırma Yöneticisi'ni kullanarak bir uygulamayı uzaktan yüklemek için:

1. Yapılandırma Yöneticisi konsolunu açın.
2. Pencerenin sağ kısmında, **Uygulama yönetimi** bölümünde **Paketler**'i seçin.
3. Kontrol panelinde konsolun üst kısmında **Oluştur** düğmesine tıklayın.

   Yeni Paket ve Uygulama Sihirbazı açılır.
4. Yeni Paket ve Uygulama Sihirbazı'nda:

   a. **Paket** bölümünde:

- **Ad** alanına yükleme paketinin adını girin.
- **Kaynak klasör** alanında Kaspersky Endpoint Security dağıtım setini içeren klasörün yolunu belirtin.

b. **Uygulama türü** bölümünde **Standart uygulama** seçeneğini seçin.

c. **Standart uygulama** bölümünde:

- **Ad** alanına yükleme paketi için benzersiz ad girin (örneğin, sürümü içeren uygulama adı).
- **Komut satırı** alanında komut satırında Kaspersky Endpoint Security yükleme seçeneklerini belirtin.
- **Gözat** düğmesine tıklayarak uygulamanın yürütülebilir dosyasının yolunu belirtin.
- **Yürütme modu** listesinin **Yönetici haklarıyla çalıştır** öğesinin seçili olduğundan emin olun.

d. **Gereklilikler** bölümünde:

- Kaspersky Endpoint Security yüklemeden önce başlatılmasını istediğiniz farklı bir uygulama varsa **Önce başka uygulama başlat** onay kutusunu işaretleyin.

  Uygulama açılır listesinden uygulama seçin veya **Gözat** düğmesine tıklayarak bu uygulamanın yürütülebilir dosyasının yolunu belirtin.
- Uygulamanın sadece belirtilen işletim sisteminde yüklenmesini isterseniz **Platform gereklilikleri** bölümünde **Uygulama sadece belirtilen platformlarda başlatılabilir** seçeneğini seçin.

  Aşağıdaki listede Kaspersky Endpoint Security'nin yükleneceği işletim sistemlerinin karşısındaki onay kutularını seçin.

Bu adım isteğe bağlıdır.

e. **Özet** seçeneğinde ayarların tüm girilen değerlerini kontrol edin ve **İleri**'ye tıklayın.

Oluşturulan yükleme paketi geçerli yükleme paketleri listesinde **Paketler** bölümünde görülür.

5. Yükleme paketinin içerik menüsünde **Dağıt**'ı seçin.

   Dağıtım Sihirbazı başlatılır.

6. Dağıtım Sihirbazında:

a. **Genel** bölümünde:

- **Yazılım** alanına yükleme paketinin benzersiz adını girin veya **Gözat** düğmesine tıklayarak listeden yükleme paketini seçin.
- **Koleksiyon** alanına uygulamanın yükleneceği bilgisayarların koleksiyonunun adını girin veya **Gözat** düğmesine tıklayarak listeden koleksiyon seçin.

b. **İçerir** bölümüne dağıtım noktalarını ekleyin (daha fazla bilgi için lütfen Sistem Merkezi Yapılandırma Yöneticisi için yardım belgelerine bakın).

c. Gerekirse, Dağıtım Sihirbazında diğer ayarların değerlerini belirtin. Bu ayarlar Kaspersky Endpoint Security'nin uzaktan yüklenmesi için isteğe bağlıdır.

d. **Özet** seçeneğinde ayarların tüm girilen değerlerini kontrol edin ve **İleri**'ye tıklayın.

Dağıtım Sihirbazı bittikten sonra Kaspersky Endpoint Security'nin uzaktan yüklenmesi için bir görev oluşturulur.

setup.ini dosyası yükleme ayarlarının açıklaması

Uygulamayı komut satırından yüklerken veya Microsoft Windows'un Grup İlkesi Düzenleyicisi'ni kullanırken setup.ini dosyası kullanılır. setup.ini file dosyasından ayarları uygulamak için bu dosyayı Kaspersky Endpoint Security dağıtım paketini içeren klasöre yerleştirin.

setup.ini dosyası aşağıdaki bölümleri içerir:

- `[Setup]` - genel uygulama yükleme seçenekleri.
- `[Components]` – yüklenecek uygulama bileşenlerinin seçimi. Bileşenlerin hiçbiri belirtilmezse işletim sistemlerinin tüm bileşenleri yüklenir. Dosya Koruması zorunlu bir bileşendir ve bu bölümde hangi ayarların belirtildiğine bakılmaksızın bilgisayara yüklenir.
- `[Tasks]` – Kaspersky Endpoint Security görevlerinin listesine eklenecek görevlerin seçimi. Herhangi bir görev belirtilmezse tüm görevler Kaspersky Endpoint Security'nin görev listesine eklenir.

`1` değerinin alternatifleri, `evet`, `açık`, `etkinleştir` ve `etkinleştirildi` seçenekleridir.

`0` değerinin alternatifleri, `hayır`, `kapalı`, `devre dışı bırak` ve `devre dışı bırakıldı` seçenekleridir.

setup.ini dosyasının ayarları

Bölüm	Parametre	Açıklama
`[Setup]`	`InstallDir`	Uygulama yükleme klasörüne giden yol.
	`ActivationCode`	Kaspersky Endpoint Security etkinleştirme kodu.
	`Eula`	Son Kullanıcı Lisans Sözleşmesi koşullarının kabul edilmesi veya reddedilmesi. Kullanılabilir değerler: • `1` – Son Kullanıcı Lisans Sözleşmesi koşullarının kabulü. • `0` – Son Kullanıcı Lisans Sözleşmesi koşullarının reddedilmesi. Lisans Sözleşmesi metni Kaspersky Endpoint Security'nin dağıtım kitinde yer alır. Uygulamayı yüklemek veya uygulama sürümünü yükseltmek için Son Kullanıcı Lisans Sözleşmesi'nin koşullarının kabul edilmesi gerekir.
	`PrivacyPolicy`	Gizlilik İlkesi'nin kabul edilmesi veya reddedilmesi. Kullanılabilir değerler: • `1` – Gizlilik İlkesi'nin kabul edilmesi. • `0` – Gizlilik İlkesi'nin reddedilmesi.

		Gizlilik İlkesi metni Kaspersky Endpoint Security dağıtım kitinde bulunur. Uygulamayı yüklemek veya uygulama sürümünü yükseltmek için Gizlilik İlkesi'ni kabul etmelisiniz.
	`KSN`	Kaspersky Security Network'e katılmayı kabul etme veya reddetme. Bu parametre için değer belirtilmezse Kaspersky Endpoint Security ilk başlatıldığında KSN'ye katılım izni veya reddinizi onaylamanızı ister. Kullanılabilir değerler: • `1` – KSN'ye katılmayı kabul etme. • `0` – KSN'ye katılmayı reddetme (varsayılan değer). Kaspersky Endpoint Security dağıtım paketi, Kaspersky Security Network ile kullanılmak üzere optimize edilmiştir. Kaspersky Security Network'e katılmamayı seçtiyseniz yükleme tamamlandıktan sonra Kaspersky Endpoint Security'yi güncellemeniz gerekir.
	`Kul. adı`	Kaspersky Endpoint Security özelliklerine ve ayarlarına erişim için kullanıcı adını ayarlayın (Parola Koruması bileşeni). Kullanıcı adı, `Parola` ve `PasswordArea` parametreleriyle birlikte ayarlanır. Varsayılan kullanıcı adı KLAdmin'dir.
	`Parola`	Kaspersky Endpoint Security özelliklerine ve ayarlarına erişim için bir parola belirtin (parola, `Kul. adı` ve `PasswordArea` parametreleriyle birlikte belirtilir). Bir parola belirlediyseniz ancak `Giriş` parametresine sahip bir kullanıcı adı belirlemediyseniz, varsayılan olarak KLAdmin kullanıcı adı kullanılır.
	`PasswordArea`	Kaspersky Endpoint Security'ye erişim için parola kapsamını belirtin. Kullanıcı bu kapsamdaki bir eylemi gerçekleştirmeye çalıştığında Kaspersky Endpoint Security kullanıcının hesap bilgilerini sorar (`Kul. Adı` ve `Parola` parametreleri). Birden çok değer belirtmek için "`;`" karakterini kullanın. Kullanılabilir değerler: • `SET` – Uygulama ayarlarını değiştirme. • `EXIT` – Uygulamadan çıkma. • `DISPROTECT` – Koruma bileşenlerini devre dışı bırakma ve tarama görevlerini durdurma. • `DISPOLICY` – Kaspersky Security Center ilkesini devre dışı bırakma. • `UNINST` – Uygulamayı bilgisayardan kaldırma. • `DISCTRL` – Denetim bileşenlerini devre dışı bırakma.

		• `REMOVELIC` – anahtarın kaldırılması. • `REPORTS` – raporların görüntülenmesi.
	`SelfProtection`	Uygulama yükleme koruma mekanizmasını etkinleştirme veya devre dışı bırakma. Kullanılabilir değerler: • `1` – Uygulama yükleme koruma mekanizması etkin. • `0` – Uygulama yükleme koruma mekanizması devre dışı. Kurulum korumasını devre dışı bırakabilirsiniz. Kurulum koruması, kötü amaçlı yazılımların kendini dağıtım paketi olarak göstermesine karşı koruma, Kaspersky Endpoint Security yükleme klasörüne erişimi engelleme ve uygulama anahtarlarını içeren sistem kayıt defteri kovanına erişimi engellemeyi içerir. Ancak uygulama yüklenemezse (örneğin Windows Uzak Masaüstü yardımıyla uzaktan kurulum gerçekleştirirken), yükleme işleminin korumasını devre dışı bırakmanız tavsiye edilir.
	`Reboot=1`	Uygulamanın yüklenmesinin veya yükseltilmesinin ardından gerekirse bilgisayarın otomatik olarak yeniden başlatılması. Bu parametre için bir değer ayarlanmadığı takdirde bilgisayarın otomatik olarak yeniden başlatılması engellenir. Kaspersky Endpoint Security'yi yüklerken yeniden başlatma gerekli değildir. Yalnızca kurulumdan önce uyumsuz uygulamaları kaldırmanız gerekirse yeniden başlatma gereklidir. Uygulama sürümünü güncellerken de yeniden başlatma gerekebilir.
	`AddEnvironment`	%PATH% sistem değişkenini, Kaspersky Endpoint Security kurulum klasöründe bulunan yürütülebilir dosya yolu ile destekleyin. Kullanılabilir değerler: • `1` – %PATH% sistem değişkeni, Kaspersky Endpoint Security kurulum klasöründe bulunan yürütülebilir dosya yolu ile desteklenir. • `0` – %PATH% sistem değişkeni, Kaspersky Endpoint Security kurulum klasöründe bulunan yürütülebilir dosya yolu ile desteklenmez.
	`AMPPL`	AM-PPL (Antimalware Protected Process Light) teknolojisini kullanan Kaspersky Endpoint Security hizmeti korumasını etkinleştirin veya devre dışı bırakın. Kullanılabilir değerler: • `1` – AM-PPL teknolojisini kullanan Kaspersky Endpoint Security hizmetinin koruması etkin. • `0` – AM-PPL teknolojisini kullanan Kaspersky Endpoint Security hizmetinin koruması devre dışı.

	SetupReg	Kayıt defteri anahtarlarının setup.reg dosyasından kayıt defterine yazılmasını etkinleştirir. SetupReg: setup.reg parametre değeri.
	EnableTraces	Uygulama yükleme izlerini etkinleştirme veya devre dışı bırakma. Kaspersky Endpoint Security, iz dosyalarını %ProgramData%/Kaspersky Lab klasörüne kaydeder. Kullanılabilir değerler: • 1 – uygulama yükleme izleri etkin. • 0 – uygulama yükleme izleri devre dışı (varsayılan değer).
	TracesLevel	İzlerin ayrıntı düzeyi. Kullanılabilir değerler: • 100 (kritik). Sadece kritik hata mesajları. • 200 (yüksek). Önemli hatalar dahil tüm hatalarla ilgili mesajlar. • 300 (tanısal). Tüm hatalarla ilgili mesajlar ve uyarıları içeren çeşitli mesajlar. • 400 (önemli). Sıradan ve kritik hatalarla ilgili tüm uyarılar ve mesajlar ve ek bilgiler içeren çeşitli mesajlar. • 500 (normal). Sıradan ve kritik hatalarla ilgili tüm uyarılar ve mesajlar ile normal modda uygulamanın çalışması hakkında ayrıntılı bilgi içeren mesajlar (varsayılan değer). • 600 (düşük). Tüm olası mesajlar.
[Components]	ALL	Tüm bileşenleri yükleyin. Parametre değeri 1 belirtilirse her bir bileşenin yükleme ayarı ne olursa olsun tüm bileşenler yüklenir.
	MailAntiVirus	Posta Koruması.
	IMAntiVirus	IM Koruması.
	WebAntiVirus	İnternet Koruması.
	ApplicationPrivilegeControl	Uygulama Ayrıcalığı Denetimi.
	SystemWatcher	Sistem İzleyici.
	Güvenlik Duvarı	Güvenlik Duvarı.
	NetworkAttackBlocker	Ağ Saldırısı Engelleyici.
	WebControl	İnternet Denetimi.
	DeviceControl	Aygıt Denetimi.
	ApplicationStartupControl	Uygulama Başlatma Denetimi.
	FileEncryption	Dosya Düzeyinde Şifreleme kitaplıkları.
	DiskEncryption	Tam Disk Şifreleme kitaplıkları.

	`VulnerabilityAssessment`	Zayıf Nokta İzleyicisi.
	`KeyboardAuthorization`	BadUSB Saldırısı Önleme.
	`AntiAPT`	KATA Endpoint Sensor.
	`MSBitLocker`	Microsoft BitLocker Manager.
	`AdminKitConnector`	Kaspersky Security Center üzerinden uygulamanın uzaktan yönetimi için Ağ Aracısı Bağlayıcısı. Kullanılabilir değerler: • `1` – Ağ Aracısı Bağlayıcısı yüklenir. • `0` – Ağ Aracısı Bağlayıcısı yüklenmez.
`[Tasks]`	`ScanMyComputer`	Tam Tarama görevi. Kullanılabilir değerler: • `1` – Görev, Kaspersky Endpoint Security görevlerinin listesine eklenir. • `0` – Görev, Kaspersky Endpoint Security görevlerinin listesine eklenmez.
	`ScanCritical`	Kritik Alanları Tarama görevi. Kullanılabilir değerler: • `1` – Görev, Kaspersky Endpoint Security görevlerinin listesine eklenir. • `0` – Görev, Kaspersky Endpoint Security görevlerinin listesine eklenmez.
	`Güncelle`	Güncelleme görevi. Kullanılabilir değerler: • `1` – Görev, Kaspersky Endpoint Security görevlerinin listesine eklenir. • `0` – Görev, Kaspersky Endpoint Security görevlerinin listesine eklenmez.

İlk Yapılandırma Sihirbazı

Kaspersky Endpoint Security'nin İlk Yapılandırma Sihirbazı uygulama kurulum işleminin sonunda başlar. İlk Yapılandırma Sihirbazı, uygulamayı etkinleştirmenize olanak tanır ve işletim sistemindeki uygulamalar hakkında bilgi toplar. Bu uygulamalar, işletim sisteminde eylemleri herhangi bir kısıtlamaya tabi olmayan güvenilir uygulamalar listesine eklenir.

İlk Yapılandırma Sihirbazı'nın arabirimi birkaç sayfadan (adımdan) oluşur. İlk Yapılandırma Sihirbazı'nın sayfaları arasında **Geri** ve **İleri** düğmelerini kullanarak gezinebilirsiniz. İlk Yapılandırma Sihirbazı işlemini tamamlamak için **Sonlandır** düğmesine basın. Herhangi bir aşamada İlk Yapılandırma Sihirbazı'nı durdurmak için **İptal**'e tıklayın.

İlk Yapılandırma Sihirbazı herhangi bir nedenle kesintiye uğrarsa belirlenen ayarlar kaydedilmez. Bir sonraki sefer uygulamayı kullanmaya çalıştığınızda İlk Yapılandırma Sihirbazı yeniden başlatılır ve ayarları en baştan yapılandırmanız gerekir.

Uygulamayı etkinleştirme

Uygulama, sistem tarihi ve saatinin güncel olduğu bir bilgisayarda etkinleştirilmelidir. Uygulama etkinleştirildikten sonra sistem tarihi ve saati değiştirilirse, anahtar çalışmaz hale gelir. Uygulama güncellemeler olmadan işletim yöntemine geçer ve Kaspersky Security Network kullanılamaz. İşletim sistemini yeniden yükleyerek anahtar tekrar çalışır hale getirilebilir.

Bu adımda, aşağıdaki Kaspersky Endpoint Security etkinleştirme seçeneklerinden birini seçin:

- **Etkinleştirme koduyla etkinleştir**. Bir etkinleştirme kodu ile uygulamayı etkinleştirmek için bu seçeneği seçin ve bir etkinleştirme kodu girin.
- **Anahtar dosyasıyla etkinleştir**. Uygulamayı bir anahtar dosyası ile etkinleştirmek için bu seçeneği seçin.
- **Deneme sürümünü etkinleştir**. Uygulamanın deneme sürümünü etkinleştirmek için bu seçeneği seçin. Kullanıcı, uygulamanın deneme sürümünün lisansıyla sınırlanan süre boyunca uygulamanın tamamen işlevsel sürümünü kullanabilir. Lisansın süresi dolduktan sonra uygulama işlevi engellenir ve deneme sürümünü tekrar etkinleştiremezsiniz.
- **Daha sonra etkinleştir**. Kaspersky Endpoint Security etkinleştirmesinin bu aşamasını atlamak isterseniz bu seçeneği seçin. Kullanıcı sadece Dosya Koruması ve Güvenlik Duvarı bileşenleriyle çalışabilir. Kullanıcı, Kaspersky Endpoint Security'nin anti-virüs veritabanlarını ve modüllerini sadece kurulumun ardından güncelleyebilecektir. **Sonra etkinleştir** seçeneği sadece uygulamanın yüklenmesinin hemen ardından İlk Yapılandırma Sihirbazı başlatıldığında kullanılabilir.

Uygulamanın deneme sürümünü etkinleştirmek veya bir etkinleştirme kodu ile uygulamayı etkinleştirmek için İnternet bağlantısı gerekir.

İlk Yapılandırma Sihirbazına devam etmek için bir etkinleştirme seçeneği seçin ve **İleri** düğmesine tıklayın. İlk Yapılandırma Sihirbazını durdurmak için **İptal** düğmesine tıklayın.

2. Adım. Etkinleştirme koduyla etkinleştirme

Bu adım yalnızca uygulamayı bir etkinleştirme koduyla etkinleştirdiğinizde kullanılabilir. Uygulamanın deneme sürümünü etkinleştirdiğinizde ya da uygulamayı bir anahtar dosyası ile etkinleştirdiğinizde bu adım atlanır.

Bu adım sırasında Kaspersky Endpoint Security, girilen etkinleştirme kodunu doğrulamak için etkinleştirme sunucusuna veri gönderir:

- Etkinleştirme kodu doğrulama başarılıysa İlk Yapılandırma Sihirbazı otomatik olarak bir sonraki pencereye ilerler.
- Etkinleştirme kodu doğrulama başarısız olursa bunu belirten bir mesaj görülür. Bu durumda size Kaspersky Endpoint Security'yi satan yazılım tedarikçisine başvurmalısınız.
- Etkinleştirme koduyla yapılabilecek etkinleştirme sayısı aşılmışsa bunu belirten bir bildirim görülür. İlk Yapılandırma Sihirbazı kesintiye uğrar ve uygulama Kaspersky Teknik Destek ile iletişim kurmanızı önerir.

İlk Yapılandırma Sihirbazının önceki adımına dönmek için **Geri** düğmesine tıklayın. İlk Yapılandırma Sihirbazını durdurmak için **İptal** düğmesine tıklayın.

Anahtar dosyasıyla etkinleştirme

Bu adım, yalnızca uygulamayı bir anahtar dosyası ile etkinleştirdiğinizde kullanılabilir.

Bu adımda, anahtar dosyasına giden yolu belirleyin. Bunun için, **Gözat** düğmesine tıklayarak `<Dosya kodu>.key` biçiminde bir anahtar dosyası seçin.

Anahtar dosyasını seçtikten sonra, pencerenin alt kısmında aşağıdaki bilgi görüntülenir:

- Anahtar
- Lisans türü (ticari veya deneme) ve bu lisansın kapsadığı bilgisayar sayısı
- Bilgisayarda uygulama etkinleştirme tarihi
- Lisans bitiş tarihi
- Lisans ile kullanılabilecek uygulama işlevselliği
- Varsa anahtar sorunları hakkında bildirimler. Örneğin, *Anahtar kara listesi bozuk*.

İlk Yapılandırma Sihirbazının önceki adımına dönmek için **Geri** düğmesine tıklayın. İlk Yapılandırma Sihirbazına devam etmek için **İleri** düğmesine tıklayın. İlk Yapılandırma Sihirbazını durdurmak için **İptal** düğmesine tıklayın.

Etkinleştirilecek işlevleri seçme

Bu adım, yalnızca uygulamanın deneme sürümünü etkinleştirdiğinizde kullanılabilir.

Bu adımda, uygulamanın etkinleştirilmesinden sonra kullanılabilir hale gelecek işlevselliği seçebilirsiniz.

- **Temel kurulum**. Bu seçenek seçilirse uygulamanın etkinleştirilmesinden sonra yalnızca koruma bileşenleri, Uygulama Ayrıcalığı Denetimi ve Zayıf Nokta İzleyicisi etkin hale gelir.
- **Standart kurulum**. Bu seçenek seçilirse etkinleştirmeden sonra yalnızca uygulamanın koruma ve denetim bileşenleri etkin hale gelir.
- **Tam kurulum**. Bu seçenek seçilirse veri şifreleme işlevselliği dahil tüm yüklenen uygulama bileşenleri, uygulamanın etkinleştirilmesinden sonra etkin hale gelir.

Yükleme sırasında lisansınızın izin verdiğinden daha fazla bileşen seçerseniz uygulamanın etkinleştirilmesinden sonra lisans kapsamındaki etkin olmayan bileşenler yüklenir fakat çalışmaz. Satın alınan lisans mevcut kurulu bileşenlerden daha fazla bileşen kullanmaya olanak tanırsa uygulama etkinleştirildikten sonra yüklenmeyen bileşenler **Lisans** bölümünde listelenir.

Varsayılan olarak standart kurulum seçilidir.

İlk Yapılandırma Sihirbazının önceki adımına dönmek için **Geri** düğmesine tıklayın. İlk Yapılandırma Sihirbazına devam etmek için **İleri** düğmesine tıklayın. İlk Yapılandırma Sihirbazını durdurmak için **İptal** düğmesine tıklayın.

Etkinleştirmeyi tamamlama

Bu adımda İlk Yapılandırma Sihirbazı, Kaspersky Endpoint Security'nin başarılı etkinleştirmesi ile ilgili bildirimde bulunur. Lisans hakkında aşağıdaki bilgiler sağlanır:

- Lisans türü (ticari veya deneme) ve bu lisansın kapsadığı bilgisayar sayısı
- Lisans bitiş tarihi
- Lisans ile kullanılabilecek uygulama işlevselliği

İlk Yapılandırma Sihirbazına devam etmek için **İleri** düğmesine tıklayın. İlk Yapılandırma Sihirbazını durdurmak için **İptal** düğmesine tıklayın.

İşletim sistemini analiz etme

Bu adım sırasında işletim sistemine dahil uygulamalar hakkında bilgi toplanır. Bu uygulamalar, işletim sisteminde eylemleri herhangi bir kısıtlamaya tabi olmayan güvenilir uygulamalar listesine eklenir.

Diğer uygulamalar, Kaspersky Endpoint Security kurulduktan sonra ilk kez başlatıldığında analiz edilir.

İlk Yapılandırma Sihirbazını durdurmak için **İptal** düğmesine tıklayın.

Uygulamanın ilk yapılandırması sonlandırılıyor

İlk Yapılandırma Sihirbazı tamamlama penceresi, Kaspersky Endpoint Security yükleme işleminin tamamlanması hakkında bilgi içerir.

Kaspersky Endpoint Security'yi başlatmak isterseniz **Bitir** düğmesine tıklayın.

Kaspersky Endpoint Security'yi başlatmadan İlk Yapılandırma Sihirbazı'ndan çıkmak isterseniz **Start Kaspersky Endpoint Security 10 for Windows** onay kutusunun işaretini kaldırın ve **Bitir** düğmesine tıklayın.

Kaspersky Security Network Bildirimi

Bu adımda, Kaspersky Security Network'e katılmaya davet edilirsiniz.

Kaspersky Security Network Bildirimi'ni gözden geçirin:

- Tüm koşulları kabul ediyorsanız, İlk Yapılandırma Sihirbazı penceresinde **Kaspersky Security Network'ün katılım koşullarını kabul ediyorum** seçeneğini seçin.
- Kaspersky Security Network'e katılım koşullarını kabul etmiyorsanız İlk Yapılandırma Sihirbazı penceresinde **Kaspersky Security Network'ün katılım koşullarını kabul etmiyorum** seçeneğini seçin.

İlk Yapılandırma Sihirbazını yapılandırmaya devam etmek için **Tamam** düğmesine tıklayın.

Eski bir uygulama sürümünü yükseltme yolları hakkında

Uygulamanın önceki bir sürümünü Kaspersky Endpoint Security 10 Service Pack 2 for Windows'a yükseltmek için tüm sabit sürücülerin şifresini çözün.

Aşağıdaki uygulamaları Kaspersky Endpoint Security 10 Service Pack 2 for Windows'a yükseltebilirsiniz:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 CF1 (yapı 6.0.4.1424) / MP4 CF2 (yapı 6.0.4.1611)
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 (yapı 6.0.4.1424) / MP4 CF2 (yapı 6.0.4.1611)
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows (yapı 10.2.2.10535)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows (yapı 10.2.2.10535(MR1))
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows (yapı 10.2.4.674)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows (yapı 10.2.5.3201)

Yukarıda belirtilen uygulamalardan herhangi biri Kaspersky Endpoint Security 10 Service Pack 2 for Windows'a yükseltildiğinde, Karantina ve Yedekleme dosyaları aktarılmaz.

Uygulamanın eski sürümünü aşağıdaki şekilde yükseltebilirsiniz:

- Uygulama Kurulum Sihirbazı'nı kullanarak yerel olarak etkileşimli modda.
- Yerel olarak etkileşimsiz modda komut satırından
- Uzaktan Kaspersky Security Center yazılım paketini kullanarak (*Kaspersky Security Center Uygulama Kılavuzu*'na bakınız).
- Microsoft Windows'un Grup İlkesi Düzenleyicisi ile uzaktan (işletim sistemi yardım dosyalarına bakınız)

Uygulamanın önceki bir sürümünü Kaspersky Endpoint Security 10 Service Pack 2 for Windows'a yükseltirken, uygulamanın önceki sürümünün kaldırılması gerekmez. Önceki uygulama sürümünü yükseltmeden önce tüm etkin uygulamalardan çıkmanızı öneririz.

Uygulamayı kaldırma

Bu bölümde, Kaspersky Endpoint Security'yi bilgisayarınızdan nasıl kaldırabileceğiniz açıklanmaktadır.

Uygulamayı kaldırma yolları hakkında

Kaspersky Endpoint Security'nin kaldırılması, bilgisayar ve kullanıcı verilerini tehditlere karşı korumasız bırakır.

Kaspersky Endpoint Security bilgisayardan çeşitli şekillerden kaldırılabilir:

- Yerel olarak etkileşimli modda Kurulum Sihirbazı'nı kullanarak
- Yerel olarak etkileşimsiz modda komut satırından
- Uzaktan Kaspersky Security Center yazılım paketini kullanarak (ayrıntılar için *Kaspersky Security Center Uygulama Kılavuzu*'na bakınız)
- Microsoft Windows'un Grup İlkesi Düzenleyicisi ile uzaktan (işletim sistemi yardım dosyalarına bakınız)

Kurulum Sihirbazını kullanarak uygulamayı kaldırma

Kurulum Sihirbazı'nı kullanarak Kaspersky Endpoint Security'yi kaldırmak için:

1. **Başlat** menüsünde, **Uygulamalar→ Kaspersky Endpoint Security 10 for Windows → Değiştir, Onar veya Kaldır**'ı seçin.

   Kurulum Sihirbazı başlatılır.

2. Kurulum Sihirbazı'nın **Uygulama Değiştir, Onar veya Kaldır** penceresinde, **Kaldır** düğmesine tıklayın.

3. Kurulum Sihirbazı talimatlarını uygulayın.

1. Adım. Gelecekte kullanmak üzere uygulama verilerini kaydetme

Bu adımda, uygulamanın sonraki yüklemesi sırasında (örneğin daha yeni bir sürüm yüklerken) ilerde kullanmak üzere tutmak istediğiniz uygulama tarafından kullanılan verileri belirleyebilirsiniz. Herhangi bir veri belirlemek istemiyorsanız uygulama tamamen kaldırılır.

Gelecekte kullanmak üzere uygulama verilerini saklamak için,

saklamak istediğiniz veri türlerinin yanındaki onay kutularını işaretleyin:

- **Etkinleştirme verisi** - gelecekte yükleyeceğiniz uygulamayı etkinleştirme ihtiyacını ortadan kaldıracak veridir. Yükleme zamanına kadar lisansın süresi sona ermedikçe mevcut lisans altında otomatik olarak etkinleştirilir.
- **Yedekleme dosyaları** uygulama tarafından taranan ve Yedekleme konumuna yerleştirilen dosyalardır.

  Uygulamanın kaldırılmasından sonra kaydedilen Yedekleme dosyalarına yalnızca söz konusu dosyaları kaydetmek için kullanılan uygulamanın aynı sürümünden erişilebilir.

  Uygulamanın kaldırılmasından sonra Yedekleme nesnelerini kullanmayı planlıyorsanız uygulamayı kaldırmadan önce söz konusu nesneleri depolama alanından geri yükleyin. Bununla birlikte Kaspersky uzmanları, bilgisayarınıza zarar verebileceği için Yedekleme konumundan nesnelerin geri yüklenmesini önermez.

- **Uygulamanın işletimsel ayarları** - uygulamanın yapılandırılması sırasında seçilen uygulama ayarlarının değerleridir.
- **Şifreleme anahtarlarının yedek depolama alanları** - uygulamanın kaldırılmasından önce şifrelenen dosyalara ve aygıtlara doğrudan erişimi sağlayan veridir. Uygulama, şifreleme işlevselliği ile yeniden yüklendikten sonra şifrelenmiş dosyalara ve sürücülere doğrudan erişilebilir.

  Varsayılan olarak, bu onay kutusu işaretlidir.

Kurulum Sihirbazına devam etmek için **İleri** düğmesine tıklayın. Kurulum Sihirbazını durdurmak için **İptal** düğmesine tıklayın.

2. Adım. Uygulama kaldırmayı onaylama

Uygulamayı kaldırmak bilgisayarınızın güvenliğini tehlikeye attığı için uygulamayı kaldırmak istediğinizi onaylamanız istenir. Bunu yapmak için **Kaldır** düğmesine tıklayın.

Herhangi bir zamanda uygulamanın kaldırılmasını durdurmak isterseniz bu işlemi, **İptal** düğmesine tıklayarak iptal edebilirsiniz.

3. Adım. Uygulamayı kaldırma. Kaldırmayı tamamlama

Bu adım sırasında Kurulum Sihirbazı uygulamayı bilgisayardan kaldırır. Uygulamayı kaldırma tamamlanana kadar bekleyin.

Uygulamayı kaldırırken işletim sisteminizi yeniden başlatmanız gerekebilir. Hemen yeniden başlatmamaya karar verirseniz uygulamayı kaldırma işleminin tamamlanması, işletim sistemi yeniden başlatılana kadar ya da bilgisayar kapatılıp daha sonra yeniden açılana kadar ertelenir.

Komut satırından uygulamayı kaldırma

Uygulama kaldırma işlemini komut satırından başlatabilirsiniz. Kaldırma işlemi etkileşimli veya sessiz modda (Uygulama Kurulum Sihirbazını başlatmadan) gerçekleştirilir.

Uygulama kaldırma işlemini etkileşimli modda başlatmak için,

komut satırında `setup.exe /x` veya `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275}` yazın.

Kurulum Sihirbazı başlatılır. Kurulum Sihirbazı talimatlarını uygulayın.

Uygulama kaldırma işlemini sessiz modda başlatmak için

komut satırında `setup.exe /s /x` veya `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} /qn` yazın.

Bu işlem uygulama kaldırma işlemini sessiz modda (Kurulum Sihirbazını başlatmadan) başlatır.

Uygulama kaldırma işlemi parola korumalı ise komut satırına kullanıcı adı ve ilgili parola girilmelidir.

Kaspersky Endpoint Security kaldırma, değiştirme veya onarma için kimlik doğrulama kullanıcı adı ve parolası belirlendiğinde uygulamayı komut satırından etkileşimli modda kaldırmak amacıyla:

Komut satırında `setup.exe /pKLLOGIN=<Kullanıcı adı> /pKLPASSWD=***** /x` veya

`msiexec.exe KLLOGIN=<Kullanıcı adı> KLPASSWD=***** /x {7911E943-32CC-45D0-A29C-56E6EF762275}` yazın.

Kurulum Sihirbazı başlatılır. Kurulum Sihirbazı talimatlarını uygulayın.

Kaspersky Endpoint Security kaldırma, değiştirme veya onarma için kimlik doğrulama kullanıcı adı ve parolası belirlendiğinde uygulamayı komut satırından sessiz modda kaldırmak amacıyla:

Komut satırında `setup.exe /pKLLOGIN=<Kullanıcı adı> /pKLPASSWD=***** /s /x` veya

`msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} KLLOGIN=<Kullanıcı adı> KLPASSWD=***** /qn` yazın.

Kimlik Doğrulama Aracısı'nın test çalışmasının ardından kalan nesneleri ve verileri kaldırma

Uygulamanın kaldırılması sırasında Kaspersky Endpoint Security, Kimlik Doğrulama Aracısı'nın test işleminden sonra sistem sabit sürücüsünde kalan nesneleri ve verileri tespit ederse uygulamanın kaldırılması işlemi yarıda kesilir ve bu nesneler ve veriler kaldırılana kadar uygulamanın kaldırılması imkansız hale gelir.

Nesneler ve veriler, yalnızca istisnai durumlarda Kimlik Doğrulama Aracısı'nın test işleminden sonra sistem sabit sürücüsünde kalabilir. Örneğin, şifreleme ayarları içeren bir Kaspersky Security Center ilkesi uygulandıktan sonra bilgisayar yeniden başlatılmadıysa veya Kimlik Doğrulama Aracısı'nın test işleminden sonra uygulama başarısız olursa bu durum görülebilir.

Kimlik Doğrulama Aracısı'nın test işleminden sonra sistem sabit sürücüsünde kalan nesneleri ve verileri iki şekilde kaldırabilirsiniz:

- Kaspersky Security Center ilkesini kullanarak.
- Geri Yükleme Yardımcı Programı'nı kullanarak.

Kimlik Doğrulama Aracısı'nın test işleminin ardından kalan nesneleri ve verileri kaldırmak amacıyla bir Kaspersky Security Center ilkesini kullanmak için:

1. Tüm bilgisayar sabit sürücülerinin şifresini çözmek için yapılandırılmış ayarlara sahip bir Kaspersky Security Center ilkesini bilgisayara uygulayın.
2. Kaspersky Endpoint Security'yi başlatın.

Kimlik Doğrulama Aracısı'nın test işleminin ardından kalan nesneleri ve verileri kaldırmak amacıyla bir Geri Yükleme Yardımcı Programı'nı kullanmak için:

1. Kimlik doğrulama aracısının test işleminden sonra nesnelerin ve verilerin üzerinde kaldığı sistem sabit sürücüsünün bağlı olduğu bilgisayarda Kaspersky Endpoint Security kullanılarak oluşturulan fdert.exe yürütülebilir dosyasını çalıştırarak Geri Yükleme Yardımcı Programı'nı başlatın.
2. Geri Yükleme Yardımcı Programı'nda **Aygıtı seçin** açılır listesinde kaldırılacak nesnelerin ve verilerin olduğu sistem sabit sürücüsünü seçin.

3. **Tara** düğmesine tıklayın.

4. **AA nesnelerini ve verilerini sil** düğmesine tıklayın.

   Kimlik Doğrulama Aracısı'nın test işleminin ardından kalan nesneleri ve verileri kaldırma işlemi başlatılır.

Kimlik Doğrulama Aracısı'nın test işleminin ardından kalan nesneleri ve verileri kaldırdıktan sonra, Kimlik Doğrulama Aracısı ile uygulama uyumsuzluğu hakkındaki bilgileri de kaldırmanız gerekebilir.

Kimlik Doğrulama Aracısı ile uygulama uyumsuzluğu hakkındaki bilgileri kaldırmak için,

komut satırına `avp pbatestreset` komutunu yazın.

`avp pbatestreset` komutunun yürütülmesi için şifreleme bileşenleri yüklenmelidir.

Uygulama arabirimi

Bu bölümde, uygulama arabiriminin temel öğeleri açıklanmaktadır.

Görev çubuğu bildirim alanındaki uygulama simgesi

Kaspersky Endpoint Security'nin yüklenmesinin hemen ardından uygulama simgesi, Microsoft Windows görev çubuğu bildirim alanında görülür.

Simge aşağıdaki amaçları karşılar:

- Uygulama etkinliğini belirtir.
- İçerik menüsü ve uygulamanın ana penceresi için kısayol oluşturur.

Uygulama etkinliğinin belirtilmesi

Uygulama simgesi, uygulama etkinliğinin göstergesidir:

-  koruma etkin simgesi, uygulamanın tüm koruma bileşenlerinin etkin olduğunu belirtir.
-  yeniden başlatma gerekiyor simgesi, Kaspersky Endpoint Security'nin çalışmasında dikkatinizi gerektiren önemli olayların gerçekleştiğini belirtir. Örneğin, Dosya Tehdidi Koruması bileşeni devre dışı bırakılmıştır ve uygulama veritabanları güncel değildir.
-  hata oluştu simgesi, Kaspersky Endpoint Security'nin çalışmasında kritik olayların gerçekleştiğini belirtir. Örneğin bir bileşenin çalışmasında hata oluşmuştur veya uygulama veritabanları bozuktur.

Uygulama simgesi içerik menüsü

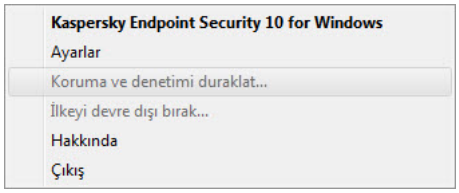
Uygulama simgesinin içerik menüsü aşağıdaki öğeleri içerir:

- **Kaspersky Endpoint Security for Windows**. Ana uygulama penceresi açılır. Bu pencerede, uygulama bileşenlerinin ve görevlerinin çalışmasını ayarlayabilir ve işlenen dosyaların ve tespit edilen tehditlerin istatistiklerini görüntüleyebilirsiniz.
- **Ayarlar**. **Ayarlar** penceresi açılır. **Ayarlar** sekmesi, varsayılan uygulama ayarlarını değiştirmenize olanak tanır.
- **Koruma ve denetimi duraklat** / **Koruma ve denetimi sürdür**. Koruma ve denetim bileşenlerinin çalışmasını geçici olarak duraklatır / sürdürür. Bu içerik menüsü, güncelleme görevi ve tarama görevlerini etkilemez, sadece Kaspersky Security Center ilkesi devre dışı olduğunda kullanılabilir.

  Kaspersky Security Network, Kaspersky Endpoint Security tarafından koruma ve denetim bileşenlerinin duraklatılmasından / sürdürülmesinden bağımsız olarak kullanılır.

- **İlkeyi devre dışı bırak** / **İlkeyi etkinleştir**. Kaspersky Security Center ilkesini devre dışı bırakır / etkinleştirir. Bu içerik menüsü, Kaspersky Endpoint Security'nin yüklü olduğu bir bilgisayara bir ilke uygulandığında ve Kaspersky Security Center ilkesini devre dışı bırakmak için bir parola belirlendiğinde kullanılabilir.

- **Hakkında**. Bu öğe, uygulama ayrıntılarını içeren bilgi penceresini açar.
- **Çıkış**. Bu öğe, Kaspersky Endpoint Security'den çıkar. Bu içerik menüsüne tıklandığında uygulama, bilgisayar RAM'inden karşıya yüklenir.



Uygulama simgesi içerik menüsü

İşaretçiyi Microsoft Windows'un görev çubuğu bildirim alanındaki uygulama simgesinin üstüne getirerek uygulama simgesinin içerik menüsünü açabilirsiniz.

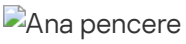
Ana uygulama penceresi

Kaspersky Endpoint Security'nin ana penceresi, uygulamanın ana işlevlerine erişim sağlayan arabirim öğelerini içerir.

Ana uygulama penceresi aşağıdaki öğeleri içerir:

- **Kaspersky Endpoint Security for Windows**'a bağlantı. Bu bağlantıya tıklandığında uygulama sürümü hakkında bilgi içeren **Hakkında** penceresi açılır.
- Yardım simgesi düğmesi. Bu düğmeye tıklandığında Kaspersky Endpoint Security yardım sistemi açılır.
- **Tehdit tespit etme teknolojileri** bölümü. Bölüm aşağıdaki bilgileri içerir:
  - Bölümün sol kısmında tehdit tespit etme teknolojileri listesi görüntülenir. Belli bir teknoloji kullanılarak tespit edilen tehdit sayısı, her tehdit tespit etme teknolojisinin adının sağ tarafında görüntülenir.
  - Etkin tehditlerin bulunup bulunmadığına bağlı olarak bölüm merkezinde aşağıdaki açıklama yazılarından biri görüntülenir:
    - **Tehdit yok**. Bu açıklama yazısı görüntülenirse **Tehdit tespit etme teknolojileri** bölümüne tıklandığında tehdit tespit etme teknolojilerinin kısa bir açıklamasının yanı sıra Kaspersky Security Network bulut hizmeti altyapısının durumunu ve küresel istatistiklerini gösteren **Tehdit tespit etme teknolojileri** penceresi açılır.
    - **N etkin tehdit**. Bu açıklama yazısı görüntülenirse **Tehdit tespit etme teknolojileri** bölümüne tıklandığında bazı nedenlerle işlenmemiş virüslü dosyalarla ilgili olaylar listesini görüntüleyen **Etkin Tehditler** penceresi açılır.
- **Koruma bileşenleri** bölümü. Bu bölüme tıklandığında **Koruma bileşenleri** penceresi açılır. Bu pencerede, yüklenen bileşenlerin çalışma durumunu görüntüleyebilirsiniz. Bu pencereden, **Ayarlar** penceresinde şifreleme bileşenleri dışında yüklenen bileşenlerin ayarlarını içeren bir alt bölüm de açabilirsiniz.
- **Görevler** bölümü. Bu bölüme tıklandığında **Görevler** penceresi açılır. Bu pencerede, uygulama modüllerini ve veritabanlarını güncellemek, virüsler ve diğer kötü amaçlı yazılımlara karşı dosyaları taramak ve bir bütünlük denetimi çalıştırmak için kullanılan Kaspersky Endpoint Security görevlerinin çalışmasını yönetebilirsiniz.
- **Raporlar** düğmesi. Bu düğmeye tıklandığında genel olarak uygulamanın veya ayrı bileşenlerinin çalışması ya da görevlerin gerçekleştirilmesi sırasında oluşan olaylarla ilgili bilgileri içeren **Raporlar** penceresi açılır.
- **Veri havuzları** düğmesi. Bu düğmeye tıklandığında **Yedekleme** penceresi açılır. Bu pencerede, uygulamanın sildiği virüslü dosyaların kopyalarının listesini görüntüleyebilirsiniz.

- **Destek** düğmesi. Bu düğmeye tıklandığında işletim sistemiyle ilgili bilgi, Kaspersky Endpoint Security'nin güncel sürümü ve Kaspersky bilgi kaynaklarının bağlantılarını içeren **Destek** penceresi açılır.
- **Ayarlar** düğmesi. Bu düğmeye tıklandığında uygulamanın varsayılan ayarlarını değiştirebileceğiniz **Ayarlar** penceresi açılır.
- / / düğmesi. Bu düğmeye tıklandığında mevcut güncellemeler ile şifreli dosyalara ve aygıtlara erişim talepleri hakkında bilgi içeren **Olaylar** penceresi açılır.
- **Lisans** bağlantısı. Bu bağlantıya tıklandığında geçerli lisans hakkında bilgi içeren **Lisanslama** penceresi açılır.


Ana pencere

Ana uygulama penceresi

Kaspersky Endpoint Security'nin ana penceresini açmak için aşağıdaki işlemlerden birini gerçekleştirin:

- Microsoft Windows görev çubuğu bildirim alanındaki uygulama simgesine tıklayın.
- Uygulama simgesinin içerik menüsünde **Kaspersky Endpoint Security for Windows** seçeneğini belirleyin.

Uygulama ayarları penceresi

Kaspersky Endpoint Security ayarları penceresi, genel uygulama ayarlarını, her bir bileşeni, raporları ve depolama alanlarını, tarama görevlerini, güncelleme görevlerini ve Kaspersky Security Network sunucularıyla iletişimi yapılandırmanıza olanak tanır.

Uygulama ayarları penceresi iki bölümden oluşur (aşağıdaki resme bakın):

- Sol kısım, uygulama bileşenleri, görevler ve çeşitli alt bölümlerden oluşan gelişmiş ayarlar bölümünü içerir.
- Sağ kısım, pencerenin sol kısmında seçilen görev veya bileşen ayarlarını yapılandırmak için kullanabileceğiniz denetim öğelerini ve gelişmiş ayarları içerir.


Ayarlar

Uygulama ayarları penceresi

Uygulama ayarları penceresini açmak için aşağıdaki eylemlerden birini gerçekleştirin:

- Ana uygulama penceresi'nde **Ayarlar** sekmesini seçin.
- Uygulama simgesi içerik menüsünde, **Ayarlar**'ı seçin.

Uygulama Koruma ve Denetim sekmesi

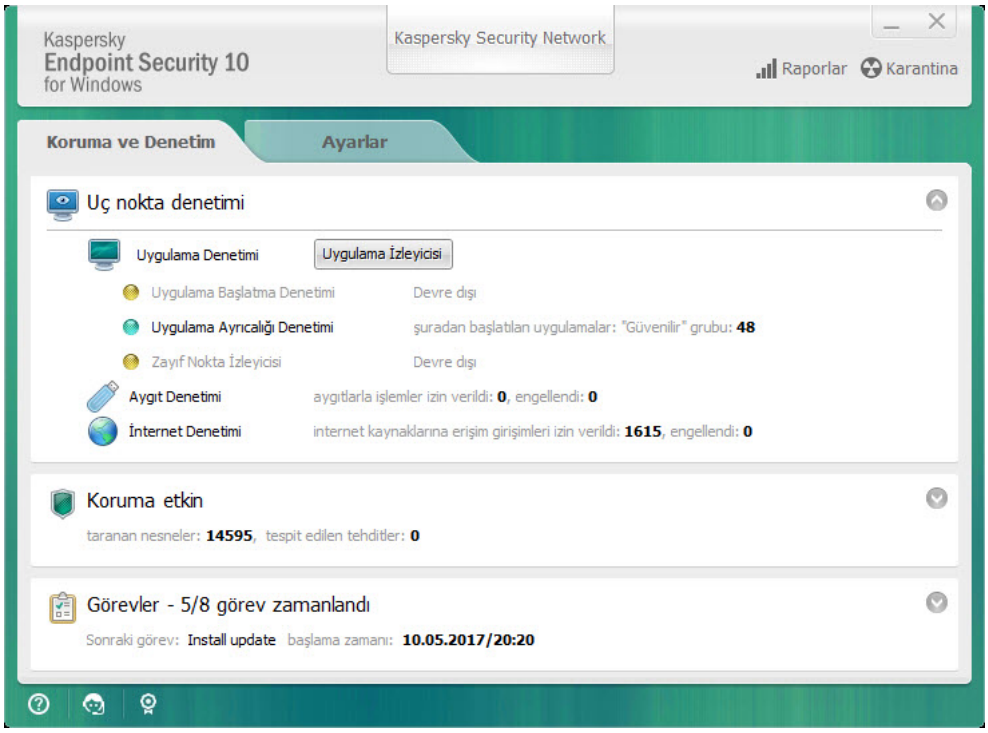
Kaspersky Endpoint Security'nin Koruma ve Denetim sekmesi tüm görevlerin performansı ve tüm uygulama bileşenlerinin çalışması hakkında genel bilgiler sağlamak için hazırlanmıştır. Bu sekmede ayrıca, bileşenlerin çalışmasını ve görevlerin gerçekleştirilmesini de düzenleyebilirsiniz.

Uygulama Koruma ve Denetim sekmesi üç bölümden oluşur (aşağıdaki resme bakınız):

- **Uç nokta denetimi** bölümü denetim bileşenlerinin bir listesini içerir.

- **Koruma yönetme** bölümü Anti-Virüs koruması bileşenlerinin bir listesini içerir.
- **Görevler** bölümü bilgisayarda çalışan yerel görevlerin bir listesini içerir.

Her bölüm, bir bileşenin çalışmasını etkinleştirmek veya devre dışı bırakmak, seçili bileşen veya görevin ayarlarına gitmek ve seçilen bileşen veya görevin işletim istatistiklerini görüntülemek için kullanabileceğiniz denetim öğelerini içerir.



Uygulama Koruma ve Denetim sekmesi

Uygulama Koruma ve Denetim sekmesini açmak için aşağıdaki eylemlerden birini gerçekleştirin:

- Ana uygulama penceresinde **Koruma ve Denetim** sekmesini seçin.
- Microsoft Windows görev çubuğu bildirim alanındaki uygulama simgesine tıklayın.
- Uygulama simgesinin içerik menüsünde **Kaspersky Endpoint Security 10 for Windows**'u seçin.

Uygulama lisanslama

Bu bölümde, uygulama lisanslama ile ilgili genel kavramlar hakkında bilgi sağlanmaktadır.

Son Kullanıcı Lisans Sözleşmesi Hakkında

Son Kullanıcı Lisans Sözleşmesi, sizinle AO Kaspersky Lab arasında uygulamanın kullanım koşullarını belirleyen bağlayıcı bir anlaşmadır.

Uygulamayı kullanmadan önce Lisans Sözleşmesi koşullarını dikkatlice okumanızı öneririz.

Lisans Sözleşmesi koşullarını aşağıdaki şekillerde görüntüleyebilirsiniz:

- Kaspersky Endpoint Security'yi etkileşimli modda yüklerken.
- license.txt dosyasını okuyarak. Bu belge, uygulama dağıtım kitinde yer almaktadır.

Uygulamayı yüklerken Son Kullanıcı Lisans Sözleşmesi'ne uymayı kabul ettiğinizi onaylayarak Son Kullanıcı Lisans Sözleşmesi koşullarını kabul ettiğinizi belirtir. Son Kullanıcı Lisans Sözleşmesi'nin koşullarını kabul etmiyorsanız kurulumu iptal etmelisiniz.

Lisans hakkında

Lisans, Son Kullanıcı Lisans Sözleşmesi ile verilen, uygulamayı kullanmak için zamanla sınırlı bir haktır.

Geçerli bir lisans, aşağıdaki hizmet türlerine hak kazandırır:

- Son Kullanıcı Lisans Sözleşmesi şartlarına uygun olarak uygulamayı kullanma
- Teknik Destek

Hizmet kapsamı ve uygulama kullanımı kapsamı, uygulamanın etkinleştirildiği lisans türüne bağlıdır.

Aşağıdaki lisans türleri sağlanmaktadır:

- *Deneme* – uygulamanın denenmesi için sağlanan ücretsiz lisanstır.

  Deneme lisansı genellikle kısa sürelidir. Deneme lisansının süresi sona erdiğinde tüm Kaspersky Endpoint Security özellikleri devre dışı bırakılır. Uygulamayı kullanmaya devam etmek için ticari lisans satın almanız gerekir.

  Uygulamayı deneme lisansı altında sadece bir kez etkinleştirebilirsiniz.

- *Ticari* – Kaspersky Endpoint Security'yi satın aldığınızda sağlanan ücretli lisanstır.

  Ticari lisans kapsamında mevcut olan uygulama işlevselliği ürün seçimine bağlıdır. Seçilen ürün Lisans Sertifikası'nda belirtilmiştir. Mevcut ürünler hakkında bilgiler Kaspersky web sitesinde bulunabilir.

  Ticari lisansın süresi dolduğunda, uygulamanın temel özellikleri devre dışı kalır. Uygulamayı kullanmaya devam etmek için ticari lisansınızı yenilemeniz gerekir. Lisansınızı yenilemeyi düşünmüyorsanız uygulamayı bilgisayarınızdan kaldırmalısınız.

Lisans sertifikası hakkında

Bir *lisans sertifikası* kullanıcıya bir anahtar dosyası veya etkinleştirme kodu ile birlikte iletilen bir dosyadır.

Lisans sertifikası aşağıdaki lisans bilgilerini içerir:

- Sipariş numarası
- Lisansın verildiği kullanıcının ayrıntıları
- Lisansı kullanarak etkinleştirilebilecek uygulamanın ayrıntıları
- Lisanslı birim sayısı hakkındaki kısıtlamalar (örnek olarak, lisans altında uygulamanın kullanılabileceği aygıt sayısı)
- Lisans dönemi başlangıç tarihi
- Lisans sona erme tarihi veya lisans dönemi
- Lisans türü

Abonelik hakkında

Kaspersky Endpoint Security aboneliği, belirli parametrelerle (aboneliğin sona erme tarihi, korunan aygıt sayısı) uygulamayı satın alma emridir. Hizmet sağlayıcınızdan (ISP'niz gibi) Kaspersky Endpoint Security için bir abonelik sipariş edebilirsiniz. Abonelik elle ya da otomatik olarak yenilenebilir veya aboneliğinizi iptal edebilirsiniz. Hizmet sağlayıcının İnternet sitesinde aboneliğinizi yönetebilirsiniz.

Abonelik sınırlı (örneğin bir yıllık) veya sınırsız (sona erme tarihi olmayan) olabilir. Sınırlı abonelik süresinin sona ermesinden sonra Kaspersky Endpoint Security'nin çalışmaya devam etmesi için aboneliğinizi yenilemeniz gereklidir. Satıcının hizmetleri için zamanında ödeme yapıldıysa sınırsız abonelik otomatik olarak yenilenir.

Sınırlı abonelik durumunda, kullanım süresi dolduktan sonra aboneliği yenilemek için ödemesiz bir süre sunulabilir, bu süre boyunca uygulama işlevini devam ettirecektir. Size ödemesiz bir süre verip vermeyeceğine ve verirse ödemesiz sürenin ne kadar olacağına hizmet sağlayıcı karar verir.

Kaspersky Endpoint Security'yi abonelik kapsamında kullanmak için hizmet sağlayıcıdan aldığınız etkinleştirme kodunu uygulamalısınız. Etkinleştirme kodu uygulandıktan sonra aktif anahtar yüklenir. Aktif anahtar, uygulamayı abonelik kapsamında kullanma lisansını tanımlar. Ek anahtar sadece etkinleştirme kodu kullanarak yüklenebilir ve bir anahtar dosyası kullanarak veya abonelikle yüklenemez.

Abonelik kapsamında sunulan uygulama işlevselliği, şu ticari lisans türlerinin uygulama işlevselliğine karşılık gelebilir: Standart, Kaspersky Business Space Security, Kaspersky Enterprise Space Security. Bu lisans türleri; dosya sunucuları, iş istasyonları ve mobil aygıtları korumak içindir ve iş istasyonları ve mobil aygıtlarda denetim bileşenlerinin kullanımını destekler.

Olası abonelik yönetimi seçenekleri, hizmet sağlayıcıya göre değişebilir. Hizmet sağlayıcı, aboneliği yenileme için uygulamanın işlevini devam ettireceği bir ödemesiz süre sunmayabilir.

Abonelik kapsamında satın alınan etkinleştirme kodları, Kaspersky Endpoint Security'nin önceki sürümlerini etkinleştirmek için kullanılamaz.

Etkinleştirme kodu hakkında

Etkinleştirme kodu, Kaspersky Endpoint Security'nin ticari lisansını satın alırken verilen yirmi benzersiz Latince harf ve sayı dizisinden oluşur.

Uygulamayı bir etkinleştirme kodu ile etkinleştirmek için Kaspersky etkinleştirme sunucularına bağlanırken İnternet erişimi gerekir.

Etkinleştirme kodunu kullanarak uygula etkinleştirildiğinde aktif anahtar yüklenir. Ek anahtar sadece etkinleştirme kodu kullanarak yüklenebilir ve bir anahtar dosyası kullanarak veya abonelikle yüklenemez.

Uygulamayı etkinleştirdikten sonra etkinleştirme kodu kaybedilirse etkinleştirme kodunu geri yükleyebilirsiniz. Örneğin Kaspersky CompanyAccount'u kaydetmek için bir etkinleştirme koduna ihtiyaç duyabilirsiniz. Etkinleştirme kodunu geri yüklemek için Kaspersky Teknik Destek ile irtibat kurmalısınız.

Anahtar hakkında

Anahtar benzersiz bir harf sayı dizisidir. Anahtar, Lisans Sertifikasında belirtilen koşullarda uygulamanın kullanımına imkan tanır (lisans türü, lisans geçerlilik süresi, lisans sınırlamaları).

Abonelik ile yüklenen bir anahtar için lisans sertifikası sağlanmaz.

Bir etkinleştirme kodu veya anahtar dosyası kullanarak uygulamaya bir anahtar eklenebilir.

Anahtarları ekleyebilir, düzenleyebilir veya silebilirsiniz. Son Kullanıcı Lisans Sözleşmesi ihlal edilirse anahtar engellenebilir. Anahtar kara listeye alındıysa uygulamayı kullanmaya devam etmek için farklı bir anahtar eklemeniz gerekir.

Süresi dolan bir anahtar silindiyse uygulama işlevi kullanılamaz. Silindikten sonra böyle bir anahtarı tekrar ekleyemezsiniz.

İki anahtar türü mevcuttur: etkin ve ek.

Aktif anahtar, uygulama tarafından kullanılmakta olan bir anahtardır. Aktif anahtar olarak bir deneme veya ticari lisans anahtarı eklenebilir. Uygulamanın birden fazla aktif anahtarı olamaz.

Ek anahtar, kullanıcıya uygulamayı kullanma hakkı verir ama şu anda kullanılmamaktadır. Aktif anahtarın süresi dolduğunda ek anahtar otomatik olarak etkinleşir. Sadece aktif anahtar kullanılabilir olduğunda ek anahtar eklenebilir.

Deneme lisansının anahtarı sadece aktif anahtar olarak eklenebilir. Ek anahtar olarak eklenemez. Deneme lisansı anahtarı, ticari lisansın aktif anahtarının yerini alamaz.

Anahtarın kara listeye alınması halinde uygulamanın etkinleştirildiği lisans ile tanımlanan uygulama işlevi sekiz gün etkin olmaya devam eder. Kaspersky Security Network ve veritabanı ve uygulama modülü güncellemeleri, kısıtlama olmadan kullanılabilir. Uygulama kullanıcıya anahtarın kara listeye alındığını bildirir. Sekiz günün ardından uygulama işlevi, lisans süresi dolduktan sonra kullanılabilir işlev düzeyiyle sınırlı hale gelir: uygulama güncellemeler olmadan çalışır ve Kaspersky Security Network kullanılamaz.

Anahtar dosyası hakkında

Anahtar dosyası, Kaspersky Endpoint Security'yi satın alırken Kaspersky tarafından verilen .key uzantılı bir dosyadır. Anahtar dosyasının amacı, uygulamayı etkinleştiren bir anahtar eklemektir.

Uygulamayı bir anahtar dosyası ile etkinleştirmek için Kaspersky etkinleştirme sunucularına bağlanmanız gerekmez.

Yanlışlıkla silindiyse anahtar dosyasını kurtarabilirsiniz. Örneğin Kaspersky CompanyAccount'u kaydetmek için bir anahtar dosyasına ihtiyaç duyabilirsiniz.

Anahtar dosyasını kurtarmak için aşağıdakilerden birini yapın:

- Lisans satıcısıyla iletişime geçin.
- Mevcut etkinleştirme kodunuza dayalı olarak Kaspersky web sitesinden bir anahtar dosyası edinin.

Veri sağlama hakkında

Kaspersky Endpoint Security'yi etkinleştirmek için etkinleştirme kodu uygulanırsa uygulamanın doğru kullanıldığını doğrulamak amacıyla aşağıdaki bilgileri düzenli bir şekilde otomatik olarak iletmeyi kabul etmiş olursunuz:

- Kaspersky Endpoint Security'nin türü, sürümü ve yerelleştirmesi
- Kaspersky Endpoint Security için yüklü güncellemelerin sürümleri
- Bilgisayarın kimliği ve bilgisayardaki özel Kaspersky Endpoint Security yüklemesinin kimliği
- Seri numarası ve aktif anahtar tanımlayıcısı
- İşletim sisteminin türü, sürümü ve bit hızı ile sanal ortamın adı (Kaspersky Endpoint Security sanal ortamda yüklüyse)
- Bilgiler iletildiğinde etkin olan Kaspersky Endpoint Security bileşenlerinin kimlikleri

Kaspersky, bu bilgileri Kaspersky yazılımının dağıtımı ve kullanımı hakkında istatistik oluşturmak için de kullanabilir.

Etkinleştirme kodu kullanarak yukarıda listelenen verileri otomatik olarak iletmeyi kabul edersiniz. Bu bilgiyi Kaspersky'ye iletmeyi kabul etmiyorsanız Kaspersky Endpoint Security ürününü etkinleştirmek için bir anahtar dosyası kullanabilirsiniz.

Son Kullanıcı Lisans Sözleşmesi'nin koşullarını kabul ederek aşağıdaki bilgileri otomatik olarak iletmeyi kabul edersiniz:

- Kaspersky Endpoint Security'i yükseltirken:
  - Kaspersky Endpoint Security sürümü

- Kaspersky Endpoint Security kimliği
- Aktif anahtar
- Yükseltme görevinin başlatılmasının benzersiz kimliği
- Kaspersky Endpoint Security yüklemesinin benzersiz kimliği

- Kaspersky Endpoint Security arabiriminden bağlantıları takip ederken:
  - Kaspersky Endpoint Security sürümü
  - İşletim sistemi sürümü
  - Kaspersky Endpoint Security'nin etkinleştirilme tarihi
  - Lisans bitiş tarihi
  - Anahtar oluşturma tarihi
  - Kaspersky Endpoint Security yükleme tarihi
  - Kaspersky Endpoint Security kimliği
  - İşletim sisteminde tespit edilen zayıf noktanın kimliği
  - Kaspersky Endpoint Security için yüklenen son güncellemenin kimliği
  - Tehdit içerdiği tespit edilen dosyanın karması ve Kaspersky sınıflandırmasına göre bu tehdidin adı
  - Kaspersky Endpoint Security etkinleştirme hatası kategorisi
  - Kaspersky Endpoint Security etkinleştirme hatası kodu
  - Anahtarın sona erme tarihine kadar gün sayısı
  - Anahtarın eklenmesinden bu yana geçen gün sayısı
  - Lisansın sona ermesinden bu yana geçen gün sayısı
  - Etkin lisansın uygulandığı bilgisayar sayısı
  - Aktif anahtar
  - Kaspersky Endpoint Security lisans süresi
  - Lisansın geçerli durumu
  - Etkin lisans türü
  - Uygulama türü
  - Yükseltme görevinin başlatılmasının benzersiz kimliği
  - Kaspersky Endpoint Security yüklemesinin benzersiz kimliği

- Bilgisayardaki benzersiz yazılım yükleme kimliği
- Kaspersky Endpoint Security arabirimi dili

Alınan bilgiler Kaspersky tarafından Kaspersky'nin ilgili yönetmeliklerine ve yasalara uygun olarak korunmaktadır.

Son Kullanıcı Lisans Sözleşmesi'ni kabul ettikten ve Kaspersky Security Network Statement'ı onayladıktan sonra uygulama kullanımıyla ilgili bilgileri nasıl aldığımız, işlediğimiz, depoladığımız ve imha ettiğimizle ilgili daha fazla bilgi için Son Kullanıcı Lisans Sözleşmesi'ni okuyun ve Kaspersky İnternet sitesini ziyaret edin. License.txt ve ksn_<language ID>.txt dosyaları Son Kullanıcı Lisans Sözleşmesi ile Kaspersky Security Network Statement metnini içerir ve uygulama dağıtım kitinde yer almaktadır.

Lisans bilgilerini görüntüleme

Bir lisans hakkındaki bilgileri görüntülemek için:

Ana uygulama penceresinin alt kısmındaki main_license / license_expired düğmesine tıklayın.

Lisans penceresi açılır. Bu pencerede lisans hakkında bilgiler görüntülenir (aşağıdaki resme bakın).

Lisanslama penceresi

Lisanslama penceresinde aşağıdaki bilgiler bulunur:

- **Anahtar durumu**. Bir bilgisayarda birden çok anahtar bulunabilir. İki anahtar türü mevcuttur: etkin ve ek. Uygulamanın birden fazla aktif anahtarı olamaz. Yalnızca aktif anahtarın süresi dolduysa veya component_malfunction düğmesini kullanarak aktif anahtarı sildiyseniz ek anahtar etkinleştirilebilir.
- **Anahtar**. *Anahtar*, bir etkinleştirme kodundan veya bir anahtar dosyasından oluşturulan benzersiz bir alfa sayısal dizidir.
- **Lisans türü**. Şu lisans türleri kullanılabilir: deneme ve ticari.
- **Uygulama adı**. Satın alınan Kaspersky ürününün tam adı.
- **İşlevsellik**. Lisansınız kapsamında kullanabileceğiniz uygulama özellikleri. Koruma, Güvenlik Denetimleri, Veri Şifreleme, Endpoint Sensor ve benzer diğer özellikler bulunur. Kullanılabilir özelliklerin listesini Lisans Sertifikasında da görebilirsiniz.
- **Lisans hakkındaki ek bilgiler**. Lisans türü, bu lisans kapsamındaki bilgisayar sayısı, lisans başlangıç tarihi ile sona erme tarihi ve saati (yalnızca aktif anahtar için).

  Lisansın sona erme zamanı, işletim sisteminde yapılandırılmış olan saat dilimine göre görüntülenir.

Lisanslama penceresinde aşağıdakilerden birini de yapabilirsiniz:

- **Lisans satın al** / **Lisansı yenile**. Lisans satın alabileceğiniz veya yenileyebileceğiniz Kaspersky çevrimiçi mağazasının internet sitesini açar. Bunun için lütfen şirket bilgilerinizi girin ve siparişinizin ödemesini yapın.
- **Uygulamayı yeni bir lisans altında etkinleştir**. Uygulama Etkinleştirme Sihirbazını başlatır. Bu sihirbazda bir etkinleştirme kodu veya anahtar dosyası kullanarak bir anahtar ekleyebilirsiniz. Uygulama Etkinleştirme Sihirbazı,

bir aktif anahtar ve yalnızca bir adet ek anahtar eklemenize izin verir.

Lisans satın alma

Uygulamayı yükledikten sonra bir lisans satın alabilirsiniz. Lisansı satın aldıktan sonra uygulamayı etkinleştirmek için bir etkinleştirme kodu veya anahtar dosyası alırsınız.

Bir lisans satın almak için:

1. Ana uygulama penceresinde  /  düğmesine tıklayın.

   Lisans penceresi açılır.

2. **Lisans** penceresinde aşağıdakilerden birini yapın:

   - Herhangi bir anahtar eklenmediyse veya deneme lisansı anahtarı eklendiyse **Lisans satın al** düğmesine tıklayın.
   - Ticari lisans anahtarı eklenirse, **Lisansı yenile** düğmesine tıklayın.

   Lisans satın alabileceğiniz Kaspersky çevrimiçi mağazasının web sitesinin bulunduğu bir pencere açılır.

Lisansı yenileme

Lisansınız sona erme tarihine yaklaştığında lisansınızı yenileyebilirsiniz. Bu sayede geçerli lisansın sona ermesinin ardından ve yeni bir lisansla uygulamayı etkinleştirene kadar bilgisayarınız korunmaya devam eder.

Lisansı yenilemek için:

1. Yeni bir uygulama etkinleştirme kodu veya anahtar dosyası alın.
2. Aldığınız etkinleştirme kodu veya anahtar dosyası ile ek anahtar ekleyin.

   Sonuç olarak ek anahtar eklenir. Lisans sona erdiğinde etkin olur.

Kaspersky'nin etkinleştirme sunucularındaki yük dağılımından dolayı anahtarın ek yerine etkin olarak güncellenmesi biraz zaman alabilir.

Aboneliği yenileme

Uygulamayı abonelikle kullandığınızda Kaspersky Endpoint Security, aboneliğinizin süresi dolana kadar etkinleştirme sunucu ile belirli aralıklarla otomatik iletişim kurar.

Uygulamayı sınırsız abonelikle kullanırsanız Kaspersky Endpoint Security, etkinleştirme sunucusundaki yenilenen anahtarları arka plan modunda otomatik olarak denetler. Etkinleştirme sunucusunda bir anahtar etkinse uygulama, önceki anahtarı değiştirerek bunu ekler. Bu şekilde Kaspersky Endpoint Security'nin sınırsız aboneliği kullanıcı müdahalesi olmadan yenilenir.

Uygulamayı sınırlı abonelikle kullanırsanız abonelik (veya abonelik yenilemenin kullanılabilir olduğu aboneliğin sona erme ermesinden sonraki ödemesiz süre) sona erdiğinde Kaspersky Endpoint Security, ilgili bildirimi görüntüler ve aboneliği otomatik olarak yenilemeye çalışmayı bırakır. Bu durumda Kaspersky Endpoint Security, uygulamanın ticari lisansının sona erdiği durumdaki gibi davranır: uygulama güncellemeler olmadan çalışır ve Kaspersky Security Network kullanılamaz.

Hizmet sağlayıcının İnternet sitesinde aboneliği yenileyebilirsiniz.

Lisanslama penceresinde abonelik durumunu el ile güncelleyebilirsiniz. Ödemesiz süre sona erdikten sonra ve uygulama abonelik durumunu otomatik olarak güncellemediği zaman abonelik yenilenmediyse bu gerekebilir.

Hizmet sağlayıcının web sitesini ziyaret etme

Uygulama arabiriminden hizmet sağlayıcının İnternet sitesini ziyaret etmek için:

1. Ana uygulama penceresinde main_license / license_expired düğmesine tıklayın.

   Lisans penceresi açılır.

2. **Lisans** penceresinde, **Lisans sağlayıcınıza başvurun**'a tıklayın.

Uygulama etkinleştirme yöntemleri hakkında

Etkinleştirme, lisans sona erene kadar uygulamanın tamamen işlevsel sürümünü kullanmanıza imkan tanıyan lisans etkinleştirme işlemidir. Uygulama etkinleştirme işlemi bir anahtar eklenmesini içerir.

Uygulamayı aşağıdaki yollardan biriyle etkinleştirebilirsiniz:

- İlk Yapılandırma Sihirbazını kullanarak uygulamayı yüklerken. Aktif anahtarı bu şekilde ekleyebilirsiniz.
- Yerel olarak uygulama arabiriminden Etkinleştirme Sihirbazı'nı kullanarak. Hem aktif anahtarı hem de ek anahtarı bu şekilde ekleyebilirsiniz.
- Uzaktan Kaspersky Security Center yazılım paketiyle bir anahtar ekleme görevi oluşturarak ve ardından başlatarak. Hem aktif anahtarı hem de ek anahtarı bu şekilde ekleyebilirsiniz.
- Kaspersky Security Center Yönetim Sunucusu anahtar deposunda saklanan anahtarları ve etkinleştirme kodlarını istemci bilgisayarlarına uzaktan dağıtarak (bu konu hakkında daha fazla bilgi için Kaspersky Security Center Yardım içeriğine bakın). Hem aktif anahtarı hem de ek anahtarı bu şekilde ekleyebilirsiniz.

  Abonelikle satın alınan etkinleştirme kodu ilk seferde dağıtılır.

- Komut satırını kullanarak.

Kaspersky'nin etkinleştirme sunucularında yük dağılımından dolayı uygulamanın bir etkinleştirme koduyla etkinleştirilmesi (uzaktan veya etkileşimsiz yükleme sırasında) biraz zaman alabilir. Uygulamayı hemen etkinleştirmek isterseniz devam eden etkinleştirme işlemini yarıda kesebilir ve Etkinleştirme Sihirbazı ile etkinleştirmeyi başlatabilirsiniz.

Uygulamayı etkinleştirmek için Etkinleştirme Sihirbazını kullanma

Etkinleştirme Sihirbazı'nı kullanarak Kaspersky Endpoint Security'yi etkinleştirmek için:

1. Ana uygulama penceresinin alt kısmındaki main_license / license_expired düğmesine tıklayın.
   Lisans penceresi açılır.
2. **Lisans** penceresinde, **Uygulamayı yeni bir lisans altında etkinleştir** düğmesine tıklayın.
   Uygulama Etkinleştirme Sihirbazı başlatılır.
3. Etkinleştirme Sihirbazı talimatlarını uygulayın.

Uygulama etkinleştirme prosedürüyle ilgili daha fazla bilgi için İlk Yapılandırma Sihirbazını açıklayan bölüme bakın.

Komut satırından uygulamayı etkinleştirme

Komut satırından uygulamayı etkinleştirmek için,

komut satırına `avp.com license /add <etkinleştirme kodu veya anahtar dosyası> /password= <parola>` yazın.

Uygulamayı başlatma ve durdurma

Bu bölümde, uygulamanın otomatik başlatılmasının nasıl yapılandırıldığı, uygulamanın elle nasıl başlatılıp durdurulduğu ve koruma ve denetim bileşenlerinin nasıl duraklatılıp sürdürüldüğü açıklanmaktadır.

Uygulamanın otomatik başlatılmasını etkinleştirme ve devre dışı bırakma

Otomatik başlatma, Kaspersky Endpoint Security'nin işletim sistemi başlatıldıktan hemen sonra kullanıcı müdahalesi olmadan başlatıldığı anlamına gelir. Bu uygulama başlatma seçeneği varsayılan olarak etkindir.

Yüklemenin ardından Kaspersky Endpoint Security ilk kez otomatik olarak başlatılır. Ardından işletim sisteminin her başlatılmasından sonra uygulama otomatik olarak başlatılır.

İşletim sistemi başlatıldıktan sonra Kaspersky Endpoint Security anti-virüs veritabanlarının indirilmesi, bilgisayarın özelliğine bağlı olarak iki dakika kadar sürebilir. Bu sürede bilgisayarı koruma düzeyi azalır. Zaten yüklenmiş işletim sisteminde Kaspersky Endpoint Security başlatıldığında anti-virüs veritabanlarının indirilmesi, bilgisayar koruma düzeyinde azalmaya neden olmaz.

Uygulamanın otomatik başlatılmasını etkinleştirmek veya devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Soldaki **Virüse karşı koruma** bölümünü seçin.

   Virüse karşı koruma ayarları, pencerenin sağında görüntülenir.
3. Aşağıdakilerden birini yapın:
   - Uygulamanın otomatik çalıştırılmasını etkinleştirmek istiyorsanız **Bilgisayar başlatılırken Kaspersky Endpoint Security 10 for Windows'u başlat** onay kutusunu işaretleyin.
   - Uygulamanın otomatik çalıştırılmasını devre dışı bırakmak istiyorsanız **Bilgisayar başlatılırken Kaspersky Endpoint Security 10 for Windows'u başlat** onay kutusunu işaretlemeyin.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Uygulamayı elle başlatma ve durdurma

Kaspersky uzmanları Kaspersky Endpoint Security'nin elle durdurulmasını önermez çünkü bu, bilgisayarınız ve kişisel veriniz açısından tehdit oluşturur. Gerekirse uygulamayı durdurmadan bilgisayar korumasını ihtiyacınız olduğu kadar duraklatabilirsiniz.

Uygulamanın otomatik başlatılmasını daha önce devre dışı bıraktıysanız Kaspersky Endpoint Security'nin elle başlatılması gerekir.

Uygulamayı elle başlatmak için,

Başlangıç menüsünde, **Uygulamalar** → **Kaspersky Endpoint Security for Windows** seçeneğini belirleyin.

Uygulamayı elle durdurmak için:

1. Sağ tıklayarak görev çubuğu bildirim alanındaki uygulama simgesinin içerik menüsünü açın.
2. İçerik menüsünde **Çıkış**'ı seçin.

Bilgisayar korumasını ve denetimini duraklatma ve sürdürme

Bilgisayar koruması ve denetimi duraklatıldığında, Kaspersky Endpoint Security'nin tüm koruma ve denetim bileşenleri bir süre devre dışı bırakılır.

Görev çubuğu bildirim alanındaki uygulama simgesi kullanılarak uygulama durumu görüntülenir.

- hata oluştu simgesi, bilgisayar koruması ve denetiminin duraklatıldığı anlamına gelir.
- koruma etkin simgesi, bilgisayar koruması ve denetiminin devre dışı bırakıldığı anlamına gelir.

Bilgisayar koruması ve denetiminin duraklatılması veya sürdürülmesi, tarama veya güncelleme görevlerini etkilemez.

Bilgisayar koruması ve denetimini duraklattığınızda veya sürdürdüğünüzde herhangi bir ağ bağlantısı zaten kurulursa bu ağ bağlantılarının sonlandırılmasıyla ilgili bir bildirim görüntülenir.

Bilgisayar koruması ve denetimini duraklatmak için:

1. Sağ tıklayarak görev çubuğu bildirim alanındaki uygulama simgesinin içerik menüsünü açın.
2. İçerik menüsünde **Koruma ve denetimi duraklat**'ı seçin.

   Korumayı duraklat penceresi açılır.
3. Aşağıdaki seçeneklerden birini seçin:
   - **Belirtilen süreyle duraklat** - Aşağıdaki açılır listede belirtilen sürenin ardından bilgisayar koruması ve denetimi devam eder.
   - **Yeniden başlatmaya kadar duraklat**- Uygulamadan çıkıp yeniden açtığınızda veya işletim sistemini yeniden başlattıktan sonra bilgisayar koruması ve denetimi devam eder. Bu seçeneği kullanmak için uygulamanın otomatik başlatılması etkin olmalıdır.
   - **Duraklat** - Yeniden etkinleştirmeye karar verdiğinizde bilgisayar koruması ve denetimi devam eder.
4. **Belirtilen süreyle duraklat** seçeneğini önceki adımda seçtiyseniz, açılır listeden gereken aralığı seçin.

Bilgisayar koruması ve denetimini sürdürmek için:

1. Sağ tıklayarak görev çubuğu bildirim alanındaki uygulama simgesinin içerik menüsünü açın.
2. İçerik menüsünde **Koruma ve denetimi sürdür**'ü seçin.

Daha önce seçtiğiniz bilgisayar koruması ve denetimini duraklatma seçeneği ne olursa olsun bilgisayar koruması ve denetimini istediğiniz zaman sürdürebilirsiniz.

Bilgisayarın dosya sistemini koruma. Dosya Koruması

Bu bölümde, Dosya Koruması hakkında bilgiler ve bileşen ayarlarının yapılandırılmasına ilişkin talimatlar bulunmaktadır.

Dosya Koruması Hakkında

Dosya Koruması, bilgisayarın dosya sistemine virüs bulaşmasını önler. Varsayılan olarak Dosya Koruması, Kaspersky Endpoint Security ile birlikte çalışır, bilgisayar belleğinde sürekli olarak etkin kalır ve bilgisayarda ve tüm bağlanan sürücülerde açılan, kaydedilen veya başlatılan tüm dosyalarda ve takılan tüm sürücülerde virüs ve başka tehditler olup olmadığını tarar.

Dosyada bir tehdit tespit edildiğinde Kaspersky Endpoint Security aşağıdakileri gerçekleştirir:

1. Dosyada tespit edilen nesne türünü algılar (*virüs* veya *Truva atı* gibi).
2. Taramada, dosyada virüs olup olmadığı tespit edilemezse dosyayı *büyük olasılıkla virüslü* olarak etiketler. Dosya, tipik olarak virüsler veya diğer zararlı yazılımlarda görülen bir kod dizisi veya bilinen bir virüsün değiştirilmiş kodunu içerebilir.
3. Uygulama, dosyada tespit edilen kötü amaçlı nesne hakkında bir bildirim görüntüler ve Dosya Koruması ayarlarında belirtilen eylemi gerçekleştirerek dosyayı işler.

Dosya Tehdidi Koruması'nı etkinleştirme ve devre dışı bırakma

Varsayılan olarak, Dosya Tehdidi Koruması bileşeni etkinleştirilmiştir ve Kaspersky uzmanları tarafından önerilen modda çalışır. Gerekirse Dosya Tehdidi Koruması'nı devre dışı bırakabilirsiniz.

Dosya Tehdidi Koruması'nı etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresinde **Ayarlar** düğmesine tıklayın.
2. Pencerenin sol kısmında, **Temel Tehdit Koruması** bölümünde, **Dosya Tehdidi Koruması** seçeneğini belirleyin.

   Dosya Tehdidi Koruması bileşeninin ayarları pencerenin sağ kısmında görüntülenir.
3. Aşağıdakilerden birini yapın:
   - Dosya Tehdidi Korumasını etkinleştirmek istiyorsanız **Dosya Tehdidi Koruması** onay kutusunu işaretleyin.
   - Dosya Tehdidi Korumasını devre dışı bırakmak istiyorsanız **Dosya Tehdidi Koruması** onay kutusunun işaretini kaldırın.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Dosya Tehdidi Koruması'nı otomatik olarak duraklatma

Dosya Tehdidi Koruması'nı belirli bir zamanda veya belirli uygulamalarla çalışırken otomatik olarak duraklatılacak şekilde yapılandırabilirsiniz.

Dosya Tehdidi Koruması, yalnızca bazı uygulamalarla çakıştığında son çare olarak duraklatılmalıdır. Bir bileşenin çalışması sırasında herhangi bir çakışma oluşması durumunda Kaspersky Teknik Destek (https://companyaccount.kaspersky.com) birimi ile irtibat kurmanızı öneririz. Destek uzmanları, Dosya Tehdidi Koruması bileşenini bilgisayarınızdaki diğer programlarla eşzamanlı olarak çalışacak şekilde ayarlamanıza yardımcı olacaktır.

Dosya Tehdidi Koruması'nın otomatik olarak duraklatılmasını yapılandırmak için:

1. Ana uygulama penceresinde **Ayarlar** düğmesine tıklayın.
2. Pencerenin sol kısmında, **Temel Tehdit Koruması** bölümünde, **Dosya Tehdidi Koruması** seçeneğini belirleyin.

   Dosya Tehdidi Koruması bileşeninin ayarları pencerenin sağ kısmında görüntülenir.
3. **Güvenlik düzeyi** bölümünde, **Ayarlar** düğmesine tıklayın.

   Dosya Tehdidi Koruması penceresi açılır.
4. **Dosya Tehdidi Koruması** penceresinde, **Diğer** sekmesini seçin.
5. **Görevi duraklat** bölümünde:

   - Dosya Tehdidi Koruması'nı belirli bir zamanda otomatik olarak duraklatmayı yapılandırmak isterseniz **Zamanlamaya göre** onay kutusunu işaretleyin ve **Zamanlama** düğmesine tıklayın.

     Görevi duraklat penceresi açılır.
   - Belirtilen uygulamalar başlatıldığında Dosya Tehdidi Koruması'nın otomatik olarak duraklatılmasını yapılandırmak isterseniz **Uygulama başlatıldığında** onay kutusunu işaretleyin ve **Seç** düğmesine tıklayın.

     Uygulamalar penceresi açılır.
6. Aşağıdakilerden birini yapın:

   - Belirli bir zamanda Dosya Tehdidi Koruması'nın otomatik olarak duraklatılmasını yapılandırmak isterseniz **Görevi duraklat** penceresinde, Dosya Tehdidi Koruması'nın duraklatılacağı zaman dilimini (SS:DD biçiminde) belirtmek için **Görevi duraklatma zamanı** ve **Göreve devam etme zamanı** alanlarını kullanın. **Tamam**'a tıklayın.
   - Belirtilen uygulamalar başlatılırken Dosya Tehdidi Koruması'nın otomatik olarak duraklatılmasını yapılandırıyorsanız çalışması sırasında Dosya Tehdidi Koruması'nın duraklatılacağı uygulamaların listesini oluşturmak için **Uygulamalar** penceresinde **Ekle**, **Düzenle** ve **Kaldır** düğmelerini kullanın. **Tamam**'a tıklayın.
7. **Dosya Tehdidi Koruması** penceresinde **Tamam**'a tıklayın.
8. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Dosya Koruması'nı Yapılandırma

Dosya Koruması'nı yapılandırmak için aşağıdakileri uygulayabilirsiniz:

- Güvenlik düzeyini değiştirebilirsiniz.

  Ön tanımlı güvenlik düzeylerinden birini seçebilir veya güvenlik düzeyi ayarlarını elle yapılandırabilirsiniz. Güvenlik düzeyi ayarlarını değiştirirseniz önerilen güvenlik düzeyi ayarlarına her zaman geri dönebilirsiniz.

- Virüslü dosya tespit edildiğinde Dosya Koruması tarafından gerçekleştirilen eylemi değiştirebilirsiniz.
- Dosya Koruması'nın koruma kapsamını düzenleyebilirsiniz.

  Tarama nesneleri ekleyerek veya çıkararak ya da taranacak dosya türünü değiştirerek koruma kapsamını genişletebilir veya sınırlayabilirsiniz.
- Sezgisel Analiz'i yapılandırabilirsiniz.

  Dosya Koruması, imza analizi adı verilen bir teknik kullanır. İmza Analizi sırasında Dosya Koruması, tespit edilen nesneyi uygulamanın anti-virüs veritabanlarındaki kayıtlarla eşleştirir. Kaspersky uzmanlarının önerilerine uygun olarak imza analizi her zaman etkindir.

  Koruma etkinliğini artırmak için sezgisel analizi kullanabilirsiniz. Sezgisel analiz sırasında Dosya Koruması, işletim sistemindeki nesnelerin etkinliğini analiz eder. Sezgisel analiz, uygulamanın anti-virüs veritabanlarında bunlarla ilgili herhangi bir kayıt bulunmayan kötü amaçlı nesnelerin tespitine olanak tanır.
- Taramayı optimize edebilirsiniz.

  Dosya Koruması tarafından gerçekleştirilen dosya taramasını optimize ederek, tarama süresini kısaltabilir ve Kaspersky Endpoint Security'nin çalışma hızını arttırabilirsiniz. Sadece yeni dosyaları tarayarak ve önceki taramadan bu yana değiştirilmiş dosyaları tarayarak bunu sağlayabilirsiniz. Bu mod hem basit hem bileşik dosyalara uygulanır.

  En son taramadan bu yana değiştirilmeyen dosyaları kapsam dışında tutarak dosya tarama hızını optimize eden iChecker ve iSwift teknolojilerinin kullanımını da etkinleştirebilirsiniz.
- Bileşik dosyaların taranmasını yapılandırabilirsiniz.
- Dosya tarama modunu değiştirebilirsiniz.

Güvenlik düzeyini değiştirme

Bilgisayarın dosya sistemini korumak için Dosya Tehdidi Koruması bileşeni çeşitli ayar gruplarını uygular. Bu ayar gruplarına *güvenlik düzeyleri* denir. Üç adet ön tanımlı güvenlik düzeyi vardır: **Yüksek**, **Önerilen** ve **Düşük**. **Önerilen** güvenlik düzeyi ayarları Kaspersky uzmanları tarafından tavsiye edilen en iyi ayarlar olarak değerlendirilir.

Güvenlik düzeyini değiştirmek için:

1. Ana uygulama penceresinde **Ayarlar** düğmesine tıklayın.
2. Pencerenin sol kısmında, **Temel Tehdit Koruması** bölümünde, **Dosya Tehdidi Koruması** seçeneğini belirleyin.

   Dosya Tehdidi Koruması bileşeninin ayarları pencerenin sağ kısmında görüntülenir.
3. **Güvenlik düzeyi** bölümünde aşağıdakilerden birini yapın:

   - Ön tanımlı güvenlik düzeylerinden birini ayarlamak isterseniz (**Yüksek**, **Önerilen**, veya **Düşük**), kaydırma çubuğuyla seçin.
   - Özel bir güvenlik düzeyi yapılandırmak isterseniz **Ayarlar** düğmesine tıklayın ve açılan **Dosya Tehdidi Koruması** penceresinde özel ayarlarınızı girin.

     Özel bir güvenlik düzeyi yapılandırdıktan sonra **Güvenlik düzeyi** bölümündeki güvenlik düzeyinin adı **Özel** olarak değişir.
   - Güvenlik düzeyini **Önerilen** olarak değiştirmek için **Varsayılan olarak** düğmesine tıklayın.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Virüslü dosyalara uygulanacak Dosya Koruması eylemini değiştirme

Virüslü dosyalara uygulanacak Dosya Koruması eylemini değiştirmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Dosya Koruması** alt bölümünü seçin.
   Pencerenin sağ kısmında, Dosya Koruması bileşeninin ayarları görüntülenir.
3. **Tehdit algılandığında uygulanacak eylem** bölümünde gereken seçeneği seçin:
   - **Eylemi otomatik olarak seç**.
   - **Eylemi gerçekleştir: Temizle. Temizleme başarısız olursa sil**.
   - **Eylemi gerçekleştir: Temizle**.

     Bu seçenek seçilse bile Kaspersky Endpoint Security, Windows Store uygulamasının parçası olan dosyalara **Kaldır** eylemini uygular.
   - **Eylemi gerçekleştir: Kaldır**.
   - **Eylemi gerçekleştir: Engelle**.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Dosya Koruması'nın koruma kapsamını düzenleme

Koruma kapsamı, etkinleştirildiği zaman bileşenin taradığı nesneleri ifade eder. Farklı bileşenlerin koruma kapsamları farklı özelliklere sahiptir. Taranacak dosyaların konumu ve türü, Dosya Koruması'nın koruma kapsamının özellikleridir. Varsayılan olarak Dosya Koruması sadece sabit sürücüler, ağ sürücüleri veya çıkarılabilir ortama kaydedilen virüs bulaşabilecek dosyaları tarar.

Koruma kapsamını oluşturmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Dosya Koruması** alt bölümünü seçin.
   Pencerenin sağ kısmında, Dosya Koruması bileşeninin ayarları görüntülenir.
3. **Güvenlik düzeyi** bölümünde, **Ayarlar** düğmesine tıklayın.
   Dosya Koruması penceresi açılır.
4. **Dosya Koruması** penceresinde, **Genel** sekmesini seçin.
5. **Dosya Türleri** bölümünde, Dosya Koruması'nın taramasını istediğiniz dosya türlerini belirtin:

- Tüm dosyaları taramak istiyorsanız **Tüm dosyalar**'ı seçin.
- Virüs bulaşmasına en hassas biçimdeki dosyaları taramak istiyorsanız **Biçime göre taranan dosyalar**'ı seçin.
- Virüs bulaşmasına en hassas uzantılara sahip dosyaları taramak istiyorsanız **Uzantısına göre taranan dosyalar**'ı seçin.

Taranacak dosya türünü seçerken aşağıdaki bilgileri unutmayın:

- Kötü amaçlı kod içerme ve sonradan etkinleştirme olasılığı oldukça düşük olan bazı dosya biçimleri (.txt gibi) bulunmaktadır. Aynı zamanda yürütülebilir kod içeren veya içerebilecek dosya biçimleri de (.exe, .dll ve .doc gibi) bulunmaktadır. Bu tür dosyaların kötü amaçlı kod içerme ve etkinleştirme riski oldukça yüksektir.
- Bir saldırgan .txt uzantılı olarak yeniden adlandırılmış yürütülebilir bir dosya şeklinde bir virüs veya kötü amaçlı programı bilgisayarınıza gönderebilir. Dosyaların uzantıya göre taranmasını seçerseniz, bu dosya taramada atlanır. Biçime göre dosyaların taranmasını seçerseniz, uzantı ne olursa olsun Dosya Koruması dosya başlığını analiz eder. Bu analizde dosya .exe biçiminde görülebilir. Bu dosyada virüs ve diğer zararlı yazılımlar kapsamlı bir şekilde taranır.

6. **Koruma kapsamı** listesinde aşağıdakilerden birini yapın:
   - Tarama kapsamına yeni bir nesne eklemek isterseniz **Ekle** düğmesine tıklayın.
   - Bir nesnenin konumunu değiştirmek isterseniz, tarama kapsamından nesneyi seçin ve **Düzenle** düğmesine tıklayın.

   Tarama kapsamını seç penceresi açılır.
   - Bir nesneyi taranacak nesneler listesinden kaldırmak isterseniz taranacak nesneler listesinden seçin ve **Kaldır** düğmesine tıklayın.

     Silmeyi onaylama penceresi açılır.
7. Aşağıdakilerden birini yapın:
   - Yeni bir nesne eklemek veya taranacak nesneler listesinden bir nesnenin konumunu değiştirmek isterseniz, **Tarama kapsamını seç** penceresinde nesneyi seçin ve **Ekle** düğmesine tıklayın.

     Tarama kapsamını seç penceresinde seçilen tüm nesneler **Koruma kapsamı** listesinde **Dosya Koruması** listesinde görüntülenir.

     Tamam'a tıklayın.
   - Bir nesneyi kaldırmak istiyorsanız, kaldırmayı onaylama penceresinde **Evet** düğmesine tıklayın.
8. Gerekirse taranacak nesneler listesine nesne eklemek, taşımak veya kaldırmak için 6-7. adımları tekrarlayın.
9. Bir nesneyi taranacak nesneler listesi dışında tutmak için **Koruma kapsamı** listesindeki nesnenin karşısındaki onay kutusunun işaretini kaldırın. Ancak Dosya Koruması tarafından tarama dışında tutulsa da nesne taranacak nesneler listesinde kalır.
10. **Dosya Koruması** penceresinde **Tamam**'a tıklayın.
11. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Dosya Koruması ile Sezgisel Analiz'i Kullanma

Dosya Koruması'nın çalışmasında Sezgisel Analiz'in kullanımını yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Dosya Koruması** alt bölümünü seçin.

   Pencerenin sağ kısmında, Dosya Koruması bileşeninin ayarları görüntülenir.
3. **Güvenlik düzeyi** bölümünde, **Ayarlar** düğmesine tıklayın.

   Dosya Koruması penceresi açılır.
4. **Dosya Koruması** penceresinde, **Performans** sekmesini seçin.
5. **Tarama yöntemleri** bölümünde:
   - Dosya Koruması'nın sezgisel analizi kullanmasını isterseniz **Sezgisel Analiz** onay kutusunu seçin ve kaydırıcıyı kullanarak sezgisel analiz düzeyini belirleyin: **Hızlı tarama**, **Normal tarama** veya **Ayrıntılı tarama**.
   - Dosya Koruması'nın sezgisel analizi kullanmasını istemiyorsanız **Sezgisel Analiz** onay kutusunu işaretlemeyin.
6. **Tamam**'a tıklayın.
7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Dosya Koruması'nın çalışmasında tarama teknolojilerini kullanma

Dosya Koruması'nın çalışmasında tarama teknolojilerinin kullanımını yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Dosya Koruması** alt bölümünü seçin.

   Pencerenin sağ kısmında, Dosya Koruması bileşeninin ayarları görüntülenir.
3. **Güvenlik düzeyi** bölümünde, **Ayarlar** düğmesine tıklayın.

   Dosya Koruması penceresi açılır.
4. **Dosya Koruması** penceresinde, **Diğer** sekmesini seçin.
5. **Tarama teknolojileri** bölümünde:
   - Dosya Koruması'nın çalışmasında kullanmak istediğiniz teknolojilerin adlarının karşısındaki onay kutularını işaretleyin.
   - Dosya Koruması'nın çalışmasında kullanmak istemediğiniz teknolojilerin adlarının karşısındaki onay kutularını işaretlemeyin.
6. **Tamam**'a tıklayın.

7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Dosya taramasını optimize etme

Dosya taramasını optimize etmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Dosya Koruması** alt bölümünü seçin.
   Pencerenin sağ kısmında, Dosya Koruması bileşeninin ayarları görüntülenir.
3. **Ayarlar** düğmesine tıklayın.
   Dosya Koruması penceresi açılır.
4. **Dosya Koruması** penceresinde, **Performans** sekmesini seçin.
5. **Tarama optimizasyonu** bölümünde, **Sadece yeni ve değiştirilmiş dosyaları tara** onay kutusunu işaretleyin.
6. **Tamam**'a tıklayın.
7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Bileşik dosyaları tarama

Virüsleri ve diğer zararlı yazılımları gizlemek için yaygın bir teknik, arşivler veya e-posta veritabanları gibi bileşik dosyaların içine gömmektir. Bu şekilde gizlenen virüsleri ve diğer zararlı yazılımları tespit etmek için bileşik dosyanın paketinin açılması gerekir ve bu da taramayı yavaşlatabilir. Taranacak bileşik dosya setini sınırlayarak, taramayı hızlandırabilirsiniz.

Virüslü bir bileşik dosyayı işlemek için kullanılan yöntem (temizleme veya silme) dosya türüne bağlıdır.

Dosya Koruması RAR, ARJ, ZIP, CAB, ve LHA biçimlerindeki bileşik dosyaları temizler ve tüm diğer biçimlerdeki dosyaları siler (posta veri tabanları haricinde).

Bileşik dosyaların taranmasını yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Dosya Koruması** alt bölümünü seçin.
   Pencerenin sağ kısmında, Dosya Koruması bileşeninin ayarları görüntülenir.
3. **Güvenlik düzeyi** bölümünde, **Ayarlar** düğmesine tıklayın.
   Dosya Koruması penceresi açılır.
4. **Dosya Koruması** penceresinde, **Performans** sekmesini seçin.

5. **Bileşik dosya taraması** bölümünde, taramak istediğiniz bileşik dosyaların türünü belirtin: arşivler, kurulum paketleri ve Office biçimlerindeki dosyalar.

6. Sadece yeni ve değiştirilmiş dosyaları taramak için **Sadece yeni ve değiştirilmiş dosyaları tara** onay kutusunu işaretleyin.

   Dosya Koruması sadece yeni ve değiştirilmiş bileşik dosya türlerini tarar.

7. **Diğer** düğmesine tıklayın.

   Bileşik dosyalar penceresi açılır.

8. **Arka plan taraması** bölümünde aşağıdakilerden birini yapın:

   - Dosya Koruması'nın bileşik dosyaları arka planda çıkartmasını engellemek için **Bileşim dosyalarını arka planda çıkart** onay kutusunu işaretleyin.
   - Arka planda tarama yaparken Dosya Koruması'nın bileşik dosyaları çıkartmasına izin vermek için **Bileşim dosyalarını arka planda çıkart** onay kutusunu işaretleyin ve **Minimum dosya boyutu** alanına gereken değeri belirtin.

9. **Boyut sınırı** bölümünde aşağıdakilerden birini yapın:

   - Dosya Koruması'nın büyük bileşik dosyaları çıkartmasını engellemek için **Büyük bileşik dosyaları açma** onay kutusunu işaretleyin ve **En büyük dosya boyutu** alanında gereken değeri belirtin. Dosya Koruması, belirtilen boyuttan büyük olan bileşik dosyaları çıkartmaz.
   - Dosya Koruması'nın büyük bileşik dosyaları çıkartmasına izin vermek için **Büyük bileşik dosyaları açma** onay kutusunu işaretlemeyin.

     En büyük dosya boyutu alanındaki değerden büyük boyuttaki bir dosyanın büyük olduğu değerlendirilir.

   Büyük bileşik dosyaları açma onay kutusunun işaretlenip işaretlenmediğine bakılmaksızın Dosya Koruması, arşivden çıkartılan büyük boyutlu dosyaları tarar.

10. **Tamam**'a tıklayın.

11. **Dosya Koruması** penceresinde **Tamam**'a tıklayın.

12. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Tarama modunu değiştirme

Tarama modu Dosya Koruması'nın dosyaları taramaya başladığı koşul anlamına gelir. Varsayılan olarak, Kaspersky Endpoint Security dosyaları akıllı modda tarar. Bu tarama modunda Dosya Koruması, kullanıcı tarafından, kullanıcı adına bir uygulama tarafından (oturum açmak için kullanılan hesabın veya başka bir kullanıcı hesabının altında) veya işletim sistemi tarafından dosya üzerinde yapılan işlemleri analiz ettikten sonra dosyaları tarayıp taramayacağına karar verir. Örneğin, bir Microsoft Office Word belgesi ile çalışırken Kaspersky Endpoint Security dosyayı ilk açıldığında ve son kapandığında tarar. Dosyanın üzerine yazan ara işlemler taranmasına neden olmaz.

Dosya tarama modunu değiştirmek için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Dosya Koruması** alt bölümünü seçin.

Pencerenin sağ kısmında, Dosya Koruması bileşeninin ayarları görüntülenir.

3. **Güvenlik düzeyi** bölümünde, **Ayarlar** düğmesine tıklayın.
   Dosya Koruması penceresi açılır.

4. **Dosya Koruması** penceresinde, **Diğer** sekmesini seçin.

5. **Tarama modu** bölümünde, gerekli modu seçin:

   - **Akıllı mod**.
   - **Erişildiğinde ve değiştirildiğinde**.
   - **Erişildiğinde**.
   - **Yürütüldüğünde**.

6. **Tamam**'a tıklayın.

7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

E-posta koruması. Posta Koruması

Bu bileşen, İş istasyonları için Microsoft Windows'un kurulu olduğu bir bilgisayara Kaspersky Endpoint Security yüklendiğinde kullanılabilir. Bu bileşen, Dosya sunucuları için Microsoft Windows'un kurulu olduğu bir bilgisayara Kaspersky Endpoint Security yüklendiğinde kullanılamaz.

Bu bölümde, Posta Koruması hakkında bilgiler ve bileşen ayarlarının yapılandırılmasına ilişkin talimatlar bulunmaktadır.

Posta Koruması Hakkında

Posta Koruması, gelen ve giden e-posta mesajlarında virüsleri ve diğer tehditleri tarar. Kaspersky Endpoint Security ile birlikte çalışır, bilgisayar belleğinde etkin kalır ve POP3, SMTP, IMAP, MAPI ve NNTP iletişim kurallarıyla alınan veya gönderilen tüm mesajlarda tarama yapar. Mesajda herhangi bir tehdit algılanmazsa kullanılabilir hale gelir ve/veya işlenir.

E-posta mesajında bir tehdit tespit edildiğinde Posta Koruması aşağıdakileri gerçekleştirir:

1. E-posta mesajında tespit edilen nesne türünü (*Truva atı* gibi) belirler.
2. E-posta mesajına aşağıdaki durumlardan biri atanır:
   - *Büyük olasılıkla virüslü*. Taramada e-posta mesajının virüslü olup olmadığı tam olarak belirlenemezse bu durum atanır. Dosya, tipik olarak virüsler veya diğer zararlı yazılımlarda görülen bir kod bölümü veya bilinen bir virüsün değiştirilmiş kodunu içerebilir.
   - *Virüslü*. E-posta mesajı taramasında Kaspersky Endpoint Security'nin anti-virüs veritabanlarında yer alan bilinen bir virüsün kod bölümü bulunursa nesneye bu durum atanır.
   - *Bulunmadı*. E-posta mesajı taramasında virüsler veya başka tehditler tespit edilmezse nesneye bu durum atanır.

Ardından uygulama e-posta mesajını engeller, tespit edilen nesne ile ilgili bir bildirim görüntüler (bildirim ayarlarında belirtiliyorsa) ve Posta Koruması ayarlarında belirtilen eylemi gerçekleştirir.

Bu bileşen, bilgisayarda yüklü e-posta istemcileri ile etkileşim kurar. Microsoft Office Outlook® e-posta istemcisinin mesaj tarama ayarlarında ince ayarlama yapmanıza olanak tanıyan gömülü bir eklenti mevcuttur. Posta Koruması eklentisi, Kaspersky Endpoint Security'nin yüklenmesi sırasında Microsoft Office Outlook e-posta istemcisine eklenir.

Posta Koruması'nın çalışması, görev çubuğu bildirim alanındaki uygulama simgesi ile belirtilir. Posta Koruması bir e-posta mesajını tararken durum simgesi olarak değişir.

Posta Tehdidi Koruması'nı etkinleştirme ve devre dışı bırakma

Varsayılan olarak, Posta Tehdidi Koruması bileşeni etkinleştirilmiştir ve Kaspersky uzmanları tarafından önerilen modda çalışır. Gerekirse Posta Tehdidi Koruması bileşenini devre dışı bırakabilirsiniz.

Posta Tehdidi Koruması bileşenini etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresinde **Ayarlar** düğmesine tıklayın.

2. Pencerenin sol kısmında, **Temel Tehdit Koruması** bölümünde, **Posta Tehdidi Koruması** seçeneğini belirleyin.

   Posta Tehdidi Koruması bileşeninin ayarları pencerenin sağ kısmında görüntülenir.

3. Aşağıdakilerden birini yapın:

   - Posta Tehdidi Koruması bileşenini etkinleştirmek için **Posta Tehdidi Koruması** onay kutusunu işaretleyin.
   - Posta Tehdidi Koruması bileşenini devre dışı bırakmak için **Posta Tehdidi Koruması** onay kutusunun işaretini kaldırın.

4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Posta Koruması'nı Yapılandırma

Posta Koruması'nı yapılandırmak için aşağıdakileri uygulayabilirsiniz:

- E-posta güvenlik düzeyini değiştirebilirsiniz.

  Önceden yüklenen e-posta güvenlik düzeylerinden birini seçebilirsiniz veya özel bir e-posta güvenlik düzeyi yapılandırabilirsiniz.

  E-posta güvenlik düzeyi ayarlarını değiştirdiyseniz önerilen e-posta güvenlik düzeyi ayarlarına her zaman geri dönebilirsiniz.

- Kaspersky Endpoint Security'nin virüslü mesajlar üzerinde gerçekleştirdiği eylemi değiştirebilirsiniz.

- Posta Koruması'nın koruma kapsamını düzenleyebilirsiniz.

- E-posta mesajlarına eklenen bileşik dosyaların taranmasını yapılandırabilirsiniz.

  Mesaj eklerinin taranmasını etkinleştirebilir veya devre dışı bırakabilirsiniz, taranacak mesaj eklerinin maksimum boyutunu sınırlayabilirsiniz ve mesaj eklerinin maksimum tarama süresini sınırlayabilirsiniz.

- E-posta mesajı eklerinin türüne göre filtrelemeyi yapılandırabilirsiniz.

  Mesaj eklerinin türüne göre filtrelenmesi belirli türlerdeki dosyaların otomatik yeniden adlandırılmasına veya silinmesine olanak tanır.

- Sezgisel Analiz'i yapılandırabilirsiniz.

  Koruma etkinliğini artırmak için sezgisel analizi kullanabilirsiniz. Sezgisel analiz sırasında Kaspersky Endpoint Security, işletim sistemindeki uygulamaların etkinliğini analiz eder. Sezgisel analiz, Kaspersky Endpoint Security'nin veritabanlarında şu anda kaydı bulunmayan mesajlardaki tehditleri tespit edebilir.

- Microsoft Office Outlook'ta e-posta taramasını yapılandırabilirsiniz.

  Microsoft Office Outlook e-posta istemcisi için e-posta tarama ayarlarının uygun yapılandırılmasına olanak tanıyan gömülü bir eklenti mevcuttur.

  Microsoft Outlook Express®, Windows Mail ve Mozilla™ Thunderbird™ dahil olmak üzere diğer e-posta istemcileri ile çalışırken Posta Koruması bileşeni; SMTP, POP3, IMAP ve NNTP e-posta iletişim kurallarının trafiğini tarar.

  Mozilla Thunderbird e-posta istemcisi ile çalışırken mesajları **Gelen Kutusu** klasöründen taşımak için filtreler kullanılıyorsa Posta Koruması, IMAP iletişim kuralı üzerinden aktarılan mesajlarda virüsler ve diğer tehditleri taramaz.

E-posta güvenlik düzeyini değiştirme

Posta Tehdidi Koruması bileşeni, e-postaları korumak için çeşitli ayar gruplarını uygular. Bu ayar gruplarına *e-posta güvenlik düzeyleri* denir. Üç adet e-posta güvenlik düzeyi vardır: **Yüksek**, **Önerilen** ve **Düşük**. **Önerilen** dosya güvenlik düzeyi en iyi ayar olarak kabul edilir ve Kaspersky tarafından önerilir.

E-posta güvenlik düzeyini değiştirmek için:

1. Ana uygulama penceresinde **Ayarlar** düğmesine tıklayın.
2. Pencerenin sol kısmında, **Temel Tehdit Koruması** bölümünde, **Posta Tehdidi Koruması** seçeneğini belirleyin.

   Posta Tehdidi Koruması bileşeninin ayarları pencerenin sağ kısmında görüntülenir.
3. **Güvenlik düzeyi** bölümünde aşağıdakilerden birini yapın:
   - Önceden yüklenen E-posta güvenlik düzeylerinden birini yüklemek isterseniz (**Yüksek**, **Önerilen** ya da **Düşük**) kaydırma çubuğunu kullanarak birini seçin.
   - Özel bir güvenlik düzeyi yapılandırmak isterseniz **Ayarlar** düğmesine tıklayın ve açılan **Posta Tehdidi Koruması** penceresinde ayarları girin.

     Özel bir e-posta güvenlik düzeyi yapılandırdıktan sonra **Güvenlik düzeyi** bölümündeki e-posta güvenlik düzeyinin adı **Özel** olarak değişir.
   - E-posta güvenlik düzeyini **Önerilen** olarak değiştirmek için **Varsayılan olarak** düğmesine tıklayın.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Virüslü e-posta mesajlarına uygulanacak eylemi değiştirme

Virüslü e-posta mesajlarına uygulanacak eylemin değiştirilmesi için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Posta Koruması** alt bölümünü seçin.

   Pencerenin sağ kısmında, Posta Koruması bileşeninin ayarları görüntülenir.
3. **Tehdit algılandığında uygulanacak eylem** bölümünde Kaspersky Endpoint Security'nin virüslü bir mesajı tespit ettiğinde gerçekleştireceği eylemi seçin.
   - **Eylemi otomatik olarak seç**.
   - **Eylemi gerçekleştir: Temizle. Temizleme başarısız olursa sil**.
   - **Eylemi gerçekleştir: Temizle**.
   - **Eylemi gerçekleştir: Kaldır**.
   - **Eylemi gerçekleştir: Engelle**.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Posta Koruması'nın koruma kapsamını düzenleme

Koruma kapsamı, etkinken bileşen tarafından taranan nesneleri ifade eder. Farklı bileşenlerin koruma kapsamları farklı özelliklere sahiptir. Posta Koruması'nın koruma kapsamının özellikleri, e-posta istemcilerine Posta Koruması entegrasyonunun ayarlarını ve trafiği Posta Koruması tarafından taranan e-posta mesajı ve e-posta iletişim kuralları türlerini içerir. Varsayılan olarak Kaspersky Endpoint Security hem gelen hem de giden e-posta mesajları ile POP3, SMTP, NNTP ve IMAP iletişim kurallarının trafiğini tarar ve Microsoft Office Outlook e-posta istemcisi ile entegredir.

Posta Koruması'nın koruma kapsamını oluşturmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Posta Koruması** alt bölümünü seçin.

   Pencerenin sağ kısmında, Posta Koruması bileşeninin ayarları görüntülenir.
3. **Ayarlar** düğmesine tıklayın.

   Posta Koruması penceresi açılır.
4. **Genel** sekmesini seçin.
5. **Koruma kapsamı** bölümünde aşağıdakilerden birini yapın:

   - Posta Koruması'nın bilgisayarınızda tüm gelen ve giden mesajları taramasını istiyorsanız **Gelen ve giden mesajlar** seçeneğini seçin.
   - Posta Koruması'nın bilgisayarınızda yalnızca gelen mesajları taramasını istiyorsanız **Sadece gelen mesajlar** seçeneğini seçin.

     Sadece gelen mesajların taranmasını seçerseniz tüm giden mesajların bir defalık taramasının gerçekleştirilmesi önerilir çünkü bilgisayarınızda e-postaya yayılan e-posta solucanları bulunması ihtimal dahilindedir. Bu, bilgisayarınızdan virüslü mesajları içeren izlenmeyen toplu e-posta gönderiminden kaynaklanan sorunların önlenmesine yardımcı olur.
6. **Bağlanabilirlik** bölümünde aşağıdakilerden birini yapın:

   - Posta Koruması'nın POP3, SMTP, NNTP ve IMAP iletişim kuralları üzerinden aktarılan mesajları bilgisayarınıza ulaşmadan taramasını istiyorsanız **POP3 / SMTP / NNTP / IMAP trafiği** onay kutusunu işaretleyin.

     Posta Koruması'nın POP3, SMTP, NNTP ve IMAP iletişim kuralları üzerinden aktarılan mesajları bilgisayarınıza ulaşmadan taramasını istemiyorsanız **POP3 / SMTP / NNTP / IMAP trafiği** onay kutusunu işaretlemeyin. Bu durumda **Ek: Microsoft Office Outlook eklentisi** onay kutusu işaretlenirse mesajlar kullanıcı bilgisayarına ulaştıktan sonra Microsoft Office Outlook e-posta istemcisine entegre olan Posta Koruması uzantısı tarafından taranır.

     Microsoft Office Outlook'tan farklı bir e-posta istemcisi kullanıyorsanız POP3, SMTP, NNTP ve IMAP iletişim kuralları üzerinden aktarılan mesajlar, **POP3 / SMTP / NNTP / IMAP trafiği** onay kutusu işaretli değilse Posta Koruması tarafından taranmaz.

- Microsoft Office Outlook'tan Posta Koruması ayarlarına erişimi açmak ve Microsoft Office Outlook'a entegre eklentiyi kullanarak POP3, SMTP, NNTP, IMAP ve MAPI iletişim kuralları üzerinden aktarılan mesajların bilgisayara ulaştıktan sonra taranmasını etkinleştirmek istiyorsanız **Ek: Microsoft Office Outlook eklentisi** onay kutusu işaretleyin.

  Microsoft Office Outlook'tan Posta Koruması ayarlarına erişimi engellemek ve Microsoft Office Outlook'a entegre eklentiyi kullanarak POP3, SMTP, NNTP, IMAP ve MAPI iletişim kuralları üzerinden aktarılan mesajların bilgisayara ulaştıktan sonra taranmasını devre dışı bırakmak istiyorsanız **Ek: Microsoft Office Outlook eklentisi** onay kutusu işaretlemeyin.

  Posta Koruması eklentisi, Kaspersky Endpoint Security'nin yüklenmesi sırasında Microsoft Office Outlook e-posta istemcisine eklenir.

7. **Tamam**'a tıklayın.
8. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

E-posta mesajlarına eklenen bileşik dosyaları tarama

E-posta mesajlarına eklenen bileşik dosyaların taranmasını yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Posta Koruması** alt bölümünü seçin.

   Pencerenin sağ kısmında, Posta Koruması bileşeninin ayarları görüntülenir.
3. **Ayarlar** düğmesine tıklayın.

   Posta Koruması penceresi açılır.
4. **Genel** sekmesini seçin.
5. **Bileşik dosya taraması** bölümünde aşağıdakileri gerçekleştirin:
   - Posta Koruması'nın mesajlara eklenen arşivleri atlamasını isterseniz **Ekli arşivleri tara** onay kutusunu işaretlemeyin.
   - Posta Koruması'nın boyutu N megabayttan daha büyük olan mesaj eklerini atlamasını isterseniz **Şundan büyük arşivleri tarama:N MB** onay kutusunu işaretleyin. Bu onay kutusunu işaretlerseniz onay kutusu adının karşısındaki alanda maksimum arşiv boyutunu belirleyin.
   - Posta Koruması'nın taraması N saniyeden daha uzun süren mesaj eklerini taramasını isterseniz **Şundan daha fazla olan arşivleri tarama:** N sn onay kutusunu işaretlemeyin.
6. **Tamam**'a tıklayın.
7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

E-posta mesajı eklerini filtreleme

Kötü amaçlı programlar, e-posta mesajlarının ekleri biçiminde dağıtılabilir. Filtrelemeyi mesaj eklerinin türüne göre yapılandırabilirsiniz, böylece belirtilen türdeki dosyalar otomatik olarak yeniden adlandırılır veya silinir. Belirli bir türdeki bir ekin adını değiştirerek Kaspersky Endpoint Security, bilgisayarınızı kötü amaçlı bir programın otomatik olarak yürütülmesine karşı koruyabilir.

Eklerin filtrelenmesini yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Posta Koruması** alt bölümünü seçin.

   Pencerenin sağ kısmında, Posta Koruması bileşeninin ayarları görüntülenir.
3. **Güvenlik düzeyi** bölümünde, **Ayarlar** düğmesine tıklayın.

   Posta Koruması penceresi açılır.
4. **Posta Koruması** penceresinde, **Eklenti filtresi** sekmesini seçin.
5. Aşağıdakilerden birini yapın:

   - Posta Koruması'nın mesaj eklerini filtrelemesini istemezseniz **Filtrelemeyi devre dışı bırak** seçeneğini seçin.
   - Posta Koruması'nın **belirli türlerdeki** mesaj eklerini yeniden adlandırmasını isterseniz **Belirtilen eklenti türlerini yeniden adlandır** seçeneğini seçin.

Bir dosyanın gerçek biçiminin dosya adı uzantısı ile uyuşmayabileceğini unutmayın.

E-posta mesajlarına eklenen nesnelerin filtrelenmesini etkinleştirirseniz Posta Koruması, aşağıdaki uzantıları içeren dosyaları yeniden adlandırabilir veya silebilir:

com – 64 KB'dan daha büyük olmayan bir uygulamanın yürütülebilir dosyası

exe – yürütülebilir dosya veya kendini açabilen arşiv

sys – Microsoft Windows sistem dosyası

prg – dBase™, Clipper veya Microsoft Visual FoxPro® veya bir WAVmaker programı için program metni

bin – ikili dosya

bat – toplu iş dosyası

cmd – Microsoft Windows NT (DOS için bat dosyasına benzerdir), OS/2 için komut dosyası

dpl – sıkıştırılmış Borland Delphi kitaplığı

dll – dinamik bağlantı kitaplığı

scr – Microsoft Windows giriş ekranı

cpl – Microsoft Windows denetim masası modülü

ocx – Microsoft OLE (Nesne Bağlama ve Ekleme) nesnesi

tsp – ara zaman modunda çalışan program

drv – aygıt sürücüsü

vxd – Microsoft Windows sanal aygıt sürücüsü

pif – program bilgi dosyası

lnk – Microsoft Windows bağlantı dosyası

reg – Microsoft Windows sistem kayıt defteri anahtarı dosyası

ini – Microsoft Windows, Windows NT ve bazı uygulamalar için yapılandırma verileri içeren yapılandırma dosyası

cla – Java sınıfı

vbs – Visual Basic® komut dizisi

vbe – BIOS video uzantısı

js, jse – JavaScript kaynak metni

htm – köprü metni belgesi

htt – Microsoft Windows köprü metni başlığı

hta – Microsoft İnternet Explorer® için köprü metni programı

asp – Etkin Sunucu Sayfaları komut dizisi

chm – derlenmiş HTML dosyası

pht – entegre PHP komut dizeli HTML dosyası

php – HTML dosyalarının içine entegre komut dizisi

wsh – Microsoft Windows Komut Dizisi Sunucusu dosyası

wsf – Microsoft Windows komut dizisi

the – Microsoft Windows 95 masaüstü duvar kağıdı dosyası

hlp – Windows Yardım dosyası

eml – Microsoft Outlook Express iletisi

nws – yeni Microsoft Outlook Express e-posta iletisi

msg – Microsoft Mail e-posta iletisi

plg – e-posta mesajı

mbx – kaydedilmiş Microsoft Office Outlook e-postalarının uzantısı

doc* – Microsoft Office Word belgeleri, örneğin: Microsoft Office Word belgeleri için doc, XML destekli Microsoft Office Word 2007 belgeleri için docx ve makro destekli Microsoft Office Word 2007 belgeleri için docm

dot* – Microsoft Office Word belgesi şablonları, örneğin: Microsoft Office Word belgesi şablonları için dot, Microsoft Office Word 2007 belgesi şablonları için dotx ve makro destekli Microsoft Office Word 2007 belge şablonları için dotm

fpm – veritabanı programı, Microsoft Visual FoxPro başlangıç dosyası

rtf – Zengin Metin Biçimi belgesi

shs – Windows Shell Scrap Object Handler parçası

dwg – AutoCAD® çizim veritabanı

msi – Microsoft Windows Installer paketi

otm – Microsoft Office Outlook için VBA projesi

pdf – Adobe Acrobat belgesi

swf – Shockwave® Flash paket nesnesi

jpg, jpeg – sıkıştırılmış görüntü grafikleri biçimi

emf – Zenginleştirilmiş Meta Dosyası biçimli dosya. Microsoft Windows İşletim Sistemlerinin yeni nesil meta dosyaları. EMF dosyaları 16 bit Microsoft Windows tarafından desteklenmemektedir.

ico – nesne simge dosyası

ov? – Microsoft Office Word yürütülebilir dosyaları

xl* – Microsoft Office Excel belgeleri ve dosyaları, örneğin: Microsoft Office Excel için xla uzantısı, şemalar için xlc, belge şablonları için xlt, Microsoft Office Excel 2007 çalışma kitapları için xlsx, makro destekli Microsoft Office Excel 2007 çalışma kitapları için xltm, ikili biçimde (XML olmayan) Microsoft Office Excel 2007 çalışma kitapları için xlsb, Microsoft Office Excel 2007 şablonları için xltx, makro destekli Microsoft Office Excel 2007 şablonları için xlsm ve makro destekli Microsoft Office Excel 2007 eklentileri için xlam

pp* – Microsoft Office PowerPoint® belgeleri ve dosyaları, örneğin: Microsoft Office PowerPoint slaytları için pps, sunumlar için ppt, Microsoft Office PowerPoint 2007 sunumları için pptx, makro destekli Microsoft Office PowerPoint 2007 sunumları için pptm, Microsoft Office PowerPoint 2007 sunum şablonları için potx, makro destekli Microsoft Office PowerPoint 2007 sunum şablonları için potm, Microsoft Office PowerPoint 2007 slayt gösterileri için ppsx, makro destekli Microsoft Office PowerPoint 2007 slayt gösterileri için ppsm ve makro destekli Microsoft Office PowerPoint 2007 eklentileri için ppam

md* – Microsoft Office Access® belgeleri ve dosyaları, örneğin: Microsoft Office Access çalışma grupları için mda ve veritabanları için mdb

sldx – bir Microsoft PowerPoint 2007 slaytı

sldm – makro destekli bir Microsoft PowerPoint 2007 slaytı

thmx – bir Microsoft Office 2007 teması

- Posta Koruması'nın belirli türlerdeki mesaj eklerini silmesini isterseniz **Belirtilen eklenti türlerini sil** seçeneğini seçin.

6. Önceki adımda **Belirtilen eklenti türlerini yeniden adlandır** seçeneğini veya **Belirtilen eklenti türlerini sil** seçeneğini seçerseniz, ilgili dosya türünün karşısındaki onay kutusunu işaretleyin.

   Ekle, **Düzenle** ve **Kaldır** düğmelerini kullanarak dosya türlerinin listesini değiştirebilirsiniz.

7. **Tamam**'a tıklayın.

8. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Microsoft Office Outlook'ta e-postaları tarama

Kaspersky Endpoint Security'nin yüklenmesi sırasında Posta Koruması eklentisi, Microsoft Office Outlook'a eklenir (bundan sonra Outlook olarak ifade edilecektir). Posta Koruması ayarlarını Outlook'tan açmanıza ve e-posta mesajlarında virüs ve diğer tehditlerin ne zaman taranacağını belirtmenize olanak tanır. Outlook'un Posta Koruması eklentisi, POP3, SMTP, NNTP, IMAP ve MAPI iletişim kuralları üzerinden aktarılan gelen ve giden mesajları tarayabilir.

Kaspersky Endpoint Security arabiriminde **Ek: Microsoft Office Outlook eklentisi** onay kutusu işaretlenirse Posta Koruması ayarları doğrudan Outlook'tan yapılandırılabilir.

Outlook'ta gelen mesajlar öncelikle Posta Koruması tarafından (Kaspersky Endpoint Security'nin arabiriminde **POP3 / SMTP / NNTP / IMAP trafiği** onay kutusu işaretlendiyse) ve ardından Outlook'un Posta Koruması eklentisi tarafından taranır. Posta Koruması bir mesajda kötü amaçlı nesne tespit ederse sizi bu olay hakkında uyarır.

Bildirim penceresindeki eylem tercihiniz, mesajdaki tehdidi hangi bileşenin ortadan kaldıracağını belirler: Posta Koruması veya Outlook için Posta Koruması eklentisi.

- Bildirim penceresinde **Temizle** veya **Kaldır**'ı seçerseniz, Posta Koruması tarafından tehdit ortadan kaldırılır.
- Kullanıcı bildirim penceresinde **Atla**'yı seçerseniz Outlook için Posta Koruması eklentisi, tehdidi ortadan kaldırır.

Giden mesajlar öncelikle Outlook için Posta Koruması tarafından taranır ve ardından Posta Koruması tarafından taranır.

Outlook'ta e-posta taramasını yapılandırma

Outlook 2007'de e-posta taramasını yapılandırmak için:

1. Outlook 2007'nin ana penceresini açın.
2. Menü çubuğundan **Hizmet** → **Ayarlar**'ı seçin.
   Seçenekler penceresi açılır.
3. **Seçenekler** penceresinde, **E-posta koruması** sekmesini seçin.

Outlook 2010 / 2013'te e-posta taramasını yapılandırma:

1. Ana Outlook penceresini açın.
   Sol üst köşedeki **Dosya** sekmesini seçin.
2. **Seçenekler** düğmesine tıklayın.
   Outlook Seçenekleri penceresi açılır.
3. **Eklentiler** bölümünü seçin.
   Outlook'a eklenmiş eklentilerin ayarları, pencerenin sağ tarafında görüntülenir.
4. **Eklenti Seçenekleri** düğmesine tıklayın.

Kaspersky Security Center'ı kullanarak e-posta taramayı yapılandırma

E-postalar, Outlook için Posta Koruması uzantısı kullanılarak taranıyorsa Önbellekli Exchange Modu'nun kullanılması önerilir. Exchange önbellekleme modu ve kullanımıyla ilgili öneriler hakkında daha ayrıntılı bilgi için lütfen Microsoft Bilgi Bankası'na bakınız: https://technet.microsoft.com/en-us/library/cc179175.aspx.

Outlook için Kaspersky Security Center'ı kullanarak Posta Koruması eklentisinin işletim modunu yapılandırmak için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, e-posta taramasını yapılandırmak istediğiniz yönetim grubunun adının bulunduğu klasörü açın.
3. Çalışma alanında, **İlkeler** sekmesini seçin.
4. Gereken ilkeyi seçin.
5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:
   - İlkenin içerik menüsünde **Özellikler**'i seçin.
   - Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.
6. **Virüse karşı koruma** bölümünde, **Posta Koruması** alt bölümünü seçin.
7. **Güvenlik düzeyi** bölümünde, **Ayarlar** düğmesine tıklayın.

   Posta Koruması penceresi açılır.
8. **Bağlanabilirlik** bölümünde **Ayarlar** düğmesine tıklayın.

   E-posta Koruması penceresi açılır.
9. **E-posta koruması** penceresinde:
   - Outlook için Posta Koruması eklentisinin gelen kutusuna gelen mesajları taramasını istiyorsanız **Alırken tara** onay kutusunu seçin.
   - Outlook için Posta Koruması eklentisinin gelen mesajları kullanıcı açtığında taramasını istiyorsanız **Okuma sırasında tara** onay kutusunu seçin.
   - Outlook için Posta Koruması eklentisinin giden mesajları gönderilirken taramasını istiyorsanız **Gönderirken tara** onay kutusunu seçin.
10. **E-posta koruması** penceresinde **Tamam**'a tıklayın
11. **Posta Koruması** penceresinde **Tamam**'a tıklayın.
12. İlkeyi uygulayın.

    Kaspersky Security Center ilkesinin uygulanmasıyla ilgili ayrıntılar için *Kaspersky Security Center Yönetici Kılavuzu*'na bakınız.

İnternet'te bilgisayar bağlantısı. İnternet Koruması

Bu bileşen, İş istasyonları için Microsoft Windows'un kurulu olduğu bir bilgisayara Kaspersky Endpoint Security yüklendiğinde kullanılabilir. Bu bileşen, Dosya sunucuları için Microsoft Windows'un kurulu olduğu bir bilgisayara Kaspersky Endpoint Security yüklendiğinde kullanılamaz.

Bu bölümde, İnternet Koruması hakkında bilgiler ve bileşen ayarlarının yapılandırılmasına ilişkin talimatlar bulunmaktadır.

İnternet Koruması Hakkında

İnternete girdiğiniz her seferde bilgisayarınızda saklanan bilgileri virüsler ve diğer zararlı yazılımlara açık hale getirirsiniz. Kullanıcı, ücretsiz yazılım indirirken veya suçluların güvenlik açıklarından yararlandığı web sitelerinde gezinirken bu virüsler bilgisayara girebilir. Bir İnternet bağlantısı oluşturduğunuzda bir web sayfası açmasanız veya bir dosya indirmeseniz bile ağ solucanları bilgisayarınıza girmenin bir yolunu bulabilir.

İnternet Koruması, HTTP ve FTP iletişim kuralları üzerinden bilgisayara veya bilgisayardan gönderilen gelen ve giden verileri korur ve URL'lerde kötü amaçlı veya e-dolandırıcılık adreslerini denetler.

İnternet Koruması, HTTP veya FTP iletişim kuralı üzerinden kullanıcı veya uygulamanın eriştiği her bir İnternet sayfası veya dosyasında virüsler ve diğer tehditleri analiz eder ve yakalar. Ardından aşağıdakiler gerçekleştirilir:

- Bir sayfa veya dosyanın kötü amaçlı kod içermediği tespit edilirse kullanıcı, bunlara anında erişim sağlar.
- Kullanıcı kötü amaçlı kod içeren bir İnternet sayfası veya dosyaya erişim sağlarsa uygulama, İnternet Koruması ayarlarında belirtilen eylemi uygular.

Web Tehdidi Koruması'nı etkinleştirme ve devre dışı bırakma

Varsayılan olarak, Web Tehdidi Koruması bileşeni etkinleştirilmiştir ve Kaspersky uzmanları tarafından önerilen modda çalışır. Gerekirse Web Tehdidi Koruması bileşenini devre dışı bırakabilirsiniz.

Web Tehdidi Koruması bileşenini etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresinde **Ayarlar** düğmesine tıklayın.
2. Pencerenin sol kısmında, **Temel Tehdit Koruması** bölümünde, **Web Tehdidi Koruması** seçeneğini belirleyin.

   Web Tehdidi Koruması bileşeninin ayarları pencerenin sağ kısmında görüntülenir.
3. Aşağıdakilerden birini yapın:
   - Web Tehdidi Koruması bileşenini etkinleştirmek için **Web Tehdidi Koruması** onay kutusunu işaretleyin.
   - Web Tehdidi Koruması bileşenini devre dışı bırakmak için **Web Tehdidi Koruması** onay kutusunun işaretini kaldırın.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

İnternet Koruması'nı Yapılandırma

İnternet Koruması'nı yapılandırmak için aşağıdakileri uygulayabilirsiniz:

- İnternet trafiği güvenlik düzeyini değiştirebilirsiniz.

  HTTP ve FTP iletişim kuralları üzerinden alınan veya aktarılan İnternet trafiğinin önceden yüklenmiş güvenlik düzeylerinden birini seçebilir veya özel bir İnternet trafiği güvenlik düzeyi yapılandırabilirsiniz.

  İnternet trafiği güvenlik düzeyi ayarlarını değiştirirseniz önerilen İnternet trafiği güvenlik düzeyi ayarlarına her zaman geri dönebilirsiniz.

- Kaspersky Endpoint Security'nin kötü amaçlı İnternet trafiği nesnelerinde gerçekleştirdiği eylemi değiştirebilirsiniz.

  Bir HTTP nesnesinin analizinde kötü amaçlı kod içeriği görülürse İnternet Koruması'nın yanıtı belirttiğiniz eyleme bağlıdır.

- İnternet Koruması tarafından URL'lerin e-dolandırıcılık ve kötü amaçlı İnternet adreslerinin veritabanlarında taranmasını yapılandırabilirsiniz.

- İnternet trafiğinde virüslerin ve diğer kötü amaçlı programların taramasını yaparken sezgisel analizin kullanımını yapılandırabilirsiniz.

  Koruma etkinliğini artırmak için sezgisel analizi kullanabilirsiniz. Sezgisel analiz sırasında Kaspersky Endpoint Security, işletim sistemindeki uygulamaların etkinliğini analiz eder. Sezgisel analiz, Kaspersky Endpoint Security'nin veritabanlarında kayıt bulunmayan tehditleri tespit edebilir.

- İnternet sayfalarında e-dolandırıcılık bağlantılarını tararken sezgisel analiz kullanımını yapılandırabilirsiniz.

- HTTP ve FTP iletişim kuralları üzerinden alınan ve gönderilen İnternet trafiğinin İnternet Koruması tarafından taranmasını optimize edebilirsiniz.

- Güvenilir URL'lerin listesini oluşturabilirsiniz.

  İçeriğine güvenmeniz gereken URL'lerin listesini oluşturabilirsiniz. İnternet Koruması, güvenilir URL'lerdeki bilgilerde virüs veya diğer tehditleri analiz etmez. Bu seçenek örneğin İnternet Koruması bilinen bir İnternet sitesinden bir dosya indirmeye karıştığında faydalı olabilir.

  > URL, belirli bir İnternet sayfasının adresi veya İnternet sitesi adresi olabilir.

İnternet trafiği güvenlik düzeyini değiştirme

HTTP ve FTP iletişim kuralları üzerinden alınan ve aktarılan verileri korumak için Web Tehdidi Koruması bileşeni çeşitli ayar gruplarını uygular. Bu ayar gruplarına *İnternet trafiği güvenlik düzeyleri* denir. Üç adet önceden yüklenen İnternet trafiği güvenlik düzeyi vardır: **Yüksek**, **Önerilen** ve **Düşük**. **Önerilen** İnternet trafiği güvenlik düzeyi en iyi ayar olarak kabul edilir ve Kaspersky tarafından önerilir.

İnternet trafiği güvenlik düzeyini değiştirmek için:

1. Ana uygulama penceresinde **Ayarlar** düğmesine tıklayın.
2. Pencerenin sol kısmında, **Temel Tehdit Koruması** bölümünde, **Web Tehdidi Koruması** seçeneğini belirleyin.

Web Tehdidi Koruması bileşeninin ayarları pencerenin sağ kısmında görüntülenir.

3. **Güvenlik düzeyi** bölümünde aşağıdakilerden birini yapın:

   - Önceden yüklenen İnternet trafiği güvenlik düzeylerinden birini yüklemek isterseniz (**Yüksek**, **Önerilen** ya da **Düşük**) kaydırma çubuğunu kullanarak birini seçin.

   - Özel bir İnternet trafiği güvenlik düzeyi yapılandırmak isterseniz **Ayarlar** düğmesine tıklayın ve açılan **Web Tehdidi Koruması** penceresinde ayarları belirtin.

     Özel bir İnternet trafiği güvenlik düzeyi yapılandırdığınızda **Güvenlik düzeyi** bölümündeki güvenlik düzeyinin adı **Özel** olarak değişir.

   - İnternet trafiği güvenlik düzeyini **Önerilen** olarak değiştirmek için **Varsayılan olarak** düğmesine tıklayın.

4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Kötü amaçlı İnternet trafiği nesnelerinde uygulanacak eylemi değiştirme

Kötü amaçlı İnternet trafiği nesnelerine uygulanacak eylemi değiştirmek için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **İnternet Koruması** alt bölümünü seçin.

   Pencerenin sağ kısmında, İnternet Koruması bileşeninin ayarları görüntülenir.

3. **Tehdit algılandığında uygulanacak eylem** bölümünde Kaspersky Endpoint Security'nin kötü amaçlı İnternet trafiği üzerinde gerçekleştireceği eylemi seçin.

   - **Eylemi otomatik olarak seç**.

   - **İndirmeyi engelle**.

   - **İndirmeye izin ver**.

4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

İnternet Koruması tarafından URL'lerin e-dolandırıcılık ve kötü amaçlı İnternet adreslerinin veritabanlarında taranması

E-dolandırıcılık İnternet adreslerinin listesinde olup olmadığını görmek için bağlantıların taranması, *e-dolandırıcılık saldırılarından* kaçınmaya imkan tanır. E-dolandırıcılık saldırısı, bankanın resmi İnternet sitesinin bağlantısını içeren bankanızdan gelen bir e-posta mesajı şeklinde gizlenebilir. Bağlantıya tıkladığınızda bankanın İnternet sitesinin bire bir kopyası açılır ve sahte bir sitede olmanıza karşın tarayıcıda gerçek İnternet sitesini bile görebilirsiniz. Bu noktadan sonra sitedeki tüm işlemleriniz takip edilir ve paranızı çalmak için kullanılabilir.

E-dolandırıcılık İnternet sitelerinin bağlantıları, e-posta mesajının yanı sıra ICQ mesajları gibi diğer kaynaklardan da gelebileceği için İnternet Koruması, İnternet trafiği düzeyinde bir e-dolandırıcılık İnternet sitesine erişim denemelerini izler ve bu sitelere erişimi engeller. E-dolandırıcılık URL'lerinin listeleri Kaspersky Endpoint Security dağıtım kitinde bulunmaktadır.

İnternet Koruması tarafından URL'lerin e-dolandırıcılık ve kötü amaçlı İnternet adreslerinin veritabanlarında taranmasını yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **İnternet Koruması** alt bölümünü seçin.

   Pencerenin sağ kısmında, İnternet Koruması bileşeninin ayarları görüntülenir.
3. **Ayarlar** düğmesine tıklayın.

   İnternet Koruması penceresi açılır.
4. **İnternet Koruması** penceresinde, **Genel** sekmesini seçin.
5. Aşağıdakileri uygulayın:

   - İnternet Koruması'nın kötü amaçlı İnternet adreslerinin veritabanlarında URL'leri denetlemesini istiyorsanız **Tarama yöntemleri** bölümünde **Bağlantıların zararlı bağlantılar veritabanında listelenip listelenmediğini denetle** onay kutusunu işaretleyin.
   - İnternet Koruması'nın e-dolandırıcılık İnternet adreslerinin veritabanlarında URL'leri denetlemesini istiyorsanız, **E-dolandırıcılık Engelleyici Ayarları** bölümünde **Bağlantıların kimlik avı bağlantıları veritabanında listelenip listelenmediğini denetle** onay kutusunu işaretleyin.

   Bağlantıları, Kaspersky Security Network'ün saygınlık veritabanlarında da kontrol edebilirsiniz.
6. **Tamam**'a tıklayın.
7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

İnternet Koruması ile Sezgisel Analiz'i Kullanma

Sezgisel analizin kullanımını yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **İnternet Koruması** alt bölümünü seçin.

   Pencerenin sağ kısmında, İnternet Koruması bileşeninin ayarları görüntülenir.
3. **Güvenlik düzeyi** bölümünde, **Ayarlar** düğmesine tıklayın.

   İnternet Koruması penceresi açılır.
4. **Genel** sekmesini seçin.
5. İnternet Koruması'nın İnternet trafiğinde virüsleri ve diğer zararlı yazılımları taramasını isterseniz, **Tarama yöntemleri** bölümünde **Virüslerin tespiti için sezgisel analiz** onay kutusunu seçin ve sezgisel analiz düzeyini ayarlamak için kaydırma çubuğunu kullanın: **Hızlı tarama**, **Normal tarama** veya **Ayrıntılı tarama**.

6. İnternet Koruması'nın İnternet sayfalarında e-dolandırıcılık bağlantılarını taramasını istiyorsanız, **E-dolandırıcılık Engelleyici Ayarları** bölümünde **E-dolandırıcılık bağlantılarını tespit etmeye yönelik sezgisel analiz** onay kutusunu işaretleyin.

7. **Tamam**'a tıklayın.

8. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Güvenilir URL'lerin listesini düzenleme

Güvenilir URL'lerin listesini oluşturmak için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **İnternet Koruması** alt bölümünü seçin.

   Pencerenin sağ kısmında, İnternet Koruması bileşeninin ayarları görüntülenir.

3. **Ayarlar** düğmesine tıklayın.

   İnternet Koruması penceresi açılır.

4. **Güvenilir URL'ler** sekmesini seçin.

5. **Güvenilir adreslerin İnternet trafiğini tarama** onay kutusunu seçin.

6. İçeriğine güvendiğiniz URL'lerin / İnternet sayfalarının bir listesini oluşturabilirsiniz. Liste oluşturmak için:

   a. **Ekle** düğmesine tıklayın.

      Adres/Adres maskesi penceresi açılır.

   b. İnternet sitesi / İnternet sayfasının adres maskesini veya İnternet sitesi / İnternet sayfasının adresini girin.

   c. **Tamam**'a tıklayın.

      Güvenilir URL'lerin listesinde yeni bir kayıt görülür.

7. **Tamam**'a tıklayın.

8. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Anlık ileti uygulamaları koruması. IM Koruması

Bu bileşen, İş istasyonları için Microsoft Windows'un kurulu olduğu bir bilgisayara Kaspersky Endpoint Security yüklendiğinde kullanılabilir. Bu bileşen, Dosya sunucuları için Microsoft Windows'un kurulu olduğu bir bilgisayara Kaspersky Endpoint Security yüklendiğinde kullanılamaz.

Bu bölümde, IM Koruması ve bileşen ayarlarının nasıl yapılandırılacağı hakkında bilgiler bulunmaktadır.

IM Koruması Hakkında

IM Koruması, anlık mesajlaşma istemcilerinin (*anlık ileti uygulamaları* olarak bilinir) trafiğini tarar.

IM Koruması, şifrelenmiş kanallar üzerinden aktarılan mesajları taramaz.

Anlık ileti uygulamaları aracılığıyla gönderilen mesajlar aşağıdaki güvenlik tehditlerinin çeşitlerini içerebilir:

- Bilgisayara kötü amaçlı bir program indirmeye teşebbüs eden URL'ler
- E-dolandırıcılık saldırıları için saldırganların kullandığı kötü amaçlı programların ve İnternet sitelerinin URL'leri

  E-dolandırıcılık saldırılarının hedefi banka kart numaraları, pasaport ayrıntıları, banka ödeme sistemlerinin parolaları ve diğer çevrimiçi hizmetler (sosyal ağ siteleri veya e-posta hesapları) gibi kullanıcıların kişisel verilerini çalmaktır.

Dosyalar, anlık ileti uygulamaları aracılığıyla aktarılabilir. Bu tür dosyalar kaydedilmeye teşebbüs edildiğinde dosyalar Dosya Koruması bileşeni tarafından taranır.

IM Koruması, kullanıcının bir anlık ileti uygulaması aracılığıyla gönderdiği veya aldığı her mesajın arasına girer ve mesajda bilgisayarın güvenliğini tehdit edebilecek bağlantıları tarar.

- Mesajda herhangi bir tehlikeli URL tespit edilmezse mesaj kullanıcı tarafından kullanılabilir hale gelir.
- Mesajda tehlikeli bağlantılar tespit edilirse IM Koruması mesajı, etkin anlık ileti uygulamasının mesaj penceresinde tehdit hakkındaki bilgi ile değiştirir.

IM Koruması'nı etkinleştirme ve devre dışı bırakma

Varsayılan olarak IM Koruması etkindir, Kaspersky uzmanları tarafından tavsiye edilen modda çalışmaktadır. Gerekirse IM Koruması'nı devre dışı bırakabilirsiniz.

Bileşeni etkinleştirmenin veya devre dışı bırakmanın iki yolu bulunmaktadır:

- Ana uygulama penceresinin **Koruma ve Denetim** sekmesinde
- Uygulama ayarları penceresinden.

Ana uygulama penceresinin Koruma ve Denetim sekmesinde IM Koruması'nı etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresini açın.
2. **Koruma ve Denetim** sekmesini seçin.
3. **Koruma** bölümüne tıklayın.
   Koruma bölümü açılır.
4. **IM Koruması** satırına sağ tıklayarak bileşen eylemlerinin içerik menüsünü görüntüleyin.
5. Aşağıdakilerden birini yapın:
   - IM Koruması'nı etkinleştirmek için içerik menüsünde **Başlat**'ı seçin.
     IM Koruması satırında solda görüntülenen bileşen durum simgesi , simgesine dönüşür.
   - IM Koruması'nı devre dışı bırakmak için içerik menüsünde **Durdur**'u seçin.
     IM Koruması satırında solda görüntülenen bileşen durum simgesi , simgesine dönüşür.

Uygulama ayarları penceresinden IM Koruması'nı etkinleştirmek veya devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **IM Koruması** alt bölümünü seçin.
   Pencerenin sağ kısmında, IM Koruması bileşeninin ayarları görüntülenir.
3. Aşağıdakilerden birini yapın:
   - IM Koruması'nı etkinleştirmek istiyorsanız **IM Koruması'nı Etkinleştir** onay kutusunu işaretleyin.
   - IM Koruması'nı devre dışı bırakmak istiyorsanız **IM Koruması'nı Etkinleştir** onay kutusunu işaretlemeyin.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

IM Koruması'nı Yapılandırma

IM Koruması'nı yapılandırmak için aşağıdaki eylemleri uygulayabilirsiniz:

- Koruma kapsamını yapılandırabilirsiniz.
  Taranan anlık ileti uygulaması mesajlarının türünü değiştirerek koruma kapsamını genişletebilir veya daraltabilirsiniz.
- Anlık ileti uygulamaları mesajlarındaki bağlantıların IM Koruması tarafından kötü amaçlı ve e-dolandırıcılık İnternet adreslerinin veritabanlarında taranmasını yapılandırabilirsiniz.

IM Koruması'nın koruma kapsamını oluşturma

Koruma kapsamı, etkinleştirildiği zaman bileşenin taradığı nesneleri ifade eder. Farklı bileşenlerin koruma kapsamları farklı özelliklere sahiptir. Taranan gelen veya giden IM istemci mesajlarının türü, IM Koruması kapsamının bir özelliğidir. Varsayılan olarak, IM Koruması gelen ve giden mesajların her ikisini de tarar. Giden trafiğin taranmasını devre dışı bırakabilirsiniz.

Koruma kapsamını oluşturmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **IM Koruması** alt bölümünü seçin.

   Pencerenin sağ kısmında, IM Koruması bileşeninin ayarları görüntülenir.
3. **Koruma kapsamı** bölümünde aşağıdakilerden birini yapın:
   - IM Koruması'nın IM istemcilerinin tüm gelen ve giden mesajlarını taramasını istiyorsanız **Gelen ve giden mesajlar** seçeneğini seçin.
   - IM Koruması'nın IM istemcilerinin yalnızca gelen mesajlarını taramasını istiyorsanız **Sadece gelen mesajlar** seçeneğini seçin.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

IM Koruması ile URL'lerin kötü amaçlı ve e-dolandırıcılık URL'lerinin veritabanlarında taranması

IM Koruması tarafından URL'lerin e-dolandırıcılık ve kötü amaçlı İnternet adreslerinin veritabanlarında taranmasını yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **IM Koruması** alt bölümünü seçin.

   Pencerenin sağ kısmında, IM Koruması bileşeninin ayarları görüntülenir.
3. **Tarama yöntemleri** bölümünde, IM Koruması'nın kullanmasını istediğiniz yöntemleri seçin:
   - Anlık ileti uygulamaları mesajlarındaki bağlantıların kötü amaçlı İnternet adreslerinin veritabanında taranmasını istiyorsanız **Bağlantıların zararlı bağlantılar veritabanında listelenip listelenmediğini denetle** onay kutusunu işaretleyin.
   - Anlık ileti uygulamaları mesajlarındaki bağlantıların e-dolandırıcılık İnternet adreslerinin veritabanında taranmasını istiyorsanız **Bağlantıların kimlik avı bağlantıları veritabanında listelenip listelenmediğini denetle** onay kutusunu işaretleyin.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Sistem İzleyici

Bu bileşen, İş istasyonları için Microsoft Windows'un kurulu olduğu bir bilgisayara Kaspersky Endpoint Security yüklendiğinde kullanılabilir. Bu bileşen, Dosya sunucuları için Microsoft Windows'un kurulu olduğu bir bilgisayara Kaspersky Endpoint Security yüklendiğinde kullanılamaz.

Bu bölümde, Sistem İzleyici hakkında bilgiler ve bileşen ayarlarının nasıl yapılandırılacağı hakkında talimatlar bulunmaktadır.

Sistem İzleyici hakkında

Sistem İzleyici, bilgisayarınızdaki uygulamaların eylemleriyle ilgili veri toplar ve bu bilgileri daha güvenilir koruma için diğer bileşenlere aktarır.

Davranış akımı imzaları

Davranış Akımı İmzaları (BSS) ("davranış akımı imzaları" olarak da adlandırılır) Kaspersky Endpoint Security'nin tehlikeli olarak sınıflandırdığı uygulama eylemleri dizisini içerir. Uygulama etkinliğinin bir davranış akımı imzası ile eşleşmesi halinde Kaspersky Endpoint Security belirtilen eylemi gerçekleştirir. Davranış akımı imzalarına dayanan Kaspersky Endpoint Security işlevi, bilgisayarınız için ileriye dönük etkili koruma sağlar.

Varsayılan olarak uygulama etkinliğinin bir davranış akımı imzası ile eşleşmesi halinde Sistem İzleyici, uygulamanın yürütülebilir dosyasını Karantina konumuna taşır.

Zararlı yazılımlar tarafından gerçekleştirilen eylemleri geri alma

Sistem İzleyici'nin topladığı bilgilere dayalı olarak Kaspersky Endpoint Security, temizlik gerçekleştirirken **işletim sisteminde zararlı yazılımlar tarafından gerçekleştirilen eylemleri geri alabilir**.

İşletim sistemindeki zararlı yazılım etkinliklerini geri alırken Kaspersky Endpoint Security, aşağıdaki zararlı yazılım türlerine işlem uygular.

- Dosya etkinliği.

  Kaspersky Endpoint Security, kötü amaçlı program tarafından oluşturulan ve ağ dışındaki herhangi bir ortamda bulunan yürütülebilir dosyaları siler.

  Kaspersky Endpoint Security, kötü amaçlı programın girdiği programın oluşturduğu yürütülebilir dosyaları siler.

  Kaspersky Endpoint Security, değiştirilen veya silinen dosyaları geri yüklemez.

- Kayıt defteri etkinliği.

  Kaspersky Endpoint Security, zararlı yazılımlar tarafından oluşturulan bölüm ve kayıt defteri anahtarlarını siler.

  Kaspersky Endpoint Security, değiştirilen veya silinen bölmeleri veya kayıt defteri anahtarlarını geri yüklemez.

- Sistem etkinliği.

  Kaspersky Endpoint Security, kötü amaçlı bir program tarafından başlatılan işlemleri sonlandırır.

  Kaspersky Endpoint Security, kötü amaçlı programın girdiği işlemleri sonlandırır.

  Kaspersky Endpoint Security, kötü amaçlı bir program tarafından durdurulan işlemleri sürdürmez.

- Ağ etkinliği.

  Kaspersky Endpoint Security, kötü amaçlı programların ağ etkinliğini engeller.

  Kaspersky Endpoint Security, kötü amaçlı programın girdiği işlemlerin ağ etkinliğini engeller.

Kötü amaçlı yazılım eylemlerini geri alma işlemi Dosya Koruması tarafından veya virüs taraması sırasında başlatılabilir.

Zararlı yazılımların işlemlerini geri almak, katı bir şekilde tanımlanan veri kümesini etkiler. Geri almanın işletim sistemi veya bilgisayar verilerinizin bütünlüğü üzerinde herhangi bir olumsuz etkisi olmaz.

Sistem İzleyici'nin etkinleştirilmesi ve devre dışı bırakılması

Varsayılan olarak Sistem İzleyici etkinleştirilmiştir ve Kaspersky tarafından önerilen modda çalışır. Gerekirse Sistem İzleyici'yi devre dışı bırakabilirsiniz.

Mutlaka gerekmedikçe Sistem İzleyici'nin devre dışı bırakılması önerilmez çünkü koruma bileşenlerinin performansı etkilenebilir. Koruma bileşenleri, tespit edilen bir tehdidin daha kesin tanımlanabilmesi için Sistem İzleyici tarafından toplanan verileri isteyebilir.

Sistem İzleyici'yi etkinleştirmenin veya devre dışı bırakmanın iki yolu bulunmaktadır:

- Ana uygulama penceresinin **Koruma ve Denetim** sekmesinde
- Uygulama ayarları penceresinden.

*Ana uygulama penceresinin **Koruma ve Denetim** sekmesinde Sistem İzleyici'yi etkinleştirmek veya devre dışı bırakmak için:*

1. Ana uygulama penceresini açın.
2. **Koruma ve Denetim** sekmesini seçin.
3. **Koruma** bölümüne tıklayın.
   Koruma bölümü açılır.
4. Sağ tıklayarak, Sistem İzleyici bileşeni hakkında bilgi içeren satırın içerik menüsünü açın.
   Bileşenlere uygulanacak eylemlerin seçilebileceği bir menü açılır.
5. Aşağıdakilerden birini yapın:
   - Sistem İzleyici'yi etkinleştirmek için **Başlat**'ı seçin.
     Sistem İzleyici satırında solda görüntülenen bileşen durumu simgesi , simgesine dönüşür.
   - Sistem İzleyici'yi devre dışı bırakmak için **Durdur**'u seçin.
     Sistem İzleyici satırında solda görüntülenen bileşen durumu simgesi , simgesine dönüşür.

Uygulama ayarları penceresinden Sistem İzleyici'yi etkinleştirmek veya devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Sistem İzleyici** alt bölümünü seçin.
   Pencerenin sağ kısmında, **Sistem İzleyici** bileşeni ayarları görüntülenir.
3. Aşağıdakilerden birini yapın:
   - Sistem İzleyici'yi etkinleştirmek için **Sistem İzleyici'yi Etkinleştir** onay kutusunu işaretleyin.
   - Sistem İzleyici'yi devre dışı bırakmak için **Sistem İzleyici'yi Etkinleştir** onay kutusunu işaretlemeyin.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Sistem İzleyici'yi Yapılandırma

Sistem İzleyici'yi yapılandırmak için aşağıdaki eylemleri gerçekleştirebilirsiniz:

- sömürüden korumayı etkinleştir veya devre dışı bırak
- bir programda kötü amaçlı etkinlik tespit edildiğinde yapılacak eylemi seçin;
- Temizlik sırasında kötü amaçlı yazılım eylemlerini geri almayı etkinleştirebilir ya da devre dışı bırakabilirsiniz.

Sömürüden korumayı etkinleştir veya devre dışı bırak

Sömürüden korumayı etkinleştirmek veya devre dışlı bırakmak için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Sistem İzleyici** alt bölümünü seçin.

   Pencerenin sağ kısmında, **Sistem İzleyici** bileşeni ayarları görüntülenir.

3. Aşağıdakilerden birini yapın:

   - Kaspersky Endpoint Security'nin güvenlik açığı bulunan programlar tarafından başlatılan dosyaları izlemesini isterseniz, **Sömürü Engellemeyi Etkinleştir** onay kutusunu seçin.

     Kaspersky Endpoint Security, güvenlik açığı olan olan bir program tarafından kullanılmakta olan bir dosyanın kullanıcı dışında bir şey tarafından başlatıldığını tespit ederse, **Tehdit algılama eylemi** açılır listesinden yaptığınız seçime göre hareket edecektir.

   - Kaspersky Endpoint Security'nin güvenlik açığı bulunan programlar tarafından başlatılan dosyaları izlemesini isterseniz, **Sömürü Engellemeyi Etkinleştir** onay kutusunu seçin.

4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Bir programda kötü amaçlı etkinlik tespit edilmesi durumunda eylemi seçin

Bir programın kötü amaçlı bir faaliyette bulunması durumunda ne yapılacağını seçmek için aşağıdaki adımları uygulayın:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Sistem İzleyici** alt bölümünü seçin.

   Pencerenin sağ kısmında, **Sistem İzleyici** bileşeni ayarları görüntülenir.

3. **Kötü amaçlı etkinlik tespit edilirse** açılır listesinden **Tehdit algılama eylemi** bölümünden aşağıdaki eylemi seçin:

   - **Eylemi otomatik olarak seç**.
   - **Dosyayı Karantinaya taşı**.
   - **Zararlı programı sonlandır**.
   - **Atla**.

4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Temizlik sırasında kötü amaçlı yazılım eylemlerini geri almayı etkinleştirme ve devre dışı bırakma

Temizlik sırasında kötü amaçlı yazılım eylemlerini geri almayı etkinleştirmek ya da devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Sistem İzleyici** alt bölümünü seçin.

   Pencerenin sağ kısmında, **Sistem İzleyici** bileşeni ayarları görüntülenir.

3. Aşağıdakilerden birini yapın:

- Kaspersky Endpoint Security'nin temizlik gerçekleştirirken işletim sisteminde zararlı yazılımların gerçekleştirdiği eylemleri geri almasını isterseniz **Temizleme sırasında kötü amaçlı yazılım eylemlerini geri al** onay kutusunu işaretleyin.

- Kaspersky Endpoint Security'nin temizlik gerçekleştirirken işletim sisteminde zararlı yazılımların gerçekleştirdiği eylemleri yok saymasını isterseniz **Temizleme sırasında kötü amaçlı yazılım eylemlerini geri al** onay kutusunu işaretlemeyin.

4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Güvenlik Duvarı

Bu bölümde, Güvenlik Duvarı hakkında bilgiler ve bileşen ayarlarının nasıl yapılandırılacağı hakkında talimatlar bulunmaktadır.

Güvenlik Duvarı Hakkında

LAN ve İnternet'te kullanım sırasında bilgisayar, işletim sistemlerinde ve yazılımlardaki zayıf noktaları kullanan virüslere, diğer zararlı yazılımlara ve çeşitli saldırılara maruz kalır.

Güvenlik duvarı, kullanıcının bilgisayarında depolanan kişisel verileri korur, bilgisayar İnternet'e veya bir yerel ağa bağlıyken işletim sistemine her türlü tehdidi engeller. Güvenlik duvarı, kullanıcının bilgisayarının bütün ağ bağlantılarını algılar ve varsayılan ağ bağlantısının durumunu belirterek IP adreslerinin bir listesini sağlar.

Güvenlik Duvarı bileşeni, ağ kurallarına göre bütün ağ etkinliğini filtreler. Ağ kurallarını yapılandırmak, bütün uygulamalar için İnternet erişimini engellemekten sınırsız erişime izin vermeye kadar istenen bilgisayar koruması düzeyini belirlemenize olanak tanır.

Güvenlik Duvarı'nın etkinleştirilmesi veya devre dışı bırakılması

Varsayılan olarak Güvenlik Duvarı etkinleştirilmiştir ve optimum modda çalışır. Gerekirse Güvenlik Duvarı'nı devre dışı bırakabilirsiniz.

Bileşeni etkinleştirmenin veya devre dışı bırakmanın iki yolu bulunmaktadır:

- Ana uygulama penceresinin **Koruma ve Denetim** sekmesinde
- Uygulama ayarları penceresinden.

Ana uygulama penceresinin Koruma ve Denetim sekmesinde Güvenlik Duvarı'nı etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresini açın.
2. **Koruma ve Denetim** sekmesini seçin.
3. **Koruma** bölümüne tıklayın.
   Koruma bölümü açılır.
4. Güvenlik Duvarı eylemlerinin içerik menüsünü açmak için **Güvenlik Duvarı** satırına sağ tıklayın.
5. Aşağıdakilerden birini yapın:
   - Güvenlik Duvarı'nı etkinleştirmek için içerik menüsünde **Başlat**'ı seçin.
     Güvenlik Duvarı satırında solda görüntülenen bileşen durumu simgesi , simgesine dönüşür.
   - Güvenlik Duvarı'nı devre dışı bırakmak için içerik menüsünden **Durdur**'u seçin.
     Güvenlik Duvarı satırında solda görüntülenen bileşen durumu simgesi , simgesine dönüşür.

Uygulama ayarları penceresinde Güvenlik Duvarı'nı etkinleştirmek veya devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Güvenlik Duvarı**'nı seçin.

   Pencerenin sağ kısmında, Güvenlik Duvarı bileşeninin ayarları görüntülenir.
3. Aşağıdakilerden birini yapın:
   - Güvenlik Duvarını etkinleştirmek için **Güvenlik Duvarı'nı Etkinleştir** onay kutusunu işaretleyin.
   - Güvenlik Duvarını devre dışı bırakmak için **Güvenlik Duvarı'nı Devre dışı bırak** onay kutusunu işaretleyin.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Ağ kuralları hakkında

Ağ kuralları, bir ağ bağlantısı girişimi algılanması üzerine Güvenlik Duvarı tarafından izin verilen veya engellenen eylemlerdir.

Güvenlik Duvarı, farklı türlerde ağ saldırılarına karşı iki düzeyde koruma sağlar: ağ düzeyi ve program düzeyi. Ağ düzeyinde koruma, ağ paketi kuralları uygulanarak sağlanır. Program düzeyinde koruma, kurulu uygulamaların ağ kaynaklarına erişebileceği kurallar uygulanarak sağlanır.

Güvenlik Duvarı korumasının iki düzeyine dayalı olarak, aşağıdakileri oluşturabilirsiniz:

- *Ağ paketi kuralları*. Ağ paketi kuralları, programa bakılmaksızın ağ paketlerine sınırlamalar getirir. Bu kurallar, seçilen veri iletişim kuralının belirli bağlantı noktaları yoluyla gelen ve giden ağ trafiğini sınırlar. Güvenlik Duvarı, varsayılan olarak belirli ağ paketi kuralları belirtir.
- *Uygulama ağ kuralları*. Uygulama ağı kuralları, belirli bir uygulamaya ağ etkinliği sınırlamaları getirir. Bunlar yalnızca ağ paketinin özelliklerini değil aynı zamanda bu ağ paketinin yönlendirildiği veya bu ağ paketini veren belirli uygulamayı da etkiler. Bu tür kurallar, ağ etkinliği filtrelemenin ince ayarını mümkün kılar: örneğin, bazı uygulamalar için belirli bir tür ağ bağlantısı engellenirken, bazılarına izin verilir.

Ağ paketi kuralları, uygulamalar için ağ kurallarından daha yüksek önceliğe sahiptir. Aynı tür ağ etkinliği için hem ağ paketi kuralları hem de uygulamalar için ağ kuralları belirtildiyse ağ etkinliği, ağ paketi kurallarına göre yürütülür.

Her bir ağ paketi kuralı ve her bir uygulamalar için ağ kuralı için yürütme önceliği belirtebilirsiniz.

Ağ paketi kuralları, uygulamalar için ağ kurallarından daha yüksek önceliğe sahiptir. Aynı tür ağ etkinliği için hem ağ paketi kuralları hem de uygulamalar için ağ kuralları belirtildiyse ağ etkinliği, ağ paketi kurallarına göre yürütülür.

Uygulamalar için ağ kuralları şu şekilde çalışır: uygulamalar için bir ağ kuralı, ağ durumuna göre erişim kuralları içerir: *genel*, *yerel* veya *güvenilir*. Örneğin, Yüksek Kısıtlamalı güvenilirlik grubundaki uygulamaların hiçbir ağ durumunda ağ etkinliği gerçekleştirmesine varsayılan olarak izin verilmez. Bir uygulama (üst uygulama) için bir ağ kuralı belirlendiğinde, diğer uygulamaların alt işlemleri üst uygulamanın ağ kuralına göre çalışır. Uygulama için herhangi bir ağ kuralı yoksa, alt işlemleri uygulamanın güvenilirlik grubunun ağ erişim kuralına göre çalışır.

Diyelim ki X tarayıcısı hariç tüm uygulamalar için tüm durumlardaki ağlarda herhangi bir ağ etkinliğini yasakladınız. Y tarayıcısının kurulumunu (alt işlem) X tarayıcısından (ana uygulama) başlatırsanız, Y tarayıcısının yükleyicisi ağa erişecek ve gerekli dosyaları indirecektir. Kurulum sonrasında, Y tarayıcısının her türlü ağ bağlantısı, Güvenlik Duvarı ayarlarına göre reddedilecektir. Y tarayıcısının bir alt işlem olarak ağ etkinliğini yasaklamak için Y tarayıcısının yükleyicisi için bir ağ kuralı eklemelisiniz.

Ağ bağlantısı durumu hakkında

Güvenlik Duvarı, kullanıcının bilgisayarındaki bütün ağ bağlantılarını denetler ve algılanan her bir ağ bağlantısına otomatik olarak bir durum atar.

Ağ bağlantısı, aşağıdaki durum türlerinden birine sahip olabilir:

- **Genel ağ**. Bu durum, herhangi bir anti-virüs uygulaması, güvenlik duvarı veya filtre tarafından korunmayan ağlar (örneğin, İnternet kafe ağları) içindir. Kullanıcı böyle bir ağa bağlı bir bilgisayarda çalışırken Güvenlik Duvarı, bu bilgisayarın dosyalarına ve yazıcılarına erişimi engeller. Dışarıdan kullanıcılar, paylaşım klasörleri ve bu bilgisayarın masaüstüne uzaktan erişim aracılığıyla da verilere erişemez. Güvenlik duvarı, kendisi için ayarlanan ağ kurallarına göre her uygulamanın ağ etkinliğini filtreler.

  Güvenlik duvarı varsayılan olarak İnternet'e *Genel ağ* durumunu atar. İnternet'in durumunu değiştiremezsiniz.

- **Yerel ağ**. Bu durum, bu bilgisayardaki dosyalara ve yazıcılara erişimine güvenilen kullanıcıların ağlarına atanır (örneğin, bir LAN veya ev ağı).

- **Güvenilir ağ**. Bu durum, bilgisayarın saldırılara veya yetkisiz veri erişim girişimlerine açık olmadığı güvenli bir ağ içindir. Güvenlik Duvarı, bu durumdaki ağlarda her tür ağ etkinliğine izin verir.

Ağ bağlantısı durumunu değiştirme

Ağ bağlantısı durumunu değiştirmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Güvenlik Duvarı** alt bölümünü seçin.

   Pencerenin sağ kısmında, Güvenlik Duvarı bileşeninin ayarları görüntülenir.
3. **Kullanılabilir ağlar** düğmesine tıklayın.

   Güvenlik Duvarı penceresi açılır.
4. Durumunu değiştirmek istediğiniz ağ bağlantısını seçin.
5. İçerik menüsünde ağ bağlantısı durumu'nu seçin:
   - **Ortak ağ**.
   - **Yerel ağ**.
   - **Güvenilir ağ**.
6. **Güvenlik Duvarı** penceresinde **Tamam**'a tıklayın.
7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Ağ paketi kurallarını yönetme

Ağ paketi kurallarını yönetirken aşağıdaki eylemleri yapabilirsiniz:

- Yeni bir ağ paketi kuralı oluşturabilirsiniz.

  Ağ paketlerine ve veri akışlarına uygulanan bir koşul ve eylem dizisi oluşturarak yeni bir ağ paketi oluşturabilirsiniz.

- Bir ağ paketi kuralını etkinleştirebilir veya devre dışı bırakabilirsiniz.

  Güvenlik Duvarı tarafından varsayılan olarak oluşturulan bütün ağ paketi kuralları *Etkinleştirildi* durumundadır. Bir ağ paketi kuralı etkinleştirildiğinde Güvenlik Duvarı bu kuralı uygular.

  Ağ paketi kuralları listesinde seçilen herhangi bir ağ paketi kuralını devre dışı bırakabilirsiniz. Bir ağ paketi kuralı devre dışı bırakıldığında Güvenlik Duvarı, bu kuralı geçici olarak uygulamaz.

  > Ağ paketi kuralları listesine varsayılan olarak *Etkinleştirildi* durumunda yeni özel bir ağ paketi kuralı eklenir.

- Mevcut bir ağ paketi kuralının ayarlarını düzenleyebilirsiniz.

  Bir ağ paketi kuralı oluşturduktan sonra her zaman dönüp ayarlarını düzenleyebilir ve gerektiği gibi değiştirebilirsiniz.

- Bir ağ paketi kuralı için Güvenlik Duvarı eylemini değiştirebilirsiniz.

  Ağ paketi kuralları listesinde, belirli bir ağ paketi kuralıyla eşleşen ağ etkinliği algılandığında Güvenlik Duvarı tarafından yapılan eylemi düzenleyebilirsiniz.

- Bir ağ paketi kuralının önceliğini değiştirebilirsiniz.

  Listede seçilen bir ağ paketi kuralının önceliğini arttırabilir ya da düşürebilirsiniz.

- Bir ağ paketi kuralını kaldırabilirsiniz.

  Güvenlik Duvarı'nın ağ etkinliği algıladığında kuralı uygulamasını durdurmak ve bu kuralın *Devre dışı bırakıldı* durumundaki ağ paketi kuralları listesinde görülmesini önlemek için bir ağ paketi kuralını kaldırabilirsiniz.

Ağ paketi kuralı oluşturma ve düzenleme

> Ağ paketi kurallarını oluştururken bunların uygulamaların ağ kurallarından daha öncelikli olduğunu unutmayın.

Ağ paketi kuralı oluşturmak veya düzenlemek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Güvenlik Duvarı**'nı seçin.
3. **Ağ paketi kuralları** düğmesine tıklayın.
4. **Güvenlik Duvarı** penceresi, **Ağ paketi kuralları** sekmesini açar.

   Bu sekmede, Güvenlik Duvarı tarafından belirlenen varsayılan ağ paketi kurallarının listesi görüntülenir.
5. Aşağıdakilerden birini yapın:

   - Yeni bir ağ paketi kuralı oluşturmak için **Ekle** düğmesine tıklayın.

- Bir ağ paketi kuralını düzenlemek için, ağ paketi kurallarının listesinde seçin ve **Düzenle** düğmesine tıklayın.

Ağ kuralı penceresi açılır.

6. **Eylem** açılır listesinde, bu ağ etkinliği tespit edildiğinde Güvenlik Duvarı tarafından gerçekleştirilecek eylemi seçin:
   - **İzin ver**
   - **Engelle**
   - **Uygulama kurallarına göre**.
7. **Ad** alanında, ağ hizmeti adını aşağıdaki yollardan biriyle belirtin:
   - **Ad** alanının sağındaki simgesine tıklayın ve açılır listeden ağ hizmetinin adını seçin.
     Açılır listede, en sık kullanılan ağ bağlantılarını tanımlayan ağ hizmetleri yer alır.
   - Ağ hizmetinin adını **Ad** alanına elle girin.
8. Veri aktarımı iletişim kuralını belirtin:
   a. **İletişim kuralı** onay kutusunu seçin.
   b. Açılır listeden, ağ etkinliğinin izleneceği iletişim kuralı türünü seçin.
      Güvenlik Duvarı; TCP, UDP, ICMP, ICMPv6, IGMP ve GRE iletişim kurallarını kullanan ağ bağlantılarını izler.
      Ad açılır listesinden bir ağ hizmeti seçerseniz, **İletişim kuralı** onay kutusu otomatik olarak seçilir ve onay kutusunun karşısındaki açılı listede seçilen ağ hizmetine denk gelen iletişim kuralı türü yer alır. Varsayılan olarak **İletişim kuralı** onay kutusu işaretli değildir.
9. **Yön** açılır listesinde, izlenen ağ etkinliği yönünü seçin.
   Güvenlik Duvarı aşağıdaki yönlerde ağ bağlantılarını izler:
   - **Gelen (paket)**.
   - **Gelen**.
   - **Gelen/Giden**
   - **Giden (paket)**.
   - **Giden**.
10. İletişim kuralı olarak ICMP veya ICMPv6 seçilirse, ICMP paket türünü ve kodunu belirtebilirsiniz:
    a. **ICMP biçimi** onay kutusunu işaretleyin ve açılır listede ICMP paket türünü seçin.
    b. **ICMP kodu** onay kutusunu işaretleyin ve açılır listede ICMP paket kodunu seçin.
11. İletişim kuralı türü olarak TCP veya UDP seçilirse, arasındaki bağlantının izleneceği yerel ve uzak bilgisayarların virgülle ayrılmış bağlantı noktası numaralarını belirtebilirsiniz:
    a. Uzak bilgisayarın bağlantı noktalarını **Uzak bağlantı noktaları** alanına yazın.
    b. Yerel bilgisayarın bağlantı noktalarını **Yerel bağlantı noktaları** alanına yazın.

12. **Ağ bağdaştırıcıları** tablosunda, ağ paketlerinin gönderileceği veya ağ paketlerini alabilecek ağ bağdaştırıcılarının ayarlarını belirtin. Bunun için **Ekle**, **Düzenle** ve **Sil** düğmelerini kullanın.

13. Ağ paketlerinin denetimini yaşama süresine (TTL) göre sınırlamak isterseniz **TTL** onay kutusunu işaretleyin ve yanındaki alana, gelen ve/veya giden ağ paketlerinin yaşama süresi değerlerinin aralığını belirtin.

    Ağ kuralı, yaşama süresi belirtilen değeri aşmayan ağ paketlerinin aktarımını denetler.

    İstemiyorsanız **TTL** onay kutusunun işaretini kaldırın.

14. Ağ paketlerini alabilecek ve/veya gönderebilecek uzak bilgisayarların ağ adreslerini belirtin. Bunun için **Uzak adresler** açılır listesindeki aşağıdaki değerlerden birini seçin:

    - **Her adres**. Ağ kuralı, herhangi bir IP adresine sahip uzak bilgisayarlar tarafından gönderilen ve/veya alınan ağ paketlerini denetler.
    - **Alt ağ adresleri**. Ağ kuralı, seçilen ağ türüyle ilişkilendirilen IP adreslerine sahip uzak bilgisayarlar tarafından gönderilen ve/veya alınan ağ paketlerini denetler: **Güvenilir ağlar**, **Yerel ağlar** veya **Genel ağlar**.
    - **Listeden adresler**. Ağ kuralı, aşağıdaki **Ekle**, **Düzenle** ve **Sil** düğmelerini kullanarak listede belirtilebilecek olan IP adreslerine sahip uzak bilgisayar tarafından gönderilen ve/veya alınan ağ paketlerini denetler.

15. Kaspersky Endpoint Security'nin yüklü olduğu ve ağ paketlerini alabilecek ve/veya gönderebilecek bilgisayarların ağ adreslerini belirtin. Bunun için **Yerel adresler** açılır listesindeki aşağıdaki değerlerden birini seçin:

    - **Her adres**. Ağ kuralı, herhangi bir IP adresine sahip ve Kaspersky Endpoint Security'nin yüklü olduğu bilgisayarlar tarafından gönderilen ve/veya alınan ağ paketlerini denetler.
    - **Listeden adresler**. Ağ kuralı, aşağıdaki **Ekle**, **Düzenle** ve **Sil** düğmelerini kullanarak listede belirtilebilecek olan IP adreslerine sahip ve Kaspersky Endpoint Security'nin yüklü olduğu uzak bilgisayarlar tarafından gönderilen ve/veya alınan ağ paketlerini denetler.

    Bazen ağ paketleri ile çalışan uygulamalar için bir yerel adres alınamaz. Bu durumda, **Yerel adresler** ayar değeri gözardı edilir.

16. Ağ kuralı eylemlerinin rapora yansımasını istiyorsanız **Olayı kaydet** onay kutusunu işaretleyin.

17. **Ağ kuralı** penceresinde **Tamam**'a tıklayın.

    Yeni bir ağ kuralı oluşturursanız kural, **Güvenlik Duvarı** penceresinin **Ağ paketi kuralları** sekmesinde görüntülenir. Varsayılan olarak yeni ağ kuralı, ağ paketi kuralları tarafından listenin sonuna eklenir.

18. **Güvenlik Duvarı** penceresinde **Tamam**'a tıklayın.

19. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Ağ paketi kuralını etkinleştirme veya devre dışı bırakma

Bir ağ paketi kuralını etkinleştirmek veya devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Güvenlik Duvarı** alt bölümünü seçin.

   Pencerenin sağ kısmında, Güvenlik Duvarı bileşeninin ayarları görüntülenir.

3. **Ağ paketi kuralları** düğmesine tıklayın.
   Güvenlik Duvarı penceresi, **Ağ paketi kuralları** sekmesini açar.
4. Listede gerekli ağ paketi kuralını seçin.
5. Aşağıdakilerden birini yapın:
   - Kuralı etkinleştirmek için ağ paketi kuralının adının yanındaki onay kutusunu işaretleyin.
   - Kuralı devre dışı bırakmak için ağ paketi kuralının adının yanındaki onay kutusunu işaretlemeyin.
6. **Tamam**'a tıklayın.
7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Ağ paketi kuralı için Güvenlik Duvarı eylemini değiştirme

Ağ paketi kuralına uygulanan Güvenlik Duvarı eylemini değiştirmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Güvenlik Duvarı** alt bölümünü seçin.
   Pencerenin sağ kısmında, Güvenlik Duvarı bileşeninin ayarları görüntülenir.
3. **Ağ paketi kuralları** düğmesine tıklayın.
   Güvenlik Duvarı penceresi, **Ağ paketi kuralları** sekmesini açar.
4. Listede eylemini değiştirmek istediğiniz ağ paketi kuralını seçin.
5. **İzin** sütununda sağ tıklayarak içerik menüsünü açın ve atamak istediğiniz eylemi seçin.
   - **İzin ver**
   - **Engelle**
   - **Uygulama kuralına göre**
   - **Olayları günlüğe kaydet**
6. **Güvenlik Duvarı** penceresinde **Tamam**'a tıklayın.
7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Ağ paketi kuralının önceliğini değiştirme

Bir ağ paketi kuralının önceliği, ağ paketi kuralları listesindeki konumuna göre belirlenir. Ağ paketi kuralları listesinin en üstündeki ağ paketi kuralı en yüksek önceliğe sahiptir.

Elle oluşturulan her ağ paketi kuralı, ağ paketi kuralları listesinin sonuna eklenir ve en düşük önceliğe sahiptir.

Güvenlik duvarı, kuralları ağ paketi kuralları listesindeki görünüm sırasına göre yukarıdan aşağıya doğru yürütür. Belirli bir ağ bağlantısına uygulanan her işlenmiş ağ paketi kuralına göre, Güvenlik Duvarı bu ağ bağlantısının ayarlarında belirtilen adrese ve bağlantı noktasına ağ erişimine izin verir veya engeller.

Ağ paketi kuralının önceliğini değiştirmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Güvenlik Duvarı** alt bölümünü seçin.

   Pencerenin sağ kısmında, Güvenlik Duvarı bileşeninin ayarları görüntülenir.
3. **Ağ paketi kuralları** düğmesine tıklayın.

   Güvenlik Duvarı penceresi, **Ağ paketi kuralları** sekmesini açar.
4. Listede önceliğini değiştirmek istediğiniz ağ paketi kuralını seçin.
5. Ağ paketi kuralını, ağ paketi kuralları listesinde istenen noktaya taşımak için **Yukarı taşı** ve **Aşağı taşı** düğmelerini kullanın.
6. **Tamam**'a tıklayın.
7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Uygulama ağ kurallarını yönetme

Varsayılan olarak Kaspersky Endpoint Security, bilgisayarda yüklü olan tüm uygulamaları, dosya veya ağ etkinliğini izlediği yazılımın satıcısının adına göre gruplandırır. Uygulama grupları da güven grupları kategorilerine ayırılır. Tüm uygulamalar ve uygulama grupları üst grubunun özelliklerini devralır: uygulama denetimi kuralları, uygulama ağ kuralları ve yürütülme öncelikleri.

Varsayılan olarak Güvenlik Duvarı bileşeni, Uygulama Ayrıcalık Denetimi bileşenine benzer şekilde, grup içindeki tüm uygulamaların ağ etkinliğini filtrelerken bir uygulama grubu için ağ kurallarını uygular. Uygulama grubu ağ kuralları, grup içindeki uygulamaların farklı ağ bağlantılarına erişim haklarını tanımlar.

Varsayılan olarak Güvenlik Duvarı, Kaspersky Endpoint Security tarafından bilgisayarda tespit edilen her uygulama grubu için bir ağ kuralları seti oluşturur. Varsayılan olarak oluşturulan uygulama grubu ağ kurallarının uygulandığı Güvenlik Duvarı eylemini değiştirebilirsiniz. Varsayılan olarak oluşturulan uygulama grubu ağ kurallarının önceliğini düzenleyemez, kaldıramaz, devre dışı bırakamaz veya değiştiremezsiniz.

Ayrıca tek bir uygulama için bir ağ kuralı oluşturabilirsiniz. Bu tür bir kural, uygulamanın ait olduğu grubun ağ kuralından daha yüksek bir önceliğe sahip olacaktır.

Uygulamanın ağ kurallarını yönetirken aşağıdaki eylemleri yapabilirsiniz:

- Yeni bir ağ kuralı oluşturabilirsiniz.

  Güvenlik Duvarı'nın uygulamanın ve seçilen uygulamalar grubuna giren uygulamaların ağ etkinliğini düzenlerken uyacağı yeni bir ağ kuralı oluşturabilirsiniz.
- Bir ağ kuralını etkinleştirebilir veya devre dışı bırakabilirsiniz.

  Tüm ağ kuralları uygulamaların ağ kuralları listesine *Etkinleştirildi* durumu ile eklenir. Bir ağ kuralı etkinleştirildiyse Güvenlik Duvarı bu kuralı uygular.

Elle oluşturulan bir ağ kuralını devre dışı bırakabilirsiniz. Bir ağ kuralı devre dışı bırakılırsa Güvenlik Duvarı bu kuralı geçici olarak uygulamaz.

- Bir ağ kuralının ayarını değiştirebilirsiniz.

  Yeni bir ağ kuralı oluşturduktan sonra, her zaman ayarlarına dönebilir ve gerektiği gibi değiştirebilirsiniz.

- Bir ağ kuralı için Güvenlik Duvarı eylemini değiştirebilirsiniz.

  Ağ kuralları listesinde, bu uygulamada veya uygulama grubunda ağ etkinliği tespit edilmesi üzerine Güvenlik Duvarı'nın ağ kuralı için uyguladığı eylemi düzenleyebilirsiniz.

- Bir ağ kuralının önceliğini değiştirebilirsiniz.

  Özel bir ağ kuralının önceliğini yükseltebilir veya düşürebilirsiniz.

- Bir ağ kuralını silebilirsiniz.

  Güvenlik Duvarı'nın ağ etkinliği tespit edilmesi üzerine bu ağ kuralını seçilen uygulamaya veya uygulama grubuna uygulamasını durdurmak ve bu kuralın uygulama ağ kuralları listesinde görüntülenmesini durdurmak için özel ağ kuralını silebilirsiniz.

Uygulama ağ kuralı oluşturma ve düzenleme

Bir uygulama grubunun ağ kuralını oluşturmak veya düzenlemek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Güvenlik Duvarı** alt bölümünü seçin.
3. **Uygulama ağ kuralları** düğmesine tıklayın.

   Güvenlik Duvarı penceresi, **Uygulama denetimi kuralları** sekmesini açar.
4. Uygulamalar listesinde, ağ kuralını oluşturmak veya düzenlemek istediğiniz uygulamayı veya uygulamalar grubunu seçin.
5. Sağ tıklayarak içerik menüsünü açın ve ne yapmanız gerektiğine bağlı olarak **Uygulama kuralları** veya **Grup kuralları**'nı seçin.

   Uygulama denetimi kuralları veya **Uygulama grubu denetim kuralları** penceresi açılır.
6. Açılan pencerede, **Ağ kuralları** sekmesini seçin.
7. Aşağıdakilerden birini yapın:

   - Yeni bir ağ kuralı oluşturmak için **Ekle** düğmesine tıklayın.
   - Bir ağ kuralını düzenlemek için, ağ kurallarının listesinde seçin ve **Düzenle** düğmesine tıklayın.

   Ağ kuralı penceresi açılır.
8. **Eylem** açılır listesinde, bu ağ etkinliği tespit edildiğinde Güvenlik Duvarı tarafından gerçekleştirilecek eylemi seçin:

   - **İzin ver**

- **Engelle**

9. **Ad** alanında, ağ hizmeti adını aşağıdaki yollardan biriyle belirtin:

   - **Ad** alanının sağındaki simgesine tıklayın ve açılır listeden ağ hizmetinin adını seçin.

     Açılır listede, en sık kullanılan ağ bağlantılarını tanımlayan ağ hizmetleri yer alır.

   - Ağ hizmetinin adını **Ad** alanına elle girin.

10. Veri aktarımı iletişim kuralını belirtin:

    a. **İletişim kuralı** onay kutusunu seçin.

    b. Açılır listeden, ağ etkinliğinin izleneceği iletişim kuralı türünü seçin.

    Güvenlik Duvarı; TCP, UDP, ICMP, ICMPv6, IGMP ve GRE iletişim kurallarını kullanan ağ bağlantılarını izler.

    Ad açılır listesinden bir ağ hizmeti seçerseniz, **İletişim kuralı** onay kutusu otomatik olarak seçilir ve onay kutusunun karşısındaki açılı listede seçilen ağ hizmetine denk gelen iletişim kuralı türü yer alır. Varsayılan olarak **İletişim kuralı** onay kutusu işaretli değildir.

11. **Yön** açılır listesinde, izlenen ağ etkinliği yönünü seçin.

    Güvenlik Duvarı aşağıdaki yönlerde ağ bağlantılarını izler:

    - **Gelen**.
    - **Gelen/Giden**.
    - **Giden**.

12. İletişim kuralı olarak ICMP veya ICMPv6 seçilirse, ICMP paket türünü ve kodunu belirtebilirsiniz:

    a. **ICMP biçimi** onay kutusunu işaretleyin ve açılır listede ICMP paket türünü seçin.

    b. **ICMP kodu** onay kutusunu işaretleyin ve açılır listede ICMP paket kodunu seçin.

13. İletişim kuralı türü olarak TCP veya UDP seçilirse, arasındaki bağlantının izleneceği yerel ve uzak bilgisayarların virgülle ayrılmış bağlantı noktası numaralarını belirtebilirsiniz:

    a. Uzak bilgisayarın bağlantı noktalarını **Uzak bağlantı noktaları** alanına yazın.

    b. Yerel bilgisayarın bağlantı noktalarını **Yerel bağlantı noktaları** alanına yazın.

14. Ağ paketlerini alabilecek ve/veya gönderebilecek uzak bilgisayarların ağ adreslerini belirtin. Bunun için **Uzak adresler** açılır listesindeki aşağıdaki değerlerden birini seçin:

    - **Her adres**. Ağ kuralı, herhangi bir IP adresine sahip uzak bilgisayarlar tarafından gönderilen ve/veya alınan ağ paketlerini denetler.
    - **Alt ağ adresleri**. Ağ kuralı, seçilen ağ türüyle ilişkilendirilen IP adreslerine sahip uzak bilgisayarlar tarafından gönderilen ve/veya alınan ağ paketlerini denetler: **Güvenilir ağlar**, **Yerel ağlar** veya **Genel ağlar**.
    - **Listeden adresler**. Ağ kuralı, aşağıdaki **Ekle**, **Düzenle** ve **Sil** düğmelerini kullanarak listede belirtilebilecek olan IP adreslerine sahip uzak bilgisayar tarafından gönderilen ve/veya alınan ağ paketlerini denetler.

15. Kaspersky Endpoint Security'nin yüklü olduğu ve ağ paketlerini alabilecek ve/veya gönderebilecek bilgisayarların ağ adreslerini belirtin. Bunun için **Yerel adresler** açılır listesindeki aşağıdaki değerlerden birini seçin:

- **Her adres**. Ağ kuralı, herhangi bir IP adresine sahip ve Kaspersky Endpoint Security'nin yüklü olduğu bilgisayarlar tarafından gönderilen ve/veya alınan ağ paketlerini denetler.
- **Listeden adresler**. Ağ kuralı, aşağıdaki **Ekle**, **Düzenle** ve **Sil** düğmelerini kullanarak listede belirtilebilecek olan IP adreslerine sahip ve Kaspersky Endpoint Security'nin yüklü olduğu uzak bilgisayarlar tarafından gönderilen ve/veya alınan ağ paketlerini denetler.

Bazen ağ paketleri ile çalışan uygulamalar için bir yerel adres alınamaz. Bu durumda, **Yerel adresler** ayar değeri gözardı edilir.

16. Ağ kuralı eylemlerinin rapora yansımasını istiyorsanız **Olayı kaydet** onay kutusunu işaretleyin.
17. **Ağ kuralı** penceresinde **Tamam**'a tıklayın.

    Yeni bir ağ kuralı oluşturursanız kural, **Ağ kuralları** sekmesinde görüntülenir.
18. Kurallar bir grup uygulama içinse **Uygulama grubu denetim kuralları** penceresinde ya da kural bir uygulama içinse **Uygulama denetimi kuralları** penceresinde **Tamam** düğmesine tıklayın.
19. **Güvenlik Duvarı** penceresinde **Tamam**'a tıklayın.
20. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Uygulama ağ kuralını etkinleştirme veya devre dışı bırakma

Bir uygulama ağ kuralını etkinleştirmek veya devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Güvenlik Duvarı** alt bölümünü seçin.

   Pencerenin sağ kısmında, Güvenlik Duvarı bileşeninin ayarları görüntülenir.
3. **Uygulama ağ kuralları** düğmesine tıklayın.

   Güvenlik Duvarı penceresi, **Uygulama denetimi kuralları** sekmesini açar.
4. Listede, ağ kuralını etkinleştirmek veya devre dışı bırakmak istediğiniz uygulamayı veya uygulamalar grubunu seçin.
5. Sağ tıklayarak içerik menüsünü açın ve ne yapmanız gerektiğine bağlı olarak **Uygulama kuralları** veya **Grup kuralları**'nı seçin.

   Uygulama denetimi kuralları veya **Uygulama grubu denetim kuralları** penceresi açılır.
6. Açılan pencerede, **Ağ kuralları** sekmesini seçin.
7. Uygulama grubu için ağ kuralları listesinde ilgili ağ kuralını seçin.
8. Aşağıdakilerden birini yapın:
   - Kuralı etkinleştirmek isterseniz ağ kuralının adının yanındaki onay kutusunu işaretleyin.
   - Kuralı devre dışı bırakmak isterseniz ağ kuralının adının yanındaki onay kutusunu işaretlemeyin.

Varsayılan olarak Güvenlik Duvarı tarafından oluşturulan uygulama grubu ağ kuralını devre dışı bırakamazsınız.

9. Kurallar bir grup uygulama içinse **Uygulama grubu denetim kuralları** penceresinde ya da kural bir uygulama içinse **Uygulama denetimi kuralları** penceresinde **Tamam** düğmesine tıklayın.
10. **Güvenlik Duvarı** penceresinde **Tamam**'a tıklayın.
11. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Ağ kuralı için Güvenlik Duvarı eylemini değiştirme

Varsayılan olarak oluşturulan bir uygulama veya uygulama grubunun tüm ağ kurallarına uygulanan Güvenlik Duvarı eylemini değiştirebilirsiniz, ayrıca bir uygulama veya uygulama grubunun tek bir özel ağ kuralı için Güvenlik Duvarı eylemini değiştirebilirsiniz.

Bir uygulama veya uygulama grubunun tüm ağ kurallarında Güvenlik Duvarı eylemini değiştirmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Güvenlik Duvarı** alt bölümünü seçin.
   Pencerenin sağ kısmında, Güvenlik Duvarı bileşeninin ayarları görüntülenir.
3. **Uygulama ağ kuralları** düğmesine tıklayın.
   Güvenlik Duvarı penceresi, **Uygulama denetimi kuralları** sekmesini açar.
4. Varsayılan olarak oluşturulan tüm ağ kurallarına uygulanan Güvenlik Duvarı eylemini değiştirmek isterseniz listede bir uygulama veya uygulama grubu seçin. Elle oluşturulan ağ kuralları değiştirilmeden kalır.
5. **Ağ** sütununda içerik menüsünü görüntülemek için tıklayın ve atamak istediğiniz eylemi seçin.
   - **Devral**
   - **İzin ver**
   - **Engelle**
6. **Tamam**'a tıklayın.
7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Bir uygulama veya uygulama grubunun tek ağ kuralına Güvenlik Duvarı yanıtını değiştirmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Güvenlik Duvarı**'nı seçin.
   Pencerenin sağ kısmında, Güvenlik Duvarı bileşeninin ayarları görüntülenir.
3. **Uygulama ağ kuralları** düğmesine tıklayın.
   Güvenlik Duvarı penceresi, **Uygulama denetimi kuralları** sekmesini açar.

4. Listede, tek ağ kuralı için değiştirmek istediğiniz uygulamayı veya uygulamalar grubunu seçin.

5. Sağ tıklayarak içerik menüsünü açın ve ne yapmanız gerektiğine bağlı olarak **Uygulama kuralları** veya **Grup kuralları**'nı seçin.

   Uygulama denetimi kuralları veya **Uygulama grubu denetim kuralları** penceresi açılır.

6. Açılan pencerede, **Ağ kuralları** sekmesini seçin.

7. Güvenlik Duvarı eylemini değiştirmek istediğiniz ağ kuralını seçin.

8. **İzin** sütununda sağ tıklayarak içerik menüsünü açın ve atamak istediğiniz eylemi seçin.

   - **İzin ver**
   - **Engelle**
   - **Olayları günlüğe kaydet**

9. Kurallar bir grup uygulama içinse **Uygulama grubu denetim kuralları** penceresinde ya da kural bir uygulama içinse **Uygulama denetimi kuralları** penceresinde **Tamam** düğmesine tıklayın.

10. **Güvenlik Duvarı** penceresinde **Tamam**'a tıklayın.

11. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Ağ kuralının önceliğini değiştirme

Bir ağ kuralının önceliği, ağ kuralları listesindeki konumuna göre belirlenir. Güvenlik duvarı, ağ kuralları listesindeki sırasına göre kuralları yukarıdan aşağıya doğru yürütür. Belirli bir ağ bağlantısına uygulanan her işlenmiş ağ kuralına göre, Güvenlik Duvarı bu ağ bağlantısının ayarlarında belirtilen adrese ve bağlantı noktasına ağ erişimine izin verir veya engeller.

Elle oluşturulan ağ kuralları varsayılan ağ kurallarından daha yüksek önceliğe sahiptir.

Varsayılan olarak oluşturulan uygulama grubu ağ kurallarının önceliğini değiştiremezsiniz.

Bir ağ kuralının önceliğini değiştirmek için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Güvenlik Duvarı** alt bölümünü seçin.

   Pencerenin sağ kısmında, Güvenlik Duvarı bileşeninin ayarları görüntülenir.

3. **Uygulama ağ kuralları** düğmesine tıklayın.

   Güvenlik Duvarı penceresi, **Uygulama denetimi kuralları** sekmesini açar.

4. Uygulamalar listesinde, ağ kuralı önceliğini değiştirmek istediğiniz uygulamayı veya uygulamalar grubunu seçin.

5. Sağ tıklayarak içerik menüsünü açın ve ne yapmanız gerektiğine bağlı olarak **Uygulama kuralları** veya **Grup kuralları**'nı seçin.

   Uygulama denetimi kuralları veya **Uygulama grubu denetim kuralları** penceresi açılır.

6. Açılan pencerede, **Ağ kuralları** sekmesini seçin.
7. Önceliğini değiştirmek istediğiniz ağ kuralını seçin.
8. Ağ kuralını, ağ kuralları listesinde istenen noktaya taşımak için **Yukarı taşı** ve **Aşağı taşı** düğmelerini kullanın.
9. Kurallar bir grup uygulama içinse **Uygulama grubu denetim kuralları** penceresinde ya da kural bir uygulama içinse **Uygulama denetimi kuralları** penceresinde **Tamam** düğmesine tıklayın.
10. **Güvenlik Duvarı** penceresinde **Tamam**'a tıklayın.
11. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Ağ İzleyicisi

Bu bölüm, Ağ İzleyicisi ve Ağ İzleyicisini başlatmak için talimatlar hakkında bilgi içermektedir.

Ağ İzleyicisini Hakkında

Ağ İzleyicisi, bir bilgisayarın ağ etkinliği hakkında gerçek zamanlı bilgi görüntülemek için tasarlanmış bir araçtır.

Ağ İzleyicisini Başlatma

Ağ İzleyicisini başlatmak için:

1. Ana uygulama penceresini açın.
2. **Koruma ve Denetim** sekmesini seçin.
3. **Koruma** bölümüne tıklayın.

   Koruma bölümü açılır.
4. Güvenlik Duvarı işlemlerinin içerik menüsünü açmak için **Güvenlik Duvarı** satırına sağ tıklayın.
5. İçerik menüsünde **Ağ İzleyicisi**'ni seçin.

   Ağ İzleyicisi penceresi açılır. Bu pencerede, bilgisayarın ağ etkinliğiyle ilgili bilgiler dört sekmede görüntülenir:

   - **Ağ etkinliği** sekmesinde, bilgisayardaki etkin tüm ağ bağlantıları görüntülenir. Hem giden hem de gelen ağ bağlantıları görüntülenir.
   - **Açık bağlantı noktaları** sekmesinde, bilgisayarın açık bağlantı noktalarının tamamı listelenir.
   - **Ağ trafiği** sekmesinde, kullanıcının bilgisayarı ile kullanıcının bağlandığı ağdaki diğer bilgisayarlar arasındaki gelen ve giden ağ trafiği hacmi görüntülenir.
   - **Engellenen bilgisayarlar** sekmesinde, IP adreslerinden ağ saldırısı denemelerinin tespit edilmesinin ardından Ağ Saldırısı Engelleyici tarafından ağ etkinliği engellenen uzak bilgisayarların IP adresleri listelenir.

Ağ Saldırısı Engelleyici

Bu bölümde, Ağ Saldırısı Engelleyici hakkında bilgiler ve bileşen ayarlarının yapılandırılmasına ilişkin talimatlar bulunmaktadır.

Ağ Saldırısı Engelleyici Hakkında

Ağ Saldırısı Engelleyici, gelen ağ trafiğinde ağ saldırılarında tipik olarak görülen etkinliği tarar. Bilgisayarınızı hedefleyen ağ saldırısı denemesinin tespit edilmesinin ardından Kaspersky Endpoint Security, saldıran bilgisayardan tüm ağ etkinliğini engeller. Ardından ekranınızda bir ağ saldırısı girişimi olduğunu belirten bir uyarı görüntülenir ve saldıran bilgisayar hakkında bilgi gösterir.

Saldıran bilgisayardan ağ trafiği bir saat boyunca engellenir. Saldıran bir bilgisayarı engellemek için ayarları düzenleyebilirsiniz.

Şu anda bilinen ağ saldırısı türlerinin açıklamaları ve bunlarla mücadele yolları, Kaspersky Endpoint Security veritabanlarında sunulmaktadır. Ağ Saldırısı Engelleyici bileşeninin algıladığı ağ saldırıları listesi, veritabanı ve uygulama modülü güncellemeleri sırasında güncellenir.

Ağ Saldırısı Engelleyici'yi etkinleştirme ve devre dışı bırakma

Varsayılan olarak Ağ Saldırısı Engelleyici etkinleştirilmiştir ve optimum modda çalışır. Gerekirse Ağ Saldırısı Engelleyici'yi devre dışı bırakabilirsiniz.

Bileşeni etkinleştirmenin veya devre dışı bırakmanın iki yolu bulunmaktadır:

- Ana uygulama penceresinin **Koruma ve Denetim** sekmesinde
- Uygulama ayarları penceresinden.

Ağ Saldırısı Engelleyici'yi etkinleştirmek veya devre dışı bırakmak için ana uygulama penceresinin Koruma ve Denetim sekmesinde aşağıdakileri yapın:

1. Ana uygulama penceresini açın.
2. **Koruma ve Denetim** sekmesini seçin.
3. **Koruma** bölümüne tıklayın.

   Koruma bölümü açılır.
4. **Ağ Saldırısı Engelleyici** satırına sağ tıklayarak Ağ Saldırısı Engelleyici eylemlerinin içerik menüsünü görüntüleyin.
5. Aşağıdakilerden birini yapın:
   - Ağ Saldırısı Engelleyici'yi etkinleştirmek için içerik menüsünde **Başlat**'ı seçin.

     Ağ Saldırısı Engelleyici satırında solda görüntülenen bileşen durum simgesi , simgesine değişir.
   - Ağ Saldırısı Engelleyici'yi devre dışı bırakmak için içerik menüsünde **Durdur**'u seçin.

     Ağ Saldırısı Engelleyici satırında solda görüntülenen bileşen durum simgesi , simgesine değişir.

Uygulama ayarları penceresinde Ağ Saldırısı Engelleyici'yi etkinleştirmek veya devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Ağ Saldırısı Engelleyici** alt bölümünü seçin.

   Ağ Saldırısı Engelleyici ayarları, pencerenin sağ kısmında görüntülenir.
3. Aşağıdakileri uygulayın:
   - Ağ Saldırısı Engelleyiciyi etkinleştirmek için **Ağ Saldırısı Engelleyiciyi Etkinleştir** onay kutusunu işaretleyin.
   - Ağ Saldırısı Engelleyiciyi devre dışı bırakmak için **Ağ Saldırısı Engelleyiciyi Etkinleştir** onay kutusunu işaretlemeyin.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Ağ Saldırısı Engelleyici ayarları

Ağ Saldırısı Engelleyici ayarlarını yapılandırmak için aşağıdaki eylemleri gerçekleştirebilirsiniz:

- Saldıran bir bilgisayarı engellemek için kullanılan ayarları yapılandırabilirsiniz.
- Engellemeden istisna tutulacaklar için bir adres listesi oluşturabilirsiniz.

Saldıran bir bilgisayarı engellemek için kullanılan ayarları düzenleme

Saldıran bir bilgisayarı engelleme ayarlarını düzenlemek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Ağ Saldırısı Engelleyici** alt bölümünü seçin.

   Ağ Saldırısı Engelleyici ayarları, pencerenin sağ kısmında görüntülenir.
3. **Saldıran bilgisayarı engellenen bilgisayarlar listesine ekle** onay kutusunu seçin.

   Bu onay kutusu işaretlenirse bir ağ saldırısı girişimi tespit edildiğinde Ağ Saldırısı Engelleyici belirtilen süre boyunca saldıran bilgisayardan gelen ağ trafiğini engeller. Bu, gelecekte aynı adresten olası ağ saldırılarına karşı bilgisayarı otomatik olarak korur.

   Onay kutusu işaretlenmezse bir ağ saldırısı girişimi tespit edildiğinde, Ağ Saldırısı Engelleyici ileride aynı adresten gelecek olası ağ saldırılarına karşı otomatik korumayı etkinleştirmez.
4. **Saldıran bilgisayarı engellenen bilgisayarlar listesine ekle** onay kutusunun yanındaki alanda, saldıran bir bilgisayarın engellendiği sürenin miktarını değiştirin.
5. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Engelleme istisnalarının adreslerini yapılandırma

Engelleme istisnalarının adreslerini yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **Ağ Saldırısı Engelleyici** alt bölümünü seçin.

   Ağ Saldırısı Engelleyici ayarları, pencerenin sağ kısmında görüntülenir.
3. **İstisnalar** düğmesine tıklayın.

   İstisnalar penceresi açılır.
4. Aşağıdakilerden birini yapın:

   - Yeni bir IP adresi eklemek isterseniz **Ekle** düğmesine tıklayın.
   - Önceden eklenen IP adresini düzenlemek isterseniz adresler listesinden seçim yapın ve **Düzenle** düğmesine tıklayın.

   IP adresi penceresi açılır.
5. Ağ saldırılarının engellenmemesi gereken bilgisayarın IP adresini girin.
6. **IP adresi** penceresinde **Tamam**'a tıklayın.
7. **İstisnalar** penceresinde **Tamam**'a tıklayın.
8. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

BadUSB Saldırısı Önleme

Bu bölüm, BadUSB Saldırı Engelleme bileşeni hakkında bilgi içerir.

BadUSB Saldırı Engelleme Hakkında

Bazı virüsler, işletim sistemini USB aygıtını bir klavye gibi algılayacak şekilde kandırmak için USB aygıtların üretici yazılımını değiştirir.

BadUSB Saldırı Engelleme bileşeni, klavyeye öykünen virüslü USB aygıtların bilgisayara bağlanmasını engeller.

Bilgisayara bir USB aygıt bağlandığında ve uygulama tarafından klavye olarak algılandığında, uygulama kullanıcıdan uygulama tarafından üretilen sayısal bir kodu bu klavyeyi ya da (varsa) Ekran Klavyesini kullanarak girmesini ister. Bu işlem, klavye yetkilendirme olarak bilinir. Uygulama yetkilendirilmiş bir klavyenin kullanımına izin verir ve yetkilendirilmemiş bir klavyeyi engeller.

BadUSB Saldırı Engelleme, yüklendiği andan itibaren arka plan modunda çalışmaya başlar. Uygulama bir Kaspersky Security Center ilkesine tabi değilse bilgisayar korumasını ve denetimini geçici olarak duraklatma ve sürdürme yoluyla BadUSB Saldırı Engellemeyi etkinleştirebilir ya da devre dışı bırakabilirsiniz.

BadUSB Saldırı Engelleme bileşenini yükleme

Kaspersky Endpoint Security kurulumu sırasında temel veya standart kurulum seçtiyseniz BadUSB Saldırı Engelleme bileşeni mevcut olmaz. Kurmak için uygulama bileşenleri setini değiştirmelisiniz.

BadUSB Saldırısı Önleme bileşenini yüklemek için:

1. **Başlat** menüsünde, **Uygulamalar→ Kaspersky Endpoint Security 10 for Windows → Değiştir, Onar veya Kaldır**'ı seçin.

   Kurulum Sihirbazı başlatılır.

2. Uygulama Kurulum Sihirbazı'nın **Uygulamayı Değiştir, Onar veya Kaldır** penceresinde **Değiştir** düğmesine tıklayın.

   Uygulama Kurulum Sihirbazı'nın **Özel kurulum** penceresi açılır.

3. **BadUSB Saldırı Engelleme** bileşeninin adının yanındaki simgenin içerik menüsünde, **Özellik yerel sabit sürücüye yüklenecek** seçeneğini seçin.

4. **İleri** düğmesine tıklayın.

5. Kurulum Sihirbazı talimatlarını uygulayın.

BadUSB Saldırı Önleme'yi Etkinleştirme ve Devre Dışı Bırakma

BadUSB Saldırı Önleme'yi etkinleştirmek ve devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **BadUSB Saldırı Engelleme** alt bölümünü seçin.

BadUSB Saldırı Önleme ayarları, pencerenin sağ kısmında görüntülenir.

3. Aşağıdakilerden birini yapın:

   - BadUSB Saldırı Önleme'yi etkinleştirmek için **BadUSB Saldırı Önleme'yi Etkinleştir** onay kutusunu işaretleyin.
   - BadUSB Saldırı Önleme'yi devre dışı bırakmak için **BadUSB Saldırı Önleme'yi Etkinleştir** onay kutusundaki seçimi kaldırın.

4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Yetkilendirme için Ekran Klavyesi'nin kullanımına izin verme ve yasaklama

Ekran Klavyesi, yalnızca rastgele karakterlerin girişin desteklemeyen USB aygıtların (örn. barkod tarayıcılar) yetkilendirilmesi için kullanılmalıdır. Bilinmeyen USB aygıtların yetkilendirilmesi için Ekran Klavyesi'nin kullanılması önerilmez.

Yetkilendirme için Ekran Klavyesi'nin kullanımına izin vermek veya yasaklamak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünde, **BadUSB Saldırı Engelleme** alt bölümünü seçin.

   Bileşen ayarları, pencerenin sağ kısmında görüntülenir.

3. Aşağıdakilerden birini yapın:

   - Yetkilendirme için Ekran Klavyesi'nin kullanımına izin vermek için **Yetkilendirme için Ekran Klavyesi'nin kullanımına izin ver** onay kutusunu seçin.
   - Yetkilendirme için Ekran Klavyesi'nin kullanımına izin vermek için **Yetkilendirme için Ekran Klavyesi'nin kullanımına izin ver** onay kutusunu seçin.

4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Klavye yetkilendirme

İşletim sistemi tarafından klavye olarak tanımlanan ve BadUSB Saldırı Engelleme bileşeni yüklenmeden önce bilgisayara bağlanmış olan USB aygıtlar, bileşenin yüklenmesinden sonra yetkilendirilmiş olarak kabul edilir.

Uygulama, yalnızca USB klavye yetkilendirme istemi etkinleştirildiğinde işletim sistemi tarafından klavye olarak algılanan bağlı USB aygıtının yetkilendirilmesini talep eder. Kullanıcı, yetkilendirilmemiş bir klavyeyi yetkilendirilene kadar kullanamaz.

USB klavye yetkilendirme istemi devre dışı bırakılırsa kullanıcı bağlanan bütün klavyeleri kullanabilir. USB klavye yetkilendirme istemi etkinleştirildikten hemen sonra, uygulama bağlanmış her bir yetkilendirilmemiş klavyenin yetkilendirilmesi için bir istem görüntüler.

Bir klavyeyi yetkilendirmek için:

1. USB klavye yetkilendirme etkinleştirilmiş haldeyken klavyeyi USB bağlantı noktasına bağlayın.

Bağlı klavyenin ayrıntılarını ve yetkilendirilmesi için sayısal bir kodu içeren **<Klavye adı> klavye yetkilendirme** penceresi açılır.

2. Rastgele üretilen sayısal kodu bağlı klavyeden ya da (varsa) Ekran Klavyesinden yetkilendirme penceresine girin.

3. **Tamam**'a tıklayın.

   Kod doğru girildiyse uygulama klavyenin VID/PID'si ve bağlandığı bağlantı noktasının numarası gibi tanımlama parametrelerini yetkilendirilen klavyeler listesine kaydeder. Klavye yeniden bağlandığında ya da işletim sistemi yeniden başlatıldıktan sonra yetkilendirmenin tekrarlanması gerekmez.

   > Yetkilendirilen klavye bilgisayarın farklı bir USB bağlantı noktasına bağlandığında, uygulama bu klavyenin yetkilendirilmesi için tekrar bir istem görüntüler.

   Sayısal kod yanlış girildiyse uygulama yeni bir kod üretir. Sayısal kodu girmek için üç deneme hakkı bulunur. Sayısal kod üç kez arka arkaya yanlış girilirse ya da **<Klavye adı> klavye yetkilendirme** penceresi kapatılırsa uygulama bu klavyeden girişleri engeller. Klavye yeniden bağlandığında ya da işletim sistemi yeniden başlatıldığında, uygulama kullanıcıdan yeniden klavye yetkilendirme yapmasını ister.

Uygulama Başlatma Denetimi

Bu bölümde, Uygulama Başlatma Denetimi ve bileşen ayarlarının nasıl yapılandırılacağı hakkında bilgiler bulunmaktadır.

Uygulama Başlatma Denetimi Hakkında

Uygulama Başlatma Denetimi bileşeni, *Uygulama Başlatma Denetimi kurallarını* kullanarak kullanıcıların uygulamaları başlatma girişimlerini izler ve uygulamaların başlatılmasını düzenler.

Ayarları herhangi bir Uygulama Başlatma Denetimi kuralına uymayan uygulamaların başlatılması bileşenin seçilen işletim modu ile düzenlenir. *Kara Liste modu* varsayılan olarak seçilmiştir. Bu mod herhangi bir kullanıcının herhangi bir uygulamayı başlatmasına imkan tanır.

Kullanıcıların tüm uygulama başlatma girişimleri raporlarda kaydedilir.

Uygulama Denetimi'ni etkinleştirme ve devre dışı bırakma

Uygulama Denetimi varsayılan olarak devre dışıdır ancak gerekirse Uygulama Denetimini etkinleştirebilirsiniz.

Uygulama Denetimi'ni etkinleştirmek veya devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Güvenlik Denetimleri** bölümünde, **Uygulama Denetimi** alt bölümünü seçin.

   Pencerenin sağ kısmında, Uygulama Denetimi bileşeni ayarları görüntülenir.
3. Aşağıdakilerden birini yapın:
   - Uygulama Denetimi'ni etkinleştirmek istiyorsanız **Uygulama Denetimini Etkinleştir** onay kutusunu işaretleyin.
   - Uygulama Denetimi'ni devre dışı bırakmak istiyorsanız **Uygulama Denetimini Etkinleştir** onay kutusunun işaretini kaldırın.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Uygulama Başlatma Denetimi işlevselliği sınırlamaları

Uygulama Başlatma Denetimi bileşeninin çalışması aşağıdaki durumlarda sınırlandırılır:

- Uygulama sürümü yükseltildiğinde, Uygulama Başlatma Denetimi bileşen ayarlarını içe aktarma desteklenmez.

  Uygulama Başlatma Denetimi'nin işlevselliğini geri yüklemek için bileşenin ayarlarını yeniden yapılandırmalısınız.

- KSN sunucuları ile bağlantı yoksa Kaspersky Endpoint Security uygulamaların ve modüllerinin saygınlığı hakkında bilgileri sadece yerel veritabanlarından alır. Yerel veritabanları uygulama hakkında bilgi içermiyorsa uygulama bir güven grubuna kategorize edilmeyecektir.

KSN sunucuları ile bağlantı varken uygulamaların kategorilere ayrılması, KSN ile bir bağlantı yokken kategorilere ayrılmasından farklı olabilir.

- Kaspersky Security Center veritabanında 150.000 işlenmiş dosya hakkında bilgi saklanabilir. Bu kayıt sayısına ulaşıldığında, yeni dosyalar işlenmeyecektir. Envanter işlemlerini sürdürmek için Kaspersky Endpoint Security'nin yüklü olduğu bilgisayardan daha önce Kaspersky Security Center veritabanında envanteri tutulmuş olan dosyaların silinmesi gerekir.

- Bileşen, komut dizisi komut satırı aracılığıyla yorumlayıcı gönderilmedikçe komut dizilerinin başlangıcını kontrol etmez.

  Bir yorumlayıcının başlatılmasına Uygulama Başlatma Denetimi kuralları tarafından izin verilirse bileşen bu yorumlayıcıdan başlayan bir komut dizisini engellemez.

- Bileşen, Kaspersky Endpoint Security tarafından desteklenmeyen yorumlayıcılar tarafından komut dizilerinin başlatılmasını denetlemez.

  Kaspersky Endpoint Security aşağıdaki yorumlayıcıları destekler:

  - Java
  - PowerShell

  Aşağıdaki yorumlayıcı türleri desteklenmektedir:

  - { cCmdLineParser::itCmd, _T("%ComSpec%") };
  - { cCmdLineParser::itReg, _T("%SystemRoot%\\system32\\reg.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedit.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\regedit.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedt32.exe") };
  - { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\cscript.exe") };
  - { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\wscript.exe") };
  - { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\system32\\msiexec.exe") };
  - { cCmdLineParser::itMmc, _T("%SystemRoot%\\system32\\mmc.exe") };
  - { cCmdLineParser::itMshta, _T("%SystemRoot%\\system32\\mshta.exe") };
  - { cCmdLineParser::itRundll, _T("%SystemRoot%\\system32\\rundll32.exe") };
  - { cCmdLineParser::itMetro, _T("%SystemRoot%\\system32\\wwahost.exe") };
  - { cCmdLineParser::itCmd, _T("%SystemRoot%\\syswow64\\cmd.exe") };
  - { cCmdLineParser::itReg, _T("%SystemRoot%\\syswow64\\reg.exe") };
  - { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedit.exe") };

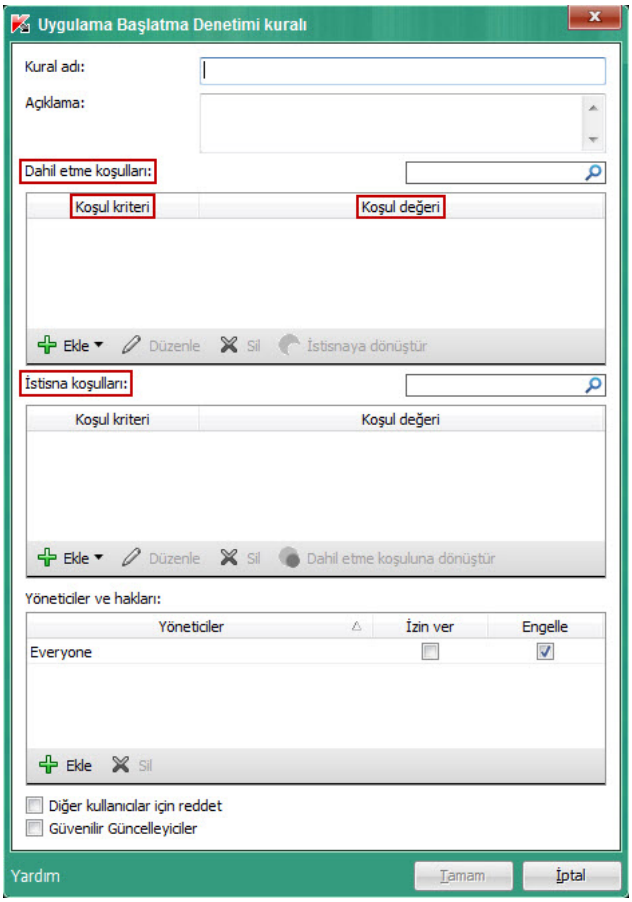
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\syswow64\\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\\syswow64\\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\\syswow64\\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\\syswow64\\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\\syswow64\\wwahost.exe") }.

Uygulama Denetimi kuralları hakkında

Kaspersky Endpoint Security, kullanıcıların uygulamaları başlatmasını kurallarla denetler. Uygulama Başlatma Denetimi kuralı, tetikleme koşullarını ve kural tetiklendiğinde (kullanıcılar tarafından uygulamanın başlatılmasına izin verir veya engeller) Uygulama Denetimi bileşeni tarafından gerçekleştirilen eylemi belirtir.

Kural tetikleme koşulları

Kuralı tetikleme koşulu şu karşılığa sahiptir: "koşul türü - koşul kriteri - koşul değeri" (aşağıdaki resme bakınız). Kural tetikleme koşullarına dayalı olarak Kaspersky Endpoint Security, uygulamaya bir kural uygular (veya uygulamaz).



Uygulama Başlatma Denetimi kuralı. Kural tetikleme koşulu parametreleri

Kurallar dahil etme ve istisna koşulları kullanır:

- *Dahil etme koşulları*. Uygulamanın dahil etme koşullarından en az biriyle eşleşmesi halinde Kaspersky Endpoint Security, uygulamaya kuralı uygular.

- *İstisna koşulları*. Uygulamanın istisna koşullarından en az biriyle eşleşmesi ve dahil etme koşullarından herhangi birini karşılamaması halinde Kaspersky Endpoint Security, uygulamaya kuralı uygulamaz.

Kural tetikleme koşulları, kriterleri kullanarak oluşturulur. Kaspersky Endpoint Security'de kuralları oluşturmak için aşağıdaki kriterler kullanılır:

- Uygulamanın yürütülebilir dosyasını içeren klasörün yolu veya uygulamanın yürütülebilir dosyasının yolu.

- Meta veri: uygulamanın yürütülebilir dosyasının adı, uygulamanın yürütülebilir dosyasının sürümü, uygulama adı, uygulama sürümü, uygulama satıcısı.

- Uygulamanın yürütülebilir dosyasının karması.

- Sertifika: veren, konu, parmak izi.

- Uygulamanın bir KL kategorisine dahil edilmesi.

- Uygulamanın yürütülebilir dosyasının çıkarılabilir sürücüdeki konumu.

Kriter değeri, koşulda kullanılan her bir kriter için belirtilmelidir. Başlatılan uygulamanın parametreleri, dahil etme koşulunda belirtilen kriterlerin değerleriyle eşleşiyorsa, kural tetiklenir. Bu durumda Uygulama Denetimi, kuralda belirtilen eylemi uygular. Uygulama parametrelerinin istisna koşulunda belirtilen kriter değerleriyle eşleşmesi halinde Uygulama Denetimi, uygulamanın başlatılmasını denetlemez.

Kural tetiklendiğinde Uygulama Denetimi bileşeni tarafından verilen kararlar

Kural tetiklendiğinde Uygulama Denetimi, kurala göre kullanıcıların (veya kullanıcı gruplarının) uygulamaları başlatmasına izin verir veya uygulamaların başlatılmasını engeller. Kuralı tetikleyen uygulamaları başlatmasına izin verilen veya verilmeyen kullanıcıları veya kullanıcı gruplarını seçebilirsiniz.

Bir kural, kuralla sağlayan uygulamaları başlatmasına izin verilen kullanıcıları belirtmiyorsa, bu kural *engelle* kuralı olarak adlandırılır.

Bir kural, kuralla eşleşen uygulamaları başlatmasına izin verilmeyen kullanıcıları belirtmiyorsa, bu kural *izin ver* kuralı olarak adlandırılır.

Engelle kuralının önceliği, izin ver kuralının önceliğinden daha yüksektir. Örneğin, bir kullanıcı grubuna Uygulama Denetimi izin ver kuralı atanmışken bu gruptaki bir kullanıcıya Uygulama Denetimi engelle kuralı atanırsa bu kullanıcının uygulamayı başlatması engellenir.

Kuralın çalışma durumu

Uygulama Başlatma Denetimi kuralları aşağıdaki çalışma durumlarından birine sahip olabilir:

- **Açık**. Bu durum, Uygulama Denetimi çalışırken kuralın kullanıldığı anlamına gelir.

- **Kapalı**. Bu durum, Uygulama Denetimi çalışırken kuralın yok sayıldığı anlamına gelir.

- **Test**. Bu durum, Kaspersky Endpoint Security'nin kuralların uygulandığı uygulamaların başlatılmasına izin verdiği fakat bu uygulamaların başlatılması hakkında bilgileri rapora kaydettiği anlamına gelir.

Uygulama Başlatma Denetimi kurallarını yönetme

Uygulama Başlatma Denetimi kuralları için aşağıdaki eylemleri gerçekleştirebilirsiniz:

- Yeni bir kural ekle
- Bir kuralı tetikleme koşullarını oluştur veya değiştir
- Kural durumunu düzenle

  Uygulama Başlatma Denetimi kuralı etkinleştirilebilir (kuralın karşısındaki onay kutusu işaretlidir) veya devre dışı bırakılabilir (kuralın karşısındaki onay kutusu işaretli değildir). Uygulama Başlatma Denetimi kuralı, oluşturulduktan sonra varsayılan olarak etkindir.
- Kuralı sil

Uygulama Başlatma Denetimi kuralının eklenmesi ve düzenlenmesi

Bir Uygulama Başlatma Denetimi kuralı eklemek veya düzenlemek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin solunda, **Uç nokta denetimi** bölümünde, **Uygulama Başlatma Denetimi** alt bölümünü seçin.

   Pencerenin sağında, Uygulama Başlatma Denetimi bileşeni ayarları görüntülenir.
3. Bileşen ayarlarını düzenlenebilir duruma getirmek için **Uygulama Başlatma Denetimini Etkinleştir** seçeneğini seçin.
4. Aşağıdakilerden birini yapın:
   - Bir kural eklemek için **Ekle** düğmesine tıklayın.
   - Mevcut bir kuralı düzenlemek isterseniz, kurallar listesinden seçin ve **Düzenle** düğmesine tıklayın.

   Uygulama Başlatma Denetimi kuralı penceresi açılır.
5. Kural ayarlarını belirtin veya düzenleyin:
   a. **Kural adı** alanında, kuralın adını girin veya düzenleyin.
   b. **Dahil etme koşulları** tablosunda, **Ekle**, **Düzenle**, **Sil** ve **İstisnaya dönüştür** düğmelerine tıklandığında bir kural tetikleyen dahil etme koşulları listesi oluşturun veya düzenleyin.
   c. **İstisna koşulları** tablosunda, **Ekle**, **Düzenle**, **Sil** ve **Dahil etme koşuluna dönüştür** düğmelerine tıklandığında bir kural tetikleyen istisna koşulları listesini oluşturun veya düzenleyin.
   d. Gerekirse kural tetikleme koşulu türünü değiştirebilirsiniz:

- Koşul türünü dahil etme koşulu yerine istisna koşuluna dönüştürmek için **Dahil etme koşulları** tablosunda bir koşul seçin ve **İstisnaya dönüştür** düğmesine tıklayın.
- Koşul türünü istisna koşulu yerine dahil etme koşuluna dönüştürmek için **İstisna koşulları** tablosunda bir koşul seçin ve **Dahil etme koşuluna dönüştür** düğmesine tıklayın.

e. Kural tetikleme koşullarını karşılayan uygulamaları başlatmasına izin verilen veya izin verilmeyen kullanıcılar ve/veya kullanıcı gruplarının bir listesini derleyin veya düzenleyin. Bunun için **Yöneticiler ve hakları** tablosunda **Ekle** düğmesine tıklayın.

Microsoft Windows'ta **Kullanıcıları veya Grupları Seç** penceresi açılır. Bu pencere, kullanıcıları ve/veya kullanıcı gruplarını seçmenize olanak tanır.

Varsayılan olarak kullanıcılar listesine **Herkes** değeri eklenir. Kural tüm kullanıcılar için geçerlidir.

> Tabloda belirtilen kullanıcı yoksa kural kaydedilemez.

f. **Yöneticiler ve hakları** tablosunda, uygulamaları başlatma haklarını belirlemek için kullanıcılar ve/veya kullanıcı gruplarının karşısındaki **İzin ver** veya **Engelle** onay kutularını seçin.

Varsayılan olarak seçilen onay kutusu Uygulama Başlatma Denetimi işletim moduna bağlıdır.

g. **Yöneticiler** sütununda görülmeyen ve **Yöneticiler** sütununda belirtilen kullanıcılar grubunun parçası olmayan tüm kullanıcıların kural tetikleme koşuluna uygun uygulamaları başlatmasının engellenmesini istiyorsanız **Diğer kullanıcılar için reddet** onay kutusunu seçin.

> **Diğer kullanıcılar için reddet** onay kutusu işaretlenmezse Kaspersky Endpoint Security, **Yöneticiler ve hakları** tablosunda belirtilmeyen ve **Yöneticiler ve hakları** tablosunda belirtilen kullanıcılar grubuna ait olmayan kullanıcılar tarafından uygulamaların başlatılmasını denetlemez.

h. Kaspersky Endpoint Security'nin kural tetikleme kurallarını karşılayan uygulamaları, Uygulama Başlatma Denetimi kuralları tanımlanmamış diğer uygulamaları başlatmasına izin verilen güvenilir güncelleyiciler olarak değerlendirmesini istiyorsanız **Güvenilir Güncelleyiciler** onay kutusunu işaretleyin.

6. **Tamam**'a tıklayın.
7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Uygulama Başlatma Denetimi kuralına tetikleme koşulu ekleme

Uygulama Başlatma Denetimi kuralına yeni bir tetikleme koşulu eklemek için:

1. Ana uygulama penceresinde **Ayarlar** düğmesine tıklayın.
2. Pencerenin sol kısmında, **Güvenlik Denetimleri** bölümünde, **Uygulama Denetimi** alt bölümünü seçin.

   Pencerenin sağ kısmında, Uygulama Denetimi bileşeni ayarları görüntülenir.
3. Bileşen ayarlarını düzenlenebilir duruma getirmek için **Uygulama Denetimi** onay kutusunu seçin.
4. Aşağıdakilerden birini yapın:
   - Yeni bir kural oluşturmak ve bir tetikleme koşulu eklemek isterseniz, **Ekle** düğmesine tıklayın.

- Mevcut bir kurala bir tetikleme koşulu eklemek isterseniz, kurallar listesinden kuralı seçin ve **Düzenle** düğmesine tıklayın.

Uygulama Başlatma Denetimi kuralı penceresi açılır.

5. **Dahil etme koşulları** veya **İstisna koşulları** tablosunda, **Ekle** düğmesine tıklayın.

Kurala çeşitli tetikleme koşulları eklemek için **Ekle** düğmesinin altında bulunan açılır listeyi kullanabilirsiniz (lütfen aşağıdaki talimatlara bakın).

Belirtilen klasördeki dosyanın özelliklerine dayalı olarak bir kural tetikleme koşulu eklemek için:

1. **Ekle** düğmesinin altındaki açılır listeden **Belirtilen klasördeki dosyaların özelliklerinden koşullar** seçeneğini belirleyin.

   Microsoft Windows'ta standart **Klasör seçin** penceresi açılır.

2. **Klasör seçin** penceresinde, özelliklerini bir kuralı tetiklemek için bir veya daha fazla koşulun temeli olarak kullanmak istediğiniz uygulamaların yürütülebilir dosyalarını içeren bir klasör seçin.

3. **Tamam**'a tıklayın.

   Koşul ekle penceresi açılır.

4. **Kriterlendirmeyi göster** açılır listesinde, hangi kurala göre bir veya daha fazla kural tetikleme koşulu oluşturmak istediğinizi seçin: **Dosya karma kodu**, **Sertifika**, **KL kategorisi**, **Meta veri** veya **Klasör yolu**.

   Kaspersky Endpoint Security, MD5 dosya karma kodunu desteklememektedir ve bu nedenle MD5 karma koduna dayalı olarak uygulamaların başlatılmasını denetlemez. Kural tetikleme koşulu olarak SHA256 karma kodu kullanılır.

5. **Kriterlendirmeyi göster** açılır listesinde **Meta veri** seçeneğini seçtiyseniz, kural tetikleme koşulunda kullanmak istediğiniz yürütülebilir dosya özelliklerinin karşısındaki onay kutusunu seçin: **Dosya adı**, **Dosya sürümü**, **Uygulama adı**, **Uygulama sürümü** ve **Satıcı**.

   Belirtilen özelliklerden hiçbiri seçilmezse kural kaydedilemez.

6. **Ölçütleri göster** açılır listesinde **Sertifika** seçeneğini seçtiyseniz, kural tetikleme koşulunda kullanmak istediğiniz ayarların karşısındaki onay kutularını işaretleyin: **Veren**, **Konu** ve **Parmak izi**.

   Belirtilen ayarlardan hiçbiri seçilmezse kural kaydedilemez.

   Kural tetikleme koşulları olarak sadece **Veren** ve **Konu** kriterlerinin kullanılması önerilir. Bu kriterlerin kullanımı güvenilir değildir.

7. Kural tetikleme koşullarına özelliklerini eklemek istediğiniz uygulama yürütülebilir dosyalarının adlarının karşısındaki onay kutularını işaretleyin.

8. **İleri** düğmesine tıklayın.

   Belirlenen kural tetikleme koşullarının listesi görülür.

9. Belirlenen kural tetikleme koşullarının listesinde, Uygulama Başlatma Denetimi kuralına eklemek istediğiniz kural tetikleme koşulunun karşısındaki onay kutularını işaretleyin.

10. **Sonlandır** düğmesine tıklayın.

Bilgisayarda başlatılan uygulamaların özelliklerine dayalı olarak bir kural tetikleme koşulu eklemek için:

1. **Ekle** düğmesinin altındaki açılır listeden **Başlatılan uygulamaların özelliklerinden koşullar** seçeneğini belirleyin.
2. **Koşul ekle** penceresinde, **Ölçütleri göster** açılır listesinde, hangi kritere göre bir veya daha fazla kural tetikleme koşulu oluşturmak istediğinizi seçin: **Dosya karma kodu**, **Sertifika**, **KL kategorisi**, **Meta veri** veya **Klasör yolu**.

   Kaspersky Endpoint Security, MD5 dosya karma kodunu desteklememektedir ve bu nedenle MD5 karma koduna dayalı olarak uygulamaların başlatılmasını denetlemez. Kural tetikleme koşulu olarak SHA256 karma kodu kullanılır.

3. **Kriterlendirmeyi göster** açılır listesinde **Meta veri** seçeneğini seçtiyseniz, kural tetikleme koşulunda kullanmak istediğiniz yürütülebilir dosya özelliklerinin karşısındaki onay kutusunu seçin: **Dosya adı**, **Dosya sürümü**, **Uygulama adı**, **Uygulama sürümü** ve **Satıcı**.

   Belirtilen özelliklerden hiçbiri seçilmezse kural kaydedilemez.

4. **Ölçütleri göster** açılır listesinde **Sertifika** seçeneğini seçtiyseniz, kural tetikleme koşulunda kullanmak istediğiniz ayarların karşısındaki onay kutularını işaretleyin: **Veren**, **Konu** ve **Parmak izi**.

   Belirtilen ayarlardan hiçbiri seçilmezse kural kaydedilemez.

   Kural tetikleme koşulları olarak sadece **Veren** ve **Konu** kriterlerinin kullanılması önerilir. Bu kriterlerin kullanımı güvenilir değildir.

5. Kural tetikleme koşullarına özelliklerini eklemek istediğiniz uygulama yürütülebilir dosyalarının adlarının karşısındaki onay kutularını işaretleyin.
6. **İleri** düğmesine tıklayın.

   Belirlenen kural tetikleme koşullarının listesi görülür.

7. Belirlenen kural tetikleme koşullarının listesinde, Uygulama Başlatma Denetimi kuralına eklemek istediğiniz kural tetikleme koşulunun karşısındaki onay kutularını işaretleyin.
8. **Sonlandır** düğmesine tıklayın.

KL kategorisine dayalı olarak bir kural tetikleme koşulu eklemek için:

1. **Ekle** düğmesinin altındaki açılır listeden **Koşullar "KL kategorisi"** seçeneğini belirleyin.

   KL kategorisi, ortak tema özelliklerine sahip bir uygulamalar listesidir. Liste, Kaspersky uzmanları tarafından düzenlenir. Örneğin "Office uygulamaları" KL kategorisi, Microsoft Office paketinden uygulamalar, Adobe® Acrobat® ve diğerlerini kapsar.

2. **Koşullar "KL kategorisi"** penceresinde, kural tetikleme koşulları oluşturmak istediğiniz KL kategorilerinin adlarının yanındaki onay kutularını işaretleyin.

   İç içe geçmiş KL kategorilerini seçerek işaretlemek için KL kategorisi adının solunda bulunan unfold_key düğmesine tıklayabilirsiniz.

3. **Tamam**'a tıklayın.

Özel kural tetikleme koşulu eklemek için:

1. **Ekle** düğmesinin altındaki açılır listede **Özel koşul**'u seçin.

2. **Özel koşul** penceresinde, **Seç** düğmesine tıklayın ve uygulamanın yürütülebilir dosyasının yolunu belirtin.

3. Hangi kritere göre kural tetikleme koşulunu oluşturmak istediğinizi seçin: **Dosya karma kodu**, **Sertifika**, **Meta veri** veya **Dosya veya klasör yolu**.

   Kaspersky Endpoint Security, MD5 dosya karma kodunu desteklememektedir ve bu nedenle MD5 karma koduna dayalı olarak uygulamaların başlatılmasını denetlemez. Kural tetikleme koşulu olarak SHA256 karma kodu kullanılır.

   Dosya veya klasör yolu alanında sembolik bağlantı kullanıyorsanız Uygulama Başlatma Denetimi kuralının doğru çalışması için sembolik bağlantıyı çözmeniz önerilir. Bunun için **Sembolik bağlantıları çöz** düğmesine tıklayın.

4. Seçili kriterlerin ayarlarını yapılandırın.

5. **Tamam**'a tıklayın.

Uygulamanın yürütülebilir dosyasının kaydedildiği sürücü ile ilgili bilgilere dayanan bir kural tetikleme koşulu eklemek için:

1. **Ekle** düğmesinin altındaki açılır listede **Dosya sürücüsüne göre koşul** seçeneğini belirleyin.

2. **Dosya sürücüsüne göre koşul** penceresinde, **Sürücü** açılır listesinde, kural tetikleme koşulu olarak kullanılacak uygulamaların başlangıcını oluşturan depolama aygıtı türünü seçin.

3. **Tamam**'a tıklayın.

Uygulama Başlatma Denetimi kuralının durumunu değiştirme

Uygulama Başlatma Denetimi kuralının durumunu değiştirmek için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin solunda, **Uç nokta denetimi** bölümünde, **Uygulama Başlatma Denetimi** alt bölümünü seçin.

   Pencerenin sağında, Uygulama Başlatma Denetimi bileşeni ayarları görüntülenir.

3. Bileşen ayarlarını düzenlenebilir duruma getirmek için **Uygulama Başlatma Denetimini Etkinleştir** seçeneğini seçin.

4. Durumunu düzenlemek istediğiniz kuralı seçin.

5. **Durum** sütununda aşağıdakilerden birini yapın:

   - Kural kullanımını etkinleştirmek isterseniz kuralın karşısındaki onay kutusunu seçin.
   - Kural kullanımını devre dışı bırakmak isterseniz kuralın karşısındaki onay kutusunun işaretini kaldırın.

6. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Uygulama Başlatma Denetimi kurallarını test etme

Uygulama Başlatma Denetimi kurallarının çalışması gereken uygulamaları engellemediğinden emin olmak için yeni oluşturulan kuralların test moduna konulup çalışmalarının analiz edilmesi önerilir.

Uygulama Başlatma Denetimi kurallarının çalışmasının analizi, Kaspersky Security Center'a rapor edilen Uygulama Başlatma Denetimi olaylarının gözden geçirilmesini gerektirir. Bilgisayar kullanıcısının çalışması için gerekli bütün uygulamaların başlatılmasına izin veriliyorsa kurallar doğru oluşturulmuştur. Aksi halde oluşturduğunuz kuralların ayarlarını düzeltmeniz önerilir.

Uygulama Başlatma Denetimi kuralları için test modu varsayılan olarak devre dışıdır.

Uygulama Başlatma Denetimi kurallarını test etmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin solunda, **Uç nokta denetimi** bölümünde, **Uygulama Başlatma Denetimi** alt bölümünü seçin.

   Pencerenin sağında, Uygulama Başlatma Denetimi bileşeni ayarları görüntülenir.
3. Bileşen ayarlarını düzenlenebilir duruma getirmek için **Uygulama Başlatma Denetimini Etkinleştir** seçeneğini seçin.
4. **Uygulama Başlatma Denetimi modu** açılır listesinde aşağıdaki öğelerden birini seçin:
   - Engelleme kurallarında belirtilen uygulamalar hariç tüm uygulamaların başlatılmasına izin vermek istiyorsanız **Kara Liste**.
   - İzin verme kurallarında belirtilen uygulamalar hariç tüm uygulamaların başlatılmasını engellemek istiyorsanız **Beyaz Liste**.
5. **Eylem** açılır listesinde, **Bilgilendir**'i seçin.
6. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Kaspersky Endpoint Security, Uygulama Başlatma Denetimi kuralları tarafından başlatılması yasaklanan uygulamaları engellemez ancak başlatıldıklarında Yönetim Sunucusu'nu bilgilendirir.

Uygulama Başlatma Denetimi mesaj şablonlarını düzenleme

Kullanıcı, Uygulama Başlatma Denetimi kuralı tarafından engellenen bir uygulamayı başlatmaya çalıştığında Kaspersky Endpoint Security, uygulamanın başlatılmasının engellendiğini belirten bir mesaj görüntüler. Kullanıcı, uygulamanın başlatılmasının yanlışlıkla engellendiğini düşünüyorsa mesaj metnindeki bağlantıyı kullanarak yerel kurumsal ağ yöneticisine bir mesaj gönderebilir.

Uygulamanın başlatılması engellendiğinde görüntülenen mesaj ve yöneticiye gönderilen mesaj için özel şablonlar mevcuttur. Mesaj şablonlarını değiştirebilirsiniz.

Bir mesaj şablonunu düzenlemek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin solunda, **Uç nokta denetimi** bölümünde, **Uygulama Başlatma Denetimi** alt bölümünü seçin.

Pencerenin sağında, Uygulama Başlatma Denetimi bileşeni ayarları görüntülenir.

3. Bileşen ayarlarını düzenlenebilir duruma getirmek için **Uygulama Başlatma Denetimini Etkinleştir** seçeneğini seçin.

4. **Şablonlar** düğmesine tıklayın.

   Mesaj şablonları penceresi açılır.

5. Aşağıdakilerden birini yapın:

   - Bir uygulamanın başlatılması engellendiğinde görüntülenen mesajın şablonunu düzenlemek isterseniz **Engelleme** sekmesini seçin.

   - LAN yöneticisine gönderilen mesajın şablonunu düzenlemek isterseniz **Yöneticiye mesaj** sekmesini seçin.

6. Uygulamanın başlatılması engellendiğinde görüntülenen mesaj ve yöneticiye gönderilen mesajın şablonunu değiştirin. Bunun için **Varsayılan** ve **Değişken** düğmelerini kullanın.

7. **Tamam**'a tıklayın.

8. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Uygulama Başlatma Denetimi işletim modları hakkında

Uygulama Başlatma Denetimi bileşeni iki modda çalışır:

- **Kara liste**. Bu modda, Uygulama Başlatma Denetimi, Uygulama Başlatma Denetimi engelleme kuralları'nda belirtilen uygulamalar haricinde tüm kullanıcıların tüm uygulamaları başlatmalarına izin verir.

  Uygulama Başlatma Denetimi'nin bu modu varsayılan olarak etkinleştirilmiştir.

- **Beyaz liste**. Bu modda Uygulama Başlatma Denetimi, Uygulama Başlatma Denetimi izin ver kurallarında belirtilen uygulamalar haricinde tüm kullanıcıların herhangi bir uygulamayı başlatmasını engeller.

  Uygulama Başlatma Denetimi izin ver kuralları tamamen yapılandırılırsa bileşen, işletim sisteminin ve kullanıcıların çalışmalarında güvendiği güvenilir uygulamaların çalışmasına izin verirken, LAN yöneticisi tarafından doğrulanmamış olan tüm yeni uygulamaların başlatılmasını engeller.

Her modda çalışan uygulamalarda kullanılabilecek iki eylem vardır: Kaspersky Endpoint Security, uygulamaların başlatılmasını engelleyebilir veya kullanıcıya, Uygulama Başlatma Denetimi kurallarının koşullarına uyan bir uygulamanın başlatılması hakkında bilgi verebilir.

Uygulama Başlatma Denetimi hem Kaspersky Endpoint Security yerel arabirimini kullanarak hem de Kaspersky Security Center'ı kullanarak bu modlarda çalışacak şekilde yapılandırılabilir.

Bununla birlikte Kaspersky Security Center, Kaspersky Endpoint Security yerel arabiriminde bulunmayan, aşağıdaki görevler için ihtiyaç duyulan araçları sunar:

- Uygulama kategorileri oluşturma.

  Kaspersky Security Center Yönetim Konsolunda oluşturulan Uygulama Başlatma Denetimi kuralları, Kaspersky Endpoint Security yerel arabiriminde olduğu gibi dahil etme ve hariç tutma koşullarına değil, özel uygulama kategorilerine dayanır.

- LAN bilgisayarlarına yüklenen uygulamalar hakkında bilgi toplama.

Uygulama Başlatma Denetimi bileşeninin çalışmasını yapılandırmak için Kaspersky Security Center'ı kullanmanın önerilmesinin nedeni budur.

Uygulama Başlatma Denetimi modunu seçme

Uygulama Başlatma Denetimi modunu seçmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin solunda, **Uç nokta denetimi** bölümünde, **Uygulama Başlatma Denetimi** alt bölümünü seçin.

   Pencerenin sağında, Uygulama Başlatma Denetimi bileşeni ayarları görüntülenir.
3. Bileşen ayarlarını düzenlenebilir duruma getirmek için **Uygulama Başlatma Denetimini Etkinleştir** seçeneğini seçin.
4. **Uygulama Başlatma Denetimi modu** açılır listesinde, aşağıdaki seçeneklerden birini seçin:

   - Engelleme kurallarında belirtilen uygulamalar hariç tüm uygulamaların başlatılmasına izin vermek istiyorsanız **Kara Liste**.
   - İzin verme kurallarında belirtilen uygulamalar hariç tüm uygulamaların başlatılmasını engellemek istiyorsanız **Beyaz Liste**.

     Bu mod seçildiğinde varsayılan olarak iki Uygulama Başlatma Denetimi kuralı oluşturulur: **Golden Image** ve **Güvenilir Güncelleyiciler**. Bu kuralları silemezsiniz. Bu kuralların ayarları düzenlenemez. İlgili kuralın karşısındaki onay kutusunu işaretleyerek veya işaretini kaldırarak bu kuralları etkinleştirebilir veya devre dışı bırakabilirsiniz. Varsayılan olarak **Golden Image** kuralı etkindir ve **Güvenilir Güncelleyiciler** kuralı devre dışıdır. Tüm kullanıcıların, bu kuralların tetikleme koşullarıyla eşleşen uygulamaları başlatmasına izin verilir.

   Seçilen mod sırasında oluşturulan tüm kurallar mod değiştirildikten sonra kaydedilerek kuralların tekrar kullanılabilmesi sağlanır. Bu kuralları kullanmaya geri dönmek için yapmanız gereken tek şey, **Uygulama Başlatma Denetimi modu** açılır listesinden gereken modu seçmektir.
5. **Eylem** açılır listesinde, Uygulama Başlatma Denetimi kuralları tarafından engellenen bir uygulamayı kullanıcı başlatmaya çalıştığı zaman bileşen tarafından gerçekleştirilecek eylemi seçin.
6. Uygulamaların kullanıcılar tarafından başlatıldığı zaman Kaspersky Endpoint Security'nin DLL modüllerinin yüklenmesini izlemesini istiyorsanız **DLL ve sürücüleri izle** onay kutusunu seçin.

   Modül ve modüle yüklenen uygulamayla ilgili bilgiler bir rapora kaydedilir.

   Onay kutusu işaretlenirse Kaspersky Endpoint Security başlatılmadan önce DLL modüller ve sürücüler izlenir. Uygulama başlatmadan önce tüm DLL modülleri ve sürücülerinin devamında izlenmesini yapılandırmak için, **DLL ve sürücüleri izle** onay kutusunu işaretledikten sonra bilgisayarı yeniden başlatın. Bilgisayarı yeniden başlatamıyorsanız, **DLL ve sürücüleri izle** onay kutusunu seçtikten sonra Kaspersky Endpoint Security çalışıyorken DLL modüllerini ve sürücüleri yükleyebilirsiniz. Bu durumda, izleme yalnızca Kaspersky Endpoint Security çalışırken yüklenen DLL modülleri ve sürücüler için etkin olur.

   DLL modülleri ve sürücüleri izlerken, KL kategorilerine göre oluşturulmuş olan Uygulama Başlangıç Kontrolü kurallarının kullanılması önerilmez. DLL modülleri ve sürücüleri için KL kategorilerinin ("İşletim sistemi ve bileşenleri" kuralları dahil) belirlenmesi düzgün olarak çalışmayabilir. Özellikle, "İşletim sistemi ve bileşenleri" kuralı varsayılan olarak oluşturulmuştur ve DLL modülü ve sürücü başlatılmasında dağıtılmaz. Bu işlev açılırken, DLL modülleri ve sürücüler için ayrı izin kuralları oluşturmanız gerekir. **DLL ve sürücüleri kontrol et** işlevinin kullanılması, bu tür izin kuralları yoksa sistemin sistemi kararsız hale getirebilir.

Program ayarlarını yapılandırmak için şifre korumasının açık olmasını öneririz böylece, süreç içerisinde Kaspersky Security Center ilke ayarlarını değiştirmezken, kritik önem taşıyan DLL modüllerinin ve sürücülerinin başlatılmasını engelleyen izin kurallarını kapatmak mümkündür.

7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Kaspersky Security Center'ı kullanarak Uygulama Başlatma Denetimi kurallarını yönetme

Bu bölüm, Uygulama Başlatma Denetimi kurallarını yapılandırmak için Kaspersky Security Center kullanımı hakkında bilgiler içerir ve Uygulama Başlatma Denetimi'nin optimum kullanımı hakkında öneriler sağlar.

Kullanıcı bilgisayarlarına yüklenen uygulamalar hakkında bilgi toplama

Optimum Uygulama Denetimi kurallarını oluşturmak için öncelikle kurumsal LAN'daki bilgisayarlarda kullanılan uygulamaların bir resmini edinmeniz önerilir. Bunu yapmak için aşağıdaki bilgileri edinebilirsiniz:

- Satıcılar, sürümler ve kurumsal LAN'da kullanılan uygulamaların yerelleştirmeleri.
- Uygulama güncellemelerinin sıklığı.
- Şirket tarafından benimsenen uygulama kullanım ilkesi (bu güvenlik ilkeleri veya yönetimsel ilkeler olabilir).
- Uygulama dağıtım paketlerinin depolama alanı konumu.

Kurumsal LAN ağı bilgisayarlarında kullanılan uygulamalar hakkındaki bilgiler, **Yürütülebilir dosyalar** klasöründe **Uygulamalar kayıt defteri** klasöründe yer almaktadır. **Uygulamalar kayıt defteri** klasörü ve **Yürütülebilir dosyalar** klasörü, Kaspersky Security Center Yönetim Konsolu ağacında **Uygulama yönetimi** klasöründe yer almaktadır.

Uygulamalar kayıt defteri klasörü, istemci bilgisayarında yüklü Ağ Aracısı tarafından tespit edilen uygulamaların listesini içerir.

Yürütülebilir dosyalar klasörü, istemci bilgisayarlarda şimdiye kadar başlatılmış veya Kaspersky Endpoint Security'nin envanter görevi sırasında tespit edilen tüm yürütülebilir dosyaların bir listesini içerir.

Uygulama ve yürütülebilir dosyaları ile bir uygulamanın yüklendiği bilgisayarların listesi hakkında genel bilgiler görüntülemek için **Uygulama kayıt defteri** klasöründe veya **Yürütülebilir dosyalar** klasöründe seçilen bir uygulamanın özellikler penceresini açın.

***Uygulama kayıt defteri** klasöründe bulunan uygulamalara yönelik özellikler penceresini açmak için:*

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacında, **Diğer** → **Uygulama yönetimi** → **Uygulama kayıt defteri** klasörünü seçin.
3. Bir uygulama seçin.
4. Uygulamanın içerik menüsünde **Özellikler**'i seçin.

   Özellikler: <Uygulama adı> penceresi açılır.

__Yürütülebilir dosyalar__ klasöründe bulunan yürütülebilir bir dosyanın özellikler penceresini açmak için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacında, **Diğer → Uygulama yönetimi → Yürütülebilir dosyalar** klasörünü seçin.
3. Yürütülebilir bir dosya seçin.
4. Yürütülebilir dosyanın içerik menüsünden **Özellikler**'i seçin.

   Özellikler: <Yürütülebilir dosya adı> penceresi açılır.

Uygulama kategorileri oluşturma

Kuralları oluştururken daha fazla kolaylık için uygulamaların kategorilerini oluşturabilirsiniz ve bunları Uygulama Başlatma Denetimi kurallarını oluştururken kullanabilirsiniz.

Şirkette kullanılan uygulamaların standart setini kapsayan bir "İş uygulamaları" kategorisi oluşturulması önerilir. Farklı kullanıcı grupları işlerinde farklı uygulama setleri kullanıyorsa her bir kullanıcı grubu için ayrı bir uygulama kategorisi oluşturulabilir.

Bir uygulama kategorisi oluşturmak için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacında, **Diğer → Uygulama yönetimi → Uygulama kategorileri** klasörünü seçin.
3. Çalışma alanında **Kategori oluştur** düğmesine tıklayın.

   Kullanıcı kategorisi oluşturma sihirbazı başlar.
4. Kullanıcı kategorisi oluşturma sihirbazının talimatlarını uygulayın.

Kaspersky Security Center'ı kullanarak Uygulama Başlatma Denetimi kuralları oluşturma

Kaspersky Security Center'ı kullanarak Uygulama Başlatma Denetimi kuralı oluşturmak için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, ilgili istemci bilgisayarların ait olduğu yönetim grubu adının bulunduğu klasörü açın.
3. Çalışma alanında, **İlkeler** sekmesini seçin.
4. Gereken ilkeyi seçin.
5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:

   - İlkenin içerik menüsünde **Özellikler**'i seçin.
   - Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.

6. **Uç nokta denetimi** bölümünde, **Uygulama Başlatma Denetimi** alt bölümünü seçin.

   Pencerenin sağında, Uygulama Başlatma Denetimi bileşeni ayarları görüntülenir.

7. **Ekle** düğmesine tıklayın.

   Uygulama Başlatma Denetimi kuralı penceresi açılır.

8. **Kategori** açılır listesinden kural oluştururken kullanmak istediğiniz oluşturulmuş uygulama kategorisini seçin.

9. Seçilen kategoriden uygulamaları başlatmak için izinlerini yapılandırmak istediğiniz kullanıcıların ve/veya kullanıcı gruplarının listesini belirleyin. Bunu yapmak için **Yöneticiler ve hakları** tablosunda **Ekle** düğmesine tıklayın.

   Microsoft Windows'ta standart **Kullanıcıları veya Grupları Seç** penceresi açılır. Bu pencere, kullanıcıları ve/veya kullanıcı gruplarını seçmenize olanak tanır.

10. **Yöneticiler ve hakları** tablosunda:

    - Kullanıcıların ve/veya kullanıcı gruplarının seçilen kategoriye ait uygulamaları başlatmalarına izin vermek isterseniz, bu kullanıcıların karşılarındaki **İzin ver** onay kutularını işaretleyin.
    - Kullanıcıların ve/veya kullanıcı gruplarının seçilen kategoriye ait uygulamaları başlatmalarını engellemek isterseniz, bu kullanıcıların karşılarındaki **Engelle** onay kutularını işaretleyin.

11. **Yöneticiler** sütununda görülmeyen ve **Yöneticiler** sütununda belirtilen kullanıcılar grubunun parçası olmayan tüm kullanıcıların seçilen kategorilere ait uygulamaları başlatmasının engellenmesini istiyorsanız **Diğer kullanıcılar için reddet** onay kutusunu seçin.

12. Kaspersky Endpoint Security'nin kuralda belirtilen kategorilerdeki uygulamaları, Uygulama Başlatma Denetimi kuralları tanımlanmamış diğer uygulamaları başlatma hakkına sahip güvenilir güncelleyiciler olarak değerlendirmesini istiyorsanız **Güvenilir Güncelleyiciler** onay kutusunu işaretleyin.

13. **Tamam**'a tıklayın.

14. İlke özellikleri penceresinin **Uygulama Başlatma Denetimi** bölümünde **Uygula** düğmesine tıklayın.

Kaspersky Security Center'ı kullanarak Uygulama Başlatma Denetimi kuralının durumunu değiştirme

Uygulama Başlatma Denetimi kuralının durumunu değiştirmek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, ilgili istemci bilgisayarların ait olduğu yönetim grubu adının bulunduğu klasörü açın.

3. Çalışma alanında, **İlkeler** sekmesini seçin.

4. Gereken ilkeyi seçin.

5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:

   - İlkenin içerik menüsünde **Özellikler**'i seçin.
   - Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.

6. **Uç nokta denetimi** bölümünde, **Uygulama Başlatma Denetimi** alt bölümünü seçin.
   Pencerenin sağında, Uygulama Başlatma Denetimi bileşeni ayarları görüntülenir.

7. Durumunu değiştirmek istediğiniz Uygulama Başlatma Denetimi kuralını seçin.

8. **Durum** sütununda aşağıdakilerden birini yapın:

   - Kural kullanımını etkinleştirmek isterseniz kuralın karşısındaki onay kutusunu seçin.
   - Kural kullanımını devre dışı bırakmak isterseniz kuralın karşısındaki onay kutusunun işaretini kaldırın.

9. **Uygula** düğmesine tıklayın.

Uygulama Ayrıcalığı Denetimi

Bu bileşen, İş istasyonları için Microsoft Windows'un kurulu olduğu bir bilgisayara Kaspersky Endpoint Security yüklendiğinde kullanılabilir. Bu bileşen, Dosya sunucuları için Microsoft Windows'un kurulu olduğu bir bilgisayara Kaspersky Endpoint Security yüklendiğinde kullanılamaz.

Bu bölümde, Uygulama Ayrıcalığı Denetimi ve bileşen ayarlarının nasıl yapılandırılacağı hakkında bilgiler bulunmaktadır.

Uygulama Ayrıcalığı Denetimi Hakkında

Uygulama Ayrıcalığı Denetimi, uygulamaların işletim sistemi için tehlikeli olabilecek işlemler yapmasını engeller ve işletim sistemi kaynaklarına ve kimlik verilerine erişim üzerinde denetim sağlar.

Bu bileşen, *uygulama denetimi kurallarını* kullanarak uygulamaların korunan kaynaklara (örn. Dosyalar ve klasörler, kayıt defteri anahtarları) erişimi dahil etkinliğini denetler. Uygulama denetimi kuralları, uygulamaların işletim sistemindeki çeşitli eylemleri ve bilgisayar kaynaklarına erişimleri için geçerli bir dizi kısıtlamadır.

Uygulamaların ağ etkinliği, Güvenlik Duvarı bileşeni tarafından izlenir.

Bir uygulama ilk kez başlatıldığında Uygulama Ayrıcalığı Denetimi, uygulamayı tarar ve bir güven grubuna yerleştirir. Güven grubu, Kaspersky Endpoint Security'nin uygulama etkinliğini denetlerken uyguladığı uygulama denetimi kurallarını tanımlar.

Uygulama Ayrıcalığı Denetiminin daha etkin çalışması için Kaspersky Security Network'e katılmanızı öneririz. Kaspersky Security Network üzerinden edinilen veriler, uygulamalarınızı daha doğru şekilde gruplandırmanıza ve optimum uygulama denetimi kuralları uygulamanıza olanak tanır.

Uygulama bir sonraki kez başlatıldığında, Uygulama Ayrıcalığı Denetimi uygulamanın bütünlüğünü doğrular. Uygulama değişmediyse bileşen geçerli uygulama denetimi kurallarını uygular. Uygulama değiştirildiyse Uygulama Ayrıcalığı Denetimi, ilk kez başlatılıyormuş gibi uygulamayı yeniden tarar.

Ses ve video aygıtı denetiminin sınırlamaları

Ses akışı koruması hakkında

Ses akışı korumasının aşağıdaki özel hususları bulunmaktadır:

- Bu işlevin çalışması için Sunucu Yetkisiz Erişim Önleme bileşeni etkin olmalıdır.
- Uygulama, ses akışını Sunucu Yetkisiz Erişim Önleme bileşeni başlatılmadan almaya başladıysa Kaspersky Endpoint Security uygulamanın ses akışını almasına izin verir ve herhangi bir bildirim göstermez.
- Uygulama ses akışını almaya başladıktan sonra uygulamayı **Güvenilmez** gruba ya da **Yüksek Sınırlamalı** gruba taşıdıysanız Kaspersky Endpoint Security, uygulamanın ses akışını almasına izin verir ve herhangi bir bildirim göstermez.

- Uygulamanın ses kayıt aygıtlarına erişimi için ayarlar değiştirildikten sonra (örn. Sunucu Yetkisiz Erişim Önleme ayarları penceresinde uygulamanın ses akışını alması engellendiyse) ses akışını almayı durdurmak için bu uygulamanın yeniden başlatılması gerekir.
- Ses kayıt aygıtlarından ses akışına erişimin kontrolü, uygulamanın web kamerası erişim ayarlarına bağlı değildir.
- Kaspersky Endpoint Security yalnızca entegre mikrofonlara ve dışarıdan mikrofonlara erişimi korur. Diğer ses akışı aygıtları desteklenmez.
- Kaspersky Endpoint Security, bir ses akışının DSLR kameralar, taşınabilir video kameralar ve aksiyon kameraları gibi aygıtlardan korunacağını garanti edemez.

Kaspersky Endpoint Security'nin kurulumu ve yükseltilmesi sırasında ses ve video aygıtlarının çalıştırılmasıyla ilgili özel hususlar

Kaspersky Endpoint Security'nin kurulmasından sonra ilk kez ses ve video kayıt veya oynatma uygulamalarını çalıştırdığınızda, ses ve video oynatma veya kaydetme kesintiye uğrayabilir. Uygulamalar tarafından ses kayıt aygıtlarına erişimi kontrol eden işlevi etkinleştirmek için bu gereklidir. Kaspersky Endpoint Security ilk kez çalıştırıldığında ses donanımını denetleyen sistem hizmeti yeniden başlatılır.

Web kameralarına uygulamaların erişimi hakkında

Web kamerası erişim koruması, aşağıdaki özel hususlara ve sınırlamalara sahiptir:

- Uygulama, web kamerası verilerinin işlenmesiyle elde edilmiş video ve resimleri denetler.
- Uygulama, web kamerasından alınan video akışının bir parçasıysa ses akışını denetler.
- Uygulama yalnızca USB veya IEEE1394 aracılığıyla bağlanmış, Windows Aygıt Yöneticisi tarafından **Görüntüleme Aygıtları** olarak gösterilen web kameralarını denetler.

Desteklenen web kameraları

Kaspersky Endpoint Security aşağıdaki web kameralarını destekler:

- Logitech HD Webcam C270
- Logitech HD Webcam C310
- Logitech Webcam C210
- Logitech Webcam Pro 9000
- Logitech HD Webcam C525
- Microsoft LifeCam VX-1000
- Microsoft LifeCam VX-2000
- Microsoft LifeCam VX-3000
- Microsoft LifeCam VX-800

- Microsoft LifeCam Cinema

Kaspersky, bu listede belirtilmeyen web kameralarının destekleneceğini garanti etmemektedir.

Sunucu Yetkisiz Erişim Önleme'yi etkinleştirme ve devre dışı bırakma

Varsayılan olarak, Sunucu Yetkisiz Erişim Önleme bileşeni etkinleştirilmiştir ve Kaspersky uzmanları tarafından önerilen modda çalışır. Gerekirse Sunucu Yetkisiz Erişim Önleme bileşenini devre dışı bırakabilirsiniz.

Sunucu Yetkisiz Erişim Önleme bileşenini etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresinde **Ayarlar** düğmesine tıklayın.
2. Pencerenin sol kısmında, **Gelişmiş Tehdit Koruması** bölümünde, **Sunucu Yetkisiz Erişim Önleme** seçeneğini belirleyin.

   Pencerenin sağ kısmında, Sunucu Yetkisiz Erişim Önleme bileşeni ayarları görüntülenir.
3. Pencerenin sağ tarafında aşağıdakilerden birini yapın:
   - Sunucu Yetkisiz Erişim Önleme bileşenini etkinleştirmek istiyorsanız **Sunucu Yetkisiz Erişim Önleme** onay kutusunu işaretleyin.
   - Sunucu Yetkisiz Erişim Önleme bileşenini devre dışı bırakmak istiyorsanız **Sunucu Yetkisiz Erişim Önleme** onay kutusunun işaretini kaldırın.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Uygulama güven gruplarını yönetme

Her uygulama ilk kez başlatıldığında Uygulama Ayrıcalığı Denetimi bileşeni, uygulamanın güvenliğini denetler ve uygulamayı bir güven grubuna yerleştirir.

Uygulama taramasının ilk aşamasında Kaspersky Endpoint Security, eşleşen bir giriş için bilinen uygulamaların dahili veritabanını arar ve eşzamanlı olarak Kaspersky Security Network veritabanına (İnternet bağlantısı varsa) bir istek gönderir. Dahili veritabanında ve Kaspersky Security Network veritabanında yapılan aramanın sonuçlarına dayanarak uygulama bir güven grubuna yerleştirilir. Uygulama her başlatıldığında Kaspersky Endpoint Security, KSN veritabanına yeni bir sorgu gönderir ve uygulamanın KSN veritabanlarındaki saygınlığı değiştiyse uygulamayı farklı bir güven grubuna yerleştirir.

Kaspersky Endpoint Security'nin bilinmeyen tüm uygulamaları otomatik olarak ataması için bir güven grubu seçebilirsiniz. Kaspersky Endpoint Security'den önce başlayan uygulamalar otomatik olarak **Güvenilirlik grubu seç** penceresinde belirtilen güven grubuna taşınır.

Bileşen sadece Güvenlik Duvarı ayarlarında düzenlenen ağ kurallarına dayanarak Kaspersky Endpoint Security'den önce başlatılan uygulamaların ağ etkinliğini denetler.

Güven gruplarına atanan uygulamalar için ayarları yapılandırma

Kaspersky Security Network'e katılım etkinleştirilirse uygulama her başlatıldığında Kaspersky Endpoint Security, KSN'ye uygulamanın saygınlığı hakkında bir sorgu gönderir. KSN'den gelen cevaba bağlı olarak uygulama, Uygulama Ayrıcalığı Denetimi ayarlarında belirtilenden farklı bir güven grubuna taşınabilir.

Uygulamaları güven gruplarına yerleştirme ayarlarını yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin solunda, **Uç nokta denetimi** bölümünde, **Uygulama Ayrıcalığı Denetimi** alt bölümünü seçin.

   Pencerenin sağında, Uygulama Ayrıcalığı Denetimi bileşeni ayarları görüntülenir.
3. Güvenilir satıcıların dijital imzalı uygulamalarını otomatik olarak Güvenilir gruba yerleştirmek isterseniz, **Dijital imzalı uygulamalara güven** onay kutusunu işaretleyin.

   Güvenilir satıcılar, Kaspersky tarafından güvenilir gruba dahil edilen yazılım satıcılarıdır. Güvenilir sistem sertifikası deposuna manuel olarak da satıcı sertifikası ekleyebilirsiniz.
4. Bilinmeyen uygulamaların güven gruplarına atanacağı yöntemi seçin:

   - Bilinmeyen uygulamaları güven gruplarına atamak amacıyla sezgisel analizi kullanmak için **Grubu tanımlamak için sezgisel analizi kullan** seçeneğini seçin ve **Grubu tanımlamak için en uzun süre** alanında başlatılan uygulamanın taranması için ayrılacak süreyi belirleyin.
   - Tüm bilinmeyen uygulamaları belirli bir güven grubuna atamak isterseniz **Gruba otomatik olarak taşı** seçeneğini seçin ve açılır listeden uygun güven grubunu seçin.

     Güvenlik nedeniyle **Güvenilir** grup, **Gruba otomatik olarak taşı** ayarının değerlerine dahil edilmemiştir.
5. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Güven grubunu değiştirme

Bir uygulama ilk kez başlatıldığında Kaspersky Endpoint Security otomatik olarak bu uygulamayı bir güven grubuna yerleştirir. Gerekirse uygulamayı elle başka bir güven grubuna taşıyabilirsiniz.

Kaspersky uzmanları, uygulamaların otomatik olarak atandıkları güven grubundan farklı bir güven grubuna taşınmasını önermez. Bunun yerine gerekirse tek bir uygulamanın haklarını değiştirebilirsiniz.

Bir uygulamanın ilk başlatıldığında Kaspersky Endpoint Security tarafından otomatik olarak atandığı güven grubunu değiştirmek için:

1. Ana uygulama penceresinde **Ayarlar** düğmesine tıklayın.
2. Pencerenin sol kısmında, **Gelişmiş Tehdit Koruması** bölümünde, **Sunucu Yetkisiz Erişim Önleme** seçeneğini belirleyin.

   Pencerenin sağ kısmında, Sunucu Yetkisiz Erişim Önleme bileşeni ayarları görüntülenir.
3. **Uygulamalar** düğmesine tıklayın.

   Bu, **Sunucu Yetkisiz Erişim Önleme** penceresinde **Uygulama hakları** sekmesini açar.

4. **Uygulama hakları** sekmesinden gerekli uygulamayı seçin.

5. Aşağıdakilerden birini yapın:

   - Uygulamanın içerik menüsünü görüntülemek için sağ tıklayın. Uygulamanın içerik menüsünde **Gruba taşı** → <γρυπ αδι> seçeneğini seçin.

   - İçerik menüsünü açmak için **Güvenilir** / **Düşük Sınırlamalı** / **Yüksek Sınırlamalı** / **Güvenilmez** bağlantısına tıklayın. İçerik menüsünde gereken uygulama grubunu seçin.

6. **Tamam**'a tıklayın.

7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Kaspersky Endpoint Security'den önce başlatılan uygulamalar için bir güven grubu seçme

Bileşen, yalnızca Kaspersky Endpoint Security'den önce başlatılan uygulamaların ağ etkinliğini denetler. Güvenlik Duvarı ayarlarında belirtilen ağ kurallarına göre denetim gerçekleştirilir. Bu tür uygulamaları izlemek için ağ etkinliğine uygulanması gereken ağ kurallarının belirlemek için bir güven grubu seçmeniz gerekir.

Kaspersky Endpoint Security'den önce başlatılan uygulamalar için bir güven grubunu seçmek için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin solunda, **Uç nokta denetimi** bölümünde, **Uygulama Ayrıcalığı Denetimi** alt bölümünü seçin.

   Pencerenin sağında, Uygulama Ayrıcalığı Denetimi bileşeni ayarları görüntülenir.

3. **Düzenle** düğmesine tıklayın.

   Uygulama grubu penceresi açılır.

4. Gerekli güven grubunu seçin.

5. **Tamam**'a tıklayın.

6. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Uygulama denetimi kurallarını yönetme

Varsayılan olarak uygulama etkinliği, Kaspersky Endpoint Security'nin uygulamayı ilk başlatmada atadığı güven grubu için tanımlanan uygulama denetimi kuralları tarafından denetlenir. Gerekirse bütün bir güven grubu, tek bir uygulamanın veya bir güven grubu içindeki bir grup uygulamanın uygulama denetimi kurallarını düzenleyebilirsiniz.

Tek tek uygulamalar ya da bir güven grubu içindeki uygulama gruplarının tanımlanmış uygulama denetimi kuralları, bir güven grubu için tanımlanmış uygulama denetimi kurallarına göre daha yüksek önceliğe sahiptir. Başka bir deyişle, tek bir uygulamanın ya da bir güven grubu içindeki bir grup uygulamanın uygulama denetimi kurallarının ayarları, güven grubunun uygulama denetimi kurallarının ayarlarından farklıysa Uygulama Ayrıcalığı Denetimi bileşeni, uygulamanın ya da güven grubu içindeki uygulama grubunun etkinliğini o uygulama ya da uygulama grubunun uygulama denetimi kurallarına göre denetler.

Güven grupları ve uygulama grupları için uygulama denetimi kurallarını değiştirme

Farklı güven grupları için en iyi uygulama denetimi kuralları varsayılan olarak oluşturulur. Uygulama grubu denetimi kurallarının ayarları, değerleri güven grubu denetim kurallarının ayarlarından devralır. Önceden ayarlanmış güven grubu denetim kurallarını ve uygulama grubu denetimi kurallarını düzenleyebilirsiniz.

Güven grubu denetim kurallarını veya uygulama grubu denetimi kurallarını düzenlemek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin solunda, **Uç nokta denetimi** bölümünde, **Uygulama Ayrıcalığı Denetimi** alt bölümünü seçin.

   Pencerenin sağında, Uygulama Ayrıcalığı Denetimi bileşeni ayarları görüntülenir.
3. **Uygulamalar** düğmesine tıklayın.

   Uygulama Ayrıcalığı Denetimi penceresinde **Uygulama Denetimi kuralları** sekmesini açar.
4. Gerekli güven grubunu veya uygulama grubunu seçin.
5. Bir güven grubunun veya uygulama grubunun içerik menüsünden **Grup kuralları**'nı seçin.

   Uygulama grubu denetim kuralları penceresi açılır.
6. **Uygulama grubu denetim kuralları** penceresinde aşağıdakilerden birini yapın:

   - İşletim sistemi kayıt defterine, kullanıcı dosyalarına ve uygulama ayarlarına erişim için güven grubunun veya uygulama grubunun haklarını yöneten güven grubu denetim kurallarını ve uygulama grubu denetim kurallarını düzenlemek için **Dosya ve sistem kayıt defteri** sekmesini seçin.
   - İşletim sistemi işlemlerine ve nesnelerine erişim için güven grubunun veya uygulama grubunun haklarını yöneten güven grubu denetim kurallarını ve uygulama grubu denetim kurallarını düzenlemek için **Haklar** sekmesini seçin.
7. Gerekli kaynak için ilişkili eylemin sütununda sağ tıklayarak içerik menüsünü açın.
8. İçerik menüsünden gerekli öğeyi seçin.

   - **Devral**
   - **İzin ver**
   - **Engelle**
   - **Olayları günlüğe kaydet**

   Güven grubu denetim kurallarını düzenliyorsanız **Devral** öğesi etkin değildir.
9. **Tamam**'a tıklayın.
10. **Uygulamalar** penceresinde **Tamam**'a tıklayın.
11. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Uygulama denetimi kuralını düzenleme

Varsayılan olarak, bir uygulama grubuna veya güven grubuna ait uygulamaların uygulama denetimi kuralları ayarları, güven grubu denetim kuralları ayarlarının değerlerini devralır. Uygulama denetimi kurallarının ayarlarını düzenleyebilirsiniz.

Bir uygulama denetimi kuralını değiştirmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin solunda, **Uç nokta denetimi** bölümünde, **Uygulama Ayrıcalığı Denetimi** alt bölümünü seçin.

   Pencerenin sağında, Uygulama Ayrıcalığı Denetimi bileşeni ayarları görüntülenir.
3. **Uygulamalar** düğmesine tıklayın.

   Uygulama Ayrıcalığı Denetimi penceresinde **Uygulama Denetimi kuralları** sekmesini açar.
4. Gereken uygulamayı seçin.
5. Aşağıdakilerden birini yapın:

   - Uygulamanın içerik menüsünden **Uygulama kuralları**'nı seçin.
   - **Uygulama denetimi kuralları** sekmesinin sağ alt köşesinde **Diğer** düğmesine tıklayın.

   Uygulama denetimi kuralları penceresi açılır.
6. **Uygulama denetimi kuralları** penceresinde aşağıdakilerden birini yapın:

   - Uygulamanın işletim sistemi kayıt defterine, kullanıcı dosyalarına ve uygulama ayarlarına erişim haklarını yöneten uygulama denetimi kurallarını düzenlemek için **Dosya ve sistem kayıt defteri** sekmesini seçin.
   - Uygulamanın işletim sistemi işlemlerine ve nesnelerine erişim haklarını yöneten uygulama denetimi kurallarını düzenlemek için **Haklar** sekmesini seçin.
7. Gerekli kaynak için ilişkili eylemin sütununda sağ tıklayarak içerik menüsünü açın.
8. İçerik menüsünden gerekli öğeyi seçin.

   - **Devral**
   - **İzin ver**
   - **Engelle**
   - **Olayları günlüğe kaydet**
9. **Tamam**'a tıklayın.
10. **Uygulamalar** penceresinde **Tamam**'a tıklayın.
11. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Kaspersky Security Network veritabanından uygulama denetimi kurallarının indirilmesini ve güncellenmesini devre dışı bırakma

Varsayılan olarak Kaspersky Security Network veritabanında bir uygulamayla ilgili yeni bir bilgi algılandığında Kaspersky Endpoint Security, bu uygulama için KSN veritabanından indirilen denetim kurallarını uygular. Daha sonra uygulamanın denetim kurallarını elle düzenleyebilirsiniz.

Bir uygulama ilk kez başlatıldığında Kaspersky Security Network veritabanında yoksa ancak bu uygulamayla ilgili bilgi daha sonra veritabanına eklendiyse varsayılan olarak Kaspersky Endpoint Security bu uygulamanın denetim kurallarını otomatik olarak günceller.

Kaspersky Security Network veritabanından uygulama denetimi kurallarının indirilmesini ve daha önceden bilinmeyen uygulamaların denetim kurallarının otomatik güncellemelerini devre dışı bırakabilirsiniz.

Kaspersky Security Network veritabanından uygulama denetimi kurallarının indirilmesini ve güncellenmesini devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin solunda, **Uç nokta denetimi** bölümünde, **Uygulama Ayrıcalığı Denetimi** alt bölümünü seçin.

   Pencerenin sağında, Uygulama Ayrıcalığı Denetimi bileşeni ayarları görüntülenir.
3. **Önceden bilinmeyen uygulamalar için denetim kurallarını KSN veritabanlarından güncelle** onay kutusunu temizleyin.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Üst işlemden sınırlamaları devralmayı devre dışı bırakma

Uygulama başlatma, kullanıcı veya bir başka çalışan uygulama tarafından başlatılabilir. Uygulama başlatma bir başka uygulama tarafından başlatıldığında üst ve bağlı işlemlerden oluşan bir başlatma dizisi oluşturulur.

Bir uygulama tarafından korunan bir kaynağa erişim elde etme girişiminde bulunulduğunda Uygulama Ayrıcalığı Denetimi, uygulamanın tüm üst işlemlerini, bu işlemlerin korunan kaynağa erişim hakkının olup olmadığını belirlemek için analiz eder. Bundan sonra, minimum öncelik kuralına uyulur: uygulamanın erişim haklarını üst işlemin haklarıyla karşılaştırırken, uygulamanın etkinliğine minimum öncelikli erişim hakları uygulanır.

Erişim haklarının önceliği aşağıdakiler gibidir:

1. **İzin ver** Erişim hakları en yüksek önceliğe sahiptir.
2. **Engelle** Bu erişim hakları en düşük önceliğe sahiptir.

Bu mekanizma, güvenilir olmayan bir uygulamanın veya sınırlı haklara sahip bir uygulamanın belirli ayrıcalıkları gerektiren eylemleri gerçekleştirmek için güvenilir bir uygulamayı kullanmasını önler.

Bir uygulamanın etkinliği, bir üst işleme sağlanan hakların eksikliği nedeniyle engellenirse bu hakları düzenleyebilirsiniz veya üst işlemden sınırlamaları devralmayı devre dışı bırakabilirsiniz.

Üst işlemden sınırlamaları devralmayı devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin solunda, **Uç nokta denetimi** bölümünde, **Uygulama Ayrıcalığı Denetimi** alt bölümünü seçin.
   Pencerenin sağında, Uygulama Ayrıcalığı Denetimi bileşeni ayarları görüntülenir.
3. **Uygulamalar** düğmesine tıklayın.
   Uygulama Ayrıcalığı Denetimi penceresinde **Uygulama Denetimi kuralları** sekmesini açar.
4. Gereken uygulamayı seçin.
5. Uygulamanın içerik menüsünden **Uygulama kuralları**'nı seçin.
   Uygulama denetimi kuralları penceresi açılır.
6. **Uygulama denetimi kuralları** penceresinde **İstisnalar** sekmesine tıklayın.
7. **Üst işlemin (uygulama) sınırlamalarını devralma** onay kutusunu işaretleyin.
8. **Tamam**'a tıklayın.
9. **Uygulamalar** penceresinde **Tamam**'a tıklayın.
10. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Belirli uygulama eylemlerini uygulama denetimi kurallarının dışında tutma

Belirli uygulama eylemlerini uygulama denetimi kurallarının dışında tutmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin solunda, **Uç nokta denetimi** bölümünde, **Uygulama Ayrıcalığı Denetimi** alt bölümünü seçin.
   Pencerenin sağında, Uygulama Ayrıcalığı Denetimi bileşeni ayarları görüntülenir.
3. **Uygulamalar** düğmesine tıklayın.
   Uygulama Ayrıcalığı Denetimi penceresinde **Uygulama Denetimi kuralları** sekmesini açar.
4. Gereken uygulamayı seçin.
5. Uygulamanın içerik menüsünden **Uygulama kuralları**'nı seçin.
   Uygulama denetimi kuralları penceresi açılır.
6. **İstisnalar** sekmesini seçin.
7. İzlenmesine ihtiyaç duyulmayan uygulama eylemlerinin yanındaki onay kutularını işaretleyin.
8. **Tamam**'a tıklayın.
9. **Uygulamalar** penceresinde **Tamam**'a tıklayın.
10. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Eski uygulama denetimi kurallarını kaldırma

Varsayılan olarak, 60 gün içinde başlatılmayan uygulamaların denetim kuralları otomatik olarak silinir. Kullanılmayan uygulamaların denetim kurallarının saklanma süresini değiştirebilir veya kuralların otomatik silinmesini devre dışı bırakabilirsiniz.

Eski uygulama denetimi kurallarını kaldırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin solunda, **Uç nokta denetimi** bölümünde, **Uygulama Ayrıcalığı Denetimi** alt bölümünü seçin.

   Pencerenin sağında, Uygulama Ayrıcalığı Denetimi bileşeni ayarları görüntülenir.
3. Aşağıdakilerden birini yapın:
   - Kaspersky Endpoint Security'nin kullanılmayan uygulamaların denetim kurallarını silmesini istiyorsanız **Şundan daha uzun süre başlatılmayan uygulama kurallarını sil** onay kutusunu işaretleyin ve ilgili gün sayısını belirtin.
   - Kullanılmayan uygulamaların denetim kurallarının otomatik olarak silinmesini devre dışı bırakmak için **Şundan daha uzun süre başlatılmayan uygulama kurallarını sil** onay kutusunu işaretleyin.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

İşletim sistemi kaynaklarını ve kimlik verilerini koruma

Uygulama Ayrıcalığı Denetimi, çeşitli işletim sistemi kaynağı ve kimlik verisi kategorileri üzerinde işlem yapmak için gereken uygulama haklarını yönetir.

Kaspersky uzmanları, önceden ayarlanmış korunan kaynaklar kategorileri oluşturmuştur. Önceden ayarlanmış korunan kaynaklar kategorilerini ya da bu kategorilerdeki korunan kaynakları düzenleyemez ya da silemezsiniz.

Aşağıdaki eylemleri yapabilirsiniz:

- Yeni bir korunan kaynaklar kategorisi ekleyebilirsiniz.
- Yeni bir korunan kaynak ekleyebilirsiniz.
- Bir kaynağın korumasını devre dışı bırakabilirsiniz.

Korunan kaynaklar kategorisi ekleme

Yeni bir korunan kaynaklar kategorisi eklemek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin solunda, **Uç nokta denetimi** bölümünde, **Uygulama Ayrıcalığı Denetimi** alt bölümünü seçin.

   Pencerenin sağında, Uygulama Ayrıcalığı Denetimi bileşeni ayarları görüntülenir.

3. **Kaynaklar** düğmesine tıklayın.

   Uygulama Ayrıcalığı Denetimi penceresinde **Korunan kaynaklar** sekmesi açılır.

4. **Korunan kaynaklar** sekmesinin sol kısmında bir bölüm veya yeni bir korunan kaynaklar kategorisi eklemek istediğiniz korunan kaynaklar kategorisini seçin.

5. **Ekle** düğmesine tıklayın ve açılır listeden **Kategori** seçin.

   Korunan kaynaklar kategorisi penceresi açılır.

6. Açılan **Korunan kaynaklar kategorisi** penceresinde yeni korunan kaynaklar kategorisi için bir ad girin.

7. **Tamam**'a tıklayın.

   Korunan kaynaklar kategorisi listesinde yeni bir öğe görünür.

8. **Uygulama Ayrıcalığı Denetimi** penceresinde **Tamam**'a tıklayın.

9. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Bir korunan kaynaklar kategorisi ekledikten sonra, bunu **Korunan kaynaklar** sekmesinin sol üst kısmında **Düzenle** veya **Kaldır** düğmelerine tıklayarak düzenleyebilir veya kaldırabilirsiniz.

Korunan kaynak ekleme

Bir korunan kaynak eklemek için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin solunda, **Uç nokta denetimi** bölümünde, **Uygulama Ayrıcalığı Denetimi** alt bölümünü seçin.

   Pencerenin sağında, Uygulama Ayrıcalığı Denetimi bileşeni ayarları görüntülenir.

3. **Kaynaklar** düğmesine tıklayın.

   Uygulama Ayrıcalığı Denetimi penceresinde **Korunan kaynaklar** sekmesi açılır.

4. **Korunan kaynaklar** sekmesinin sol kısmında yeni bir korunan kaynak eklemek istediğiniz korunan kaynaklar kategorisini seçin.

5. **Ekle** düğmesine tıklayın ve eklemek istediğiniz kaynak türünü açılır listeden seçin.

   - **Dosya veya klasör**.
   - **Kayıt defteri anahtarı**.

   Korunan kaynaklar penceresi açılır.

6. **Korunan kaynaklar** penceresinde, korunan kaynağın adını **Ad** alanına girin.

7. **Gözat** düğmesine tıklayın.

8. Açılan pencerede eklemek istediğiniz korunan kaynağın türüne bağlı olarak gerekli ayarları belirleyin. **Tamam**'a tıklayın.

9. **Korunan kaynak** penceresinde **Tamam**'a tıklayın.

   Korunan kaynaklar sekmesinde seçilen kategorinin korunan kaynaklar listesinde yeni bir öğe görünür.

10. **Uygulama Ayrıcalığı Denetimi** penceresinde **Tamam**'a tıklayın.

11. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Bir korunan kaynak ekledikten sonra, bunu **Korunan kaynaklar** sekmesinin sol üst kısmında **Düzenle** veya **Kaldır** düğmelerine tıklayarak düzenleyebilir veya kaldırabilirsiniz.

Kaynak korumasını devre dışı bırakma

Kaynak korumasını devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin solunda, **Uç nokta denetimi** bölümünde, **Uygulama Ayrıcalığı Denetimi** alt bölümünü seçin.

   Pencerenin sağında, Uygulama Ayrıcalığı Denetimi bileşeni ayarları görüntülenir.

3. Pencerenin sağ kısmında, **Kaynaklar** düğmesine tıklayın.

   Uygulama Ayrıcalığı Denetimi penceresinde **Korunan kaynaklar** sekmesi açılır.

4. Aşağıdakilerden birini yapın:

   - Sekmenin sol kısmında korunan kaynaklar listesinde, korumayı devre dışı bırakmak istediğiniz kaynağı seçin ve isminin yanındaki onay kutusunu işaretlemeyin.

   - **İstisnalar**'a tıklayın ve aşağıdakileri yapın:

     a. **İstisnalar** penceresinde **Ekle** düğmesine tıklayın. Açılır listede, Uygulama Ayrıcalığı Denetimi bileşeni tarafından korumadan istisna tutulacaklar listesine eklemek istediğiniz kaynağın türünü seçin: **Dosya veya klasör** veya **Kayıt defteri anahtarı**.

     Korunan kaynaklar penceresi açılır.

     b. **Korunan kaynaklar** penceresinde, korunan kaynağın adını **Ad** alanına girin.

     c. **Gözat** düğmesine tıklayın.

     d. Açılan pencerede, Uygulama Ayrıcalığı Denetimi bileşeni tarafından korumadan istisna tutulacaklar listesine eklemek istediğiniz koruma kaynağı türüne bağlı olarak gerekli ayarları belirleyin.

     e. **Tamam**'a tıklayın.

     f. **Korunan kaynak** penceresinde **Tamam**'a tıklayın.

     Uygulama Ayrıcalığı Denetimi bileşeni tarafından korumadan istisna tutulan kaynaklar listesinde yeni bir öğe görünür.

Uygulama Ayrıcalığı Denetimi tarafından korumadan istisna tutulanlar listesine bir kaynak ekledikten sonra, bu kaynağı **İstisnalar** penceresinin üst kısmındaki **Düzenle** veya **Kaldır** düğmelerine tıklayarak düzenleyebilir veya kaldırabilirsiniz.

g. **İstisnalar** penceresinde **Tamam**'a tıklayın.

5. **Uygulama Ayrıcalığı Denetimi** penceresinde **Tamam**'a tıklayın.

6. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Zayıf Nokta İzleyicisi

Bu bileşen, İş istasyonları için Microsoft Windows'un kurulu olduğu bir bilgisayara Kaspersky Endpoint Security yüklendiğinde kullanılabilir. Bu bileşen, Kaspersky Endpoint Security Windows for File Servers ile çalışan bir bilgisayara kurulduğunda kullanılamaz.

Bu bölüm, Zayıf Nokta İzleyicisi hakkında bilgiler ve bileşenin nasıl etkinleştirileceği veya devre dışı bırakılacağı konusunda talimatlar içermektedir.

Zayıf Nokta İzleyicisi Hakkında

Zayıf Nokta İzleyicisi bileşeni, kullanıcının bilgisayarında çalışan ve kullanıcı tarafından başlatılan uygulamaların gerçek zamanlı zayıf nokta taramasını çalıştırır. Zayıf Nokta İzleyicisi bileşeni etkinleştirildiğinde Zayıf Nokta Taraması görevini başlatmanıza gerek yoktur. Bu tarama, kullanıcının bilgisayarında yüklü olan uygulamalar için bir Zayıf Nokta Taraması görevi gerçekleştirilmediğinde veya uzun zaman önce gerçekleştirildiğinde gereklidir.

Zayıf Nokta İzleyicisi'ni etkinleştirme ve devre dışı bırakma

Zayıf Nokta İzleyicisi bileşeni varsayılan olarak devre dışıdır. Gerekirse Zayıf Nokta İzleyicisi'ni etkinleştirebilirsiniz.

Bileşeni etkinleştirmenin veya devre dışı bırakmanın iki yolu bulunmaktadır:

- Ana uygulama penceresinin **Koruma ve Denetim** sekmesinde
- Uygulama ayarları penceresinden.

Ana uygulama penceresinin Koruma ve Denetim sekmesinde Zayıf Nokta İzleyicisi'ni etkinleştirmek veya devre dışı bırakmak için:

1. Ana uygulama penceresini açın.
2. **Koruma ve Denetim** sekmesini seçin.
3. **Uç nokta denetimi** bölümüne tıklayın.
   Uç nokta denetimi bölümü açılır.
4. Sağ tıklayarak, Zayıf Nokta İzleyicisi bileşeni hakkında bilgi içeren satırın içerik menüsünü açın.
   Bileşenlere uygulanacak eylemlerin seçilebileceği bir menü açılır.
5. Aşağıdakilerden birini yapın:
   - Zayıf Nokta İzleyicisi'ni etkinleştirmek için **Başlat**'ı seçin.
     Zayıf Nokta İzleyicisi satırında solda görüntülenen bileşen durumu simgesi , simgesine dönüşür.
   - Zayıf Nokta İzleyicisi'ni devre dışı bırakmak için **Durdur**'u seçin.
     Zayıf Nokta İzleyicisi satırında solda görüntülenen bileşen durumu simgesi , simgesine dönüşür.

Uygulama ayarları penceresinden Zayıf Nokta İzleyicisi'ni etkinleştirmek veya devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol tarafında, **Uç nokta denetimi** bölümünde **Zayıf Nokta İzleyicisi**'ni seçin.

   Pencerenin sağ kısmında, Zayıf Nokta İzleyicisi bileşeninin ayarları görüntülenir.
3. Pencerenin sağ tarafında aşağıdakilerden birini yapın:

   - Kaspersky Endpoint Security'nin kullanıcının bilgisayarında çalışan veya kullanıcı tarafından başlatılan uygulamalarda bir zayıf nokta taraması başlatmasını istiyorsanız **Zayıf Nokta İzleyicisini Etkinleştir** onay kutusunu işaretleyin.
   - Kaspersky Endpoint Security'nin kullanıcının bilgisayarında çalışan veya kullanıcı tarafından başlatılan uygulamalarda bir zayıf nokta taraması başlatmasını istemiyorsanız **Zayıf Nokta İzleyicisini Etkinleştir** onay kutusunu işaretlemeyin.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Aygıt Denetimi

Bu bileşen, İş istasyonları için Microsoft Windows'un kurulu olduğu bir bilgisayara Kaspersky Endpoint Security yüklendiğinde kullanılabilir. Bu bileşen, Dosya sunucuları için Microsoft Windows'un kurulu olduğu bir bilgisayara Kaspersky Endpoint Security yüklendiğinde kullanılamaz.

Bu bölümde, Aygıt Denetimi hakkında bilgiler ve bileşen ayarlarını yapılandırmak için talimatlar bulunmaktadır.

Aygıt Denetimi Hakkında

Aygıt Denetimi, aşağıdakiler dahil bilgisayara yüklenen veya bağlanan aygıtlara kullanıcı erişimini kısıtlayarak gizli verilerin güvenliğini sağlar:

- Veri depolama aygıtları (sabit sürücüler, çıkarılabilir sürücüler, kaset sürücüler, CD/DVD sürücüleri)
- Veri aktarma araçları (modemler, harici ağ kartları)
- Verileri basılı kopyalara dönüştürmek için tasarlanmış aygıtlar (yazıcılar)
- Aygıtların bilgisayara bağlanmasını sağlayan arabirimlerin (USB, FireWire ve Kızılötesi gibi) bağlantı veri yolları ("sadece veri yolu" olarak da ifade edilir)

Aygıt Denetimi, *aygıtlara erişim kuralları* ("erişim kuralları" olarak da ifade edilir) ve *bağlantı veri yolu erişim kuralları* ("veri yolu erişim kuralları" olarak da ifade edilir) uygulayarak aygıtlara kullanıcı erişimini yönetir.

Aygıt Denetimini etkinleştirme ve devre dışı bırakma

Varsayılan olarak Aygıt Denetimi etkindir. Gerekirse Aygıt Denetimi'ni devre dışı bırakabilirsiniz.

Bileşeni etkinleştirmenin veya devre dışı bırakmanın iki yolu bulunmaktadır:

- Ana uygulama penceresinde **Koruma ve Denetim** sekmesinde
- Uygulama ayarları penceresinden.

*Ana uygulama penceresinin **Koruma ve Denetim** sekmesinde Aygıt Denetimi'ni etkinleştirmek veya devre dışı bırakmak için:*

1. Ana uygulama penceresini açın.
2. **Koruma ve Denetim** sekmesini seçin.
3. **Uç nokta denetimi** bölümüne tıklayın.

   Uç nokta denetimi bölümü açılır.
4. Sağ tıklayarak, Aygıt Denetimi bileşeni hakkında bilgi içeren satırın içerik menüsünü açın.

   Bileşenlere uygulanacak eylemlerin seçilebileceği bir menü açılır.
5. Aşağıdakilerden birini yapın:

- Aygıt Denetimi'ni etkinleştirmek için menüden **Başlat**'ı seçin.
- Aygıt Denetimi'ni devre dışı bırakmak için menüden **Durdur**'u seçin.

Uygulama ayarları penceresinden Aygıt Denetimi'ni etkinleştirmek veya devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Uç nokta denetimi** bölümünde, **Aygıt Denetimi** alt bölümünü seçin.
   Pencerenin sağ kısmında, Aygıt Denetimi bileşeni ayarları görüntülenir.
3. Aşağıdakilerden birini yapın:
   - Aygıt Denetimi'ni etkinleştirmek istiyorsanız **Aygıt Denetimini etkinleştir** onay kutusunu işaretleyin.
   - Aygıt Denetimi'ni devre dışı bırakmak istiyorsanız **Aygıt Denetimini etkinleştir** onay kutusunu işaretlemeyin.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Aygıtlar ve bağlantı veri yollarına erişim kuralları hakkında

Bir aygıt erişim kuralı, Aygıt Denetimi bileşeninin aşağıdaki işlevlerini tanımlayan parametrelerin birleşimidir:

- Seçilen kullanıcılar ve / veya kullanıcı grubunun belirli zamanlarda belirli türde aygıtlara erişimine izin verme.
  Bir kullanıcı ve / veya kullanıcı grubu seçerek onlar için bir aygıt erişim zamanlaması oluşturabilirsiniz.
- Bellek aygıtlarının içeriğini okuma hakkını ayarlama.
- Bellek aygıtlarının içeriğini düzenleme hakkını ayarlama.

Varsayılan olarak, erişim kuralları Aygıt Denetimi bileşeninin sınıflandırılmasında her tür aygıt için oluşturulur. Bu kurallar, ilgili aygıt türlerinin bağlantı veri yollarına erişime izin veriliyorsa bütün kullanıcılara aygıtlara her zaman tam erişim sunar.

Bağlantı veri yolu erişim kuralı, bağlantı erişim yoluna erişime izin verir ya da erişimi engeller.

Veri yollarına erişime izin veren kurallar, varsayılan olarak Aygıt Denetimi bileşeni sınıflandırmasında bulunan bütün bağlantı veri yolları için oluşturulur.

Aygıt erişim kurallarını veya bağlantı veri yolu erişim kurallarını oluşturamaz veya silemezsiniz; yalnızca düzenleyebilirsiniz.

Güvenilir aygıtlar hakkında

Güvenilir aygıtlar, güvenilir aygıt ayarlarında belirtilen kullanıcıların her zaman tam erişime sahip olduğu aygıtlardır.

Güvenilir aygıtlarla çalışırken aşağıdaki eylemler kullanılabilir:

- Aygıtı güvenilir aygıtlar listesine ekleyebilirsiniz.
- Güvenilir aygıta erişimine izin verilen kullanıcı ve / veya kullanıcı grubunu değiştirebilirsiniz.

- Aygıtı güvenilir aygıtlar listesinden silebilirsiniz.

Bir aygıtı güvenilir aygıtlar listesine eklediyseniz ve erişimi engelleyen veya kısıtlayan bu aygıt türü için bir erişim kuralı oluşturduysanız Kaspersky Endpoint Security, güvenilir aygıtlar listesinde bulunup bulunmadığına bağlı olarak aygıta erişim sağlanıp sağlanmayacağına karar verir. Güvenilir aygıtlar listesinde bulunmak, bir erişim kuralından daha yüksek önceliğe sahiptir.

Aygıtlara erişim hakkında standart kararlar

Kaspersky Endpoint Security, kullanıcı aygıtı bilgisayara bağladıktan sonra aygıta erişime izin verip vermeyeceği hakkında bir karar verir.

Aygıtlara erişim hakkında standart kararlar

No.	Başlangıç koşulları	Aygıta erişim hakkında bir karar verilene kadar atılacak ara adımlar			Aygıta erişim hakkında karar
		Aygıtın güvenilir aygıtlar listesinde olup olmadığını kontrol etme	Erişim kuralına dayanarak aygıta erişimi test etme	Veri yolu erişim kuralına dayanarak veri yoluna erişimi test etme	
1	Aygıt, Aygıt Denetimi bileşeninin aygıt sınıflandırmasında mevcut değil.	Güvenilir aygıtlar listesinde yok.	Erişim kuralı yok.	Taramaya tabi değil.	Erişime izin verildi.
2	Aygıt güvenilir.	Güvenilir aygıtlar listesinde var.	Taramaya tabi değil.	Taramaya tabi değil.	Erişime izin verildi.
3	Aygıta erişime izin verildi.	Güvenilir aygıtlar listesinde yok.	Erişime izin verildi.	Taramaya tabi değil.	Erişime izin verildi.
4	Aygıta erişim, veri yoluna bağlıdır.	Güvenilir aygıtlar listesinde yok.	Erişim veri yoluna bağlıdır.	Erişime izin verildi.	Erişime izin verildi.
5	Aygıta erişim, veri yoluna bağlıdır.	Güvenilir aygıtlar listesinde yok.	Erişim veri yoluna bağlıdır.	Erişim engellendi.	Erişim engellendi.
6	Aygıta erişime izin verildi. Veri yolu erişim kuralı bulunamadı.	Güvenilir aygıtlar listesinde yok.	Erişime izin verildi.	Veri yolu erişim kuralı yok.	Erişime izin verildi.
7	Aygıta erişim engellendi.	Güvenilir aygıtlar listesinde yok.	Erişim engellendi.	Taramaya tabi değil.	Erişim engellendi.
8	Aygıt erişim kuralı ya da veri yolu erişim kuralı bulunamadı.	Güvenilir aygıtlar listesinde yok.	Erişim kuralı yok.	Veri yolu erişim kuralı yok.	Erişime izin verildi.

9	Aygıt erişim kuralı yok.	Güvenilir aygıtlar listesinde yok.	Erişim kuralı yok.	Erişime izin verildi.	Erişime izin verildi.
10	Aygıt erişim kuralı yok.	Güvenilir aygıtlar listesinde yok.	Erişim kuralı yok.	Erişim engellendi.	Erişim engellendi.

Aygıtı bağladıktan sonra aygıt erişim kuralını düzenleyebilirsiniz. Aygıt bağlandıysa ve erişim kuralı erişime izin veriyorsa ancak daha sonra erişim kuralını düzenleyip erişimi engellerseniz bir daha aygıttan herhangi bir dosya işlemi (klasör ağacını görüntüleme, okuma, yazma) talep edildiğinde Kaspersky Endpoint Security erişimi engeller. Dosya sistemi olmayan bir aygıt ancak aygıt bir sonraki kez bağlandığında engellenir.

Kaspersky Endpoint Security kurulu bir bilgisayarın kullanıcısının, yanlışlıkla engellendiğini düşündüğü bir aygıta erişim talep etmesi gerekiyorsa kullanıcıya erişim isteme talimatlarını gönderin.

Aygıt erişim kuralını düzenleme

Aygıt türüne bağlı olarak aygıta erişim sağlayan kullanıcıların listesi, erişim zamanlaması ve izin verilen / engellenen erişim gibi çeşitli erişim ayarlarını değiştirebilirsiniz.

Bir aygıt erişim kuralını düzenlemek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Uç nokta denetimi** bölümünde, **Aygıt Denetimi** alt bölümünü seçin.

   Pencerenin sağ kısmında, Aygıt Denetimi bileşeni ayarları görüntülenir.
3. Pencerenin sağ kısmında, **Aygıt türleri** sekmesini seçin.

   Aygıt türleri sekmesi, Aygıt Denetimi bileşeni sınıflandırmasında yer alan tüm aygıtların erişim kurallarını içerir.
4. Düzenlemek istediğiniz erişim kuralını seçin.
5. **Düzenle** düğmesine tıklayın. Bu düğme sadece dosya sistemine sahip aygıt türleriyle kullanılabilir.

   Aygıta erişim kuralı yapılandırılıyor penceresi açılır.

   Varsayılan olarak aygıt erişim kuralı, tüm kullanıcılara herhangi bir zamanda belirtilen türden cihazlara tam erişim sağlar. **Kullanıcılar ve/veya kullanıcı grupları** listesinde bu erişim kuralı **Tüm** grupları içerir. **Seçilen kullanıcı grubunun erişim zamanlamalarına göre hakları** tablosunda bu erişim kuralı, aygıtlarla her tür işlemi gerçekleştirme haklarının bulunduğu aygıtlara erişim için **Varsayılan zamanlama**'yı içerir.
6. Aygıta erişim kuralının ayarlarını düzenleme:

   a. **Kullanıcılar ve/veya kullanıcı grupları** listesinden bir kullanıcılar ve/veya kullanıcı grubu seçin.

      Kullanıcılar ve/veya kullanıcı grupları listesini düzenlemek için **Ekle**, **Düzenle** ve **Kaldır** düğmelerini kullanın.

   b. **Seçilen kullanıcı grubunun erişim zamanlamalarına göre hakları** tablosunda, seçilen kullanıcılar ve/veya kullanıcı grupları için aygıta erişim zamanlamasını yapılandırın. Bu amaçla, düzenlenecek aygıt erişim kuralında kullanmak istediğiniz aygıtların erişim zamanlamasının adlarının karşısındaki onay kutularını işaretleyin.

      Aygıtların erişim zamanlamalarının listesini düzenlemek için **Seçilen kullanıcı grubunun erişim zamanlamalarına göre hakları** tablosundaki **Oluştur**, **Düzenle**, **Kopyala** ve **Kaldır** düğmelerini kullanın.

c. Düzenlenen kuralda kullanılan her bir aygıtın erişim kodu zamanlaması için aygıtlarla çalışırken izin verilen işlemleri belirtin. Bunun için **Seçilen kullanıcı grubunun erişim zamanlamalarına göre hakları** tablosunda, ilgili işlemlerin adlarının yer aldığı sütunlardaki onay kutularını işaretleyin.

d. **Tamam**'a tıklayın.

Bir aygıt erişim kuralının varsayılan ayarlarını düzenledikten sonra, **Aygıt türleri** sekmesinde tablodaki **Erişim** sütunundaki aygıt türüne erişim ayarları *Kurallara göre kısıtla* değeriyle değiştirilir.

7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Olay günlüğüne kayıtları ekleme veya günlük dışında tutma

Olay günlüğü tutma yalnızca çıkarılabilir sürücülerdeki dosyalarla işlemler için mevcuttur.

Olay günlüğü tutmayı etkinleştirmek veya devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Uç nokta denetimi** bölümünde, **Aygıt Denetimi** alt bölümünü seçin.

   Pencerenin sağ kısmında, Aygıt Denetimi bileşeni ayarları görüntülenir.
3. Pencerenin sağ kısmında, **Aygıt türleri** sekmesini seçin.

   Aygıt türleri sekmesi, Aygıt Denetimi bileşeni sınıflandırmasında yer alan tüm aygıtların erişim kurallarını içerir.
4. Aygıtlar tablosunda **Çıkarılabilir sürücüler**'i seçin.

   Tablonun üst kısmında **Günlük Tutma** düğmesi görülür.
5. **Günlük Tutma** düğmesine tıklayın.

   Günlük Ayarları penceresi açılır.
6. Aşağıdakilerden birini yapın:

   - Çıkarılabilir sürücülerdeki dosya silme ve yazma işlemlerinin günlüğünün oluşturulmasını etkinleştirmek istiyorsanız **Günlük oluşturmayı etkinleştir** onay kutusunu seçin.

     Kullanıcı, çıkarılabilir sürücülerdeki dosyalarla yazma veya silme işlemleri yaptığı her seferde Kaspersky Endpoint Security günlük dosyasına bir olay kaydeder ve Kaspersky Security Center Yönetim Sunucusu'na bir mesaj gönderir.

   - İstemiyorsanız **Günlük oluşturmayı etkinleştir** onay kutusunu işaretlemeyin.
7. Hangi işlemlerin kaydedileceğini belirtin. Bunun için aşağıdakilerden birini gerçekleştirin:

   - Kaspersky Endpoint Security'nin bütün olayları kaydetmesini istiyorsanız **Tüm dosyalar hakkındaki bilgileri kaydet** onay kutusunu seçin.

   - Kaspersky Endpoint Security'nin yalnızca belirli bir formattaki dosyalar hakkında bilgileri kaydetmesini istiyorsanız **Dosya formatı filtreleri** bölümünde ilgili dosya formatlarının karşısındaki onay kutularını seçin.
8. Hangi Kaspersky Endpoint Security kullanıcılarının eylemlerinin olay olarak kaydedilmesi gerektiğini belirtin. Bunun için:

a. **Kullanıcılar** bölümünde **Seç** düğmesine tıklayın.

Microsoft Windows'ta standart **Kullanıcıları veya Grupları Seç** penceresi açılır.

b. Kullanıcılar ve/veya kullanıcı grupları listesini belirtin ya da düzenleyin.

Kullanıcılar alanında belirtilen kullanıcılar çıkarılabilir sürücülerdeki dosyalara yazdığında ya da çıkarılabilir sürücülerden dosya sildiklerinde Kaspersky Endpoint Security bu işlemler hakkında olay günlüğüne bilgi kaydeder ve Kaspersky Security Center Yönetim Sunucusu'na bir mesaj gönderir.

9. **Günlük ayarları** penceresinde **Tamam**'a tıklayın.

10. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Çıkarılabilir sürücülerdeki dosyalarla ilişkili olayları Kaspersky Security Center Yönetim Konsolunda **Olaylar** sekmesindeki **Yönetim Sunucusu** düğümünün çalışma alanından görüntüleyebilirsiniz. Olayların yerel Kaspersky Endpoint Security olay günlüğünde görüntülenmesi için, Aygıt Kontrol bileşeni için bildirim ayarlarındaki **Gerçekleştirilen dosya operasyonu** onay kutusunu seçmelisiniz.

Güvenilir listeye bir Wi-Fi ağı ekleme

Kullanıcıların, kurumsal Wi-Fi ağı gibi güvenli olduğunu düşündüğünüz Wi-Fi ağlarına bağlanmalarına izin verebilirsiniz. Bunu yapmak için ağı, güvenilir Wi-Fi ağları listesine eklemelisiniz. Aygıt Denetimi, güvenilir listede belirtilenlerin haricinde tüm Wi-Fi ağlarına erişimi engeller.

Güvenilir listeye bir Wi-Fi ağını eklemek için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol kısmında, **Uç nokta denetimi** bölümünde, **Aygıt Denetimi** alt bölümünü seçin.

Pencerenin sağ kısmında, Aygıt Denetimi bileşeni ayarları görüntülenir.

3. Pencerenin sağ kısmında, **Aygıt türleri** sekmesini seçin.

Aygıt türleri sekmesi, Aygıt Denetimi bileşeni sınıflandırmasında yer alan tüm aygıtların erişim kurallarını içerir.

4. **Wi-Fi** aygıtının karşısındaki **Erişim** sütununda sağ tıklayarak içerik menüsünü açın.

5. **İstisnalar ile engelle** seçeneğini seçin.

6. Aygıtlar listesinden **Wi-Fi**'ı seçin ve **Düzenle** düğmesine tıklayın.

Aygıtlara erişim zamanlaması penceresi açılır.

7. **Ekle** düğmesine tıklayın.

Aygıtlara erişim zamanlaması penceresi açılır.

8. **Aygıtlara erişim zamanlaması** penceresinde:

- **Ağ adı** alanında güvenilir listeye eklemek istediğiniz Wi-Fi ağının adını belirleyin.
- **Kimlik doğrulama türü** açılır listesinde güvenilir Wi-Fi ağına bağlanırken kullanılan kimlik doğrulama türünü seçin.
- **Şifreleme türü** açılır listesinde güvenilir Wi-Fi ağının trafiğini güvene almak için kullanılan şifreleme türünü seçin.

- **Yorum** alanında, eklenen Wi-Fi ağı hakkında herhangi bir bilgi belirtebilirsiniz.

Bir Wi-Fi ağı, ayarları kuralda belirtilen tüm ayarlarla eşleşiyorsa güvenilir kabul edilir.

9. **Aygıtlara erişim zamanlaması** penceresinde, **Tamam**'a tıklayın.
10. **Aygıta erişim iste** penceresinde, **Tamam**'a tıklayın.

Bir bağlantı veri yolu erişim kuralını düzenleme

Bir bağlantı veri yolu erişim kuralını düzenlemek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Uç nokta denetimi** bölümünde, **Aygıt Denetimi** alt bölümünü seçin.

   Pencerenin sağ kısmında, Aygıt Denetimi bileşeni ayarları görüntülenir.
3. **Bağlantı veri yolları** sekmesini seçin.

   Bağlantı veri yolları sekmesi, Aygıt Denetimi bileşeninde sınıflandırılan bütün bağlantı veri yollarının erişim kurallarını görüntüler.
4. Düzenlemek istediğiniz veri yolu bağlantı kuralını seçin.
5. Erişim parametresinin değerini değiştirin:
   - Bağlantı veri yoluna erişime izin vermek için **Erişim** sütununa tıklayarak içerik menüsünü açın ve **İzin ver**'i seçin.
   - Bağlantı veri yoluna erişimi engellemek için **Erişim** sütununa tıklayarak içerik menüsünü açın ve **Engelle**'yi seçin.
6. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Güvenilir aygıtlarla eylemler

Bu bölüm, güvenilir aygıtlarla ilgili eylemler hakkında bilgi içerir.

Uygulama arabiriminden Güvenilir listesine aygıt ekleme

Varsayılan olarak güvenilir aygıtlar listesine bir aygıt eklendiğinde tüm kullanıcılara aygıtlara erişim izni verilir (Herkes kullanıcı grubu).

Uygulama arabiriminden Güvenilir listesine bir aygıt eklemek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Uç nokta denetimi** bölümünde, **Aygıt Denetimi** alt bölümünü seçin.

Pencerenin sağ kısmında, Aygıt Denetimi bileşeni ayarları görüntülenir.

3. Pencerenin sağ kısmında, **Güvenilir aygıtlar** sekmesini seçin.

4. **Seç** düğmesine tıklayın.

   Güvenilir aygıtları seç penceresi açılır.

5. Güvenilir aygıtlar listesine eklemek istediğiniz aygıt adının karşısındaki onay kutusunu seçin.

   Aygıtlar sütunundaki liste, **Bağlı aygıtları görüntüleyin** açılır listesinde seçilen değere bağlıdır.

6. **Seç** düğmesine tıklayın.

   Microsoft Windows'ta **Kullanıcıları veya Grupları Seç** penceresi açılır.

7. Microsoft Windows'ta **Kullanıcılar veya Grupları Seç** penceresinde, Kaspersky Endpoint Security'nin aygıtlarını güvenilir olarak tanıyacağı kullanıcılar ve/veya kullanıcı gruplarını belirtin.

   Microsoft Windows'un **Kullanıcılar ve/veya kullanıcı gruplarını seçin** penceresinde belirtilen kullanıcılar ve/veya kullanıcı grupları, **Kullanıcılara ve/veya kullanıcı gruplarına izin verin** alanında görüntülenir.

8. **Güvenilir aygıtları seç** penceresinde **Tamam** düğmesine tıklayın.

   Tabloda, **Aygıt Denetimi** bileşeni ayarları penceresinin **Güvenilir aygıtlar** sekmesinde bir satır görülür ve eklenen güvenilir aygıtların parametrelerini görüntüler.

9. Belirtilen kullanıcılar ve/veya kullanıcı grupları için güvenilir aygıtlar listesine eklemek istediğiniz her bir aygıt için adım 4-7'yi tekrarlayın.

10. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Aygıt modeli veya kimliğine göre aygıtları Güvenilir listesine ekleme

Varsayılan olarak güvenilir aygıtlar listesine bir aygıt eklendiğinde tüm kullanıcılara aygıtlara erişim izni verilir (Herkes kullanıcı grubu).

Aygıt modeli veya kimliğine göre aygıtları Güvenilir listesine eklemek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, güvenilir aygıtların listesini oluşturmak istediğiniz yönetim grubunun adına sahip klasörü açın.

3. Çalışma alanında, **İlkeler** sekmesini seçin.

4. Gereken ilkeyi seçin.

5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:

   - İlkenin içerik menüsünde **Özellikler**'i seçin.

   - Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.

6. **Uç nokta denetimi** bölümünde, **Aygıt Denetimi** alt bölümünü seçin.

7. Pencerenin sağ kısmında, **Güvenilir aygıtlar** sekmesini seçin.

8. **Ekle** düğmesine tıklayın.

   Düğmenin içerik menüsü açılır.

9. **Ekle** düğmesinin içerik menüsünde aşağıdakilerden birini yapın:

   - Benzersiz bilinen kimliklere sahip aygıtları güvenilir aygıtlar listesine eklenmek üzere seçmek isterseniz **Kimliğe göre aygıtlar** düğmesini seçin.
   - VID (satıcı kimliği) ve PID (ürün kimliği) bilinen güvenilir aygıtları listeye eklemek için **Modele göre aygıtlar** öğesini seçin.

10. Açılan pencerede, **Aygıt türü** açılır listesinden aşağıdaki tabloda görüntülenecek aygıt türlerini seçin.

11. **Yenile** düğmesine tıklayın.

    Tabloda, aygıt kimliği ve/veya modeli bilinen ve **Aygıt türü** açılır listesinde seçilen türdeki aygıtların bir listesi görüntülenir.

12. Güvenilir aygıtlar listesine eklemek istediğiniz aygıt adlarının karşısındaki onay kutularını işaretleyin.

13. **Seç** düğmesine tıklayın.

    Microsoft Windows'ta **Kullanıcıları veya Grupları Seç** penceresi açılır.

14. Microsoft Windows'ta **Kullanıcılar veya Grupları Seç** penceresinde, Kaspersky Endpoint Security'nin aygıtlarını güvenilir olarak tanıyacağı kullanıcılar ve/veya kullanıcı gruplarını belirtin.

    Microsoft Windows'un **Kullanıcılar ve/veya kullanıcı gruplarını seçin** penceresinde belirtilen kullanıcılar ve/veya kullanıcı grupları, **Kullanıcılara ve/veya kullanıcı gruplarına izin verin** alanında görüntülenir.

15. **Tamam**'a tıklayın.

    Eklenen güvenilir aygıt parametrelerinin bulunduğu satırlar tabloda **Güvenilir aygıtlar** sekmesinde görülür.

16. Değişiklikleri kaydetmek için **Tamam** veya **Uygula** düğmesine tıklayın.

Aygıt kimliği maskesine göre aygıtları Güvenilir listesine ekleme

Varsayılan olarak güvenilir aygıtlar listesine bir aygıt eklendiğinde tüm kullanıcılara aygıtlara erişim izni verilir (Herkes kullanıcı grubu).

> Aygıtlar sadece Kaspersky Security Center Yönetim Konsolu'ndaki kimlik maskelerine göre Güvenilir listesine eklenebilir.

Kimlik maskesine göre aygıtları Güvenilir listesine eklemek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, güvenilir aygıtların listesini oluşturmak istediğiniz yönetim grubunun adına sahip klasörü açın.

3. Çalışma alanında, **İlkeler** sekmesini seçin.

4. Gereken ilkeyi seçin.

5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:

   - İlkenin içerik menüsünde **Özellikler**'i seçin.
   - Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.

6. **Uç nokta denetimi** bölümünde, **Aygıt Denetimi** alt bölümünü seçin.
7. Pencerenin sağ kısmında, **Güvenilir aygıtlar** sekmesini seçin.
8. **Ekle** düğmesine tıklayın.

   Düğmenin içerik menüsü açılır.

9. **Ekle** düğmesinin içerik menüsünde, **Kimlik maskesine göre aygıtlar** öğesini seçin.

   Kimlik maskesine göre güvenilir aygıt ekle penceresi açılır.

10. **Kimlik maskesine göre güvenilir aygıt ekle** penceresinde, aygıt kimliklerinin maskesini **Maske** alanına girin.
11. **Seç** düğmesine tıklayın.

    Microsoft Windows'ta **Kullanıcıları veya Grupları Seç** penceresi açılır.

12. Microsoft Windows'ta **Kullanıcılar veya Grupları Seç** penceresinde, Kaspersky Endpoint Security'nin modelleri veya kimlikleri belirtilen maskeyle eşleşen aygıtları güvenilir olarak tanıyacağı kullanıcılar ve/veya kullanıcı gruplarını belirtin.

    Microsoft Windows'un **Kullanıcılar ve/veya kullanıcı gruplarını seçin** penceresinde belirtilen kullanıcılar ve/veya kullanıcı grupları, **Kullanıcılara ve/veya kullanıcı gruplarına izin verin** alanında görüntülenir.

13. **Tamam**'a tıklayın.

    Aygıt Denetimi bileşen ayarları penceresinin **Güvenilir aygıtlar** sekmesindeki tabloda, aygıtların kimlik maskesine göre güvenilir aygıtların listesine eklenmesi kuralının ayarlarını içeren bir satır görülür.

14. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Güvenilir aygıta kullanıcı erişimini yapılandırma

Varsayılan olarak güvenilir aygıtlar listesine bir aygıt eklendiğinde tüm kullanıcılara aygıtlara erişim izni verilir (Herkes kullanıcı grubu). Kullanıcıların (veya kullanıcı gruplarının) bir güvenilir aygıta erişimini yapılandırabilirsiniz.

Bir güvenilir aygıta kullanıcı erişimini yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Uç nokta denetimi** bölümünde, **Aygıt Denetimi** alt bölümünü seçin.

   Pencerenin sağ kısmında, Aygıt Denetimi bileşeni ayarları görüntülenir.

3. Pencerenin sağ kısmında, **Güvenilir aygıtlar** sekmesini seçin.
4. Güvenilir aygıtlar listesinde, erişim kurallarını düzenlemek istediğiniz bir aygıt seçin.
5. **Düzenle** düğmesine tıklayın.

   Güvenilir aygıta erişim kuralı yapılandırılıyor penceresi açılır.

6. **Seç** düğmesine tıklayın.

   Microsoft Windows'ta **Kullanıcıları veya Grupları Seç** penceresi açılır.

7. Microsoft Windows'ta **Kullanıcılar veya Grupları Seç** penceresinde, Kaspersky Endpoint Security'nin aygıtlarını güvenilir olarak tanıyacağı kullanıcılar ve/veya kullanıcı gruplarını belirtin.

8. **Tamam**'a tıklayın.

   Microsoft Windows'un **Kullanıcılar ve/veya kullanıcı gruplarını seçin** penceresinde belirtilen kullanıcılar ve/veya kullanıcı grupları, **Güvenilir aygıta erişim kuralı yapılandırılıyor** penceresindeki **Kullanıcılara ve/veya kullanıcı gruplarına izin verin** alanında görüntülenir.

9. **Tamam**'a tıklayın.

10. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Güvenilir aygıtlar listesinden bir aygıtı kaldırma

Güvenilir aygıtlar listesinden bir aygıtı kaldırmak için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol kısmında, **Uç nokta denetimi** bölümünde, **Aygıt Denetimi** alt bölümünü seçin.

   Pencerenin sağ kısmında, Aygıt Denetimi bileşeni ayarları görüntülenir.

3. Pencerenin sağ kısmında, **Güvenilir aygıtlar** sekmesini seçin.

4. Güvenilir aygıtlar listesinden kaldırmak istediğiniz aygıtı seçin.

5. **Kaldır** düğmesine tıklayın.

6. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Güvenilir aygıtlar listesinden kaldırdığınız bir aygıta erişim hakkındaki karar, aygıt erişim kurallarına ve bağlantı veri yolu erişim kurallarına dayalı olarak Kaspersky Endpoint Security tarafından yapılır.

Aygıt Denetimi mesajlarının şablonlarını düzenleme

Engellenmiş bir aygıta kullanıcı tarafından erişim sağlanmaya çalışıldığında Kaspersky Endpoint Security, aygıta erişimin engellendiğini ve aygıt içeriğiyle işlem yapmanın yasak olduğunu belirten bir mesaj görüntüler. Kullanıcı, aygıta erişimin yanlışlıkla engellendiğini veya aygıt içeriğiyle işlem yapmanın yanlışlıkla yasaklandığını düşünüyorsa engellenen işlemle ilgili mesajda görüntülenen bağlantıya tıklayarak yerel kurumsal ağ yöneticisine bir mesaj gönderebilir.

Engellenen aygıt erişimi veya yasaklanan aygıt içeriği işlemleriyle ilgili mesajlar ve yöneticiye gönderilen mesajlar için şablonlar mevcuttur. Mesaj şablonlarını değiştirebilirsiniz.

Aygıt Denetimi mesajlarının şablonlarını düzenlemek için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol kısmında, **Uç nokta denetimi** bölümünde, **Aygıt Denetimi** alt bölümünü seçin.

Pencerenin sağ kısmında, Aygıt Denetimi bileşeni ayarları görüntülenir.

3. Pencerenin sağ kısmında, **Şablonlar** düğmesine tıklayın.

   Mesaj şablonları penceresi açılır.

4. Aşağıdakilerden birini yapın:

   - Engellenen aygıt erişimi veya yasaklanan aygıt içeriğiyle işlem hakkındaki mesajın şablonunu değiştirmek için **Engelleme** sekmesini seçin.
   - LAN yöneticisine gönderilen mesajın şablonunu düzenlemek için **Yöneticiye mesaj** sekmesini seçin.

5. Mesaj şablonunu düzenleyin. Aşağıdaki düğmeleri de kullanabilirsiniz: **Değişken**, **Varsayılan** ve **Bağlantı** (bu düğme sadece **Engelleme** sekmesinde kullanılabilir).

6. **Tamam**'a tıklayın.

7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Engellenen bir aygıta erişim elde etme

Bu talimatlar, Kaspersky Endpoint Security'nin yüklü olduğu istemci bilgisayarların kullanıcılarına yöneliktir.

Bir aygıta geçici olarak erişim izni veren Kaspersky Endpoint Security işlevselliği, yalnızca Kaspersky Endpoint Security'nin Kaspersky Security Center ilkesinin altında çalıştığı ve bu işlevselliğin ilke ayarlarında etkinleştirildiği durumda kullanılabilir (*Kaspersky Security Center Yönetici Kılavuzu*'na bakınız).

Aygıt Denetimi bileşeni ayarları penceresinden engellenen bir aygıta erişim istemek için:

1. Ana uygulama penceresinde **Koruma ve Denetim** sekmesini seçin.

2. **Uç nokta denetimi** bölümüne tıklayın.

   Uç nokta denetimi bölümü açılır.

3. Sağ tıklayarak, Aygıt Denetimi bileşeni hakkında bilgi içeren satırın içerik menüsünü açın.

   Bileşenlere uygulanacak eylemlerin seçilebileceği bir menü açılır.

4. **Aygıta erişim** düğmesine tıklayın.

   Aygıta erişim anahtarını al penceresi açılır.

5. Bağlanan aygıtlar listesinden erişim elde etmek istediğiniz aygıtı seçin.

6. **İstek erişim dosyası oluştur** düğmesine tıklayın.

   İstek erişim dosyası oluşturuluyor penceresi açılır.

7. **Erişim süresi** alanında aygıta erişmek istediğiniz süreyi belirtin.

8. **Kaydet** düğmesine tıklayın.

   Microsoft Windows'un standart **Erişim anahtarını kaydet** penceresi açılır.

9. Microsoft Windows'un **Erişim anahtarını kaydet** penceresinde aygıt için istek erişim dosyasını kaydetmek istediğiniz klasörü seçin ve **Kaydet** düğmesine tıklayın.
10. Aygıt istek erişim dosyasını LAN yöneticisine gönderin.
11. Aygıt erişim anahtarını LAN yöneticisinden alın.
12. **Aygıt erişim anahtarını al** penceresinde **Erişim kodunu etkinleştir** düğmesine tıklayın.

    Microsoft Windows'un standart **Erişim anahtarını aç** penceresi açılır.
13. Microsoft Windows'un **Erişim anahtarını aç** penceresinde LAN yöneticisinden alınan aygıt erişim anahtarı dosyasını seçin ve **Aç** düğmesine tıklayın.

    Cihaz için erişim anahtarı etkinleştiriliyor penceresi açılır ve erişim verilmesi hakkında bilgi görüntülenir.
14. **Cihaz için erişim anahtarı etkinleştiriliyor** penceresinde **Tamam**'a tıklayın.

Aygıtın engellendiğini bildiren mesajdaki bağlantıya tıklayarak engellenen bir aygıta erişim istemek için:

1. Bir aygıt veya bağlantı veri yolunun engellendiğini bildiren mesajı içeren pencerede **Erişim iste** bağlantısına tıklayın.

   İstek erişim dosyası oluşturuluyor penceresi açılır.
2. **Erişim süresi** alanında aygıta erişmek istediğiniz süreyi belirtin.
3. **Kaydet** düğmesine tıklayın.

   Microsoft Windows'un standart **Erişim anahtarını kaydet** penceresi açılır.
4. Microsoft Windows'un **Erişim anahtarını kaydet** penceresinde aygıt için istek erişim dosyasını kaydetmek istediğiniz klasörü seçin ve **Kaydet** düğmesine tıklayın.
5. Aygıt istek erişim dosyasını LAN yöneticisine gönderin.
6. Aygıt erişim anahtarını LAN yöneticisinden alın.
7. **Aygıt erişim anahtarını al** penceresinde **Erişim kodunu etkinleştir** düğmesine tıklayın.

   Microsoft Windows'un standart **Erişim anahtarını aç** penceresi açılır.
8. Microsoft Windows'un **Erişim anahtarını aç** penceresinde LAN yöneticisinden alınan aygıt erişim anahtarı dosyasını seçin ve **Aç** düğmesine tıklayın.

   Cihaz için erişim anahtarı etkinleştiriliyor penceresi açılır ve erişim verilmesi hakkında bilgi görüntülenir.
9. **Cihaz için erişim anahtarı etkinleştiriliyor** penceresinde **Tamam**'a tıklayın.

Aygıta erişim izni verilen süre, istediğiniz süreden farklı olabilir. Aygıt erişim anahtarı oluşturulurken yerel ağ yöneticisinin belirlediği süre boyunca aygıta erişim izni verilir.

Kaspersky Security Center'ı kullanarak engellenen aygıt erişim anahtarı oluşturma

Engellenen aygıta geçici olarak kullanıcı erişimi sağlamak için aygıtın erişim anahtarı gereklidir. Kaspersky Security Center'ı kullanarak bir erişim anahtarı oluşturabilirsiniz.

Engellenen aygıtın erişim anahtarını oluşturmak için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, ilgili istemci bilgisayarın ait olduğu yönetim grubu adının bulunduğu klasörü açın.
3. Çalışma alanında, **Aygıtlar** sekmesini seçin.
4. İstemci bilgisayarların listesinde, kullanıcısına kilitli aygıta geçici erişim verilmesi gereken bilgisayarı seçin.
5. Bilgisayarın içerik menüsünde **Aygıtlara ve verilere çevrimdışı modda erişim ver** seçeneğini seçin.

   Aygıtlara ve verilere çevrimdışı modda erişim ver penceresi açılır.
6. **Aygıt Denetimi** sekmesini seçin.
7. **Aygıt Denetimi** sekmesinde, **Gözat** düğmesine tıklayın.

   Microsoft Windows'ta standart **İstek dosyasını seç** penceresi açılır.
8. **İstek dosyasını seç** penceresinde, kullanıcıdan aldığınız istek erişim dosyasını seçin ve **Aç** düğmesine tıklayın.

   Aygıt Denetimi penceresinde, kullanıcının erişim istediği kilitli aygıtın ayrıntıları görüntülenir.
9. **Erişim süresi** ayarının değerini belirtin.

   Bu ayar, kilitli aygıta kullanıcı erişimi verdiğiniz süre uzunluğunu tanımlar. Varsayılan değer, istek erişim dosyasını oluştururken kullanıcı tarafından belirtilen değerdir.
10. **Etkinleştirme süresi** ayarını belirtin.

    Bu ayar, sağlanan erişim anahtarını kullanarak kullanıcının engellenen aygıta erişimi etkinleştirebileceği süreyi tanımlar.
11. **Kaydet** düğmesine tıklayın.

    Microsoft Windows'un standart **Erişim anahtar dosyasını kaydet** penceresi açılır.
12. Engellenen aygıtın erişim anahtarının yer aldığı dosyayı kaydetmek istediğiniz hedef klasörü seçin.
13. **Kaydet** düğmesine tıklayın.

İnternet Denetimi

Bu bileşen, İş istasyonları için Microsoft Windows'un kurulu olduğu bir bilgisayara Kaspersky Endpoint Security yüklendiğinde kullanılabilir. Bu bileşen, Dosya sunucuları için Microsoft Windows'un kurulu olduğu bir bilgisayara Kaspersky Endpoint Security yüklendiğinde kullanılamaz.

Bu bölümde, İnternet Denetimi ve bileşen ayarlarının yapılandırılması talimatlarıyla ilgili bilgi yer almaktadır.

İnternet Denetimi Hakkında

İnternet Denetimi, İnternet kaynaklarına erişimi kısıtlayarak veya engelleyerek LAN kullanıcılarının eylemlerinin denetlenmesini sağlar.

İnternet kaynağı tek bir İnternet sayfası veya birkaç İnternet sayfası ya da ortak bir özelliğe sahip bir İnternet sitesi ya da birkaç İnternet sitesi olabilir.

İnternet Denetimi aşağıdaki seçenekleri sunar:

- Trafiği azaltma.

  Multimedya dosyalarının indirilmesini kısıtlayarak veya engelleyerek ya da kullanıcının iş sorumluluklarıyla ilgili olmayan İnternet kaynaklarına erişimi sınırlayarak veya engelleyerek trafik denetlenir.

- İnternet kaynaklarının içerik kategorilerine göre erişimi sınırlama.

  Trafiği azaltmak ve çalışan süresinin suistimal edilmesinden kaynaklanan olası kayıpları azaltmak amacıyla belirli İnternet kaynağı kategorilerine erişimi sınırlayabilir veya engelleyebilirsiniz (örneğin "İnternet iletişim medyası" kategorisine giren İnternet kaynaklarına erişimi engelleyebilirsiniz).

- İnternet kaynaklarına erişimin merkezi denetimi.

  Kaspersky Security Center'ı kullanırken İnternet kaynaklarına erişimin kişisel ve grup ayarları kullanılamaz.

İnternet kaynaklarına erişime uygulanan tüm sınırlamalar ve engellemeler, İnternet kaynağına erişim kuralları olarak uygulanır.

İnternet Denetimi'ni etkinleştirme ve devre dışı bırakma

Varsayılan olarak İnternet Denetimi etkindir. Gerekirse İnternet Denetimi'ni devre dışı bırakabilirsiniz.

Bileşeni etkinleştirmenin veya devre dışı bırakmanın iki yolu bulunmaktadır:

- Ana uygulama penceresinde **Koruma ve Denetim** sekmesinde
- Uygulama ayarları penceresinden.

*Ana uygulama penceresinin **Koruma ve Denetim** sekmesinde İnternet Denetimi'ni etkinleştirmek veya devre dışı bırakmak için:*

1. Ana uygulama penceresini açın.

2. **Koruma ve Denetim** sekmesini seçin.
3. **Uç nokta denetimi** bölümüne tıklayın.

   Uç nokta denetimi bölümü açılır.
4. Sağ tıklayarak, İnternet Denetimi bileşeni hakkında bilgi içeren satırın içerik menüsünü açın.

   Bileşenlere uygulanacak eylemlerin seçilebileceği bir menü açılır.
5. Aşağıdakilerden birini yapın:

   - İnternet Denetimi'ni etkinleştirmek için menüden **Başlat**'ı seçin.
   - İnternet Denetimi'ni devre dışı bırakmak için menüden **Durdur**'u seçin.

Uygulama ayarları penceresinden İnternet Denetimi'ni etkinleştirmek veya devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Uç nokta denetimi** bölümünde, **İnternet Denetimi** alt bölümünü seçin.

   Pencerenin sağ kısmında, İnternet Denetimi bileşeni ayarları görüntülenir.
3. Aşağıdakilerden birini yapın:

   - İnternet Denetimi'ni etkinleştirmek istiyorsanız **İnternet Denetimini Etkinleştir** onay kutusunu işaretleyin.
   - İnternet Denetimi'ni devre dışı bırakmak istiyorsanız **İnternet Denetimini Etkinleştir** onay kutusunu işaretlemeyin.

   İnternet Denetimi devre dışı bırakılırsa Kaspersky Endpoint Security, İnternet kaynaklarına erişimi denetlemez.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

İnternet kaynağı içerik kategorileri

Aşağıda belirtilen İnternet kaynağı içerik kategorileri (bundan sonra "kategoriler" olarak da adlandırılacaktır) işlevsel ve tematik özelliklerini göz önünde bulundurarak İnternet kaynaklarının barındırdığı veri bloklarını en kapsamlı olarak açıklayacak şekilde seçilmiştir. Kategorilerin bu listede görülme sırası, bu kategorilerin İnternet'teki nispi önemini veya yaygınlığını yansıtmamaktadır. Kategori adları geçicidir ve sadece Kaspersky ürünleri ve web siteleri ile ilgili olarak kullanılmaktadır. Adlar, yasayla kastedilen anlamı yansıtmayabilir. Bir İnternet kaynağı aynı anda birden fazla kategoriye girebilir.

Yetişkinlere yönelik içerik

Bu kategori aşağıdaki İnternet kaynağı türlerini içermektedir:

- İnsanların veya insana benzer yaratıkların cinsel organlarının teşhir edildiği, cinsel ilişki eylemlerinin veya insanların ya da insana benzer yaratıkların kendi kendini uyarmasının görüntülendiği fotoğraf veya video materyallerini içeren İnternet kaynakları.
- İnsanların veya insana benzer yaratıkların cinsel organlarının, cinsel ilişki eylemlerinin veya insanların ya da insana benzer yaratıkların kendi kendini uyarmasının tasvir edildiği edebi ve sanatsal materyalleri içeren yazılı materyallerin bulunduğu İnternet kaynakları.

- İnsan ilişkilerinin cinsel boyutunun tartışıldığı İnternet kaynakları.

  "İnternet iletişim medyası" kategorisi ile örtüşür.

- Erotik materyaller, insanların cinsel davranışının gerçekçi bir şekilde resmedilmesini sağlayan çalışmalar veya cinsel uyarım sağlamak üzere tasarlanan sanat eserlerini içeren İnternet kaynakları.
- İnsan ilişkilerinin cinsel yönüne odaklanan özel bir bölüm ve/veya ayrı makalelerin yer aldığı, belirli bir hedef kitlesi olan resmi medya organları ve çevrimiçi toplulukların İnternet kaynakları.
- Cinsel sapıklıklara odaklanan İnternet kaynakları.
- Cinsel ilişkide veya cinsel uyarım sağlamada kullanılan ürünler, erotik video sohbetleri, "telefonla seks", "seksting" (sanal seks) vasıtasıyla çevrimiçi olarak sağlanan servisleri de kapsayan cinsel servisleri ve flört hizmetlerini pazarlayan ve satan İnternet kaynakları.
- Aşağıdaki içeriğe sahip İnternet kaynakları:
  - Hem bilimsel hem de popüler temalı seks eğitimini kapsayan makaleler ve bloglar.
  - Tıp ansiklopedileri, özellikle cinsel üreme ile ilgili bölümleri.
  - Sağlık kurumlarının kaynakları, özellikle cinsel organların tedavisini kapsayan bölümleri.

Yazılım, ses, video

Bu kategori, tek tek seçebileceğiniz aşağıdaki alt kategorileri içerir:

- **Ses ve video**.

  Bu alt kategori, ses ve video materyallerini dağıtan İnternet kaynaklarını içerir: filmler, spor yayını kayıtları, konser kayıtları, şarkılar, film klipleri, videolar, sesli ve görüntülü eğitim kayıtları vs.

- **Torrentler**.

  Bu alt kategori, sınırsız boyuttaki dosyaların paylaşılmasını amaçlayan torrent takipçilerinin web sitelerini içerir.

- **Dosya paylaşımı**.

  Bu alt kategori, dağıtılan dosyaların fiziksel konumundan bağımsız olarak dosya paylaşımı web sitelerini içerir.

Alkol, tütün, uyuşturucu

Bu kategori; içeriği doğrudan veya dolaylı olarak alkollü veya alkol içeren ürünler, tütün ürünleri ve uyuşturucu, psikotropik ve/veya sarhoş edici maddelerle ilgili olan İnternet kaynaklarını içerir.

- Bu tür maddeleri ve bunların tüketim donanımlarını pazarlayan ve satan İnternet kaynakları.

  "Elektronik ticaret" kategorisi ile örtüşür.

- Narkotik, psikotropik ve/veya sarhoş edici maddelerin nasıl tüketileceği veya üretileceğiyle ilgili talimatlar içeren İnternet kaynakları.

Bu kategori, bilimsel ve tıbbi konuları ele alan İnternet kaynaklarını içerir.

Şiddet

Bu kategori, insanlara yönelik fiziksel veya psikolojik şiddet eylemlerini veya hayvanlara yapılan vahşice muameleleri tasvir eden yazılı materyaller, fotoğraf veya video içeren İnternet kaynaklarını kapsar.

- İdam, işkence veya taciz sahnelerini veya bu tür eylemler için kullanılan araçları resmeden veya tasvir eden İnternet kaynakları.

  "Silahlar, patlayıcı maddeler, piroteknik" kategorisi ile örtüşür.

- Cinayet, dövüş, kötü muamele veya tecavüz sahnelerinin resmedildiği veya tasvir edildiği, insanlar, hayvanlar veya hayali varlıkların taciz veya aşağılamaya maruz kaldığı sahnelerin yer aldığı İnternet kaynakları.
- Kendi kendine zarar verme veya intihar dahil olmak üzere hayat ve/veya sağlığı tehlikeye atan eylemleri teşvik eden bilgiler içeren İnternet kaynakları.
- Şiddet ve/veya vahşetin kabul edilebilirliğini haklı gösteren veya meşrulaştıran ya da insanlara veya hayvanlara karşı şiddet eylemlerini teşvik eden bilgilerin yer aldığı İnternet kaynakları.
- Savaş kurbanlarının ve vahşetinin, silahlı çatışmaların, askeri çatışmaların, felaketlerin, doğal afetlerin, endüstriyel ve sosyal karışıklıkların veya insan acılarının özellikle gerçekçi bir şekilde resmedildiği veya tasvir edildiği İnternet kaynakları.
- "Nişancı", "dövüş", "kesici" oyunları vs. olarak adlandırılan şiddet ve vahşet sahneleri içeren tarayıcı bilgisayar oyunları.

  "Bilgisayar oyunları" kategorisi ile örtüşür.

Silahlar, patlayıcı maddeler, piroteknik

Bu kategori, silahlar, patlayıcı maddeler, piroteknik ürünlerle ilgili bilgi veren İnternet kaynaklarını içerir:

- Silahlar, patlayıcı maddeler, piroteknik ürün üreticileri ve mağazalarının İnternet siteleri.

  "Elektronik ticaret" kategorisi ile örtüşür.

- Silahlar, patlayıcı maddeler ve piroteknik ürünlerinin üretimi veya kullanımını konu eden İnternet kaynakları.
- Silahlar, patlayıcı maddeler ve piroteknik ürünleri konu eden analitik, tarihi, üretimsel ve ansiklopedik materyaller içeren İnternet kaynakları.

"Silahlar" terimi, insanların ve hayvanların hayatına ve sağlığına zarar vermek ve/veya ekipman ve yapılara hasar vermek üzere tasarlanan cihazlar, öğeler ve araçlar anlamına gelmektedir.

Küfür

Bu kategori, küfürlü dilin tespit edildiği İnternet kaynaklarını içerir.

"Yetişkinlere yönelik içerik" kategorisi ile örtüşür.

Bu kategori, araştırma konusu olarak küfür içeren dilbilimsel ve filolojik materyaller içeren İnternet kaynaklarını da kapsar.

Kumar, piyango, çekiliş

Bu kategori, İnternet sitesine erişim için finansal katılım zorunlu bir koşul olmasa dahi kullanıcılara kumara finansal olarak katılım sunan İnternet kaynaklarını da içerir. Bu kategori şunu sunan İnternet kaynaklarını da içerir:

- Katılımcıların parasal katkıda bulunması gereken kumar.

  "Bilgisayar oyunları" kategorisi ile örtüşür.

- Parayla bahse girmeyi kapsayan çekilişler.
- Piyango bileti veya rakam satın almayı kapsayan piyangolar.
- Kumar, çekiliş ve piyangoya katılma isteğini tetikleyebilecek bilgiler.

"Elektronik ticaret" kategorisi ile örtüşür.

Bu kategori ayrı bir mod olarak ücretsiz katılım sunan oyunları ve bu kategoriye giren İnternet kaynaklarını aktif olarak tanıtan İnternet kaynaklarını kapsar.

Ağ İletişimleri

Bu kategori, (kayıtlı veya kayıtsız) kullanıcıların ilgili İnternet kaynaklarının veya çevrimiçi hizmetlerin diğer kullanıcılarına kişisel mesaj göndermesine ve/veya ilgili İnternet kaynaklarına belirli koşullarla (genel erişime açık ya da kısıtlı olarak) içerik eklemesine imkan tanıyan İnternet kaynaklarını kapsar. Aşağıdaki kategorileri tek tek seçebilirsiniz:

- **Sohbet ve forumlar**.

  Bu alt kategori, özel İnternet uygulamalarının kullanıldığı çeşitli konuların genel olarak tartışılmasına yönelik İnternet kaynaklarını ve gerçek zamanlı etkileşime imkan tanıyan anlık mesajlaşma uygulamalarını dağıtmak ya da desteklemek üzere tasarlanan İnternet kaynaklarını içerir.

- **Bloglar**.

  Bu alt kategori, bloglar oluşturmak veya yayınlamak için ücretli veya ücretsiz hizmetler sağlayan web sitelerinden oluşan blog platformlarını içerir.

- **Sosyal ağlar**.

Bu alt kategori, katılım koşulu olarak bir kullanıcı hesabının kaydedilmesini gerektiren kişiler, kuruluşlar ve hükümetler arasında irtibatların oluşturulması, görüntülenmesi ve yönetilmesi amacıyla tasarlanan İnternet sitelerini içerir.

- **Arkadaşlık siteleri**.

  Bu alt kategori, ücretli veya ücretsiz hizmetler sunan çeşitli sosyal ağlar olarak hizmet veren İnternet kaynaklarını içerir.

  > "Yetişkinlere yönelik içerik" ve "Elektronik ticaret" kategorileriyle örtüşür.

- **Web tabanlı e-posta**.

  Bu alt kategori, e-postalar ve ilişkili verileri (kişisel irtibatlar gibi) içeren e-posta hizmeti ve posta kutusu sayfalarının özellikle oturum açma sayfalarını içerir. Bu kategori, e-posta hizmeti de sunan bir İnternet hizmet sağlayıcısının diğer İnternet sayfalarını kapsar.

E-ticaret, bankalar ve ödeme sistemleri

Bu kategori, özel amaçlı İnternet uygulamaları kullanılarak nakdi olmayan parasal fonlardaki online işlemler için tasarlanan İnternet kaynaklarını içerir. Aşağıdaki kategorileri tek tek seçebilirsiniz:

- **Dükkan ve açık artırmalar**.

  Bu alt kategori, bireyler ve/veya tüzel kişiliklere ürün, iş veya hizmet satan çevrimiçi dükkan ve açık artırma mağazalarını ve sadece çevrimiçi satış yapan mağazaların İnternet sitelerini ve çevrimiçi ödeme kabul eden fiziksel mağazaların çevrimiçi profillerini içerir.

- **Bankalar**.

  Bu alt kategori, banka hesapları arasında elektronik transfer, banka hesabına para yatırma, döviz işlemleri, üçüncü taraf hizmetlere ödeme vs. dahil olmak üzere çevrimiçi bankacılık işlevine sahip uzmanlaşmış bankacılık İnternet sayfalarını içerir.

- **Ödeme sistemleri**.

  Bu alt kategori, kullanıcının kişisel hesaplarına erişim sağlayan e-para sistemlerinin İnternet sayfalarını içerir.

> Teknik açıdan ödeme, herhangi bir türden (plastik veya sanal, banka veya kredi, yerel veya uluslararası) banka kartları ve e-para kullanılarak gerçekleştirilebilir. İnternet kaynakları, SSL iletişim kuralı üzerinden veri aktarımı, 3D Secure kimlik doğrulaması vs. gibi teknik boyutları olup olmadığına bakılmaksızın bu kategoriye girer.

İş arama

Bu kategori, işverenleri ve iş arayanları bir araya getirmek üzere tasarlanan İnternet kaynaklarını içerir.

- İş bulma kuruluşlarının (istihdam ajansları ve/veya eleman bulma ajansları) web siteleri.
- Açık pozisyonların ve avantajlarının açıklamalarının yer aldığı işverenlerin web siteleri.
- İşverenlerin ve iş bulma kuruluşlarının istihdam fırsatlarının bulunduğu bağımsız portallar.
- Aktif olarak iş aramayan uzmanlar hakkında bilgi yayınlanmasına veya bulunmasına imkan tanıyan profesyonel sosyal ağlar.

"İnternet iletişim medyası" kategorisi ile örtüşür.

Anonim erişim sistemleri

Bu kategori, aşağıdaki amaçlarla özel İnternet uygulamalarını kullanarak İnternet kaynaklarının içeriğinin indirilmesine aracılık eden İnternet kaynaklarını kapsar.

- İnternet adreslerine veya IP adreslerine erişimde LAN yöneticisi tarafından getirilen kısıtlamaların aşılması;
- Belirli IP adreslerinden veya gruplarından HTTP isteklerini özel olarak reddeden İnternet kaynaklarını içeren İnternet kaynaklarına anonim erişim (örneğin kaynak ülkeye göre gruplanan IP adresleri).

Bu kategori, hem yukarıda belirtilen amaçlarla özel olarak geliştirilen İnternet kaynaklarını ("anonimleştiriciler") ve teknik olarak benzer işleve sahip İnternet kaynaklarını içerir.

Bilgisayar oyunları

Bu kategori, çeşitli türlerdeki bilgisayar oyunlarına odaklanan İnternet kaynaklarını içerir:

- Bilgisayar oyunu geliştiricilerin web siteleri.
- Bilgisayar oyunlarının tartışılmasına odaklanan İnternet kaynakları.

  "İnternet iletişim medyası" kategorisi ile örtüşür.

- Uygulamaların yerel kurulumuyla veya bu tür kurulum olmadan ("tarayıcı oyunları") diğer katılımcılarla veya bireysel olarak oyunlara çevrimiçi katılım için teknik imkan sağlayan İnternet kaynakları.
- Oyun yazılımının reklamını, dağıtımı yapmak ve desteklemek amacıyla tasarlanan İnternet kaynakları.

  "Elektronik ticaret" kategorisi ile örtüşür.

Dinler, dini dernekler

Bu kategori, dini bir ideolojiye sahip ve/veya inanç gösterisinde bulunan halk hareketleri, dernekler ve organizasyonlarla ilgili materyaller sunan İnternet kaynaklarını içerir.

- Uluslararası dini düzeyden yerel dini topluluklara kadar farklı düzeylerdeki resmi dini organizasyonların İnternet siteleri.
- Hakim bir dini cemiyet veya topluluktan ayrılarak oluşan kayıtlı olmayan dini cemiyet ve toplulukların İnternet siteleri.
- Belirli bir kurucunun girişimiyle geleneksel dini hareketlerden bağımsız olarak ortaya çıkan dini cemiyetler ve toplulukların İnternet siteleri.
- Farklı geleneksel dinlerin temsilcileri arasında iş birliği amaçlayan dinler arası organizasyonların İnternet siteleri.

- Dini konularda akademik, tarihi ve ansiklopedik materyaller içeren İnternet kaynakları.
- Tanrıya, doğa üstü güçleri olduğuna inanılan varlık ve/veya eşyalara ibadeti kapsayan ayin ve törenler, dini ibadetlerin bir parçası olarak dini ibadetlerin ayrıntılı şekilde resmedildiği veya tasvir edildiği İnternet kaynakları.

Haber medyası

Bu kategori, kullanıcıların kendi haberlerini eklemesine imkan tanıyan kitle iletişim veya çevrimiçi yayınlar tarafından oluşturulan genel haber içeriğine sahip İnternet kaynaklarını içerir.

- Resmi medya kuruluşlarının web siteleri.
- Resmi bilgi kaynaklarının atıflarını içeren bilgi hizmetleri sunan İnternet siteleri.
- Çeşitli resmi ve gayri resmi kaynakların haber bilgilerinin toplanması hizmetini sunan İnternet siteleri.
- Haber içeriğinin kullanıcıların kendileri tarafından oluşturulduğu İnternet siteleri ("sosyal haber siteleri").

> "İnternet iletişim medyası" kategorisi ile örtüşür.

Reklam pencereleri

Bu kategori, reklam pencereli İnternet kaynaklarını içerir. Reklam pencerelerinde bilgi yayınlamak, kullanıcıların etkinliklerden dikkatini dağıtırken reklam pencerelerinde indirmeler trafik miktarını artırır.

İnternet kaynağı erişim kuralları hakkında

Bir İnternet kaynağı erişim kuralı, kullanıcının kural zamanlamasında belirtilen süre boyunca kuralda açıklanan İnternet kaynaklarını ziyaret ettiği zaman Kaspersky Endpoint Security'nin gerçekleştirdiği filtreler veya eylemler kümesidir. Filtreler, İnternet Denetimi bileşeni tarafından erişimin denetlendiği İnternet kaynakları havuzunu doğru bir şekilde belirtmenize olanak tanır.

Aşağıdaki filtreler kullanılabilir:

- **İçeriğe göre filtrele**. İnternet Denetimi, içeriğe göre İnternet kaynaklarını ve veri türünü kategorilere ayırır. İnternet kaynaklarına kullanıcı erişimini belirli kategorilerdeki içerik ve veri türleri ile denetleyebilirsiniz. Kullanıcının seçilen içerik kategorisi ve / veya veri türü kategorisine giren İnternet kaynaklarını ziyaret ettiği zaman Kaspersky Endpoint Security, kuralda belirtilen eylemi gerçekleştirir.
- **İnternet kaynağı adreslerine göre filtrele**. Tüm İnternet kaynağı adreslerine veya tek tek İnternet kaynağı adreslerine ve/veya İnternet kaynağı adresi gruplarına kullanıcı erişimini denetleyebilirsiniz.

  İçeriğe göre filtreleme ve İnternet kaynağı adreslerine göre filtreleme belirtilirse ve belirtilen İnternet kaynağı adresleri ve/veya İnternet kaynağı adreslerinin grupları seçilen içerik kategorilerine veya veri türü kategorilerine girdiğinde Kaspersky Endpoint Security, seçilen içerik kategorilerindeki ve/veya veri türü kategorilerindeki tüm İnternet kaynaklarına erişimi denetlemez. Bunun yerine uygulama sadece belirtilen İnternet kaynağı adreslerine ve/veya İnternet kaynağı adres gruplarına erişimi denetler.
- **Kullanıcıların ve kullanıcı gruplarının adlarına göre filtrele**. İnternet kaynaklarına erişimi kurala göre denetlenen kullanıcılar ve/veya kullanıcı gruplarının adlarını belirtebilirsiniz.

- **Kural zamanlaması**. Kural zamanlamasını belirtebilirsiniz. Kural zamanlaması, Kaspersky Endpoint Security'nin İnternet kaynaklarına erişimi kurala göre izlediği süreyi belirler.

Kaspersky Endpoint Security yüklendikten sonra İnternet Denetimi bileşeni kurallarının listesi boş değildir. İki kural önceden ayarlanmıştır:

- Adresleri css, js veya vbs uzantılarına sahip dosyaların adreslerini içeren İnternet kaynaklarına her zaman tüm kullanıcılara erişim veren Senaryolar ve Stil Tablosu kuralı. Örneğin: http://www.example.com/style.css, http://www.example.com/style.css?mode=normal.

- Tüm kullanıcılara herhangi bir zamanda herhangi bir İnternet kaynağına erişim veren "Varsayılan kural"dır.

İnternet kaynağı erişim kurallarıyla ilgili eylemler

İnternet kaynağı erişim kurallarında aşağıdaki eylemleri uygulayabilirsiniz:

- Yeni bir kural ekle

- Bir kural düzenle

- Bir kurala öncelik ata

  Bir kuralın önceliği, İnternet Denetimi bileşeninin ayarlar penceresindeki erişim kuralı tablosunda bu kuralın kısa açıklamasını içeren satırın konumuna göre belirlenir. Bu durumda erişim kuralları tablosunda daha yüksek olan bir kural, aşağıda yer alandan daha yüksek önceliğe sahiptir.

  Kullanıcının erişmeye çalıştığı bir İnternet kaynağının birden fazla kuralın parametreleri ile eşleşmesi halinde Kaspersky Endpoint Security, en yüksek önceliğe sahip kurala göre bir eylem gerçekleştirir.

- Kuralı test etme.

  Kuralları tanılama işlevini kullanarak kuralların tutarlılığını denetleyebilirsiniz.

- Kuralı etkinleştirme ve devre dışı bırakma.

  Bir İnternet kaynağı erişim kuralı etkinleştirilebilir (çalışma durumu: *Açık*) veya devre dışı bırakılabilir (çalışma durumu: *Kapalı*). Varsayılan olarak bir kural oluşturulduktan sonra etkinleştirilir (çalışma durumu: *Açık)*. Kuralı devre dışı bırakabilirsiniz.

- Kuralı sil

İnternet kaynağı erişim kuralı ekleme ve düzenleme

Bir İnternet kaynağı erişim kuralı eklemek veya düzenlemek için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol kısmında, **Uç nokta denetimi** bölümünde, **İnternet Denetimi** alt bölümünü seçin.

   Pencerenin sağ kısmında, İnternet Denetimi bileşeni ayarları görüntülenir.

3. Aşağıdakilerden birini yapın:

   - Bir kural eklemek için **Ekle** düğmesine tıklayın.

- Bir kuralı düzenlemek isterseniz, kuralı tablodan seçin ve **Düzenle** düğmesine tıklayın.

İnternet kaynaklarına erişim kuralı penceresi açılır.

4. Kural ayarlarını belirtin veya düzenleyin. Bunun için:

   a. **Ad** alanına, kuralın adını girin veya düzenleyin.

   b. **Filtre içeriği** açılır listesinden gereken seçeneği seçin:

      - **Her türlü içerik**.
      - **İçerik kategorilerine göre**.
      - **Veri türlerine göre**.
      - **İçerik kategorilerine ve veri türlerine göre**.

   c. **Her türlü içerik** dışında bir seçenek seçildiğinde, içerik ve/veya veri türü kategorilerinin seçileceği bölümler açılır. Gereken içerik ve/veya veri türü kategorilerinin adlarının karşısındaki onay kutularını seçin.

      Bir içerik kategorisi adının ve/veya veri türünün karşısındaki onay kutusu seçildiğinde Kaspersky Endpoint Security, seçilen içerik kategorisine ve/veya veri türlerine ait olan İnternet kaynaklarına erişimi denetleyen kuralı uygular.

   d. **Adreslere uygula** açılır listesinden gereken seçeneği seçin:

      - **Tüm adreslere**.
      - **Tek tek adreslere**.

   e. **Tek tek adreslere** seçeneği seçilirse, İnternet kaynaklarının listesini oluşturduğunuz bir bölüm açılır. **Ekle**, **Düzenle** ve **Sil** düğmelerini kullanarak İnternet kaynaklarının adreslerini ekleyebilir veya düzenleyebilirsiniz.

   f. **Kullanıcıları ve/veya grupları belirtin** onay kutusunu seçin.

   g. **Seç** düğmesine tıklayın.

      Microsoft Windows'ta **Kullanıcıları veya Grupları Seç** penceresi açılır.

   h. Kurala göre açıklanan İnternet kaynaklarına erişimin izin verileceği veya engelleneceği kullanıcılar ve/veya kullanıcı gruplarının listesini belirtin veya düzenleyin.

   i. **Eylem** açılır listesinden gereken seçeneği seçin:

      - **İzin ver** Bu değer seçiliyse, Kaspersky Endpoint Security, kural parametreleriyle eşleşen İnternet kaynaklarına erişime izin verir.
      - **Engelle** Bu değer seçiliyse, Kaspersky Endpoint Security, kural parametreleriyle eşleşen İnternet kaynaklarına erişimi engeller.
      - **Uyar**. Bu değer seçilirse Kaspersky Endpoint Security, kullanıcının kuralla eşleşen İnternet kaynaklarına erişim girişimi sırasında bir İnternet kaynağının istenmediği şeklinde bir uyarı görüntüler. Uyarı mesajındaki bağlantıları kullanarak kullanıcı, istenen İnternet kaynağına erişim elde edebilir.

   j. **Kural zamanlaması** açılır listesinde, gereken zamanlamanın adını seçin veya seçilen kural zamanlamasına dayalı olarak yeni bir zamanlama oluşturun. Bunun için:

1. **Kural zamanlaması** açılır listesinin karşısında, **Ayarlar** düğmesine tıklayın.

   Kural zamanlaması penceresi açılır.

2. Kural zamanlamasına kuralın geçerli olmayacağı bir zaman aralığı eklemek için kural zamanlamasının görüntülendiği tabloda, seçmek istediğiniz haftanın günü ve saatine denk gelen tablo hücrelerine tıklayın.

   Hücrelerin rengi griye döner.

3. Kuralın uygulanacağı bir zaman aralığı yerine kuralın geçerli olmayacağı bir zaman aralığı koymak için seçmek istediğiniz haftanın günü ve saatine denk gelen tablodaki gri hücrelere tıklayın.

   Hücrelerin rengi yeşile döner.

4. **Farklı kaydet** düğmesine tıklayın.

   Kural zamanlaması adı penceresi açılır.

5. Bir kural zamanlaması adı yazın veya önerilen varsayılan adı bırakın.

6. **Tamam**'a tıklayın.

5. **İnternet kaynaklarına erişim kuralı** penceresinde **Tamam** düğmesine tıklayın.

6. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

İnternet kaynağı erişim kurallarına öncelikler atama

Kuralları belirli bir sırayla düzenleyerek kurallar listesinden her bir kurala öncelik atayabilirsiniz.

Bir İnternet kaynağı erişim kuralına öncelik atamak için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol kısmında, **Uç nokta denetimi** bölümünde, **İnternet Denetimi** alt bölümünü seçin.

   Pencerenin sağ kısmında, İnternet Denetimi bileşeni ayarları görüntülenir.

3. Pencerenin sağ kısmında, önceliğini değiştirmek istediğiniz kuralı seçin.

4. Kuralı, kurallar listesinde gereken sıraya taşımak için **Yukarı taşı** ve **Aşağı taşı** düğmelerini kullanın.

5. Önceliğini değiştirmek istediğiniz kurallar için 3.–4. Adımları tekrarlayın.

6. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

İnternet kaynağı erişim kurallarını test etme

İnternet Denetimi kurallarının tutarlılığını denetlemek amacıyla bunları test edebilirsiniz. Bu amaçla İnternet Denetimi bileşeni, Kural Tanılama işlevini içerir.

İnternet kaynağı erişim kurallarını test etmek için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol kısmında, **Uç nokta denetimi** bölümünde, **İnternet Denetimi** alt bölümünü seçin.

   Pencerenin sağ kısmında, İnternet Denetimi bileşeni ayarları görüntülenir.

3. Pencerenin sağ kısmında, **Tanılama** düğmesine tıklayın.

   Kural tanılama penceresi açılır.

4. **Koşullar** bölümündeki alanları doldurun:

   a. Kaspersky Endpoint Security'nin belirli bir İnternet kaynağına erişimi denetlemek için kullandığı kuralları test etmek istiyorsanız, **Adresi belirtin** onay kutusunu seçin. Aşağıdaki alana İnternet kaynağının adresini girin.

   b. Kaspersky Endpoint Security'nin belirtilen kullanıcılar ve/veya kullanıcı gruplarının İnternet kaynaklarına erişimi denetlemek için kullandığı kuralları test etmek isterseniz, kullanıcılar ve/veya kullanıcı gruplarının listesini belirtin.

   c. Kaspersky Endpoint Security'nin belirtilen içerik kategorilerinin ve/veya veri türü kategorilerinin İnternet kaynaklarına erişimi denetlemek için kullandığı kuralları test etmek isterseniz, **Filtre içeriği** açılır listesinden gereken seçeneği seçin (**İçerik kategorilerine göre**, **Veri türlerine göre** veya **İçerik kategorilerine ve veri türlerine göre**).

   d. Kural tanılama koşullarında belirtilen İnternet kaynaklarına erişim girişiminde bulunulduğunda haftanın günü ve saatinin hesabı ile kuralları test etmek isterseniz, **Erişim girişiminin saatini ekle** onay kutusunu seçin. Ardından haftanın günü ve saatini belirtin.

5. **Test** düğmesine tıklayın.

Testin tamamlanmasının ardından, belirtilen İnternet kaynağına erişim girişiminde tetiklenen ilk kurala göre Kaspersky Endpoint Security tarafından uygulanan işlem (izin ver, engelle veya uyar) hakkında bilgi yer alan bir mesaj görüntülenir. Tetiklenecek ilk kural, İnternet Denetimi kurallarında tanılama koşullarını karşılayan diğer kurallardan daha yüksek bir sıradaki kuraldır. Mesaj, **Test** düğmesinin sağında görüntülenir. Aşağıdaki tabloda, Kaspersky Endpoint Security tarafından uygulanan işlemi belirten diğer tetiklenen kurallar yer almaktadır. Kurallar yukarıdan aşağı öncelik sıralamasına göre belirtilmiştir.

İnternet kaynağı erişim kuralını etkinleştirme ve devre dışı bırakma

Bir İnternet kaynağı erişim kuralını etkinleştirmek veya devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol kısmında, **Uç nokta denetimi** bölümünde, **İnternet Denetimi** alt bölümünü seçin.

   Pencerenin sağ kısmında, İnternet Denetimi bileşeni ayarları görüntülenir.

3. Pencerenin sağ kısmında, etkinleştirmek veya devre dışı bırakmak istediğiniz kuralı seçin.

4. **Durum** sütununda aşağıdakilerden birini yapın:

   - Kuralın kullanımını etkinleştirmek istiyorsanız *Açık* değerini seçin.

   - Kuralın kullanımını devre dışı bırakmak istiyorsanız *Kapalı* değerini seçin.

5. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Uygulamanın önceki sürümlerinden İnternet kaynağı erişim kurallarını taşıma

Uygulamanın Service Pack 1 Maintenance Release 1 veya daha eski bir sürümü, Kaspersky Endpoint Security 10 Service Pack 2 for Windows'a yükseltildiğinde İnternet kaynağı içerik kategorilerine dayalı İnternet kaynağı erişim kuralları aşağıdaki gibi taşınır:

- "Forumlar ve sohbetler", "Web e-posta" ve "Sosyal ağlar" listelerinden bir ya da daha fazla İnternet kaynağı içerik kategorisine dayalı İnternet kaynağı erişim kuralları, "İnternet iletişim medyası" İnternet kaynağı içerik kategorisine taşınır.
- "İnternet mağazaları" ve "Ödeme Sistemleri" listelerinden bir ya da daha fazla İnternet kaynağı içerik kategorisine dayalı İnternet kaynağı erişim kuralları, "Elektronik ticaret" İnternet kaynağı içerik kategorisine taşınır.
- "Kumar" İnternet kaynağı içerik kategorisine dayalı İnternet kaynağı erişim kuralları, "Kumar, piyango, çekiliş" içerik kategorisine taşınır.
- "Tarayıcı oyunları" İnternet kaynağı içerik kategorisine dayalı İnternet kaynağı erişim kuralları, "Bilgisayar oyunları" içerik kategorisine taşınır.
- Yukarıdaki listede adı geçmeyen İnternet kaynağı içerik kategorilerine dayalı İnternet kaynağı erişim kuralları, değişiklik olmadan taşınır.

İnternet kaynağı adreslerinin listesini dışa aktarma ve içe aktarma

Bir İnternet kaynağı erişim kuralında İnternet kaynağı adreslerinin listesini oluşturduysanız .txt dosyasına dışa aktarabilirsiniz. Ardından bir erişim kuralını yapılandırırken İnternet kaynağı adreslerinin yeni listesini elle oluşturmaktan kaçınmak için dosyadan bu listeyi içe aktarabilirsiniz. Örneğin benzer parametrelerle erişim kuralları oluşturursanız İnternet kaynağı adreslerinin listesini dışa aktarma ve içe aktarma seçeneği faydalı olabilir.

İnternet kaynağı adreslerinin listesini bir dosyaya dışa aktarmak için:

1. Ana uygulama penceresinde **Ayarlar** düğmesine tıklayın.
2. Pencerenin sol kısmında, **Güvenlik Denetimleri** bölümünde, **İnternet Denetimi** bölümünü seçin.

   Pencerenin sağ kısmında, İnternet Denetimi bileşeni ayarları görüntülenir.
3. İnternet kaynağı adreslerinin listesini bir dosyaya dışa aktarmak istediğiniz kuralı seçin.
4. **Düzenle** düğmesine tıklayın.

   İnternet kaynaklarına erişim kuralı penceresi açılır.
5. İnternet adreslerinin tüm listesini dışa aktarmak istemiyorsanız ama sadece bir kısmını dışa aktarmayı tercih ediyorsanız gereken İnternet kaynağı adreslerini seçin.
6. İnternet kaynağı adreslerinin listesinin bulunduğu sağdaki alanda düğmesine tıklayın.

   İşlem onay penceresi açılır.
7. Aşağıdakilerden birini yapın:

- İnternet kaynağı adreslerinin listesinin sadece seçilen öğelerini dışa aktarmak isterseniz işlem onayı penceresinde **Evet** düğmesine tıklayın.
- İnternet kaynağı adreslerinin listesinin tüm öğelerini dışa aktarmak isterseniz işlem onayı penceresinde **Hayır** düğmesine tıklayın.

  Microsoft Windows'ta standart **Farklı kaydet** penceresi açılır.

8. **Farklı kaydet** Microsoft Windows penceresinde, İnternet kaynağı adreslerinin listesini dışa aktarmak istediğiniz dosyayı seçin. **Kaydet** düğmesine tıklayın.

Bir dosyadan kurala İnternet kaynağı adreslerinin listesini içe aktarmak için:

1. Ana uygulama penceresinde **Ayarlar** düğmesine tıklayın.
2. Pencerenin sol kısmında, **Güvenlik Denetimleri** bölümünde, **İnternet Denetimi** bölümünü seçin.

   Pencerenin sağ kısmında, İnternet Denetimi bileşeni ayarları görüntülenir.
3. Aşağıdakilerden birini yapın:
   - Yeni bir İnternet kaynağı erişim kuralı oluşturmak isterseniz **Ekle** düğmesine tıklayın.
   - Düzenlemek istediğiniz İnternet kaynağı erişim kuralını seçin. Ardından **Düzenle** düğmesine tıklayın.

   İnternet kaynaklarına erişim kuralı penceresi açılır.
4. Aşağıdakilerden birini yapın:
   - Yeni bir İnternet kaynağı erişim kuralı oluşturuyorsanız **Adreslere uygula** açılır listesinden **Tek tek adreslere** seçeneğini seçin.
   - İnternet kaynağı erişim kuralını düzenliyorsanız bu talimatların 5. adımına gidin.
5. İnternet kaynağı adreslerinin listesinin bulunduğu sağdaki alanda düğmesine tıklayın.

   Yeni bir kural oluşturuyorsanız Microsoft Windows'un standart **Dosyayı aç** penceresi açılır.

   Bir kuralı düzenliyorsanız onayınızı isteyen bir pencere açılır.
6. Aşağıdakilerden birini yapın:
   - Yeni bir İnternet kaynağı erişim kuralını düzenliyorsanız bu talimatların 7. adımına gidin.
   - Bir İntrenet kaynağı erişim kuralını düzenliyorsanız işlem onayı penceresinde aşağıdaki işlemlerden birini yapın:
     - İnternet kaynağı adreslerinin listesinden içe aktarılan öğeleri mevcut öğelerin içine aktarmak isterseniz **Evet** düğmesine tıklayın.
     - İnternet kaynağı adreslerinin listesinden mevcut öğeleri silmek ve içe aktarılan öğelere eklemek isterseniz **Hayır** düğmesine tıklayın.

   Microsoft Windows'ta **Dosyayı aç** penceresi açılır.
7. Microsoft Windows'ta **Dosyayı aç** penceresinde, içe aktarılacak İnternet kaynağı adreslerinin listesini içeren bir dosya seçin.
8. **Aç** düğmesine tıklayın.

9. **İnternet kaynaklarına erişim kuralı** penceresinde **Tamam** düğmesine tıklayın.

İnternet kaynağı adreslerinin maskelerini düzenleme

Bir İnternet kaynağı adresi kuralı oluştururken çok sayıda benzer İnternet kaynağı adresi girmeniz gerekiyorsa *İnternet kaynağı adresi maskesi* (aynı zamanda "adresi maskesi" olarak da adlandırılır) kullanmak faydalı olabilir. İyi tasarlanırsa bir adres maskesi, çok sayıda İnternet kaynağı adresinin yerini alabilir.

Bir adres maskesi oluştururken aşağıdaki kuralları uygulayın:

1. `*` karakteri, sıfır veya daha fazla karakter içeren herhangi bir dizinin yerini alır.

   Örneğin *abc* adres maskesini girerseniz abc dizisini içeren tüm İnternet kaynaklarına erişim kuralı uygulanır. Örneğin: http://www.example.com/page_0-9abcdef.html.

   `*` karakterini adres maskesine eklemek için `*` karakterini iki kez girin.

2. Adres maskesinin başındaki `www.` karakter dizisi, `*.` dizisi olarak yorumlanır.

   Örneğin: www.example.com adres maskesi *.example.com olarak işlenir.

3. Adres maskesi `*` karakteri ile başlamıyorsa adres maskesinin içeriği `*.` ön ekli aynı içeriğe eşdeğerdir.

4. Adres maskesinin başlangıcındaki `*.` karakter dizisi, `*.` veya boş dizi olarak yorumlanır.

   Örneğin: http://www.*.example.com adres maskesi, http://www2.example.com adresini kapsar.

5. Adres maskesi `/` veya `*` dışında bir karakterle bitiyorsa adres maskesinin içeriği `/*` son ekli aynı içeriğe eşdeğerdir.

   Örneğin: http://www.example.com adres maskesi; a, b ve c'nin herhangi bir karakter olduğu http://www.example.com/abc gibi adresleri kapsar.

6. Adres maskesi `/` karakteri ile bitiyorsa adres maskesinin içeriği `/*.` Son ekli aynı içeriğe eşdeğerdir.

7. Adres maskesinin sonundaki `/*` karakter dizisi, `/*` veya boş bir dizi olarak yorumlanır.

8. İnternet kaynağı adresleri, iletişim kuralını (http veya https) göz önünde bulundurarak bir adres maskesi ile doğrulanır:

   - Adres maskesi herhangi bir ağ iletişim kuralı içermiyorsa bu adres maskesi herhangi bir ağ iletişim kuralına sahip adresleri kapsar.

     Örneğin: example.com adres maskesi, http://example.com ve https://example.com adreslerini kapsar.

   - Adres maskesi bir ağ iletişim kuralını içeriyorsa bu adres maskesi sadece adres maskesi ile aynı ağ iletişim kuralına sahip adresleri kapsar.

     Örneğin: http://*.example.com adres maskesi http://www.example.com adresini kapsar ancak https://www.example.com adresini kapsamaz.

9. Çift tırnak içindeki bir adres maskesi ek değiştirmeleri göz önünde bulundurmadan işlenir ancak başlangıçta adres maskesine dahil edildiyse `*` karakteri istisnadır. Çift tırnak işareti ile çevrelenen adres maskeleri için kural 5 ve 7 geçerli değildir (aşağıdaki tabloda örnek 14 – 18'e bakınız).

10. Bir İnternet kaynağının adres maskesiyle karşılaştırma yaparken kullanıcı adı ve parolası, bağlantı noktası ve karakterin büyük/küçük harf durumu göz önünde bulundurulur.

No.	Adres maskesi	Doğrulanacak İnternet kaynağının adresi	Adres maskesi adresi kapsıyor mu?	Yorum
1	*.example.com	http://www.123example.com	Hayır	1. kurala bakınız.
2	*.example.com	http://www.123.example.com	Evet	1. kurala bakınız.
3	*example.com	http://www.123example.com	Evet	1. kurala bakınız.
4	*example.com	http://www.123.example.com	Evet	1. kurala bakınız.
5	http://www.*.example.com	http://www.123example.com	Hayır	1. kurala bakınız.
6	www.example.com	http://www.example.com	Evet	2. ve 1. kurala bakınız.
7	www.example.com	https://www.example.com	Evet	2. ve 1. kurala bakınız.
8	http://www.*.example.com	http://123.example.com	Evet	2., 4. ve 1. kurala bakınız.
9	www.example.com	http://www.example.com/abc	Evet	2., 5. ve 1. kurala bakınız.
10	example.com	http://www.example.com	Evet	3. ve 1. kurala bakınız.
11	http://example.com/	http://example.com/abc	Evet	6. kurala bakınız.
12	http://example.com/*	http://example.com	Evet	7. kurala bakınız.
13	http://example.com	https://example.com	Hayır	8. kurala bakınız.
14	"example.com"	http://www.example.com	Hayır	9. kurala bakınız.
15	"http://www.example.com"	http://www.example.com/abc	Hayır	9. kurala bakınız.
16	"*.example.com"	http://www.example.com	Evet	1. ve 9. kurala bakınız.
17	"http://www.example.com/*"	http://www.example.com/abc	Evet	1. ve 9. kurala bakınız.
18	"www.example.com"	http://www.example.com; https://www.example.com	Evet	9. ve 8. kurala bakınız.
19	www.example.com/abc/123	http://www.example.com/abc	Hayır	Bir adres maskesi, bir İnternet kaynağının adresinden daha fazla bilgi içerir.

İnternet Denetimi mesajlarının şablonlarını düzenleme

İnternet Denetimi kurallarının özelliklerinde belirtilen eylem türüne bağlı olarak Kaspersky Endpoint Security, kullanıcının İnternet kaynaklarına erişmeye çalıştığı zamanda aşağıdaki türden bir mesaj görüntüler (uygulama, HTML sayfasını HTTP sunucu yanıtı mesajı ile değiştirir):

- Uyarı mesajı. Bu mesaj kullanıcıya, İnternet kaynağını ziyaret etmenin önerilmediği ve/veya kurumsal güvenlik ilkesini ihlal ettiği uyarısında bulunur. Bu İnternet kaynağını açıklayan kuralın ayarlarındaki **Eylem** açılır listesinden **Uyar** seçeneği seçilirse Kaspersky Endpoint Security bir uyarı mesajı görüntüler.

Kullanıcı uyarının hatalı olduğunu düşünüyorsa, yerel kurumsal ağ yöneticisine önceden oluşturulmuş bir mesaj göndermek için uyarıdaki bağlantıya tıklayabilir.

- İnternet kaynağının engellendiğini bildiren mesaj. Bu İnternet kaynağını açıklayan kuralın ayarlarındaki **Eylem** açılır listesinden **Engelle** seçeneği seçilirse Kaspersky Endpoint Security, İnternet kaynağının engellendiğini bildiren bir mesaj görüntüler.

  Kullanıcı İnternet kaynağının yanlışlıkla engellendiğini düşünüyorsa, yerel kurumsal ağ yöneticisine önceden oluşturulmuş bir mesaj göndermek için İnternet kaynağı engelleme bildirimi mesajındaki bağlantıya tıklayabilir.

Uyarı mesajı, bir İnternet kaynağının engellendiğini bildiren mesaj ve LAN yöneticisine gönderilen mesaj için özel şablonlar sağlanmaktadır. Bunların içeriğini değiştirebilirsiniz.

İnternet Denetimi mesajlarının şablonunu değiştirmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Uç nokta denetimi** bölümünde, **İnternet Denetimi** alt bölümünü seçin.

   Pencerenin sağ kısmında, İnternet Denetimi bileşeni ayarları görüntülenir.
3. Pencerenin sağ kısmında, **Şablonlar** düğmesine tıklayın.

   Mesaj şablonları penceresi açılır.
4. Aşağıdakilerden birini yapın:

   - Kullanıcıyı bir İnternet kaynağını ziyaret etmeme konusunda uyaran mesajın şablonunu düzenlemek isterseniz **Uyarı** sekmesini seçin.
   - Kullanıcıya bir İnternet kaynağına erişimin engellendiğini bildiren mesajın şablonunu düzenlemek isterseniz **Engelleme** sekmesini seçin.
   - Yöneticiye gönderilen mesajın şablonunu düzenlemek için **Yöneticiye mesaj** sekmesini seçin.
5. Mesaj şablonunu düzenleyin. **Değişken** açılır listesinin yanı sıra **Varsayılan** ve **Bağlantı** (bu düğme **Yöneticiye mesaj** sekmesinde kullanılamaz) düğmelerini kullanabilirsiniz.
6. **Tamam**'a tıklayın.
7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

KATA Endpoint Sensor

KATA Endpoint Sensor bileşeninin ayarları yalnızca Kaspersky Security Center Yönetim Konsolu'nda bulunmaktadır. Bu bileşeni kullanmak için yönetim eklentisini yüklemelisiniz.

Bu bölümde, KATA Endpoint Sensor ve bu bileşeni etkinleştirme ve devre dışı bırakma talimatları bulunmaktadır.

KATA Endpoint Sensor hakkında

KATA Endpoint Sensor, Kaspersky Anti Targeted Attack Platform'un bir bileşenidir. Bu çözüm, hedeflenen saldırılar gibi tehditlerin hızlı tespitine yöneliktir.

Bu bileşen, istemci bilgisayarlarda kurulur. Bu bilgisayarlarda, bileşen sürekli olarak işlemleri, etkin ağ bağlantılarını ve değiştirilen dosyaları izler ve bu bilgileri Kaspersky Anti Targeted Attack Platform'a aktarır.

Bileşen işlevselliği aşağıdaki işletim sistemlerinde kullanılabilir:

- Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP1, Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1.
- Microsoft Windows 8.1 Enterprise x86 Edition, Microsoft Windows 8.1 Enterprise x64 Edition.
- Microsoft Windows 10 Pro / Enterprise x86 Edition, Microsoft Windows 10 Pro / Enterprise x64 Edition.
- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1.
- Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition, Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition.
- Microsoft Windows Server 2016

Kaspersky Anti Targeted Attack Platform hakkında bu belgede bulunmayan ek bilgi için Kaspersky Anti Targeted Attack Platform yardımına başvurun.

KATA Endpoint Sensor bileşeni olan bilgisayarlara gelen bağlantılara, proxy sunucusu olmadan doğrudan Kaspersky Anti Targeted Attack Platform sunucusundan izin verilmemelidir.

KATA Endpoint Sensor bileşenini etkinleştirme veya devre dışı bırakma

KATA Endpoint Sensor bileşenini etkinleştirmek veya devre dışı bırakmak için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacının **Yönetilen aygıtlar** klasöründe, ilke ayarlarını düzenlemek istediğiniz ilgili yönetim grubunun adının bulunduğu klasörü açın.
3. Çalışma alanında, **İlkeler** sekmesini seçin.

4. Gereken ilkeyi seçin.

5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:

   - İlkenin içerik menüsünde **Özellikler**'i seçin.

   - Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.

6. **Gelişmiş ayarlar** bölümünde **KATA Endpoint Sensor** alt bölümünü seçin.

7. Aşağıdakilerden birini yapın:

   - KATA Endpoint Sensor'u etkinleştirmek isterseniz **KATA Endpoint Sensor** onay kutusunu işaretleyin.

   - KATA Endpoint Sensor'u devre dışı bırakmak isterseniz **KATA Endpoint Sensor** onay kutusunu işaretlemeyin.

8. Önceki adımda **KATA Endpoint Sensor** onay kutusunu seçtiyseniz **Sunucu adresi** alanında aşağıdaki bölümlerden oluşan Kaspersky Anti Targeted Attack Platform sunucu adresini belirtin.

   a. İletişim kuralı adı

   b. Sunucunun IP adresi veya tam etki alanı adı (FQDN)

   c. Sunucu üzerindeki Windows Olay Toplayıcısı yolu

9. **Tamam**'a tıklayın.

10. İlkeyi uygulayın.

    Kaspersky Security Center ilkesinin uygulanmasıyla ilgili ayrıntılar için *Kaspersky Security Center Yönetici Kılavuzu*'na bakınız.

Veri Şifreleme

Kaspersky Endpoint Security, Microsoft Windows for Workstations altında çalışan bir bilgisayara yüklenirse, veri şifreleme işlevselliği tam olarak kullanılabilir. Kaspersky Endpoint Security, Microsoft Windows for File Servers çalıştıran bir bilgisayara yüklenirse, sadece BitLocker Drive Encryption teknolojisini kullanaran sabit sürücü şifreleme mvcuttur.

Bu bölümde sabit sürücülerin, çıkarılabilir sürücülerin ve yerel bilgisayar sürücülerindeki dosya ve klasörlerin şifrelenmesi ve şifresinin çözülmesi hakkında bilgi yer almakta ve Kaspersky Endpoint Security'yi ve Kaspersky Endpoint Security yönetim eklentisini kullanarak veri şifreleme ve şifre çözmenin nasıl yapılandırılacağı ve gerçekleştirileceği konusunda talimatlar sağlanmaktadır.

Şifrelenmiş verilere hiçbir erişim yoksa şifrelenmiş verilerle çalışmak için özel talimatlar bölümüne bakın (Kısıtlı dosya şifreleme işlevselliği durumunda şifrelenmiş dosyalarla çalışma, Erişim olmayan şifrelenmiş aygıtlarla çalışma).

Kaspersky Security Center ilkesinde şifreleme ayarlarının görüntülenmesini etkinleştirme

Kaspersky Security Center ilkesinde şifreleme ayarlarının görüntülenmesini etkinleştirmek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. **Yönetim Sunucusu**'nun içerik menüsünde Yönetim Konsolu ağacının **– <Bilgisayar adı>** düğümünde **Göster → Arabirim ayarları**'nı seçin.

   Arabirim ayarları penceresi açılır.
3. **Arabirim ayarları** penceresinde **Şifrelemeyi ve veri korumasını göster** onay kutusunu işaretleyin.
4. **Tamam**'a tıklayın.

Veri şifreleme hakkında

Kaspersky Endpoint Security, yerel bilgisayar sürücülerinde ve çıkarılabilir sürücülerde veya çıkarılabilir sürücülerin ve sabit sürücülerin tamamında depolanan dosya ve klasörleri şifrelemenize olanak tanır. Veri şifreleme, bir taşınabilir bilgisayar, çıkarılabilir sürücü veya sabit sürücü kaybedildiğinde veya çalındığında ya da verilere yetkisiz kullanıcı veya uygulamalar tarafından erişim sağlandığında oluşabilecek bilgi sızması riskini en aza indirir.

Lisansın süresi sona erdiyse uygulama yeni verileri şifrelemez ve eski şifrelenmiş veriler şifrelenmiş olarak kalmaya ve kullanılabilir olmaya devam eder. Bu durmda, yeni verilerin şifrelenmesi programın şifrelemeye izin veren yeni bir lisans ile etkinleştirilmesini gerektirir.

Lisansınızın süresi sona erdiyse veya Son Kullanıcı Lisans Sözleşmesi ihlal edildiyse, anahtar, Kaspersky Endpoint Security veya şifreleme bileşenleri kaldırıldıysa, önceden şifrelenmiş dosyaların şifreleme durumu garanti edilemez. Çünkü Microsoft Office Word gibi bazı uygulamalar, düzenleme sırasında dosyaların geçici bir kopyasını oluşturur. Orijinal dosya kaydedildiğinde geçici kopya, orijinal dosyanın yerini alır. Sonuç olarak şifreleme işlevi olmayan veya erişilemeyen bir bilgisayarda dosya şifrelenmeden kalır.

Kaspersky Endpoint Security aşağıdaki veri koruma özelliklerini sunar:

- **Yerel bilgisayar sürücülerindeki dosyaları şifreleme**. Uzantıya veya uzantı gruplarına ve yerel bilgisayar sürücülerinde kayıtlı klasörlerin listelerine göre dosya listelerini derleyebilirsiniz ve belirli uygulamaların oluşturduğu dosyaların şifrelenmesi için kurallar oluşturabilirsiniz. Bir Kaspersky Security Center ilkesi uygulandıktan sonra Kaspersky Endpoint Security aşağıdaki dosyaları şifreler ve şifrelerini çözer:

  - Şifreleme ve şifre çözme için listelere tek tek eklenen dosyalar.
  - Şifreleme ve şifre çözme için listelere eklenen klasörlerde saklanan dosyalar.
  - ayrı uygulamalar tarafından oluşturulan dosyalar.

  Kaspersky Security Center ilkesinin uygulanmasıyla ilgili ayrıntılar için *Kaspersky Security Center Yönetici Kılavuzu*'na bakınız.

- **Çıkarılabilir sürücülerin şifrelenmesi**. Uygulamanın aynı eylemi tüm çıkarılabilir sürücülere uygulamak için kullanacağı varsayılan şifreleme kuralını belirtebilir veya tek tek çıkarılabilir sürücüler için şifreleme kuralları belirtebilirsiniz.

  Varsayılan şifreleme kuralı, tek tek çıkarılabilir sürücüler için oluşturulan şifreleme kuralından daha düşük önceliğe sahiptir. Belirtilen cihaz modelinin çıkarılabilir sürücüleri için oluşturulan şifreleme kuralları, belirtilen aygıt kimliğine sahip çıkarılabilir sürücüler için oluşturulan şifreleme kurallarından daha düşük önceliğe sahiptir.

  Çıkarılabilir sürücüdeki dosyalar için bir şifreleme kuralı seçmek amacıyla Kaspersky Endpoint Security, aygıt modeli ve kimliğinin bilinip bilinmediğini denetler. Ardından uygulama aşağıdaki işlemlerden birini gerçekleştirir:

  - Sadece aygıt modeli biliniyorsa uygulama, belirli aygıt modelinin çıkarılabilir sürücüleri için oluşturulan şifreleme kuralını (varsa) kullanır.
  - Sadece aygıt kimliği biliniyorsa uygulama, belirli aygıt kimliğine sahip çıkarılabilir sürücüler için oluşturulan şifreleme kuralını (varsa) kullanır.
  - Aygıt modeli ve kimliği biliniyorsa uygulama, belirli aygıt kimliğine sahip çıkarılabilir sürücüler için oluşturulan şifreleme kuralını (varsa) uygular. Böyle bir kural bulunmuyorsa ancak belirli aygıt modelindeki çıkarılabilir sürücüler için oluşturulmuş bir şifreleme kuralı bulunuyorsa uygulama, bu kuralı uygular. Belirli aygıt kimliği veya belirli aygıt modeli için herhangi bir şifreleme kuralı belirtilmemişse uygulama, varsayılan şifreleme kuralını uygular.
  - Ne aygıt modeli ne de aygıt kimliği biliniyorsa uygulama, varsayılan şifreleme kuralını kullanır.

  Uygulama, taşınabilir modda çıkarılabilir sürücü üzerinde kayıtlı bulunan şifreli verileri kullanarak bir çıkarılabilir sürücü hazırlamanıza olanak tanır. Taşınabilir modu etkinleştirdikten sonra şifreleme işlevi bulunmayan bir bilgisayara bağlı çıkarılabilir sürücülerdeki şifreli dosyalara erişebilirsiniz.

  Uygulama, Kaspersky Security Center ilkesi uygulandığında şifreleme kuralında belirtilen eylemi gerçekleştirir.

- **Şifrelenmiş dosyalara uygulama erişimi kurallarını yönetme**. Herhangi bir uygulama için, şifrelenmiş dosyalara erişimi engelleyen veya şifrelenmiş dosyalara, şifreleme uygulandığında elde edilen bir karakter dizisi olan şifreli metin şeklinde erişim imkanı tanıyan bir şifrelenmiş dosya erişim kuralı oluşturabilirsiniz.

- **Şifrelenmiş arşivler oluşturma**. Şifrelenmiş arşivler oluşturabilir ve bu arşivleri bir parola ile koruyabilirsiniz. Şifrelenmiş arşivlerin içeriğine sadece bu arşivlere erişimi korumak amacıyla kullandığınız parola girilerek erişilebilir. Bu arşivler, ağlar üzerinden veya çıkarılabilir sürücülerle güvenli bir şekilde iletilebilir.

- **Sabit sürücülerin şifrelenmesi**. Bir şifreleme teknolojisi seçebilirsiniz: Kaspersky Disk Encryption veya BitLocker Drive Encryption (bundan sonra "BitLocker" olarak ifade edilecektir).

BitLocker, Windows işletim sisteminin parçası olan bir teknolojidir. Bir bilgisayarda Güvenilir Platform Modülü (TPM) bulunuyorsa BitLocker, şifrelenmiş sabit sürücüye erişim sağlayan kurtarma anahtarlarını bu modülü kullanarak depolar. Bilgisayar başlatıldığında BitLocker, Güvenilir Platform Modülü'nden sabit sürücü şifreleme anahtarlarını ister ve sürücünün kilidini açar. Kurtarma anahtarlarına erişim için parola ve/veya PIN kodunun kullanımını yapılandırabilirsiniz.

Varsayılan sabit sürücü şifreleme kuralını belirtebilir ve şifreleme dışında tutulacak sabit sürücülerin bir listesini oluşturabilirsiniz. Kaspersky Security Center ilkesi uygulandıktan sonra Kaspersky Endpoint Security sabit sürücülerin şifrelenmesini sektör sektör gerçekleştirir. Uygulama, sabit sürücülerin tüm mantıksal bölmelerini eşzamanlı olarak şifreler. Kaspersky Security Center ilkesinin uygulanmasıyla ilgili ayrıntılar için *Kaspersky Security Center Yönetici Kılavuzu*'na bakınız.

Sistem sabit sürücüler şifrelendikten sonra bilgisayarın başlatıldığı bir sonraki seferde kullanıcı, sabit sürücülere erişim sağlanmadan ve işletim sistemi yüklenmeden önce Kimlik Doğrulama Aracısı kullanılarak kimlik doğrulamayı tamamlamalıdır. Bu, bilgisayara bağlanan belirteç veya akıllı kartın parolasının ya da Kimlik Doğrulama Aracısı hesap yönetimi görevlerini kullanarak yerel alan ağı yöneticisi tarafından oluşturulan Kimlik Doğrulama Aracısı hesabının kullanıcı adı ve parolasının girilmesini gerektirir. Bu hesaplar, kullanıcıların işletim sisteminde oturum açmak için kullandığı Microsoft Windows hesaplarını temel alır. Kimlik Doğrulama Aracısı hesaplarını yönetebilir ve Kimlik Doğrulama Aracısı hesabının kullanıcı adı ve parolasını kullanarak işletim sisteminde otomatik olarak oturum açmanızı sağlayan Tek Oturum Açma (SSO) teknolojisini kullanabilirsiniz.

Bilgisayarı yedekleyip bilgisayar verilerini şifrelerseniz ve ardından bilgisayarın yedek kopyasını geri yükler ve bilgisayar verilerini yeniden şifrelerseniz Kaspersky Endpoint Security, Kimlik Doğrulama Aracısı hesaplarının kopyalarını oluşturur. Hesapların kopyalarını kaldırmak için klmover yardımcı programını `dupfix` anahtarı ile kullanmanız gerekir. Klmover yardımcı programı, Kaspersky Security Center yapısının içinde yer almaktadır. *Kaspersky Security Center Yönetici Kılavuzu*'ndan programın kullanımıyla ilgili daha fazla bilgi alabilirsiniz.

Uygulama sürümü Kaspersky Endpoint Security 10 Service Pack 2 for Windows'a yükseltildiğinde, Kimlik Doğrulama Aracısı hesapları kaydedilmez.

Şifrelenmiş sabit sürücülere erişim sadece Kaspersky Endpoint Security'nin sabit sürücü şifreleme işlevinin yüklü olduğu bilgisayarlardan mümkündür. Bu önlem, şirketin yerel alan ağı dışında bir erişim girişiminde bulunulduğunda şifrelenmiş sabit sürücüden veri sızıntısı riskini en aza indirir.

Sabit sürücüleri ve çıkarılabilir sürücüleri şifrelemek için **Sadece kullanılan disk alanını şifrele** işlevini kullanabilirsiniz. Bu işlevi sadece daha önceden kullanılmamış yeni aygıtlar için kullanmanız önerilir. Şifrelemeyi zaten kullanımda olan bir sürücüye uyguluyorsanız, tüm sürücüyü şifrelemeniz önerilir. Böylece, hala kurtarılabilir bilgi içeren silinmiş veriler dahil tüm veriler korunur.

Şifrelemeye başlamadan önce Kaspersky Endpoint Security, dosya sistemi sektörlerinin haritasını elde eder. İlk şifreleme dalgası, şifrelemenin başlatıldığı anda dosyalar tarafından kullanılmakta olan sektörleri kapsar. İkinci şifreleme dalgası, şifreleme başladıktan sonra yazılan sektörleri kapsar. Şifreleme tamamlandıktan sonra veri içeren tüm sektörler şifrelenir.

Şifreleme tamamlandıktan ve kullanıcı dosyayı sildikten sonra, silinen verilerin kaydedildiği sektörler dosya sistemi düzeyinde yeni verileri kaydetmek için kullanılabilir hale gelir ama şifreli olarak kalır. Böylece, **Sadece kullanılan disk alanını şifrele** işlevi etkin olan bilgisayarda düzenli şifrelemenin başlatılması sırasında yeni dosyalar yeni bir aygıta yazılırken, bir süre sonra tüm kesimler şifrelenir.

Dosyaların şifresini çözmek için gereken veriler, şifreleme zamanında bilgisayarı kontrol eden Kaspersky Security Center Yönetim Sunucusu tarafından sağlanır. Şifrelenmiş dosyaların bulunduğu bilgisayar herhangi bir nedenle kendisini başka bir Yönetim Sunucusunun denetimi altında bulursa ve şifrelenmiş verilere tek bir sefer erişim sağlanmadıysa aşağıdaki şekillerde erişim sağlanabilir:

- LAN yöneticisinden şifrelenmiş nesnelere erişim talep etme;

- Geri Yükleme Yardımcı Programını kullanarak şifreli aygıtlara erişimi geri yükleme
- Şifreleme sırasında bilgisayarı denetleyen Kaspersky Security Center Yönetim Sunucusu'nun yapılandırmasını yedek bir kopyadan geri yükleyin ve bu yapılandırmayı, şifrelenmiş nesnelerin bulunduğu bilgisayarı denetleyen Yönetim Sunucusu'nda kullanın.

Uygulama, şifreleme sırasında servis dosyaları oluşturur. Bunları kaydetmek için sabit sürücüdeki parçalanmamış kullanılabilir alanın yaklaşık yüzde iki ila yüzde üçü gerekir. Sabit sürücüde parçalanmamış yeterli kullanılabilir alan yoksa yeterli alan açılana kadar şifreleme başlamaz.

Kaspersky Endpoint Security ile Kaspersky Anti-Virus for UEFI arasında şifreleme işlevi uyumluluğu desteklenmemektedir. Kaspersky Anti-Virus for UEFI'nin yüklendiği bilgisayarların sabit sürücülerinin şifrelenmesi, Kaspersky Anti-Virus for UEFI'yi kullanılamaz hale getirir.

Şifreleme işlevi sınırlamaları

Şifrelenmiş sabit sürücülerin mevcut bölümlerini biçimlendirmenin yanı sıra şifrelenmiş sabit sürücülerde yeni bölümler oluşturmak, bu sabit sürücülerde veri kaybına neden olabilir.

Kaspersky Disk Encryption teknolojisini kullanan sabit sürücü şifrelemesi, donanım ve yazılım gereksinimlerini karşılamayan sabit sürücüler için kullanılamaz.

Kaspersky Endpoint Security aşağıdaki yapılandırmaları desteklemez:

- Önyükleme yükleyicisi işletim sisteminden farklı bir sürücüde bulunmaktadır.
- Sistem UEFI 32 standardının gömülü yazılımını içermektedir.
- Intel® Hızlı Başlatma Teknolojisi devre dışı bırakıldığında bile hazırda bekleme bölümüne sahip Intel® Hızlı Başlatma Teknolojisi ve sürücüler.
- Dört genişletilmiş bölümden daha fazla MBR biçiminde sürücüler.
- Bir sistem dışı dosyada bulunan takas dosyası.
- Aynı anda yüklenen birkaç işletim sistemini içeren çoklu önyükleme sistemi.
- Dinamik bölümler (sadece birincil bölümler desteklenmektedir).
- %2'den daha az parçalanmamış disk alanı içeren sürücüler.
- 512 bayt veya 512 bayta öykünen 4096 bayttan farklı bir kesim boyutu içeren sürücüler.
- Karma sürücüler.

Şifreleme algoritmasını değiştirme

Kaspersky Endpoint Security tarafından veri şifreleme için kullanılan şifreleme algoritması, dağıtım kitinde yer alan şifreleme kitaplıklarına bağlıdır.

Şifreleme algoritmasını değiştirmek için:

1. Şifreleme algoritmasını değiştirmeye başlamadan önce Kaspersky Endpoint Security'nin şifrelediği nesnelerin şifresini çözün.

   Şifreleme algoritmasını değiştirdikten sonra, önceden şifrelenen nesneler kullanılamaz duruma gelir.

2. Kaspersky Endpoint Security'yi Kaldır.

3. Dağıtım kitindeki Kaspersky Endpoint Security Yükle farklı bit sayıları için şifreleme kitaplıklarını içerir.

Tek Oturum Açma (SSO) teknolojisini kullanma

Tek Oturum Açma (SSO) teknolojisi, üçüncü taraf hesap kimlik bilgileri sağlayıcıları ile uyumsuzdur.

Tek Oturum Açma (SSO) teknolojisini etkinleştirmek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, Tek Oturum Açma (SSO) teknolojisini etkinleştirmek istediğiniz yönetim grubunun adının bulunduğu klasörü açın.

3. Çalışma alanında, **İlkeler** sekmesini seçin.

4. Gereken ilkeyi seçin.

5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:

   - İlkenin içerik menüsünde **Özellikler**'i seçin.
   - Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.

6. **Veri Şifreleme** bölümünde, **Ortak şifreleme ayarları** alt bölümünü seçin.

7. **Ortak şifreleme ayarları** alt bölümünde, **Parola ayarları** bölümünde **Yapılandır** düğmesine tıklayın.

   Şifreleme parolası ayarları penceresinin **Kimlik Doğrulama Aracısı** sekmesi açılır.

8. **Tek Oturum Açma (SSO) teknolojisi kullan** onay kutusunu işaretleyin.

9. **Tamam**'a tıklayın.

10. Değişikliklerinizi kaydetmek için **Özellikler: <İlke adı>** penceresinde **Tamam**'a tıklayın.

11. İlkeyi uygulayın.

    Kaspersky Security Center ilkesinin uygulanmasıyla ilgili ayrıntılar için *Kaspersky Security Center Yönetici Kılavuzu*'na bakınız.

Dosya şifreleme ile ilgili özel hususlar

Dosya şifreleme işlevini kullanırken aşağıdaki noktaları göz önünde bulundurun:

- Belirli bir grup yönetilen bilgisayar için kaldırılabilir sürücü şifreleme ön ayarlarına sahip Kaspersky Security Center ilkesi oluşturulur. Bu nedenle çıkarılabilir sürücülerde şifreleme / şifre çözme için yapılandırılan Kaspersky Security Center ilkesinin uygulanmasının sonucu, çıkarılabilir sürücünün bağlı olduğu bilgisayara bağlıdır.

- Kaspersky Endpoint Security, çıkarılabilir sürücülerde saklanan salt okunur durumdaki dosyaları şifrelemez / şifresini çözmez.

- Kaspersky Endpoint Security önceden tanımlanmış klasörlerdeki dosyaları sadece işletim sisteminin yerel kullanıcı profilleri için şifreler / şifresini çözer. Kaspersky Endpoint Security, gezici kullanıcı profilleri, zorunlu kullanıcı profilleri, geçici kullanıcı profilleri ve yeniden yönlendirilen klasörlerin önceden tanımlanmış klasörlerindeki dosyaları şifrelemez / şifresini çözmez. Kaspersky tarafından şifreleme için önerilen standart klasörler listesi aşağıdaki klasörleri içerir:

  - Belgelerim
  - Sık Kullanılanlar
  - Çerezler
  - Masaüstü
  - Geçici Internet Explorer dosyaları
  - Geçici dosyalar
  - Outlook dosyaları

- Kaspersky Endpoint Security, değiştirilmesi işletim sistemine ve yüklü uygulamalara zarar verebilecek dosyaları şifrelemez. Örneğin iç içe geçmiş klasörlerin olduğu aşağıdaki dosya ve klasörler şifrelemeden istisnalar listesindedir:

  - %WINDIR%.
  - %PROGRAMFILES%, %PROGRAMFILES(X86)%.
  - Windows kayıt defteri dosyaları.

  Şifreleme istisnaları listesi görüntülenemez veya düzenlenemez. Şifreleme istisnaları listesindeki dosyalar ve klasörler şifreleme listesine eklenebilir ancak dosya şifreleme görevi sırasında şifrelenmez.

- Aşağıdaki aygıt türleri çıkarılabilir sürücüler olarak desteklenmektedir:

  - USB veri yolundan bağlanan veri ortamları
  - USB ve FireWire veri yollarından bağlanan sabit sürücüler
  - USB ve FireWire veri yollarından bağlanan SSD sürücüler

Yerel bilgisayar sürücülerindeki dosyaları şifreleme

Kaspersky Endpoint Security, iş istasyonları için Microsoft Windows kurulu bir bilgisayara yüklenmişse yerel bilgisayar sürücülerindeki dosyaları şifreleme seçeneği mevcuttur. Kaspersky Endpoint Security, dosya sunucuları için Microsoft Windows kurulu bir bilgisayara yüklenmişse yerel bilgisayar sürücülerindeki dosyaları şifreleme seçeneği mevcut değildir.

Bu bölümde, yerel bilgisayar sürücülerindeki dosyaları şifreleme ele alınmakta ve Kaspersky Endpoint Security ve Kaspersky Endpoint Security Console Eklentisi ile yerel bilgisayar sürücülerindeki dosyaları şifrelemenin nasıl yapıldığı ve yapılandırıldığı hakkında bilgi sağlanmaktadır.

Yerel bilgisayar sürücülerindeki dosyaları şifreleme

Kaspersky Endpoint Security, içeriği OneDrive bulut depolama alanında bulunan dosyaları şifrelemez ve bu dosyalar şifre çözme kuralına eklenmezse şifrelenmiş dosyaların OneDrive bulut depolama alanına kopyalanmasını engeller.

Kaspersky Endpoint Security, dosyaların FAT32 ve NTFS dosya sistemlerinde şifrelemesini destekler. Bilgisayara, desteklenmeyen bir dosya sistemine sahip çıkarılabilir sürücü bağlandıysa bu çıkarılabilir sürücünün şifreleme görevi bir hatayla sonlanır ve Kaspersky Endpoint Security çıkarılabilir sürücüye salt okunur durumunu atar.

Yerel sürücülerdeki dosyaları şifrelemek için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen cihazlar** klasöründe, ilgili istemci bilgisayarların ait olduğu yönetim grubu adının bulunduğu klasörü açın.
3. Çalışma alanında, **İlkeler** sekmesini seçin.
4. Gereken ilkeyi seçin.
5. İlke özellikleri penceresini açmak için çift tıklayın.
6. **Veri şifreleme** bölümünde, **Dosya Düzeyinde Şifreleme** seçeneğini belirleyin.
7. Pencerenin sağ kısmında, **Şifreleme** sekmesini seçin.
8. **Şifreleme modu** açılır listesinde, **Varsayılan kurallar** öğesini seçin.
9. **Şifreleme** sekmesinde, **Ekle** düğmesine tıklayın ve açılır listeden aşağıdaki öğelerden birini seçin:
   a. Kaspersky uzmanları tarafından bir şifreleme kuralına önerilen yerel kullanıcı profillerindeki klasörlerden dosya eklemek için **Ön tanımlı klasörler** öğesini seçin.

      Ön tanımlı klasörleri seçin penceresi açılır.

b. Şifreleme kuralının elle girilen klasör yolunu eklemek için **Özel klasör** öğesini seçin.

Özel klasör ekleyin penceresi açılır.

c. Bir şifreleme kuralına dosya uzantılarını eklemek için **Uzantıya göre dosyalar** öğesini seçin. Kaspersky Endpoint Security bilgisayarın tüm yerel sürücülerindeki belirtilen uzantılara sahip dosyaları şifreler.

Dosya uzantıları listesi ekleyin / düzenleyin penceresi açılır.

d. Bir şifreleme kuralına dosya uzantıları grubunu eklemek için **Uzantı gruplarına göre dosyalar** öğesini seçin. Kaspersky Endpoint Security, bilgisayarın tüm yerel sürücülerindeki uzantı gruplarında belirtilen uzantılara sahip dosyaları şifreler.

Dosya uzantıları grubunu seçin penceresi açılır.

10. Değişikliklerinizi kaydetmek için **Özellikler: <İlke adı>** penceresinde **Tamam**'a tıklayın.

11. İlkeyi uygulayın.

Kaspersky Security Center ilkesinin uygulanmasıyla ilgili ayrıntılar için Kaspersky Security Center Yardım içeriğine bakın.

İlke uygulanır uygulanmaz Kaspersky Endpoint Security, şifreleme kuralında yer alan ve şifre çözme kuralında yer almayan dosyaları şifreler.

Aynı dosya şifreleme kuralına ve şifre çözme kuralına eklendiyse Kaspersky Endpoint Security, şifrelenmediyse bu dosyayı şifrelemez ve şifrelendiyse dosyanın şifresini çözer.

Kaspersky Endpoint Security, özellikleri (dosya yolu / dosya adı / dosya uzantısı) değişikliğin ardından hala şifreleme kuralını karşılayan şifrelenmemiş dosyaları şifreler.

Kaspersky Endpoint Security, kapatılana kadar açık dosyaların şifrelemesini erteler.

Kullanıcı tarafından özellikleri şifreleme kuralı kriterlerini karşılayan yeni bir dosya oluşturulduğunda Kaspersky Endpoint Security, açılır açılmaz dosyayı şifreler.

Şifrelenmiş bir dosyayı yerel sürücüdeki başka bir klasöre taşırsanız bu klasörün şifreleme kuralında yer alıp almadığına bakılmaksızın dosya şifreli olarak kalır.

Uygulamalar için şifreli dosyaya erişim kuralları oluşturma

Uygulamalar için şifreli dosyaya erişim kuralları oluşturmak amacıyla:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, uygulamalar için şifreli dosyaya erişim kurallarını yapılandırmak istediğiniz ilgili yönetim grubunun adının bulunduğu klasörü açın.

3. Çalışma alanında, **İlkeler** sekmesini seçin.

4. Gereken ilkeyi seçin.

5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:

- İlkenin içerik menüsünde **Özellikler**'i seçin.

- Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.

6. **Veri şifreleme** bölümünde, **Dosya ve klasörlerin şifrelenmesi** alt bölümünü seçin.

7. **Şifreleme modu** açılır listesinde, **Varsayılan kurallar** öğesini seçin.

   Erişim kuralları sadece **Varsayılan kurallar** modundayken uygulanır. **Varsayılan kurallar** modunda erişim kurallarını uyguladıktan sonra **Değiştirmeden bırak** moduna geçerseniz Kaspersky Endpoint Security tüm erişim kurallarını gözardı eder. Tüm uygulamaların tüm şifreli dosyalara erişimi olacaktır.

8. Pencerenin sağ kısmında, **Uygulamalar için kurallar** sekmesini seçin.

9. Uygulamaları sadece Kaspersky Security Center listesinden seçmek isterseniz, **Ekle** düğmesine tıklayın ve açılır listeden **Kaspersky Security Center listesinden uygulamalar** öğesini seçin.

   Kaspersky Security Center listesinden uygulamaları ekle penceresi açılır.

   Aşağıdakileri uygulayın:

   a. Tablodaki uygulamalar listesini daraltmak için filtreler belirtin. Bunu yapmak için **Uygulama**, **Satıcı** ve **Eklendiği dönem** parametrelerinin ve **Grup** bölümündeki bütün parametrelerin değerlerini belirtin.

   b. **Yenile** düğmesine tıklayın.

      Tabloda, uygulanan filtrelerle eşleşen uygulamalar listelenir.

   c. **Uygulamalar** sütununda, şifreli dosya erişim kurallarını oluşturmak istediğiniz uygulamaların karşısındaki onay kutularını işaretleyin.

   d. **Uygulamalar için kural** açılır listesinde, şifreli dosyalara uygulanacak erişim kurallarını belirleyecek olan kuralı seçin.

   e. **Daha önce seçilen uygulamalar için eylemler** açılır listesinden, bu uygulamalar için daha önceden oluşturulan şifreli dosya erişim kurallarına Kaspersky Endpoint Security tarafından uygulanacak eylemi seçin.

   f. **Tamam**'a tıklayın.

   Uygulamalar için şifrelenen dosya erişim kurallarının ayrıntıları, **Uygulamalar için kurallar** sekmesindeki tabloda görülür.

10. Uygulamaları elle seçmek isterseniz **Ekle** düğmesine tıklayın ve açılır listeden **Özel uygulamalar** öğesini seçin.

    Uygulamaların yürütülebilir dosya adları listesini ekle / düzenle penceresi açılır.

    Aşağıdakileri uygulayın:

    a. Giriş alanında, uygulamaların yürütülebilir dosyalarının adlarını veya adlarının listesini uzantılarıyla birlikte yazın.

       Ayrıca **Kaspersky Security Center listesinden ekle** düğmesine tıklayarak Kaspersky Security Center listesinden uygulamaların yürütülebilir dosyalarının adlarını da ekleyebilirsiniz.

    b. Gerekirse **Açıklama** alanına, uygulamalar listesinin bir açıklamasını girin.

    c. **Uygulamalar için kural** açılır listesinde, şifreli dosyalara uygulanacak erişim kurallarını belirleyecek olan kuralı seçin.

    d. **Tamam**'a tıklayın.

Uygulamalar için şifrelenen dosya erişim kurallarının ayrıntıları, **Uygulamalar için kurallar** sekmesindeki tabloda görülür.

11. Değişiklikleri kaydetmek için **Tamam** düğmesine tıklayın.

Belirli uygulamaların oluşturduğu veya değiştirdiği dosyaları şifreleme

Kaspersky Endpoint Security'nin kuralda belirtilen uygulamalar tarafından oluşturulan veya değiştirilen bütün dosyaları şifreleyeceği bir kural oluşturabilirsiniz.

Şifreleme kuralı uygulanmadan önce belirtilen uygulamalar tarafından oluşturulan dosyalar şifrelenmeyecektir.

Belirli uygulamalar tarafından oluşturulan veya değiştirilen dosyaların şifrelenmesini yapılandırmak için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, belirli uygulamalar tarafından oluşturulan dosyaların şifrelenmesini yapılandırmak istediğiniz yönetim grubunun adının bulunduğu klasörü açın.
3. Çalışma alanında, **İlkeler** sekmesini seçin.
4. Gereken ilkeyi seçin.
5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:
   - İlkenin içerik menüsünde **Özellikler**'i seçin.
   - Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.
6. **Veri şifreleme** bölümünde, **Dosya ve klasörlerin şifrelenmesi** alt bölümünü seçin.
7. **Şifreleme modu** açılır listesinde, **Varsayılan kurallar** öğesini seçin.

   Şifreleme kuralları yalnızca **Varsayılan kurallar** modundayken uygulanır. **Varsayılan kurallar** modunda şifreleme kurallarını uyguladıktan sonra **Değiştirmeden bırak** moduna geçerseniz Kaspersky Endpoint Security tüm şifreleme kurallarını gözardı eder. Önceden şifrelenmiş dosyalar şifrelenmiş olarak kalır.

8. Pencerenin sağ kısmında, **Uygulamalar için kurallar** sekmesini seçin.
9. Uygulamaları sadece Kaspersky Security Center listesinden seçmek isterseniz, **Ekle** düğmesine tıklayın ve açılır listeden **Kaspersky Security Center listesinden uygulamalar** öğesini seçin.

   Kaspersky Security Center listesinden uygulamaları ekle penceresi açılır.

   Aşağıdakileri uygulayın:

   a. Tablodaki uygulamalar listesini daraltmak için filtreler belirtin. Bunu yapmak için **Uygulama**, **Satıcı** ve **Eklendiği dönem** parametrelerinin ve **Grup** bölümündeki bütün parametrelerin değerlerini belirtin.

   b. **Yenile** düğmesine tıklayın.

      Tabloda, uygulanan filtrelerle eşleşen uygulamalar listelenir.

c. **Uygulama** sütununda, oluşturduğu dosyalar şifrelenecek olan uygulamaların karşısındaki onay kutularını seçin.

d. **Uygulamalar için kural** açılır listesinden **Tüm oluşturulan dosyaları şifrele** seçeneğini seçin.

e. **Daha önce seçilen uygulamalar için eylemler** açılır listesinden, bu uygulamalar için daha önceden oluşturulan dosya şifreleme kurallarına Kaspersky Endpoint Security tarafından uygulanacak eylemi seçin.

f. **Tamam**'a tıklayın.

Seçilen uygulamalar tarafından oluşturulan veya değiştirilen dosyalar için şifreleme kuralı hakkında bilgi, **Uygulamalar** sekmesindeki tabloda görülür.

10. Uygulamaları elle seçmek isterseniz **Ekle** düğmesine tıklayın ve açılır listeden **Özel uygulamalar** öğesini seçin.

Uygulamaların yürütülebilir dosya adları listesini ekle / düzenle penceresi açılır.

Aşağıdakileri uygulayın:

a. Giriş alanında, uygulamaların yürütülebilir dosyalarının adlarını veya adlarının listesini uzantılarıyla birlikte yazın.

Ayrıca **Kaspersky Security Center listesinden ekle** düğmesine tıklayarak Kaspersky Security Center listesinden uygulamaların yürütülebilir dosyalarının adlarını da ekleyebilirsiniz.

b. Gerekirse **Açıklama** alanına, uygulamalar listesinin bir açıklamasını girin.

c. **Uygulamalar için kural** açılır listesinden **Tüm oluşturulan dosyaları şifrele** seçeneğini seçin.

d. **Tamam**'a tıklayın.

Seçilen uygulamalar tarafından oluşturulan veya değiştirilen dosyalar için şifreleme kuralı hakkında bilgi, **Uygulamalar** sekmesindeki tabloda görülür.

11. Değişiklikleri kaydetmek için **Tamam** düğmesine tıklayın.

Şifre çözme kuralı oluşturma

Bir şifre çözme kuralı oluşturmak için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen cihazlar** klasöründe, ilgili istemci bilgisayarların ait olduğu yönetim grubu adının bulunduğu klasörü açın.
3. Çalışma alanında, **İlkeler** sekmesini seçin.
4. Gereken ilkeyi seçin.
5. İlke özellikleri penceresini açmak için çift tıklayın.
6. **Veri Şifreleme** bölümünde, **Dosya Düzeyinde Şifreleme** seçeneğini belirleyin.
7. Pencerenin sağ kısmında, **Şifre çözme** sekmesini seçin.
8. **Şifreleme modu** açılır listesinde, **Varsayılan kurallar** öğesini seçin.
9. **Şifre çözme** sekmesinde, **Ekle** düğmesine tıklayın ve açılır listeden aşağıdaki öğelerden birini seçin:

a. Kaspersky uzmanları tarafından önerilen yerel kullanıcı profillerindeki klasörlerden bir şifre çözme kuralına dosya eklemek için **Ön tanımlı klasörler** öğesini seçin.

Ön tanımlı klasörleri seçin penceresi açılır.

b. Şifre çözme kuralının elle girilen klasör yolunu eklemek için **Özel klasör** öğesini seçin.

Özel klasör ekleyin penceresi açılır.

c. Bir şifre çözme kuralına dosya uzantılarını eklemek için **Uzantıya göre dosyalar** öğesini seçin. Kaspersky Endpoint Security bilgisayarın tüm yerel sürücülerindeki belirtilen uzantılara sahip dosyaları şifrelemez.

Dosya uzantıları listesi ekleyin / düzenleyin penceresi açılır.

d. Bir şifre çözme kuralına dosya uzantıları gruplarını eklemek için **Uzantı gruplarına göre dosyalar** öğesini seçin. Kaspersky Endpoint Security, bilgisayarların tüm yerel sürücülerindeki uzantı gruplarında belirtilen uzantılara sahip dosyaları şifrelemez.

Dosya uzantıları grubunu seçin penceresi açılır.

10. Değişikliklerinizi kaydetmek için **Özellikler: <İlke adı>** penceresinde **Tamam**'a tıklayın.

11. İlkeyi uygulayın.

Kaspersky Security Center ilkesinin uygulanmasıyla ilgili ayrıntılar için Kaspersky Security Center Yardım içeriğine bakın.

Aynı dosya şifreleme kuralına ve şifre çözme kuralına eklendiyse Kaspersky Endpoint Security, şifrelenmediyse bu dosyayı şifrelemez ve şifrelendiyse dosyanın şifresini çözer.

Yerel bilgisayar sürücülerindeki dosyaların şifresini çözme

Yerel sürücülerdeki dosyaların şifresini çözmek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, yerel sürücülerdeki dosyaların şifrelerinin çözülmesini yapılandırmak istediğiniz yönetim grubunun adının bulunduğu klasörü açın.

3. Çalışma alanında, **İlkeler** sekmesini seçin.

4. Gereken ilkeyi seçin.

5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:

   - İlkenin içerik menüsünde **Özellikler**'i seçin.

   - Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.

6. **Veri Şifreleme** bölümünde, **Dosya ve klasörlerin şifrelenmesi** alt bölümünü seçin.

7. Pencerenin sağ kısmında, **Şifreleme** sekmesini seçin.

8. Şifresini çözmek istediğiniz dosya ve klasörleri şifreleme listesinden kaldırın. Bunun için dosyaları seçin ve **Kaldır** düğmesinin içerik menüsündeki **Kuralı silin ve dosyaların şifresini çözün** öğesini seçin.

Şifreleme listesinden bir seferde birden fazla öğe silebilirsiniz. Bunun için **CTRL** tuşunu basılı tutarak ihtiyacınız olan dosyaları sol tıklama ile seçin ve **Kaldır** düğmesinin içerik menüsündeki **Kuralı silin ve dosyaların şifresini çözün** öğesini seçin.

Şifreleme listesinden kaldırılan dosya ve klasörler otomatik olarak şifre çözme listesine eklenir.

9. Dosya şifre çözme listesi oluşturma.
10. Değişikliklerinizi kaydetmek için **Özellikler: <İlke adı>** penceresinde **Tamam**'a tıklayın.
11. İlkeyi uygulayın.

Kaspersky Security Center ilkesinin uygulanmasıyla ilgili ayrıntılar için *Kaspersky Security Center Yönetici Kılavuzu*'na bakınız.

İlke uygulanır uygulanmaz Kaspersky Endpoint Security, şifre çözme listesine eklenen şifreli dosyaların şifresini çözer.

Kaspersky Endpoint Security, parametreleri (dosya yolu / dosya adı / dosya uzantısı) şifre çözme listesine eklenen nesnelerin parametreleriyle eşleşecek şekilde değişirse şifrelenen dosyaların şifresini çözer.

Kaspersky Endpoint Security, kapatılana kadar açık dosyaların şifresinin çözülmesini erteler.

Şifrelenmiş paketler oluşturma

Kaspersky Endpoint Security, şifrelenmiş bir paket oluşturduğunda dosyaları sıkıştırmaz.

Şifrelenmiş bir paket oluşturmak için:

1. Kaspersky Endpoint Security yüklenmiş ve şifreleme işlevi etkinleştirilmiş bir bilgisayarda, şifrelenmiş bir pakete eklemek istediğiniz dosyaları ve/veya klasörleri seçmek için herhangi bir dosya yöneticisini kullanın. İçerik menüsünü açmak için sağ tıklayın.
2. İçerik menüsünde, **Şifrelenmiş pakete ekle**'yi seçin.

   Standart Microsoft Windows **Şifrelenmiş paketi kaydetmek için yolu seçin** iletişim kutusu açılır.
3. Standart Microsoft Windows **Şifrelenmiş paketi kaydetmek için yolu seçin** iletişim kutusunda, şifrelenmiş paketi kaydetmek için çıkarılabilir sürücüde bir hedef seçin. **Kaydet** düğmesine tıklayın.

   Şifrelenmiş pakete ekle penceresi açılır.
4. **Şifrelenmiş pakete ekle** penceresinde bir parola yazın ve doğrulayın.
5. **Oluştur** düğmesine tıklayın.

   Şifrelenmiş paket oluşturma işlemi başlar. İşlem bittiğinde, çıkarılabilir sürücüde seçilen hedef klasörde kendiliğinden açılan, parola korumalı şifrelenmiş bir paket oluşturulur.

Şifrelenmiş bir paketin oluşturulmasını iptal ederseniz Kaspersky Endpoint Security aşağıdaki işlemleri yapar:

1. Dosyaları pakete kopyalama işlemlerini sonlandırır ve varsa bütün devam eden paket şifreleme işlemlerini sona erdirir.
2. Paket oluşturma ve şifreleme sırasında oluşturulan bütün geçici dosyaları ve şifrelenmiş paketin dosyasını kaldırır.
3. Kullanıcıya, şifrelenmiş paket oluşturma işleminin zorla sonlandırıldığını bildirir.

Şifrelenmiş paketleri çıkarma

Şifrelenmiş bir paketi çıkarmak için:

1. Herhangi bir dosya yöneticisinde şifrelenmiş bir paket seçin. Paket Açma Sihirbazını başlatmak için tıklayın.

   Parola gir penceresi açılır.

2. Şifrelenmiş paketi koruyan parolayı girin.

3. **Parolayı gir** penceresinde **Tamam**'a tıklayın.

   Parola giriş başarılı olursa standart Microsoft Windows **Gözat** iletişim kutusu açılır.

4. Standart Microsoft Windows **Gözat** iletişim kutusunda şifrelenmiş paketin çıkarılacağı hedef klasörü seçin ve **Tamam**'a tıklayın.

   Şifrelenmiş paketin hedef klasöre çıkarılması işlemi başlar.

Şifrelenmiş paket belirlenen hedef klasöre daha önce çıkarılmışsa şifrelenmiş paketteki dosyalar klasördeki mevcut dosyaların üstüne yazılır.

Şifrelenmiş bir paketin çıkarılmasını iptal ederseniz Kaspersky Endpoint Security aşağıdaki işlemleri yapar:

1. Paketin şifresini çözme işlemini durdurur ve devam eden işlemler varsa şifrelenmiş paketten dosyaların kopyalanması işlemlerinin tümünü sonlandırır.

2. Şifre çözme ve şifrelenmiş paketin çıkarılması sırasında oluşturulan tüm geçici dosyalar ile birlikte şifrelenmiş paketten hedef klasöre kopyalanmış tüm dosyalar silinir.

3. Kullanıcıya, şifrelenmiş paket çıkarma işleminin zorla sonlandırıldığını bildirir.

Çıkarılabilir sürücülerin şifrelenmesi

Kaspersky Endpoint Security, İş istasyonları için Microsoft Windows'un kurulu olduğu bir bilgisayara yüklenmişse çıkarılabilir sürücülerin şifrelenmesi mümkündür. Kaspersky Endpoint Security, Dosya sunucuları için Microsoft Windows'un kurulu olduğu bir bilgisayara yüklenmişse çıkarılabilir sürücülerin şifrelenmesi kullanılamaz.

Bu bölümde, çıkarılabilir sürücülerin şifrelenmesi hakkında bilgi ve Kaspersky Endpoint Security'yi ve Kaspersky Endpoint Security yönetim eklentisini kullanarak çıkarılabilir sürücülerin şifrelenmesini yapılandırma ve gerçekleştirme talimatları bulunmaktadır.

Çıkarılabilir sürücülerin şifrelenmesini başlatma

Çıkarılabilir sürücüleri şifrelemek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, çıkarılabilir sürücülerin şifrelenmesini yapılandırmak istediğiniz yönetim grubunun adının bulunduğu klasörü açın.

3. Çalışma alanında, **İlkeler** sekmesini seçin.

4. Gereken ilkeyi seçin.

5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:

   - İlkenin içerik menüsünde **Özellikler**'i seçin.

   - Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.

6. **Veri Şifreleme** bölümünde, **Çıkarılabilir sürücülerin şifrelenmesi** alt bölümünü seçin.

7. **Şifreleme modu** açılır listesinde, seçilen yönetim grubundaki bilgisayarlara bağlanan tüm çıkarılabilir sürücülerde Kaspersky Endpoint Security tarafından gerçekleştirilecek varsayılan eylemi seçin:

   - **Çıkarılabilir sürücünün tamamını kriptola**. Bu öğe seçilirse çıkarılabilir sürücülerin belirtilen şifreleme ayarlarıyla Kaspersky Security Center ilkesini uygularken Kaspersky Endpoint Security, çıkarılabilir sürücülerin içeriğini sektör sektör şifreler. Sonuç olarak uygulama sade çıkarılabilir sürücülerde kayıtlı dosyaları şifrelemez aynı zamanda dosya adları ve klasör yapılarını içeren çıkarılabilir sürücülerin dosya sistemlerini de şifreler. Kaspersky Endpoint Security, zaten şifrelenmiş olan çıkarılabilir sürücüleri yeniden şifrelemez.

     Bu şifreleme senaryosu, Kaspersky Endpoint Security'nin sabit sürücü şifreleme işlevi ile etkinleştirilir.

   - **Tüm dosyaları şifrele**. Bu öğe seçilirse çıkarılabilir sürücüler için belirtilen şifreleme ayarlarıyla birlikte Kaspersky Security Center ilkesi uygulanırken Kaspersky Endpoint Security, çıkarılabilir sürücülerde depolanan tüm dosyaları şifreler. Kaspersky Endpoint Security zaten şifrelenmiş dosyaları tekrar şifrelemez. Uygulama, şifrelenmiş dosya ve klasör yapıları dahil olmak üzere çıkarılabilir sürücülerin dosya sistemlerini şifrelemez.

   - **Sadece yeni dosyaları şifrele**. Bu öğe seçilirse çıkarılabilir sürücülerin belirtilen şifreleme ayarları ile Kaspersky Security Center ilkesi uygulanırken Kaspersky Endpoint Security, sadece çıkarılabilir sürücülere eklenen dosyaları veya çıkarılabilir sürücülere kaydedilmiş ve Kaspersky Security Center ilkesi son uygulandığından bu yana değiştirilmiş olan dosyaları şifreler.

   - **Çıkarılabilir sürücünün tamamının kriptosunu çöz**. Bu öğe seçilirse çıkarılabilir sürücülerin belirtilen şifreleme ayarları ile Kaspersky Security Center ilkesi uygulanırken Kaspersky Endpoint Security, çıkarılabilir sürücülere kaydedilen tüm şifrelenmiş dosyaların ve daha önce şifrelenmişse çıkarılabilir sürücülerin dosya sistemlerinin şifresini çözer.

     Bu şifreleme senaryosu Kaspersky Endpoint Security'nin hem dosya şifreleme işlevi hem de sabit sürücü şifreleme işlevi ile mümkün olur.

   - **Değiştirmeden bırak** Bu öğe seçilirse çıkarılabilir sürücülerin belirtilen şifreleme ayarlarıyla Kaspersky Security Center ilkesini uygularken Kaspersky Endpoint Security, çıkarılabilir sürücülerdeki dosyaları şifrelemez veya şifrelerini çözmez.

8. İçeriğini şifrelemek istediğiniz çıkarılabilir sürücülerdeki dosyalar için şifreleme kuralları oluşturun.

9. İlkeyi uygulayın.

Kaspersky Security Center ilkesinin uygulanmasıyla ilgili ayrıntılar için *Kaspersky Security Center Yönetici Kılavuzu*'na bakınız.

İlke uygulanır uygulanmaz kullanıcı bir çıkarılabilir sürücü bağladığında veya bir çıkarılabilir sürücü zaten bağlı olduğunda Kaspersky Endpoint Security, kullanıcıya çıkarılabilir sürücünün bir şifreleme kuralına tabi olduğunu ve bu kurala göre çıkarılabilir sürücüde kayıtlı verilerin şifreleneceğini bildirir.

Çıkarılabilir sürücüdeki verilerin şifrelenmesi için *Değiştirmeden bırak* kuralı belirtilirse uygulama kullanıcıya herhangi bir bildirim göstermez.

Uygulama kullanıcıya şifreleme işleminin biraz zaman alabileceği uyarısında bulunur.

Uygulama, kullanıcıdan şifreleme işlemini onaylamasını ister ve aşağıdaki işlemleri gerçekleştirir:

- Kullanıcının şifrelemeye onay vermesi halinde ilke ayarlarına göre verileri şifreler.
- Kullanıcının şifrelemeyi reddetmesi halinde verileri şifrelemeden bırakır ve çıkarılabilir sürücü dosyalarına erişimi salt okunur olarak sınırlar.
- Kullanıcının şifreleme istemini gözardı etmesi, çıkarılabilir sürücü dosyalarına erişimi salt okunur olarak sınırlaması ve Kaspersky Security Center ilkesinin uygulandığı veya çıkarılabilir sürücünün bağlandığı bir sonraki seferde kullanıcıdan veri şifrelemeyi tekrar onaylamasını istemesi halinde verileri şifrelemeden bırakır.

Belirli yönetilen bilgisayar grubu için çıkarılabilir sürücülerde veri şifreleme ön ayarlarına sahip Kaspersky Security Center ilkesi oluşturulur. Bu nedenle çıkarılabilir sürücülerde veri şifrelemenin sonucu, çıkarılabilir sürücünün bağlandığı bilgisayara bağlıdır.

Kullanıcının veri şifreleme sırasında çıkarılabilir sürücünün güvenli kaldırılmasını başlatması durumunda Kaspersky Endpoint Security, veri şifreleme işlemini yarıda keser ve şifreleme işlemi tamamlanmadan çıkarılabilir sürücünün çıkarılabilmesine imkan tanır.

Bir çıkarılabilir sürücüde şifre çözme işleminin başarısız olması halinde Kaspersky Endpoint Security arabirimindeki **Veri şifreleme** raporuna bakın. Dosyalara erişim başka bir uygulama tarafından engellenmiş olabilir. bu durumda çıkarılabilir sürücüyü bilgisayardan çıkarıp tekrar bağlamayı deneyin.

Çıkarılabilir sürücülere şifreleme kuralı ekleme

Çıkarılabilir sürücülere şifreleme kuralı eklemek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, çıkarılabilir sürücü şifreleme kuralları eklemek istediğiniz yönetim grubunun adının bulunduğu klasörü açın.
3. Çalışma alanında, **İlkeler** sekmesini seçin.
4. Gereken ilkeyi seçin.
5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:
   - İlkenin içerik menüsünde **Özellikler**'i seçin.

- Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.

6. **Veri Şifreleme** bölümünde, **Çıkarılabilir sürücülerin şifrelenmesi** alt bölümünü seçin.
7. **Ekle** düğmesine sol tıklayın ve açılır listeden aşağıdaki öğelerden birini seçin:

   - Aygıt Denetimi bileşeninin güvenilir aygıtlar listesindeki çıkarılabilir sürücüler için şifreleme kuralları eklemek isterseniz **Bu ilkenin güvenilir aygıtlar listesinden** seçeneğini seçin.

     Güvenilir aygıtlar listesinden aygıt ekle penceresi açılır.

   - Kaspersky Security Center listesindeki çıkarılabilir sürücülere şifreleme kuralları eklemek isterseniz **Kaspersky Security Center aygıt listesinden** seçeneğini seçin.

     Kaspersky Security Center listesinden aygıtları ekle penceresi açılır.

8. Önceki adımda **Kaspersky Security Center aygıt listesinden** seçeneğini seçtiyseniz aygıtların tablodan görüntülenmesi için filtreleri belirtin. Bunun için:

   a. Aşağıdaki parametrelerin değerlerini belirtin: **Tabloda şunların tanımlandığı aygıtları göster**, **Aygıt türü**, **Ad**, **Bilgisayar** ve **Kaspersky Disk Encryption**.

   b. **Yenile** düğmesine tıklayın.

9. **Aygıt türü** sütununda, şifreleme kuralları oluşturmak istediğiniz çıkarılabilir sürücülerin adlarının karşısındaki onay kutularını işaretleyin.
10. **Seçili cihazlar için şifreleme modu** açılır listesinde, Kaspersky Endpoint Security tarafından seçilen çıkarılabilir sürücülerde kayıtlı dosyalara uygulanacak eylemi seçin.
11. Kaspersky Endpoint Security'nin şifreleme öncesinde çıkarılabilir sürücüleri hazırlamasını ve kayıtlı şifreli dosyaları taşınabilir modda kullanılabilir hale getirmesini istiyorsanız **Taşınabilir mod** seçeneğini seçin.

    Taşınabilir mod, şifreleme işlevi bulunmayan bilgisayarlara bağlı çıkarılabilir sürücülerde kayıtlı şifreli dosyaları kullanmanıza imkan tanır.
12. Kaspersky Endpoint Security'nin sadece dosyalar tarafından kullanılan disk sektörlerini şifrelemesini istiyorsanız **Sadece kullanılan disk alanını şifrele** onay kutusunu seçin.

    Şifrelemeyi zaten kullanımda olan bir sürücüye uyguluyorsanız, tüm sürücünün şifrelenmesi önerilir. Böylece, hala kurtarılabilir bilgi içeren silinmiş veriler dahil tüm veriler korunur. **Sadece kullanılan disk alanını şifrele** işlevi, daha önce kullanılmamış yeni sürücüler için önerilir.

    Bir aygıt daha önce **Sadece kullanılan disk alanını şifrele** işlevini kullanarak şifrelendiyse **Çıkarılabilir sürücünün tamamını kriptola** modunda bir ilke uygulandıktan sonra, dosyalar tarafından kullanılmayan sektörler yine de şifrelenmez.
13. **Daha önce seçilmiş aygıtlar için eylemler** açılır listesinden, çıkarılabilir sürücüler için daha önceden oluşturulan şifreleme kurallarına Kaspersky Endpoint Security tarafından uygulanacak eylemi seçin:

    - Çıkarılabilir sürücü için oluşturulan şifreleme kuralının değişmemesini istiyorsanız **Atla** seçeneğini seçin.
    - Bir çıkarılabilir sürücü için daha önceden oluşturulan şifreleme kuralının yeni bir kuralla değiştirilmesini isterseniz **Güncelle**'yi seçin.
14. **Tamam**'a tıklayın.

    Oluşturulan şifreleme kurallarının parametrelerini içeren satırlar **Özel kurallar** tablosunda görülür.

15. Değişiklikleri kaydetmek için **Tamam** düğmesine tıklayın.

    Eklenen çıkarılabilir sürücü şifreleme kuralları, Kaspersky Security Center'ın değiştirilen ilkesiyle denetlenen herhangi bir bilgisayara bağlanan çıkarılabilir sürücülere uygulanır.

Çıkarılabilir sürücülerin şifreleme kuralını düzenleme

Çıkarılabilir sürücünün şifreleme kuralını düzenlemek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, çıkarılabilir sürücü şifreleme kuralını düzenlemek istediğiniz yönetim grubunun adının bulunduğu klasörü açın.
3. Çalışma alanında, **İlkeler** sekmesini seçin.
4. Gereken ilkeyi seçin.
5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:
   - İlkenin içerik menüsünde **Özellikler**'i seçin.
   - Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.
6. **Veri Şifreleme** bölümünde, **Çıkarılabilir sürücülerin şifrelenmesi** alt bölümünü seçin.
7. Şifreleme kurallarının yapılandırıldığı çıkarılabilir sürücülerin listesinde, ihtiyacınız olan çıkarılabilir sürücüye uygun bir giriş seçin.
8. Seçilen çıkarılabilir sürücünün şifreleme kuralını düzenlemek için **Bir kural ayarla** düğmesine tıklayın.

   Bir kural ayarla düğmesinin içerik menüsü açılır.
9. **Bir kural ayarla** düğmesinin içerik menüsünde, Kaspersky Endpoint Security tarafından seçilen çıkarılabilir sürücülerde kayıtlı dosyalara uygulanacak eylemi seçin.
10. Değişiklikleri kaydetmek için **Tamam** düğmesine tıklayın.

Değiştirilen çıkarılabilir sürücü şifreleme kuralları, Kaspersky Security Center'ın değiştirilen ilkesiyle denetlenen herhangi bir bilgisayara bağlanan çıkarılabilir sürücülere uygulanır.

Çıkarılabilir sürücülerdeki şifreli dosyalara erişim için taşınabilir modu etkinleştirme

Çıkarılabilir sürücülerdeki şifreli dosyalara erişim için taşınabilir modu etkinleştirmek amacıyla:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, çıkarılabilir sürücülerdeki şifreli dosyalara erişim için taşınabilir modu etkinleştirmek istediğiniz yönetim grubunun adının bulunduğu klasörü açın.
3. Çalışma alanında, **İlkeler** sekmesini seçin.

4. Gereken ilkeyi seçin.
5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:
   - İlkenin içerik menüsünde **Özellikler**'i seçin.
   - Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.
6. **Veri Şifreleme** bölümünde, **Çıkarılabilir sürücülerin şifrelenmesi** alt bölümünü seçin.
7. **Taşınabilir mod** onay kutusunu seçin.

   Taşınabilir mod tüm dosyaların veya sadece yeni dosyaların şifrelenmesi için kullanılabilir.
8. **Tamam**'a tıklayın.
9. İlkeyi uygulayın.

   Kaspersky Security Center ilkesinin uygulanmasıyla ilgili ayrıntılar için *Kaspersky Security Center Yönetici Kılavuzu*'na bakınız.
10. çıkarılabilir sürücüyü, Kaspersky Security Center ilkesinin uygulanmış olduğu bir aygıta bağlayın.
11. Çıkarılabilir sürücü şifreleme işlemini onaylayın.

    Bu, Taşınabilir Dosya Yöneticisi için bir parola oluşturabileceğiniz penereyi açar.
12. Güç gereksinimlerini karşılayan bir şifre belirleyin ve onaylayın.
13. **Tamam**'a tıklayın.

    Kaspersky Endpoint Security, çıkarılabilir bir sürücüdeki dosyaları Kaspersky Security Center ilkesinde tanımlanan şifreleme kurallarına göre şifreler. Şifrelenmiş dosyalarla çalışmak için kullanılan Taşınabilir Dosya Yöneticisi ayrıca çıkarılabilir sürücüye de kopyalanabilir.

Taşınabilir modu etkinleştirdikten sonra şifreleme işlevi bulunmayan bir bilgisayara bağlı çıkarılabilir sürücülerdeki şifreli dosyalara erişebilirsiniz.

Çıkarılabilir sürücülerin şifresini çözme

Çıkarılabilir sürücülerin şifresini çözmek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, çıkarılabilir sürücülerin şifrelerinin çözülmesini yapılandırmak istediğiniz yönetim grubunun adının bulunduğu klasörü açın.
3. Çalışma alanında, **İlkeler** sekmesini seçin.
4. Gereken ilkeyi seçin.
5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:
   - İlkenin içerik menüsünde **Özellikler**'i seçin.

- Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.

6. **Veri Şifreleme** bölümünde, **Çıkarılabilir sürücülerin şifrelenmesi** alt bölümünü seçin.

7. Çıkarılabilir sürücülerde kayıtlı tüm şifrelenmiş dosyaların şifresini çözmek isterseniz, **Şifreleme modu** açılır listesinde **Çıkarılabilir sürücünün tamamının kriptosunu çöz** seçeneğini seçin.

8. Ayrı çıkarılabilir sürücülerde kayıtlı verilerin şifresini çözmek için verilerinin şifresini çözmek istediğiniz çıkarılabilir sürücülerin şifreleme kurallarını düzenleyin. Bunun için:

   a. Şifreleme kurallarının yapılandırıldığı çıkarılabilir sürücülerin listesinde, ihtiyacınız olan çıkarılabilir sürücüye uygun bir giriş seçin.

   b. Seçilen çıkarılabilir sürücünün şifreleme kuralını düzenlemek için **Bir kural ayarla** düğmesine tıklayın.

   Bir kural ayarla düğmesinin içerik menüsü açılır.

   c. **Bir kural ayarla** düğmesinin içerik menüsünde **Tüm dosyaların şifresini çöz** öğesini seçin.

9. Değişiklikleri kaydetmek için **Tamam** düğmesine tıklayın.

10. İlkeyi uygulayın.

Kaspersky Security Center ilkesinin uygulanmasıyla ilgili ayrıntılar için *Kaspersky Security Center Yönetici Kılavuzu*'na bakınız.

İlke uygulandıktan sonra kullanıcı bir çıkarılabilir sürücü bağladığında veya bir çıkarılabilir sürücü zaten bağlı olduğunda Kaspersky Endpoint Security, kullanıcıya çıkarılabilir sürücünün bir şifreleme kuralına tabi olduğunu ve bu kurala göre hem çıkarılabilir sürücüde kayıtlı şifrelenmiş dosyaların hem de çıkarılabilir sürücünün dosya sisteminin (şifrelenmişse) şifresinin çözüleceğini bildirir. Uygulama kullanıcıya şifre çözme işleminin biraz zaman alabileceği uyarısında bulunur.

Belirli yönetilen bilgisayar grubu için çıkarılabilir sürücülerde veri şifreleme ön ayarlarına sahip Kaspersky Security Center ilkesi oluşturulur. Bu nedenle çıkarılabilir sürücülerde veri şifresi çözmenin sonucu, çıkarılabilir sürücünün bağlandığı bilgisayara bağlıdır.

Kullanıcının veri şifresi çözme sırasında çıkarılabilir sürücünün güvenli kaldırılmasını başlatması durumunda Kaspersky Endpoint Security, veri şifresini çözme işlemini yarıda keser ve şifre çözme işlemi tamamlanmadan çıkarılabilir sürücünün çıkarılabilmesine imkan tanır.

Bir çıkarılabilir sürücü şifrelemesinin başarısız olması halinde Kaspersky Endpoint Security arabirimindeki **Veri şifreleme** raporuna bakın. Dosyalara erişim başka bir uygulama tarafından engellenmiş olabilir. bu durumda çıkarılabilir sürücüyü bilgisayardan çıkarıp tekrar bağlamayı deneyin.

Sabit sürücülerin şifrelenmesi

Kaspersky Endpoint Security, Microsoft Windows for Workstations çalıştıran bir bilgisayara yüklenirse, BitLocker Drive Encryption ve Kaspersky Disk Encryption teknolojileri şifreleme için kullanılabilir. Kaspersky Endpoint Security, Microsoft Windows for File Servers altında çalışan bir bilgisayara yüklenirse, sadece BitLocker Drive Encryption teknolojisi kullanılabilir.

Bu bölümde, sabit sürücülerin şifrelenmesi hakkında bilgi ve Kaspersky Endpoint Security'yi ve Kaspersky Endpoint Security Console Eklentisi'ni kullanarak sabit sürücülerin şifrelenmesini yapılandırma ve gerçekleştirme talimatları bulunmaktadır.

Sabit sürücülerin şifrelenmesi hakkında

Sabit sürücüyü şifrelemeye başlamadan önce uygulama, sistem sabit sürücüsünün Kimlik Doğrulama Aracısı ve BitLocker şifreleme bileşenleriyle uyumluluğunu denetlemeyi de kapsayan şekilde aygıtın şifrelenip şifrelenemeyeceğini belirlemek amacıyla bir dizi denetim gerçekleştirir. Uyumluluğu denetlemek amacıyla bilgisayarın yeniden başlatılması gerekir. Bilgisayar yeniden başlatıldıktan sonra uygulama, tüm gereken denetimleri otomatik olarak gerçekleştirir. Uyumluluk kontrolü başarılı olursa, sabit sürücü şifrelemesi işletim sistemi önyüklenip, uygulama başladıktan sonra başlar. Sistem sabit sürücüsünün Kimlik Doğrulama Aracısı veya BitLocker şifreleme bileşenleriyle uyumsuz olduğu tespit edilirse Sıfırla donanım düğmesine basılarak bilgisayarın yeniden başlatılması gerekir. Kaspersky Endpoint Security uyumsuzlukla ilgili bilgileri kaydeder. Bu bilgilere dayalı olarak uygulama, işletim sistemi başlatıldığında sabit sürücülerin şifrelenmesini başlatmaz. Bu olayla ilgili bilgiler, Kaspersky Security Center raporlarına kaydedilir.

Bilgisayarın donanım yapılandırması değiştiyse sistem sabit sürücüsünün Kimlik Doğrulama Aracısı ve BitLocker şifreleme bileşenleri ile uyumluluğunu denetlemek amacıyla önceki denetim sırasında uygulama tarafından kaydedilen uyumsuzluk bilgileri silinmelidir. Bunun için sabit sürücü şifrelenmeden önce komut satırına `avp pbatestreset` yazın. Sistem sabit sürücüsünün Kimlik Doğrulama Aracısı ile uyumluluğunu denetledikten sonra işletim sistemi yüklenmezse Geri Yükleme Yardımcı Programını kullanarak Kimlik Doğrulama Aracısı'nın test çalışmasının ardından kalan nesne ve verileri kaldırmalı, Kaspersky Endpoint Security'yi başlatmalı ve `avp pbatestreset` komutunu yeniden uygulamalısınız.

Sabit sürücü şifrelemesi başladıktan sonra Kaspersky Endpoint Security, sabit sürücülere yazılan tüm verileri şifreler.

Sabit sürücünün şifresinin çözülmesi sırasında kullanıcı bilgisayarı kapatır veya yeniden başlatırsa Kimlik Doğrulama Aracısı işletim sisteminin bir sonraki başlatılmasından önce yüklenir. Kimlik Doğrulama Aracısı'nda başarılı kimlik doğrulamanın ve işletim sisteminin başlatılmasının ardından Kaspersky Endpoint Security sabit sürücülerin şifrelenmesini sürdürür.

Sabit sürücüler şifrelenirken işletim sistemi hazırda bekleme moduna geçerse Kimlik Doğrulama Aracısı, işletim sistemi hazırda bekleme modundan çıktığında yüklenir. Kimlik Doğrulama Aracısı'nda başarılı kimlik doğrulamanın ve işletim sisteminin başlatılmasının ardından Kaspersky Endpoint Security sabit sürücülerin şifrelenmesini sürdürür.

Sabit sürücü şifresini çözme sırasında işletim sistemi uyku moduna geçerse Kaspersky Endpoint Security, Kimlik Doğrulama Aracısı yüklenmeden işletim sistemi uyku modundan çıktığında sabit sürücüyü şifrelemeyi sürdürür.

Kimlik Doğrulama Aracısı'nda kullanıcı kimlik doğrulaması iki şekilde gerçekleştirilebilir:

- Kaspersky Security Center araçlarını kullanarak LAN yöneticisi tarafından oluşturulan Kimlik Doğrulama Aracısı hesabının adını ve parolasını girin.
- Bilgisayara bağlanan belirteç veya akıllı kartın parolasını girin.

Kimlik doğrulama aracısı aşağıdaki dillerin klavye düzenlerini desteklemektedir:

- İngilizce (İngiltere)
- İngilizce (ABD)
- Arapça (Cezayir, Fas, Tunus; AZERTY düzeni)
- İspanyolca (Latin Amerika)

- İtalyanca
- Almanca (Almanya ve Avusturya)
- Almanca (İsviçre)
- Portekizce (Brezilya, ABNT2 düzeni)
- Rusça (105 tuşlu QWERTY düzenindeki IBM / Windows klavyeleri)
- Türkçe (QWERTY düzeni)
- Fransızca (Fransa)
- Fransızca (İsviçre)
- Fransızca (Belçika, AZERTY düzeni)
- Japonca (106 tuşlu QWERTY düzenindeki klavyeleri)

İşletim sisteminin dil ve bölge standart ayarlarında düzen eklendiğinde ve Microsoft Windows'un açılış ekranında kullanılabilir olduğunda klavye düzeni, Kimlik Doğrulama Aracısı'nda kullanılabilir hale gelir.

Kimlik Doğrulama Aracısı hesap adı, Kimlik Doğrulama Aracısı'nda kullanılabilir olan klavye düzenlerini kullanarak girilemeyen semboller içeriyorsa şifrelenmiş sabit sürücülere sadece Geri Yükleme Yardımcı Programını kullanarak geri yüklendikten veya Kimlik Doğrulama Aracısı hesap adı ve parolası sıfırlandıktan sonra erişim sağlanabilir.

Kaspersky Endpoint Security aşağıdaki belirteçler, akıllı kart okuyucular ve akıllı kartları destekler:

- SafeNet eToken PRO 64K (4.2b) (USB)
- SafeNet eToken PRO 72K Java (USB)
- SafeNet eToken PRO 72K Java (Akıllı Kart)
- SafeNet eToken 4100 72K Java (Akıllı Kart)
- SafeNet eToken 5100 (USB)
- SafeNet eToken 5105 (USB)
- SafeNet eToken 7300 (USB)
- EMC RSA SecurID 800 (USB).
- Rutoken EDS (USB)
- Rutoken EDS (Flash)
- Aladdin-RD JaCarta PKI (USB)
- Aladdin-RD JaCarta PKI (Akıllı Kart)

- Athena IDProtect Laser (USB)
- Gemalto IDBridge CT40 (Reader)
- Gemalto IDPrime .NET 511

Kaspersky Disk Encryption teknolojisini kullanarak sabit sürücülerin şifrelenmesi

Bir bilgisayardaki sabit sürücüleri şifrelemeden önce, bilgisayarda virüs bulunmadığından emin olmanızı öneririz. Bunun için Tam Tarama veya Kritik Alanları Tarama görevini başlatın. Rootkit virüsü bulaşmış bir bilgisayarın sabit sürücüsünün şifrelenmesi bilgisayarın çalışmamasına neden olabilir.

Kaspersky Disk Encryption teknolojisini kullanarak sabit sürücüleri şifrelenmek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, sabit sürücülerin şifrelenmesini yapılandırmak istediğiniz yönetim grubunun adının bulunduğu klasörü açın.
3. Çalışma alanında, **İlkeler** sekmesini seçin.
4. Gereken ilkeyi seçin.
5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:
   - İlkenin içerik menüsünde **Özellikler**'i seçin.
   - Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.
6. **Veri Şifreleme** bölümünde, **Sabit sürücülerin şifrelenmesi** alt bölümünü seçin.
7. **Şifreleme teknolojisi** açılır listesinde, **Kaspersky Disk Encryption** seçeneğini seçin.

   Kaspersky Disk Encryption teknolojisi, bilgisayarda BitLocker ile şifrelenen sabit sürücüler varsa kullanılamaz.

8. **Şifreleme modu** açılır listesinden **Tüm sabit sürücüleri şifrele** seçeneğini seçin.

   Sabit sürücülerin bir kısmını şifreleme dışında tutmak isterseniz bu sabit sürücülerin bir listesini oluşturun.

9. Aşağıdaki şifreleme yöntemlerinden birini seçin:
   - Şifrelemeyi sadece dosyalar tarafından kullanılan sabit sürücü sektörlerine uygulamak isterseniz **Sadece kullanılan disk alanını şifrele** onay kutusunu işaretleyin.

     Şifrelemeyi zaten kullanımda olan bir sürücüye uyguluyorsanız, tüm sürücünün şifrelenmesi önerilir. Böylece, hala kurtarılabilir bilgi içeren silinmiş veriler dahil tüm veriler korunur. **Sadece kullanılan disk alanını şifrele** işlevi, daha önce kullanılmamış yeni sürücüler için önerilir.

- Tüm sabit sürücüye şifreleme uygulamak isterseniz **Sadece kullanılan disk alanını şifrele** onay kutusunun işaretini kaldırın.

  Bu işlev sadece şifrelenmemiş sürücülere uygulanabilir. Bir aygıt daha önce **Sadece kullanılan disk alanını şifrele** işlevini kullanarak şifrelendiyse **Tüm sabit sürücüleri şifrele** modunda bir ilke uygulandıktan sonra, dosyalar tarafından kullanılmayan sektörler yine de şifrelenmez.

10. Değişiklikleri kaydetmek için **Tamam** düğmesine tıklayın.

11. İlkeyi uygulayın.

    Kaspersky Security Center ilkesinin uygulanmasıyla ilgili ayrıntılar için *Kaspersky Security Center Yönetici Kılavuzu*'na bakınız.

BitLocker Drive Encryption teknolojisini kullanarak sabit sürücüleri şifreleme

Bir bilgisayardaki sabit sürücüleri şifrelemeden önce, bilgisayarda virüs bulunmadığından emin olmanızı öneririz. Bunun için Tam Tarama veya Kritik Alanları Tarama görevini başlatın. Rootkit virüsü bulaşmış bir bilgisayarın sabit sürücüsünün şifrelenmesi bilgisayarın çalışmamasına neden olabilir.

BitLocker Drive Encryption teknolojisinin sunucu işletim sistemine sahip bilgisayarlarda kullanılması, Rol ve bileşen ekle sihirbazı kullanılarak **BitLocker Drive Encryption** bileşeninin yüklenmesini gerektirebilir.

BitLocker Drive Encryption teknolojisini kullanarak sabit sürücüleri şifrelemek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, sabit sürücülerin şifrelenmesini yapılandırmak istediğiniz yönetim grubunun adının bulunduğu klasörü açın.

3. Çalışma alanında, **İlkeler** sekmesini seçin.

4. Gereken ilkeyi seçin.

5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:

   - İlkenin içerik menüsünde **Özellikler**'i seçin.

   - Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.

6. **Veri Şifreleme** bölümünde, **Sabit sürücülerin şifrelenmesi** alt bölümünü seçin.

7. **Şifreleme teknolojisi** açılır listesinde **BitLocker Drive Encryption** seçeneğini seçin.

8. **Şifreleme modu** açılır listesinde **Tüm sabit sürücüleri şifrele** seçeneğini seçin.

9. Bir ön yükleme ortamına bilgi girmek için dokunmatik ekran klavyesi kullanmak isterseniz **Tabletlerde önyükleme klavyesi girişi gerektiren kimlik doğrulamasının kullanılmasına izin ver** onay kutusunu işaretleyin.

Bu ayarın yalnızca bir önyükleme ortamında USB klavyesi gibi alternatif veri girişi araçlarına sahip aygıtlar için kullanılması önerilir.

10. Aşağıdaki şifreleme türlerinden birini seçin:

    - Donanım şifrelemesi kullanmak isterseniz **Donanım şifrelemesi kullan** onay kutusunu işaretleyin.
    - Yazılım şifrelemesi kullanmak isterseniz **Donanım şifrelemesi kullan** onay kutusunu işaretlemeyin.

11. Aşağıdaki şifreleme yöntemlerinden birini seçin:

    - Şifrelemeyi sadece dosyalar tarafından kullanılan sabit sürücü sektörlerine uygulamak isterseniz **Sadece kullanılan disk alanını şifrele** onay kutusunu işaretleyin.
    - Tüm sabit sürücüye şifreleme uygulamak isterseniz **Sadece kullanılan disk alanını şifrele** onay kutusunun işaretini kaldırın.

      Bu işlev sadece şifrelenmemiş sürücülere uygulanabilir. Bir aygıt daha önce **Sadece kullanılan disk alanını şifrele** işlevini kullanarak şifrelendiyse **Tüm sabit sürücüleri şifrele** modunda bir ilke uygulandıktan sonra, dosyalar tarafından kullanılmayan sektörler yine de şifrelenmez.

12. BitLocker ile şifrelenen sabit sürücülere erişim için bir yöntem seçin.

    - Şifreleme anahtarlarını saklamak için bir Güvenilir Platform Modülü (TPM) kullanmak isterseniz **Güvenilir Platform Modülü kullan (TPM-Trusted Platform Module)** seçeneğini seçin.
    - Sabit sürücülerin şifrelenmesi için bir Güvenilir Platform Modülü (TPM) kullanmıyorsanız **Parola kullan** seçeneğini seçin ve bir parolanın içermesi gereken minimum karakter sayısını **Minimum parola uzunluğu** alanında belirtin.

Güvenilir Bir Platform Modülü (TPM-Trusted Platform Module) mevcudiyeti, Windows 7 ve Windows 2008 R2 işletim sistemlerinin yanı sıra eski sürümleri için de zorunludur.

13. Önceki adım sırasında **Güvenilir Platform Modülü kullan (TPM-Trusted Platform Module)** seçeneğini seçtiyseniz:

    - Kullanıcı şifreleme anahtarına erişim girişiminde bulunduğunda istenecek bir PIN kodu ayarlamak isterseniz **PIN kullan** onay kutusunu işaretleyin ve **Minimum PIN** uzunluğu alanında bir PIN kodunun içermesi gereken minimum hane sayısını belirleyin.
    - Şifrelenmiş sabit sürücülere bilgisayarda bir güvenilir platform modülü olmadan bir parola kullanarak erişmek isterseniz, **Güvenilir platform Modülü (TPM) kullanılamıyorsa parola kullan** onay kutusunu seçin ve **Minimum parola uzunluğu** alanında parolanın içermesi gereken minimum karakter sayısını belirtin.

      Bu durumda, şifreleme anahtarlarına erişim **Parola kullan** onay kutusu seçilmiş gibi verilen parolanın kullanılmasıyla meydana gelir.

      Güvenilir platform Modülü (TPM) kullanılamıyorsa parola kullan seçili değilse ve güvenilir platform modülü kullanılamıyorsa sabit sürücü şifreleme başlamayacaktır.

14. Değişiklikleri kaydetmek için **Tamam** düğmesine tıklayın.

15. İlkeyi uygulayın.

    Kaspersky Security Center ilkesinin uygulanmasıyla ilgili ayrıntılar için *Kaspersky Security Center Yönetici Kılavuzu*'na bakınız.

Kaspersky Endpoint Security yüklü istemci bilgisayarda ilke uygulandıktan sonra aşağıdaki sorguları yapılacaktır:

- Şifreleme ilkesi bir sistem sabit sürücüsüne uygulanırsa, güvenilir platform modülü kullanımdaysa PIN kodu penceresi görünür veya aksi halde önyükleme yetkilendirmesi için parola isteme penceresi görünür.
- Bilgisayarın işletim sisteminde Federal Bilgi İşleme Standart Uyumluluk Modu açıksa, Windows 8 ve daha üstü işletim sistemi, kurtarma anahtarı dosyasını kaydetmek için bir USB aygıtı bağlantı isteği penceresi görüntüleyecektir.

Şifreleme anahtarlarına erişim yoksa kullanıcı, yerel ağ yöneticisinden bir kurtarma anahtarı isteyebilir (kurtarma anahtarının USB aygıta daha önce kaydedilmemiş olması veya kaybolması gerekir).

Şifreleme dışında tutulan sabit sürücülerin listesini oluşturma

Sadece Kaspersky Disk Encryption teknolojisi için şifrelemeden istisnalar listesi oluşturabilirsiniz.

Şifreleme dışında tutulan sabit sürücülerin listesini oluşturmak için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, şifreleme dışında tutulacak sabit sürücüler listesini oluşturmak istediğiniz yönetim grubunun adına sahip klasörü açın.
3. Çalışma alanında, **İlkeler** sekmesini seçin.
4. Gereken ilkeyi seçin.
5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:
   - İlkenin içerik menüsünde **Özellikler**'i seçin.
   - Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.
6. **Veri Şifreleme** bölümünde, **Sabit sürücülerin şifrelenmesi** alt bölümünü seçin.
7. **Şifreleme teknolojisi** açılır listesinde, **Kaspersky Disk Encryption** seçeneğini seçin.

   Şifreleme dışında tutulan sabit sürücülerin girişleri, **Aşağıdaki sabit sürücüleri şifreleme** tablosunda görülür. Daha önce şifreleme dışında tutulacak sabit sürücülerin listesini oluşturmadıysanız bu tablo boş olur.
8. Şifreleme dışında tutulan sabit sürücülerin listesine sabit sürücüleri eklemek için:
   a. **Ekle** düğmesine tıklayın.

      Kaspersky Security Center listesinden aygıtları ekle penceresi açılır.

   b. **Kaspersky Security Center listesinden aygıtları ekle** penceresinde, aşağıdaki parametrelerin değerlerini belirtin: **Ad**, **Bilgisayar**, **Önyüklenebilir** ve **Kaspersky Disk Encryption**.

   c. **Yenile** düğmesine tıklayın.

d. **Ad** sütununda, şifrelemeden hariç tutulan sürücülerin listesine eklemek istediğiniz sabit sürücülerin adlarının karşısındaki onay kutularını işaretleyin.

e. **Tamam**'a tıklayın.

Seçilen sabit sürücüler, **Aşağıdaki sabit sürücüleri şifreleme** tablosunda görülür.

9. İstisnalar tablosundan sabit sürücüleri çıkarmak isterseniz, **Aşağıdaki sabit sürücüleri şifreleme** tablosundan bir veya daha fazla satır seçin ve **Sil** düğmesine tıklayın.

> Tabloda birden fazla satır seçmek için **CTRL** tuşunu basılı tutarak seçim yapın.

10. Değişiklikleri kaydetmek için **Tamam** düğmesine tıklayın.

Sabit sürücü şifresini çözme

> Veri şifrelemesine izin veren etkin bir lisans olmasa dahi sabit sürücülerin şifresini çözebilirsiniz.

Sabit sürücülerin şifresini çözmek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, sabit sürücülerin şifrelerinin çözülmesini yapılandırmak istediğiniz yönetim grubunun adının bulunduğu klasörü açın.
3. Çalışma alanında, **İlkeler** sekmesini seçin.
4. Gereken ilkeyi seçin.
5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:
   - İlkenin içerik menüsünde **Özellikler**'i seçin.
   - Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.
6. **Veri Şifreleme** bölümünde, **Sabit sürücülerin şifrelenmesi** alt bölümünü seçin.
7. **Şifreleme teknolojisi** açılır listesinde, sabit sürücülerin şifrelendiği teknolojiyi seçin.
8. Aşağıdakilerden birini yapın:
   - **Şifreleme modu** açılır listesinde, tüm şifrelenmiş sabit sürücülerin şifresini çözmek isterseniz **Tüm sabit sürücülerin şifresini çöz** seçeneğini seçin.
   - Şifresini çözmek istediğiniz şifrelenmiş sabit sürücüleri **Aşağıdaki sabit sürücüleri şifreleme** tablosuna ekleyin.

     > Bu seçenek sadece Kaspersky Disk Encryption teknolojisi için kullanılabilir.

9. Değişiklikleri kaydetmek için **Tamam** düğmesine tıklayın.

10. İlkeyi uygulayın.

    Kaspersky Security Center ilkesinin uygulanmasıyla ilgili ayrıntılar için *Kaspersky Security Center Yönetici Kılavuzu*'na bakınız.

Kaspersky Disk Encryption teknolojisi kullanılarak şifrelenmiş sabit sürücülerin şifresi çözülürken kullanıcı bilgisayarı kapatır veya yeniden başlatırsa Kimlik Doğrulama Aracısı işletim sisteminin bir sonraki başlatılmasından önce yüklenir. Kimlik Doğrulama Aracısı'nda başarılı kimlik doğrulamanın ve işletim sisteminin başlatılmasının ardından Kaspersky Endpoint Security sabit sürücü şifresini çözmeyi sürdürür.

Kaspersky Disk Encryption teknolojisi kullanılarak şifrelenmiş sabit sürücülerin şifresi çözülürken sistemi hazırda bekleme moduna geçerse Kimlik Doğrulama Aracısı, işletim sistemi hazırda bekleme modundan çıktığında yüklenir. Kimlik Doğrulama Aracısı'nda başarılı kimlik doğrulamanın ve işletim sisteminin başlatılmasının ardından Kaspersky Endpoint Security sabit sürücü şifresini çözmeyi sürdürür. Sabit sürücü şifresini çözmenin ardından işletim sisteminin ilk önyüklemesine kadar hazırda bekleme modu kullanılamaz.

Sabit sürücü şifresini çözme sırasında işletim sistemi uyku moduna geçerse Kaspersky Endpoint Security, Kimlik Doğrulama Aracısı yüklenmeden işletim sistemi uyku modundan çıktığında sabit sürücü şifresini çözmeyi sürdürür.

Kimlik Doğrulama Aracısı'nı yönetme

Sistem sabit sürücüleri şifrelenmişse işletim sistemi başlatılmadan önce Kimlik Doğrulama Aracısı yüklenir. Şifrelenmiş sabit sürücülere erişim sağlamak ve işletim sistemini yüklemek için Kimlik Doğrulama Aracısı'nı kullanarak kimlik doğrulamayı tamamlayın.

Kimlik doğrulama prosedürünün başarılı bir şekilde tamamlanmasından sonra, işletim sistemi yüklenir. İşletim sisteminin yeniden başlatıldığı her seferde kimlik doğrulama işlemi tekrarlanır.

Kullanıcı bazı durumlarda kimlik doğrulamasını geçemeyebilir. Örneğin kullanıcı, Kimlik Doğrulama Aracısı hesabının kullanıcı adı ve/veya parolasını unuttuysa, şifrematik veya akıllı kartın parolasını unuttuysa ya da şifrematik veya akıllı kartını kaybettiyse kimlik doğrulaması imkansızdır.

Kullanıcı Kimlik Doğrulama Aracısı hesap kimlik bilgilerini veya şifrematik veya akıllı kart parolasını unutmuşsa, bunları kurtarmak için kurumsal LAN yöneticisine başvurmalısınız.

Kullanıcı bir şifrematik veya akıllı kartı kaybetmişse yönetici, bir Kimlik Doğrulama Aracısı hesabı oluşturmak için şifrematik veya akıllı kart elektronik sertifika dosyasını komuta eklemelidir. Daha sonra kullanıcı, şifrelenmiş aygıtlardaki verilerin kurtarılması için prosedürü tamamlamalıdır.

Kimlik Doğrulama Aracısı ile belirteç ve akıllı kart kullanma

Şifrelenmiş sabit sürücülere erişirken kimlik doğrulama için bir belirteç veya akıllı kart kullanılabilir. Bunun için bir belirteç veya akıllı kart elektronik sertifikasının dosyasını Kimlik Doğrulama Aracısı hesabı oluşturma komutuna eklemeniz gerekir.

Saedece bilgisayarın sabit sürücüleri AES256 şifreleme algoritması kullanılarak şifrelendiyse şifrematik veya akıllı kart kullanımı mümkündür. Bilgisayarın sabit sürücüleri AES56 şifreleme algoritması kullanılarak şifrelenişse, elektronik sertifika dosyasının komuta eklenmesi reddedilecektir.

Bir Kimlik Doğrulama Aracısı hesabı oluşturma komutuna bir belirteç veya akıllı kart elektronik sertifikası dosyasını eklemek için, önce dosyayı üçüncü taraf sertifika yönetme yazılımı kullanarak kaydetmeniz gerekir.

Belirteç veya akıllı kart sertifikası aşağıdaki özelliklere sahip olmalıdır:

- Sertifika X.509 standardıyla uyumlu olmalıdır ve sertifika dosyasında DER kodlaması olmalıdır.

  Belirteç veya akıllı kartın elektronik sertifikası bu gereksinimi karşılamıyorsa, yönetim eklentisi bu sertifikanın dosyasını bir Kimlik Doğrulama Aracısı hesabı oluşturma komutuna yüklemez ve hata mesajı görüntüler.

- Sertifikanın amacını tanımlayan `KeyUsage` parametresi, `keyEncipherment` veya `dataEncipherment` değerine sahip olmalıdır.

  Belirteç veya akıllı kartın elektronik sertifikası bu gereksinimi karşılamıyorsa, yönetim eklentisi bu sertifikanın dosyasını bir Kimlik Doğrulama Aracısı hesabı oluşturma komutuna yükler ve bir uyarı mesajı görüntüler.

- Sertifika, en az 1024 bit uzunluğunda bir RSA anahtarı içerir.

  Belirteç veya akıllı kartın elektronik sertifikası bu gereksinimi karşılamıyorsa, yönetim eklentisi bu sertifikanın dosyasını bir Kimlik Doğrulama Aracısı hesabı oluşturma komutuna yüklemez ve hata mesajı görüntüler.

Kimlik Doğrulama Aracısı yardım mesajlarını düzenleme

Kimlik Doğrulama Aracısı'nın yardım mesajlarını düzenlemeden önce lütfen önyükleme ortamında desteklenen karakterlerin listesi'ni gözden geçirin.

Kimlik Doğrulama Aracısı yardım mesajlarını düzenlemek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, Kimlik Doğrulama Aracısı yardım mesajlarını düzenlemek istediğiniz yönetim grubunun adının bulunduğu klasörü açın.
3. Çalışma alanında, **İlkeler** sekmesini seçin.
4. Gereken ilkeyi seçin.
5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:
   - İlkenin içerik menüsünde **Özellikler**'i seçin.
   - Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.
6. **Veri Şifreleme** bölümünde, **Ortak şifreleme ayarları** alt bölümünü seçin.
7. **Şablonlar** bölümünde, **Yardım** düğmesine tıklayın.

   Kimlik Doğrulama Aracısı yardım mesajları penceresi açılır.
8. Aşağıdakileri uygulayın:
   - Hesap kimlik doğrulama bilgileri girildiğinde Kimlik Doğrulama Aracısı penceresinde görüntülenen yardım metnini düzenlemek için **Kimlik Doğrulama** sekmesini seçin.
   - Kimlik Doğrulama Aracısı hesabının parolası değiştirildiğinde Kimlik Doğrulama Aracısı penceresinde görüntülenen yardım metnini düzenlemek için **Parolayı değiştir** sekmesini seçin.

- Kimlik Doğrulama Aracısı hesabının parolası kurtarıldığında Kimlik Doğrulama Aracısı penceresinde görüntülenen yardım metnini düzenlemek için **Parolayı kurtar** sekmesini seçin.

9. Yardım mesajlarını düzenleyin.

   Orijinal metni geri yüklemek isterseniz, **Varsayılan** düğmeye tıklayın.

10. **Tamam**'a tıklayın.

11. Değişikliklerinizi kaydetmek için **Özellikler: <İlke adı>** penceresinde **Tamam**'a tıklayın.

Kimlik Doğrulama Aracısı yardım mesajlarında karakterler için sınırlı destek

Bir önyükleme ortamında aşağıdaki Unicode karakterleri desteklenmektedir:

- Temel Latin alfabesi (0000 - 007F)
- Diğer Latin-1 karakterleri (0080 - 00FF)
- Genişletilmiş Latin-A (0100 - 017F)
- Genişletilmiş Latin-B (0180 - 024F)
- Birleşmemiş genişletilmiş ID karakterleri (02B0 - 02FF)
- Birleşmiş vurgu işaretleri (0300 - 036F)
- Yunan ve Kıpti alfabeleri (0370 - 03FF)
- Kiril (0400 - 04FF)
- İbranice (0590 - 05FF)
- Arapça yazı (0600 - 06FF)
- Diğer genişletilmiş Latince (1E00 - 1EFF)
- Noktalama işaretleri (2000 - 206F)
- Para birimi simgeleri (20A0 - 20CF)
- Harf benzeri simgeler (2100 - 214F)
- Geometrik şekiller (25A0 - 25FF)
- Arapça yazı-B'nin sunum şekilleri (FE70 - FEFF)

Bu listede belirtilmeyen karakterler bir önyükleme ortamında desteklenmemektedir. Bu tür karakterleri Kimlik doğrulama aracısı yardım mesajlarında kullanmamanız önerilir.

Kimlik Doğrulama Aracısı izleme düzeyini seçme

Uygulama, Kimlik Doğrulama Aracısı'nın işlemleri hakkında hizmet bilgisini ve Kimlik Doğrulama Aracısı ile kullanıcının yaptığı işlemler hakkındaki bilgiyi izleme dosyasına kaydeder.

Kimlik Doğrulama Aracısı izleme düzeyini seçmek için:

1. Şifrelenmiş sabit sürücüye sahip bir bilgisayar açılır açılmaz Kimlik Doğrulama Aracısı ayarlarını yapılandırmak amacıyla pencere açmak için **F3** tuşuna basın.

2. Kimlik Doğrulama Aracısı ayarları penceresinden izleme düzeyini seçin:

   - **Hata ayıklama günlüğünü devre dışı bırak (varsayılan)**. Bu seçenek seçilirse uygulama, Kimlik Doğrulama Aracısı olayları hakkında izleme dosyasına bilgi kaydetmez.

   - **Hata ayıklama günlüğünü etkinleştir**. Bu seçenek seçilirse uygulama, Kimlik Doğrulama Aracısı'nın işlemleri ve Kimlik Doğrulama Aracısı ile gerçekleştirilen kullanıcı işlemleri hakkındaki bilgileri izleme dosyasına kaydeder.

   - **Ayrıntılı günlüğü etkinleştir**. Bu seçenek seçilirse uygulama, Kimlik Doğrulama Aracısı'nın işlemleri ve Kimlik Doğrulama Aracısı ile gerçekleştirilen kullanıcı işlemleri hakkındaki ayrıntılı bilgilerin günlüğünü izleme dosyasında tutar.

     Hata ayıklama günlüğünü etkinleştir seçeneğinin düzeyi ile karşılaştırıldığında bu seçenek altındaki giriş ayrıntılarının düzeyi daha yüksektir. Yüksek düzeyde giriş ayrıntıları Kimlik Doğrulama Aracısı ve işletim sisteminin açılışını yavaşlatabilir.

   - **Hata ayıklama günlüğünü etkinleştir ve seri bağlantı noktasını seç**. Bu seçenek seçilirse uygulama, Kimlik Doğrulama Aracısı'nın işlemleri ve Kimlik Doğrulama Aracısı ile gerçekleştirilen kullanıcı işlemleri hakkındaki bilgilerin günlüğünü izleme dosyasında tutar ve bunu COM bağlantı noktası üzerinden aktarır.

     Şifrelenmiş sabit sürücülü bir bilgisayar COM bağlantı noktası üzerinden başka bir bilgisayara bağlanırsa Kimlik Doğrulama Aracısı olayları söz konusu diğer bilgisayardan incelenebilir.

   - **Ayrıntılı hata ayıklama günlüğünü etkinleştir ve seri bağlantı noktasını seç**. Bu seçenek seçilirse uygulama, Kimlik Doğrulama Aracısı'nın işlemleri ve Kimlik Doğrulama Aracısı ile gerçekleştirilen kullanıcı işlemleri hakkındaki bilgilerin ayrıntılı günlüğünü izleme dosyasında tutar ve bunu COM bağlantı noktası üzerinden aktarır.

     Hata ayıklama günlüğünü etkinleştir ve seri bağlantı noktasını seç seçeneğinin düzeyi ile karşılaştırıldığında bu seçenek altındaki giriş ayrıntılarının düzeyi daha yüksektir. Yüksek düzeyde giriş ayrıntıları Kimlik Doğrulama Aracısı ve işletim sisteminin açılışını yavaşlatabilir.

Bilgisayarda şifrelenmiş sabit sürücüler varsa veya tam disk şifreleme sırasında, veriler Kimlik Doğrulama Aracısı izleme dosyasına kaydedilir.

Uygulamanın diğer iz dosyalarından farklı olarak Kimlik Doğrulama Aracısı iz dosyası Kaspersky'ye gönderilmez. Gerekirse Kimlik Doğrulama Aracısı iz dosyasını analiz için Kaspersky'ye elle gönderebilirsiniz.

Kimlik Doğrulama Aracısı hesaplarını yönetme

Aşağıdaki Kaspersky Security Center araçları, Kimlik Doğrulama Aracısı hesaplarının yönetilmesi için kullanılabilir:

- Kimlik doğrulama aracısı hesaplarını yönetmek için grup görevi. Bu görev, bir grup istemci bilgisayarı için Kimlik Doğrulama Aracısı hesaplarını yönetmenize olanak tanır.
- **Şifreleme (hesap yönetimi)** yerel görevi. Bu görev, istemci bilgisayarları için Kimlik Doğrulama Aracısı hesaplarını yönetmenize olanak tanır.

Kimlik Doğrulama Aracısı hesap yönetimi görevi ayarlarını yapılandırmak için:

1. Bir (Yerel bir görev oluşturma, Bir grup görevi oluşturma) Kimlik Doğrulama Aracısı hesap yönetim görevi oluştur.
2. **Özellikler: <Kimlik Doğrulama Aracısı hesap yönetimi görevinin adı>** penceresinde **Ayarlar** bölümünü açın.
3. Kimlik Doğrulama Aracısı hesaplarını oluşturma komutları ekleyin.
4. Kimlik Doğrulama Aracısı hesaplarını düzenlenme komutları ekleyin.
5. Kimlik Doğrulama Aracısı kullanıcı hesaplarını silmek için komutları ekleyin.
6. Gerekirse eklenen Kimlik doğrulama aracısı hesaplarını yönetme komutlarını düzenleyin. Bunun için **Kimlik doğrulama aracısı hesaplarını yönetme komutları** tablosunda **Düzenle** düğmesine tıklayın.
7. Gerekirse, eklenen Kimlik doğrulama aracısı hesaplarını yönetme komutlarını silin. Bunun için **Kimlik Doğrulama Aracısı hesaplarını yönetmek için komutlar** tablosunda bir veya daha fazla komutu seçin ve **Kaldır** düğmesine tıklayın.

   Tabloda birden fazla satır seçmek için **CTRL** tuşunu basılı tutarak seçim yapın.

8. Değişiklikleri kaydetmek için görev özellikleri penceresinde **Tamam**'a tıklayın.
9. Görevi çalıştırın.

Göreve eklenen Kimlik Doğrulama Aracısı hesap yönetim komutları yürütülecektir.

Kimlik Doğrulama Aracısı hesabı oluşturmak için komut ekleme

Kimlik Doğrulama Aracısı hesabı oluşturmak amacıyla bir komut eklemek için:

1. **Özellikler: <Kimlik Doğrulama Aracısı hesap yönetimi görevinin adı>** penceresinde **Ayarlar** bölümünü açın.
2. **Ekle** düğmesine tıklayın ve açılır listeden aşağıdaki **Hesap ekleme komutu**'nu seçin.

   Kullanıcı hesabı ekle penceresi açılır.
3. **Windows hesabı** penceresinde, **Kullanıcı hesabı ekle** alanında, Kimlik Doğrulama Aracısı hesabı oluştururken temel alınacak Microsoft Windows hesabının adını belirtin.

   Bunun için hesabın adını elle yazın veya **Seç** düğmesine tıklayın.
4. Microsoft Windows hesabının adını elle girdiyseniz hesabın güvenlik tanımlayıcısını (SID) belirlemek için **İzin ver** düğmesine tıklayın.

   İzin ver düğmesine tıklayarak güvenlik tanımlayıcısını (SID) belirlememeyi tercih ederseniz bilgisayarda görev gerçekleştirildiğinde belirlenir.

Bir Kimlik Doğrulama Aracısı hesabı oluşturma komutu eklerken Microsoft Windows hesabının SID bilgisinin belirlenmesi, elle girilen Microsoft Windows hesabı adının doğru olmasını sağlamanın rahat bir yoludur. Girilen Microsoft Windows hesabı mevcut değilse, güvenilir olmayan bir etki alanına aitse veya **Şifreleme (hesap yönetimi)** yerel görevinin değiştirildiği bir bilgisayarda yer almıyorsa Kimlik Doğrulama Aracısı hesap yönetimi görevi bir hata ile sonlanır.

5. Kimlik Doğrulama Aracısı için önceden oluşturulmuş aynı adlı bir hesabın oluşturulan hesapla değiştirilmesini sağlamak için **Mevcut kullanıcı hesabını değiştir** onay kutusunu işaretleyin.

   Bu adım, Kimlik Doğrulama Aracısı hesaplarını yönetmek için grup görevinin özelliklerine bir Kimlik Doğrulama Aracısı hesabı oluşturma komutu eklerken kullanılabilir. Bu adım, bir Kimlik Doğrulama Aracısı hesabı oluşturma komutunu **Şifreleme (hesap yönetimi)** yerel görevinin özelliklerine eklerken kullanılamaz.

6. **Kullanıcı adı** alanına, şifrelenmiş sabit sürücülere erişim için kimlik doğrulama sırasında girilmesi gereken Kimlik Doğrulama Aracısı hesabının adını yazın.

7. Uygulamanın şifrelenmiş sabit sürücülere erişim için kimlik doğrulaması sırasında Kimlik Doğrulama Aracısı hesabının parolasını sormasını istiyorsanız **Parola tabanlı kimlik doğrulamasına izin ver** onay kutusunu işaretleyin.

8. Önceki adımda **Parola tabanlı kimlik doğrulamasına izin ver** onay kutusunu işaretlediyseniz:

   a. **Parola** alanına, şifrelenmiş sabit sürücülere erişim kimlik doğrulaması sırasında girilmesi gereken Kimlik Doğrulama Aracısı hesabının parolasını yazın.

   b. **Parolayı onaylayın** alanında, önceki adımda girilen Kimlik Doğrulama Aracısı hesabının parolasını onaylayın.

   c. Aşağıdakilerden birini yapın:

   - Uygulamanın, komut satırında belirtilen kimlik doğrulamasını ilk kez geçen kullanıcıya bir parola değiştirme isteği görüntülemesini istiyorsanız **İlk kimlik doğrulamada parolayı değiştir** seçeneğini seçin.
   - İstemiyorsanız **Parola değişikliği gerekmesin** seçeneğini seçin.

9. Uygulamanın şifrelenmiş sabit sürücülere erişim kimlik doğrulaması sırasında kullanıcıdan bilgisayara bir belirteç veya akıllı kart takmasını istemesini ayarlamak için **Sertifika tabanlı kimlik doğrulamasına izin ver** onay kutusunu işaretleyin.

10. Önceki adımda **Sertifika tabanlı kimlik doğrulamasına izin ver** onay kutusunu işaretlediyseniz **Gözat** düğmesine tıklayın ve **Sertifika dosyasını seç** penceresinden belirteç veya akıllı kart elektronik sertifikasının dosyasını seçin.

11. Gerekirse **Komut açıklaması** alanına, komutu yönetmek için ihtiyaç duyduğunuz Kimlik Doğrulama Aracısı hesabının ayrıntılarını girin.

12. Aşağıdakilerden birini yapın:

    - Uygulamanın, komutta belirtilen hesap altında çalışan kullanıcının Kimlik Doğrulama Aracısı'ndaki kimlik doğrulama iletişim kutusuna erişimine izin vermek istiyorsanız **Kimlik doğrulamaya izin ver** onay kutusunu seçin.
    - Uygulamanın, komutta belirtilen hesap altında çalışan kullanıcının Kimlik Doğrulama Aracısı'ndaki kimlik doğrulama iletişim kutusuna erişimini engellemek istiyorsanız **Kimlik doğrulamayı engelle** onay kutusunu seçin.

13. **Kullanıcı hesabı ekle** penceresinde **Tamam**'a tıklayın.

Kimlik Doğrulama Aracısı hesap düzenleme komutunu ekleme

Kimlik Doğrulama Aracısı hesabını düzenlemek amacıyla bir komut eklemek için:

1. **Özellikler: <Kimlik Doğrulama Aracısı hesap yönetimi görevinin adı>** penceresinin **Ayarlar** bölümünde, **Ekle** düğmesinin içerik menüsünü açın ve **Hesap düzenleme komutu** öğesini seçin.

   Kullanıcı hesabını düzenle penceresi açılır.

2. **Kullanıcı hesabını düzenle** penceresindeki **Windows hesabı** alanında, düzenlemek istediğiniz Kimlik Doğrulama Aracısı hesabını oluşturmak için kullanılan Microsoft Windows hesabının adını belirtin. Bunun için hesabın adını elle yazın veya **Seç** düğmesine tıklayın.

3. Microsoft Windows kullanıcı hesabının adını elle girdiyseniz kullanıcı hesabının güvenlik tanımlayıcısını (SID) belirlemek için **İzin ver** düğmesine tıklayın.

   İzin ver düğmesine tıklayarak güvenlik tanımlayıcısını (SID) belirlememeyi tercih ederseniz bilgisayarda görev gerçekleştirildiğinde belirlenir.

   Bir Kimlik Doğrulama Aracısı hesabı düzenleme komutu eklerken Microsoft Windows kullanıcı hesabının SID bilgisinin belirlenmesi, elle girilen Microsoft Windows kullanıcı hesabı adının doğru olmasını sağlamanın rahat bir yoludur. Girilen Microsoft Windows kullanıcı hesabı mevcut değilse veya güvenilir olmayan bir etki alanına aitse Kimlik Doğrulama Aracısı hesaplarını yönetme grup görevi bir hata ile sonlanır.

4. **Kullanıcı adını değiştir** onay kutusunu işaretleyin ve Kaspersky Endpoint Security'nin Microsoft Windows hesabı kullanılarak **Windows hesabı** alanında belirtilen adla oluşturulan tüm Kimlik Doğrulama Aracısı hesaplarının kullanıcı adını, aşağıdaki alanda belirtilen adla değiştirmesini isterseniz Kimlik Doğrulama Aracısı hesabı için yeni bir ad girin.

5. Parola tabanlı kimlik doğrulaması ayarlarını düzenlenebilir hale getirmek için **Parola tabanlı kimlik doğrulaması ayarlarını değiştir** onay kutusunu işaretleyin.

6. Uygulamanın şifrelenmiş sabit sürücülere erişim için kimlik doğrulaması sırasında Kimlik Doğrulama Aracısı hesabının parolasını sormasını istiyorsanız **Parola tabanlı kimlik doğrulamasına izin ver** onay kutusunu işaretleyin.

7. Önceki adımda **Parola tabanlı kimlik doğrulamasına izin ver** onay kutusunu işaretlediyseniz:

   a. **Parola** alanına, Kimlik Doğrulama Aracısı hesabının yeni parolasını girin.

   b. **Parolayı onayla** alanında, önceki adımda girilen parolayı onaylayın.

8. Kaspersky Endpoint Security'nin **Microsoft Windows** hesabı kullanılarak Windows hesabı alanında belirtilen adla oluşturulan tüm Kimlik Doğrulama Aracısı hesaplarının parola değiştirme ayarının değerini, aşağıdaki alanda belirtilen adla değiştirmesini isterseniz **Kimlik doğrulama aracısı'nda kimlik doğrulama üzerine parola değiştirme kuralını düzenle** onay kutusunu işaretleyin.

9. Kimlik Doğrulama Aracısı'nda kimlik doğrulama üzerine parola değiştirme ayarı değerini belirtin.

10. Bir belirteç veya akıllı kartın elektronik sertifikasına dayalı olarak kimlik doğrulaması ayarlarını düzenlenebilir yapmak için **Sertifika tabanlı kimlik doğrulaması ayarlarını değiştir** onay kutusunu seçin.

11. Uygulamanın şifrelenmiş sabit sürücülere erişim için kimlik doğrulaması sırasında kullanıcıdan bilgisayara takılı belirteç veya akıllı kartın parolasını istemesini ayarlamak için **Sertifika tabanlı kimlik doğrulamasına izin ver** onay kutusunu işaretleyin.

12. Önceki adımda **Sertifika tabanlı kimlik doğrulamasına izin ver** onay kutusunu işaretlediyseniz **Gözat** düğmesine tıklayın ve **Sertifika dosyasını seç** penceresinden belirteç veya akıllı kart elektronik sertifikasının dosyasını seçin.

13. **Komut açıklamasını düzenle** onay kutusunu işaretleyin ve Kaspersky Endpoint Security'nin Microsoft Windows hesabı kullanılarak oluşturulan tüm Kimlik Doğrulama Aracısı hesaplarının komut açıklamasını **Windows hesabı** alanında belirtilen adla değiştirmesini isterseniz komut açıklamasını düzenleyin.

14. Kaspersky Endpoint Security'nin Kimlik Doğrulama Aracısı'nda kullanıcının kimlik doğrulama iletişim kutusuna erişim kuralını, Microsoft Windows hesabı kullanılarak **Windows hesabı** alanında belirtilen adla oluşturulan tüm Kimlik Doğrulama Aracısı hesapları için belirtilen değerle değiştirmek isterseniz **Kimlik doğrulama aracısı'nda kimlik doğrulama için erişim kuralını düzenle** onay kutusunu işaretleyin.

15. Kimlik Doğrulama Aracısı'nda kimlik doğrulama iletişim kutusuna erişim kuralını belirtin.

16. **Kullanıcı hesabını düzenle** penceresinde **Tamam**'a tıklayın.

Kimlik Doğrulama Aracısı hesabını silmek için komut ekleme

Kimlik Doğrulama Aracısı hesabını silmek amacıyla bir komut eklemek için:

1. **Özellikler: <Kimlik Doğrulama Aracısı hesap yönetimi görevinin adı>** penceresinin **Ayarlar** bölümünde, **Ekle** düğmesinin içerik menüsünü açın ve **Hesap silme komutu** öğesini seçin.

   Kullanıcı hesabını sil penceresi açılır.

2. **Kullanıcı hesabını sil** penceresindeki **Windows hesabı** alanında, silmek istediğiniz Kimlik Doğrulama Aracısı hesabını oluşturmak için kullanılan Microsoft Windows hesabının adını belirtin. Bunun için hesabın adını elle yazın veya **Seç** düğmesine tıklayın.

3. Microsoft Windows kullanıcı hesabının adını elle girdiyseniz kullanıcı hesabının güvenlik tanımlayıcısını (SID) belirlemek için **İzin ver** düğmesine tıklayın.

   İzin ver düğmesine tıklayarak güvenlik tanımlayıcısını (SID) belirlememeyi tercih ederseniz bilgisayarda görev gerçekleştirildiğinde belirlenir.

   Bir Kimlik Doğrulama Aracısı hesabı silme komutu eklerken Microsoft Windows kullanıcı hesabının SID bilgisinin belirlenmesi, elle girilen Microsoft Windows kullanıcı hesabı adının doğru olmasını sağlamanın rahat bir yoludur. Girilen Microsoft Windows kullanıcı hesabı mevcut değilse veya güvenilir olmayan bir etki alanına aitse Kimlik Doğrulama Aracısı hesaplarını yönetme grup görevi bir hata ile sonlanır.

4. **Kullanıcı hesabını sil** penceresinde **Tamam**'a tıklayın.

Kimlik Doğrulama Aracısı hesabı kimlik bilgilerini sıfırlama

Bu talimatlar, Kaspersky Endpoint Security'nin yüklü olduğu istemci bilgisayarların kullanıcılarına yöneliktir.

Kimlik Doğrulama Aracısı hesabının kullanıcı adı ve parolasını sıfırlamak için:

1. Şifrelenmiş sabit sürücüye sahip bir bilgisayarda işletim sistemi yüklenmeden önce Kimlik Doğrulama Aracısı yüklenir. Kimlik Doğrulama Aracısı arabiriminde, Kimlik Doğrulama Aracısı hesabının kullanıcı adını ve parolasını

sıfırlama işlemini başlatmak için **Parolamı Unuttum** düğmesine tıklayın.

2. Kimlik Doğrulama Aracısı hesabının kullanıcı adı ve parolasını sıfırlamak üzere istek dosyalarını almak için Kimlik Doğrulama Aracısı talimatlarını uygulayın.

3. Bilgisayar adıyla birlikte şirketinizin LAN yöneticisine istek bloklarının içeriğini belirtin.

4. LAN yöneticisi tarafından oluşturulan ve size sağlanan Kimlik Doğrulama Aracısı kullanıcı adı ve parola sıfırlama isteği yanıtının bölümlerini girin.

5. Kimlik Doğrulama Aracısı hesabının yeni parolasını girin ve onaylayın.

   Kimlik Doğrulama Aracısı hesabının kullanıcı adı, Kimlik Doğrulama Aracısı hesabının kullanıcı adı ve parolasını sıfırlama isteği yanıtının bölümleri kullanılarak belirlenir.

Kimlik Doğrulama Aracısı hesabının yeni parolasını girip onayladıktan sonra parola kaydedilir ve şifrelenmiş sabit sürücülere erişim sağlanır.

Kimlik Doğrulama Aracısı hesap kimlik bilgilerini sıfırlama kullanıcı isteğine yanıt verme

Kimlik Doğrulama Aracısı hesabının kullanıcı adı ve parolasını sıfırlama isteği yanıtının kullanıcı bölümlerini oluşturmak ve göndermek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, Kimlik Doğrulama Aracısı hesabının kullanıcı adının ve parolasının sıfırlanmasını talep eden kullanıcının bilgisayarını da içeren yönetim grubunun adının bulunduğu klasörü açın.

3. Çalışma alanında, **Aygıtlar** sekmesini seçin.

4. **Aygıtlar** sekmesinde, Kimlik Doğrulama Aracısı hesabının kullanıcı adının ve parolasının sıfırlanmasını talep eden kullanıcının bilgisayarını seçin ve içerik menüsünü açmak için sağ tıklayın.

5. İçerik menüsünde **Aygıtlara ve verilere çevrimdışı modda erişim ver** seçeneğini seçin.

   Aygıtlara ve verilere çevrimdışı modda erişim ver penceresi açılır.

6. **Aygıtlara ve verilere çevrimdışı modda erişim ver** penceresinde, **Kimlik Doğrulama Aracısı** sekmesini seçin.

7. **Kullanılmakta olan şifreleme modülü** bölümünde şifreleme algoritmasının türünü seçin.

8. **Hesap** açılır listesinde, Kimlik Doğrulama Aracısı hesabı adının ve parolasının kurtarılmasını isteyen kullanıcı için oluşturulan Kimlik Doğrulama Aracısı hesabının adını seçin.

9. **Sabit sürücü** açılır listesinde, erişimi kurtarmanız gereken şifrelenmiş sabit sürücüyü seçin.

10. **Kullanıcı isteği** bölümüne, kullanıcı tarafından belirtilen istek bloklarını girin.

    Kimlik Doğrulama Aracısı hesabının kullanıcı adı ve parolasının kurtarılması kullanıcı isteğine verilen yanıtın bölümleri, **Erişim anahtarı** alanında görüntülenir.

11. Kullanıcı yanıtının blok içeriğini belirtin.

Veri şifreleme ayrıntılarını görüntüleme

Bu bölümde, veri şifrelemenin ayrıntılarını nasıl görüntüleyebileceğiniz açıklanmaktadır.

Şifreleme durumu hakkında

Şifreleme veya şifre çözme devam ederken Kaspersky Endpoint Security, Kaspersky Security Center'ın istemci bilgisayarlarına uygulanan şifreleme parametrelerinin durumu hakkında bilgi aktarır.

Aşağıdaki şifreleme durumu ayarları mümkündür:

- *Tanımlanmamış ilke*. Bilgisayar için bir Kaspersky Security Center ilkesi tanımlanmamıştır.
- *Şifreleme / şifre çözme devam ediyor*. Bilgisayarda veri şifreleme ve/veya şifre çözme devam ediyor.
- *Hata*. Bilgisayarda veri şifreleme ve/veya şifre çözme sırasında bir hata oluştu.
- *Yeniden başlatma gerekli*. Bilgisayarda veri şifrelemeyi veya şifre çözmeyi başlatmak veya tamamlamak için işletim sisteminin yeniden başlatılması gerekir.
- *İlke ile uyumlu*. Bilgisayarda veri şifreleme ve/veya şifre çözme, bilgisayara uygulanan Kaspersky Security Center ilkesinde belirtilen şifreleme ayarları kullanılarak tamamlandı.
- *Kullanıcı tarafından iptal edildi*. Kullanıcı, çıkarılabilir sürücüde dosya şifreleme işlemini onaylamayı reddetti.
- *Desteklenmiyor*. Veri şifreleme işlevi bilgisayarda kullanılamıyor.

Şifreleme durumunu görüntüleme

Bilgisayar verilerinin şifreleme durumunu görüntülemek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, ilgili bilgisayarın ait olduğu yönetim grubu adının bulunduğu klasörü açın.
3. Çalışma alanında, **Aygıtlar** sekmesini seçin.

   Çalışma alanındaki **Aygıtlar** sekmesinde, seçilen yönetim grubundaki bilgisayarların özellikleri görüntülenir.
4. Çalışma alanındaki **Aygıtlar** sekmesinde, kaydırma çubuğunu sonuna kadar sağa sürükleyin.

   Şifreleme durumu sütununda, seçilen yönetim grubundaki bilgisayarların şifreleme durumu görüntülenir. Bu durum; bilgisayarın yerel sürücülerindeki dosyaların şifrelenmesi, bilgisayar sabit sürücülerinin şifrelenmesi ve bilgisayara takılan çıkarılabilir sürücülerin şifrelenmesi ile ilgili bilgilere dayalı olarak oluşur.

Kaspersky Security Center'ın ayrıntılar bölmesindeki şifreleme istatistiklerini görüntüleme

Kaspersky Security Center'ın ayrıntılar bölmesindeki şifreleme durumunu görüntülemek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Konsol ağacında **Yönetim Sunucusu – <Bilgisayar adı>** düğümünü seçin.
3. Yönetim Konsolu ağacının sağındaki çalışma alanında **İstatistikler** sekmesini seçin.
4. Veri şifreleme istatistiklerini içeren ayrıntılar bölmesinin bulunduğu yeni bir sayfa oluşturun. Bunun için:
   a. **İstatistikler** sekmesinde, **Görünümü özelleştir** düğmesine tıklayın.
      Özellikler: İstatistikler penceresi açılır.
   b. **Özellikler: İstatistikler** penceresinde **Ekle**'ye tıklayın.
      Özellikler: Yeni Sayfa penceresi açılır.
   c. **Özellikler: Yeni Sayfa** penceresinin **Genel** bölümünde sayfa adını yazın.
   d. **Ayrıntılar bölmeleri** bölümünde **Ekle** düğmesine tıklayın.
      Yeni ayrıntılar bölmesi penceresi açılır.
   e. **Koruma durumu** grubundaki **Yeni ayrıntılar bölmesi** penceresinde, **Aygıt şifrelemesi** öğesini seçin.
   f. **Tamam**'a tıklayın.
      Özellikler: Şifreleme Denetimi penceresi açılır.
   g. Gerekirse ayrıntılar bölmesinin ayarlarını düzenleyin. Bunun için **Özellikler: Aygıt şifreleme** penceresinin **Görünüm** ve **Aygıtlar** bölümlerini kullanın.
   h. **Tamam**'a tıklayın.
   i. Talimatların d – h adımlarını tekrarlayın; **Yeni ayrıntılar bölmesi** penceresinin **Koruma durumu** bölümünde **Çıkarılabilir sürücülerin şifrelenmesi** öğesini seçin.
      Ayrıntılar bölmeleri, **Özellikler: Yeni sayfa** penceresindeki **Ayrıntılar bölmeleri** listesinde görülür.
   j. **Özellikler: Yeni sayfa** penceresinde, **Tamam**'a tıklayın.
      Önceki adımda oluşturulan ayrıntılar bölmelerinin olduğu sayfanın adı, **Özellikler: İstatistikler** penceresinin **Sayfalar** listesinde görülür.
   k. **Özellikler: İstatistikler** penceresinde **Kapat**'a tıklayın.
5. **İstatistikler** sekmesinde,talimatların önceki adımlarında oluşturulan sayfayı açın.

Bilgisayarların ve çıkarılabilir sürücülerin şifreleme durumunu görüntüleyen ayrıntılar bölmeleri açılır.

Yerel bilgisayar sürücülerinde dosya şifreleme hatalarını görüntüleme

Yerel bilgisayar sürücülerinde dosya şifreleme hatalarını görüntülemek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, dosya şifreleme hatalarını görüntülemek istediğiniz istemci bilgisayarı içeren yönetim grubunun adının bulunduğu klasörü açın.
3. Çalışma alanında, **Aygıtlar** sekmesini seçin.
4. **Aygıtlar** sekmesinde, listeden bilgisayar adını seçin ve sağ tıklayarak içerik menüsünü açın.
5. Aşağıdakilerden birini yapın:
   - Bilgisayarın içerik menüsünden **Koruma** öğesini seçin.
   - Bilgisayarın içerik menüsünden **Özellikler** öğesini seçin. **Özellikler: <bilgisayar adı>** penceresinden **Koruma** bölümünü seçin.
6. **Özellikler: <bilgisayar adı>** penceresinin **Koruma** bölümünde, **Veri şifreleme hatalarının listesini görüntüle** bağlantısına tıklayarak **Veri şifreleme hataları** penceresini açın.

   Bu pencerede yerel bilgisayar sürücülerindeki dosya şifreleme hatalarının ayrıntıları yer alır. Bir hata düzeltildiğinde Kaspersky Security Center, hata ayrıntılarını **Veri şifreleme hataları** penceresinden kaldırır.

Veri şifreleme raporunu görüntüleme

Veri şifreleme raporunu görüntülemek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacının **Yönetim Sunucusu** düğümünde **Raporlar** sekmesini seçin.
3. **Rapor şablonu oluştur** düğmesine tıklayın.

   Rapor Şablonu Sihirbazı başlatılır.
4. Rapor Şablonu Sihirbazı talimatlarını uygulayın. **Diğer** bölümünde **Rapor şablonu türünü seçin** penceresinde aşağıdaki öğelerden birini seçin:
   - **Yönetilen aygıt şifreleme durumu raporu**.
   - **Depolanan aygıt veri şifreleme raporu**.
   - **Şifreleme hataları raporu**.
   - **Şifrelenmiş dosyalara erişimi engelleme raporu**.

   Yeni Rapor Şablonu Sihirbazı ile işlemi tamamladıktan sonra yeni rapor şablonu **Raporlar** sekmesindeki tabloda görünür.
5. Talimatların önceki adımlarında oluşturulan rapor şablonunu seçin.

Rapor üretme işlemi başlar. Rapor yeni bir pencerede görüntülenir.

Sınırlı dosya şifreleme işlevine sahip şifreli dosyaları yönetme

Kaspersky Security Center ilkesi uygulandığında ve dosyalar şifrelendiğinde Kaspersky Endpoint Security, şifrelenmiş dosyalara doğrudan erişim için gerekli olan bir erişim anahtarı alır. Bu erişim anahtarını kullanarak, dosyaların şifrelenmesi sırasında etkin olan herhangi bir Windows hesabı altında çalışan bir kullanıcı şifrelenmiş dosyalara doğrudan erişim sağlayabilir. Dosya şifreleme sırasında etkin olmayan Windows hesapları altında çalışan kullanıcılar, şifrelenmiş dosyalara erişim sağlamak amacıyla Kaspersky Security Center'a bağlanmalıdır.

Şifreli dosyalar aşağıdaki durumlarda erişilebilir olmayabilir:

- Kullanıcının bilgisayarı şifreleme anahtarlarını depolar, ancak bunları yönetmek için Kaspersky Security Center ile bağlantı yoktur. Bu durumda kullanıcının, LAN yöneticisinden şifrelenmiş dosyalara erişim talep etmesi gerekir.

  Kaspersky Security Center'a erişim yosa şunu yapmanız gerekir:

  - bilgisayarın sabit disklerindeki şifrelenmiş dosyalara erişim için bir erişim anahtarı isteyin;
  - çıkarılabilir sürücülerde saklanan şifrelenmiş dosyalara erişim için kullanıcının her bir çıkarılabilir sürücülerdeki şifrelenmiş dosyalar için ayrı erişim anahtarları talep etmesi gerekir.

- Şifreleme bileşenleri kullanıcının bilgisayarından silinir. Bu durumda, kullanıcı yerel ve çıkarılabilir disklerdeki şifrelenmiş dosyaları açabilir, ancak bu dosyaların içeriği şifreli görünür.

  Kullanıcı, şifrelenmiş dosyalarla aşağıdaki durumlarda çalışabilir:

  - Dosyalar Kaspersky Endpoint Security yüklü bir bilgisayarda oluşturulmuş şifreli paketlerin içindedir.
  - Dosyalar taşınabilir moda izin verilmiş çıkarılabilir sürücülerde saklanmaktadır.

Kaspersky Security Center'a bağlantı olmadan şifrelenmiş dosyalara erişim

Bu talimatlar, Kaspersky Endpoint Security'nin yüklü olduğu istemci bilgisayarların kullanıcılarına yöneliktir.

Kaspersky Security Center'a bağlantı olmadan şifrelenmiş dosyalara erişim sağlamak için:

1. İhtiyacınız olan şifrelenmiş dosyaya erişim sağlamaya çalışın.

   Bilgisayarın yerel sürücüsünde depolanan bir dosyaya erişim sağlamaya çalıştığınızda Kaspersky Security Center bağlantısı yoksa Kaspersky Endpoint Security, yerel bilgisayar sürücülerinde depolanan tüm şifrelenmiş dosyalara erişim talebi ile bir dosya oluşturur. Çıkarılabilir sürücü depolanan bir dosyaya erişim sağlamaya çalıştığınızda Kaspersky Security Center, çıkarılabilir sürücüde depolanan tüm şifrelenmiş dosyalara erişim talebi ile bir dosya oluşturur. **Dosya erişimi engellendi** penceresi açılır.

2. Şifrelenmiş dosyalara erişim talebini içeren dosyayı yerel alan ağı yöneticisine gönderin. Bunun için aşağıdakilerden birini gerçekleştirin:

   - Şifrelenmiş dosyalara erişim talep eden dosyayı yerel alan ağı yöneticisine e-posta ile göndermek için **E-posta ile gönder** düğmesine tıklayın.
   - Şifrelenmiş dosyalara erişim talep eden dosyayı kaydetmek ve başka bir yöntemle LAN yöneticisine göndermek için **Kaydet** düğmesine tıklayın.

3. Yerel alan ağı yöneticisi tarafından oluşturulan ve size sağlanan şifrelenmiş dosyalara erişim anahtar dosyasını elde edin.

4. Şifrelenmiş dosyalara erişim anahtarını aşağıdaki yöntemlerden biriyle etkinleştirin:

   - Herhangi bir dosya yöneticisinde, şifrelenmiş dosyalara erişim anahtarı dosyasını seçin. Çift tıklayarak açın.
   - Aşağıdakileri uygulayın:

     a. Kaspersky Endpoint Security'nin ana penceresini açın.

     b. düğmesine tıklayın.

     Olaylar penceresi açılır.

     c. **Dosya ve aygıtlara erişim durumu** sekmesini seçin.

     Bu sekmede şifrelenmiş dosyalara erişim taleplerinin tamamının bir listesi görüntülenir.

     d. Şifrelenmiş dosyalara erişmek için anahtar dosyasını aldığınız isteği seçin.

     e. Şifrelenmiş dosyalara erişim için sağlanan anahtar dosyasını yüklemek amacıyla **Gözat**'a tıklayın.

     Standart **Erişim anahtarı dosyasını seç** Microsoft Windows iletişim kutusu açılır.

     f. Microsoft Windows'un standart **Erişim anahtarı dosyasını seç** penceresinde, .kesdr uzantısına ve erişim isteği dosyasının adıyla eşleşen ada sahip yönetici tarafından sağlanan dosyayı seçin.

     g. **Aç** düğmesine tıklayın.

     h. **Olaylar** penceresinde **Tamam**'a tıklayın.

Bilgisayarın yerel sürücüsünde depolanan bir dosyaya erişim denemesi sırasında şifrelenmiş dosyalara erişim talebini içeren bir dosya oluşturulursa Kaspersky Endpoint Security, yerel bilgisayar sürücülerinde depolanan tüm şifrelenmiş dosyalara erişim sunar. Çıkarılabilir sürücüde depolanan bir dosyaya erişim denemesi sırasında şifrelenmiş dosyalara erişim için bir erişim isteği dosyası oluşturulursa Kaspersky Endpoint Security, çıkarılabilir sürücüde depolanan tüm şifrelenmiş dosyalara erişim sunar. Diğer çıkarılabilir sürücülerde saklanan şifrelenmiş dosyalara erişim amacıyla her bir çıkarılabilir sürücü için ayrı bir erişim anahtarları dosyası elde etmeniz gerekir.

Kaspersky Security Center'a bağlantı olmadan şifrelenmiş dosyalara kullanıcı erişimi sağlama

Kaspersky Security Center'a bağlantı olmadan şifrelenmiş dosyalara kullanıcı erişimi sağlamak için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, şifrelenmiş dosyalara erişim talep eden kullanıcının bilgisayarının ait olduğu yönetim grubu adının bulunduğu klasörü açın.

3. Çalışma alanında, **Aygıtlar** sekmesini seçin.

4. **Aygıtlar** sekmesinde, şifrelenmiş dosyalara erişim talep eden kullanıcının bilgisayarını seçin ve içerik menüsünü görüntülemek için sağ tıklayın.

5. İçerik menüsünde **Aygıtlara ve verilere çevrimdışı modda erişim ver** seçeneğini seçin.

   Aygıtlara ve verilere çevrimdışı modda erişim ver penceresi açılır.

6. **Aygıtlara ve verilere çevrimdışı modda erişim ver** penceresinde, **Şifreleme** sekmesini seçin.

7. **Şifreleme** sekmesinde, **Gözat** düğmesine tıklayın.

   Standart **İstek dosyasını seç** Microsoft Windows iletişim kutusu açılır.

8. **İstek dosyasını seç** penceresinde, kullanıcıdan alınan istek dosyasının yolunu belirtin ve **Aç** düğmesine tıklayın.

   Kaspersky Security Center, şifrelenmiş dosyalara erişim için bir anahtar dosyası oluşturur. Kullanıcı isteğinin ayrıntıları **Şifreleme** sekmesinde görüntülenir.

9. Aşağıdakilerden birini yapın:

   - Oluşturulan erişim anahtarı dosyasını kullanıcıya e-posta ile göndermek için **E-posta ile gönder** düğmesine tıklayın.

   - Şifrelenmiş dosyalara erişim anahtarı dosyasını kaydetmek ve farklı bir yöntemle kullanıcıya göndermek için **Kaydet** düğmesine tıklayın.

Şifrelenmiş dosya erişim mesajlarının şablonlarını düzenleme

Şifrelenmiş dosya erişim mesajlarının şablonlarını düzenlemek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, şifrelenmiş dosya erişim isteği mesajlarının şablonlarını düzenlemek istediğiniz yönetim grubunun adını içeren klasörü açın.

3. Çalışma alanında, **İlkeler** sekmesini seçin.

4. Gereken ilkeyi seçin.

5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:

   - İlkenin içerik menüsünde **Özellikler**'i seçin.

   - Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.

6. **Veri Şifreleme** bölümünde, **Ortak şifreleme ayarları** alt bölümünü seçin.

7. **Şablonlar** bölümünde, **Şablonlar** düğmesine tıklayın.

   Şablonlar penceresi açılır.

8. Aşağıdakileri uygulayın:

   - Kullanıcı mesajı şablonunu düzenlemek isterseniz **Kullanıcı mesajı** sekmesini seçin. Şifreli dosyalara erişim için bilgisayarda anahtar bulunmadığında şifreli bir dosyaya kullanıcı erişim sağlamaya çalıştığında **Dosya erişimi reddedildi** penceresi açılır. **Dosya erişimi reddedildi** penceresinde **E-posta ile gönder** düğmesine tıklandığında otomatik olarak bir kullanıcı mesajı oluşturulur. Bu mesaj, şifrelenmiş dosyalara erişim talep eden dosya ile birlikte kurumsal LAN yöneticisine gönderilir.

   - Yönetici mesajı şablonunu düzenlemek isterseniz **Yönetici mesajı** sekmesini seçin. Bu mesaj, **Şifrelenmiş dosyalara erişim ver** penceresinde **E-posta ile gönder** düğmesine tıklandığında otomatik olarak oluşturulur ve kullanıcıya şifrelenmiş dosyalara erişim tanındıktan sonra kullanıcıya gönderilir.

9. Mesaj şablonlarını düzenleyin.

   Varsayılan düğmesini ve **Değişken** açılır listesini kullanabilirsiniz.

10. **Tamam**'a tıklayın.

11. Değişikliklerinizi kaydetmek için **Özellikler: <İlke adı>** penceresinde **Tamam**'a tıklayın.

Şifrelenmiş aygıtlara erişim olmadığında şifrelenmiş aygıtlarla çalışma

Şifrelenmiş aygıtlara erişim sağlama

Bir kullanıcının şifrelenmiş aygıtlara erişim istemesi aşağıdaki durumlarda gerekebilir:

- Sabit sürücü başka bir bilgisayarda şifrelenmiş.
- Bir aygıt için şifreleme anahtarı bilgisayarda değil (örnek olarak, bilgisayardaki şifrelenmiş çıkarılabilir sürücüye ilk erişim denemesi üzerinde) ve bilgisayar Kaspersky Security Center'a bağlı değil.

  Kullanıcı erişim anahtarını şifrelenmiş aygıta uyguladıktan sonra, Kaspersky Security Center'a bağlantı yoksa bile Kaspersky Endpoint Security şifreleme anahtarını kullanıcının bilgisayarına kaydeder ve sonraki erişim girişimleri üzerine bu aygıta erişime izin verir.

Şifrelenmiş aygıtlara erişim aşağıdaki şekilde elde edilebilir:

1. Kullanıcı kesdc uzantılı bir erişim isteği dosyasını oluşturmak için Kaspersky Endpoint Security uygulamasının arayüzünü kullanır ve dosyayı kurumsal LAN yöneticisine gönderir.
2. Yönetici kesdr uzantılı bir erişim anahtarı dosyasını oluşturmak için Kaspersky Security Center Yönetim Konsolu'nu kullanır ve dosyayı kullanıcıya gönderir.
3. Kullanıcı erişim anahtarını uygular.

Şifrelenmiş cihazlarda verilerin geri yüklenmesi

Bir kullanıcı şifrelenmiş aygıtlarla çalışmak için Şifrelenmiş Aygıt Geri Yükleme Yardımcı Programı (buradan sonra Geri Yükleme Yardımcı Programı olarak anılacaktır) uygulamasını kullanabilir. Bu, aşağıdaki durumlarda gerekebilir:

- Erişim elde etmek için bir erişim anahtarı kullanma prosedürü başarısız oldu.
- Şifreli aygıta sahip bilgisayarda şifreleme bileşenleri yüklü değil.

Geri Yükleme Yardımcı Programı kullanılarak şifreli aygıtlara erişimi geri yüklemek için gereken veriler bir süredir kullanıcı bilgisayarının belleğinde şifrelenmemiş biçimde bulunuyor. Bu tür verilere yetkisiz erişim riskini azaltmak için, şifrelenmiş aygıtlara erişimi güvenilir bilgisayarlarda geri yüklemeniz önerilir.

Şifrelenmiş aygıtlardaki veriler aşağıdaki şekilde geri yüklenebilir:

1. Kullanıcı fdertc uzantılı bir istek erişim dosyası oluşturmak için Geri Yükleme Yardımcı Programını ve dosyayı kurumsal LAN yöneticisine gönderir.

2. Yönetici fdertr uzantılı bir erişim anahtarı dosyasını oluşturmak için Kaspersky Security Center Yönetim Konsolu'nu kullanır ve dosyayı kullanıcıya gönderir.

3. Kullanıcı erişim anahtarını uygular.

Şifreli sistem sabit disklerindeki verileri geri yüklemek için kullanıcı, Kimlik Doğrulama Aracısı hesap kimlik bilgilerini Geri Yükleme Yardımcı Programında da belirleyebilir. Kimlik Doğrulama Aracısı hesabının meta verileri bozulmuşsa, kullanıcı geri yükleme prosedürünü bir istek erişim dosyası kullanarak tamamlamalıdır.

Şifrelenmiş aygıtlarda veriler geri yüklenmeden önce, bu işlemin gerçekleştirileceği bilgisayarda Kaspersky Security Center şifreleme ilkesinin iptal edilmesi önerilir. Bu şekilde sürücünün yeniden şifrelenmesi önlenir.

Uygulama arayüzü üzerinden şifrelenmiş aygıtlara erişim sağlama

Bu talimatlar, Kaspersky Endpoint Security'nin yüklü olduğu istemci bilgisayarların kullanıcılarına yöneliktir.

Uygulama arayüzü üzerinden şifrelenmiş aygıtlara erişim sağlamak için:

1. İhtiyacınız olan şifrelenmiş dosyaya erişim sağlamayı deneyin.

   Verilere erişim engellendi penceresi açılır.

2. Şifrelenmiş aygıt için kesdc uzantılı istek erişim dosyasını kurumsal LAN yöneticisine gönderin. Bunun için aşağıdakilerden birini gerçekleştirin:

   - Şifrelenmiş aygıt için oluşturulan istek erişim dosyasını e-postayla kurumsal LAN yöneticisine göndermek için, **E-postayla gönder** düğmesine tıklayın.
   - Şifrelenmiş dosyalara erişim talep eden dosyayı kaydetmek ve başka bir yöntemle LAN yöneticisine göndermek için **Kaydet** düğmesine tıklayın.

   İstek erişim dosyasını kaydetmeden veya kurumsal LAN yöneticisine göndermeden **Verilere erişim engellendi** penceresini kapattıysanız, bunu herhangi bir zamanda **Dosyalara ve aygıtlara erişim durumu** sekmesindeki **Olaylar** penceresinden yapabilirsiniz. Bu pencereyi açmak için ana uygulama penceresinde düğmesine tıklayın.

3. Kurumsal LAN yöneticisi tarafından oluşturulan ve size gönderilen şifrelenmiş aygıt erişim anahtarı dosyasını alın ve kaydedin.

4. Şifrelenmiş aygıta erişmek için erişim anahtarını uygulamak için aşağıdaki yöntemlerden birini kullanın:

   - Herhangi bir dosya yöneticisinde şifrelenmiş aygıt erişim anahtarı dosyasını bulun ve açmak için çift tıklayın.
   - Aşağıdakileri uygulayın:

     a. Kaspersky Endpoint Security'nin ana penceresini açın.

     b. **Olaylar** penceresini açmak için düğmesine tıklayın.

     c. **Dosya ve aygıtlara erişim durumu** sekmesini seçin.

Bu sekmede, şifrelenmiş dosyalara ve cihazlara erişim taleplerinin tamamının bir listesi görüntülenir.

d. Şifrelenmiş aygıta erişmek için erişim anahtar dosyasını aldığınız isteği seçin.

e. Şifrelenmiş aygıta erişim için sağlanan anahtar dosyasını yüklemek amacıyla **Gözat**'a tıklayın.

Standart **Erişim anahtarı dosyasını seç** Microsoft Windows iletişim kutusu açılır.

f. Microsoft Windows'un standart **Erişim anahtarı dosyasını seç** penceresinde, kesdr uzantılı ve şifrelenmiş çıkarılabilir sürücünün erişim isteği dosyasının adıyla eşleşen ada sahip yönetici tarafından sağlanan dosyayı seçin.

g. **Aç** düğmesine tıklayın.

h. **Dosya ve aygıtlara erişim durumu** penceresinde **Tamam**'a tıklayın.

Sonuç olarak Kaspersky Endpoint Security, şifrelenmiş aygıta erişim izni verir.

Şifrelenmiş aygıtlara kullanıcı erişimi sağlama

Şifrelenmiş bir aygıta kullanıcı erişimi vermek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, şifrelenen sürücüye erişim isteyen kullanıcının bilgisayarını içeren yönetim grubunun adının bulunduğu klasörü açın.
3. Çalışma alanında, **Aygıtlar** sekmesini seçin.
4. **Aygıtlar** sekmesinde, şifrelenmiş dosyalara erişim talep eden kullanıcının bilgisayarını seçin ve içerik menüsünü görüntülemek için sağ tıklayın.
5. İçerik menüsünde **Aygıtlara ve verilere çevrimdışı modda erişim ver** seçeneğini seçin.

   Aygıtlara ve verilere çevrimdışı modda erişim ver penceresi açılır.
6. **Aygıtlara ve verilere çevrimdışı modda erişim ver** penceresinde, **Şifreleme** sekmesini seçin.
7. **Şifreleme** sekmesinde, **Gözat** düğmesine tıklayın.

   Standart **İstek dosyasını seç** Microsoft Windows iletişim kutusu açılır.
8. **İstek erişim dosyayı seç** penceresinde, kullanıcıdan aldığınız kesdc uzantılı istek dosyasının yolunu belirtin.
9. **Aç** düğmesine tıklayın.

   Kaspersky Security Center, kesdr uzantılı bir şifrelenmiş aygıt erişim anahtarı dosyası üretir. Kullanıcı isteğinin ayrıntıları **Şifreleme** sekmesinde görüntülenir.
10. Aşağıdakilerden birini yapın:

    - Oluşturulan erişim anahtarı dosyasını kullanıcıya e-posta ile göndermek için **E-posta ile gönder** düğmesine tıklayın.
    - Şifrelenmiş aygıtın erişim anahtarı dosyasını kaydetmek ve başka bir yöntemle kullanıcıya göndermek için **Kaydet** düğmesine tıklayın.

Kullanıcıya, BitLocker ile şifrelenmiş sabit sürücülerin kurtarma anahtarını sağlama

Bir kullanıcıya BitLocker kullanılarak şifrelenen bir sistem sabit sürücüsü kurtarma anahtarı göndermek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, şifrelenen sürücüye erişim isteyen kullanıcının bilgisayarını içeren yönetim grubunun adının bulunduğu klasörü açın.
3. Çalışma alanında, **Aygıtlar** sekmesini seçin.
4. **Aygıtlar** sekmesinde şifrelenen sürücüye erişim isteyen kullanıcıya ait bilgisayarı seçin.
5. Sağ tıklayarak içerik menüsünü açın ve **Aygıtlara ve verilere çevrimdışı modda erişim ver**'i seçin.

   Aygıtlara ve verilere çevrimdışı modda erişim ver penceresi açılır.
6. **Aygıtlara ve verilere çevrimdışı modda erişim ver** penceresinde **BitLocker-korumalı bir sistem sürücüsüne erişim** sekmesini seçin.
7. Kullanıcıya BitLocker parola giriş penceresinde belirtilen kurtarma anahtarı kimliğini sorun ve **Kurtarma anahtarı kimliği** alanındaki kimlik ile karşılaştırın.

   Kimlikler eşleşmezse bu anahtar belirtilen sistem sürücüsüne erişimin geri yüklenmesi için geçerli değildir. Seçilen bilgisayarın adının kullanıcı bilgisayarının adı ile eşleştiğinden emin olun.
8. Kullanıcıya **Kurtarma anahtarı** alanında gösterilen anahtarı gönderin.

Bir kullanıcıya BitLocker kullanılarak şifrelenen bir sistem dışı sabit sürücü kurtarma anahtarı göndermek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacında, **Diğer → Şifreleme ve veri koruma → Şifrelenmiş aygıtlar** klasörünü seçin.

   Çalışma alanında şifrelenmiş aygıtların bir listesi görüntülenir.
3. Çalışma alanında erişimin geri yüklenmesine gerek duyduğunuz şifrelenmiş aygıtı seçin.
4. Sağ tıklayarak içerik menüsünü açın ve **Şifrelenmiş aygıtın erişim anahtarını al** seçeneğini seçin.

   BitLocker ile şifrelenen bir sürücüye erişimin geri yüklenmesi penceresi açılır.
5. Kullanıcıya BitLocker parola giriş penceresinde belirtilen kurtarma anahtarı kimliğini sorun ve **Kurtarma anahtarı kimliği** alanındaki kimlik ile karşılaştırın.

   Kimlikler eşleşmezse bu anahtar belirtilen sürücüye erişimin geri yüklenmesi için geçerli değildir. Seçilen bilgisayarın adının kullanıcı bilgisayarının adı ile eşleştiğinden emin olun.
6. Kullanıcıya **Kurtarma anahtarı** alanında gösterilen anahtarı gönderin.

Geri Yükleme Yardımcı Programının yürütülebilir dosyasını oluşturma

Bu talimatlar, Kaspersky Endpoint Security'nin yüklü olduğu istemci bilgisayarların kullanıcılarına yöneliktir.

Geri Yükleme Yardımcı Programı'nın yürütülebilir dosyasını oluşturmak için:

1. Ana uygulama penceresini açın.
2. Ana uygulama penceresinin sol alt köşesindeki düğmesine tıklayarak **Destek** penceresini açın.
3. **Destek** penceresinde **Şifrelenmiş aygıtı geri yükle** düğmesine tıklayın.

   Şifreli Cihaz Geri Yükleme Yardımcı Programı başlatılır.
4. Geri Yükleme Yardımcı Programı penceresinde **Bağımsız Geri Yükleme Yardımcı Uygulaması Oluştur** düğmesine tıklayın.

   Bağımsız Geri Yükleme Yardımcı Programı Oluşturma penceresi açılır.
5. **Kaydetme yeri** penceresinde Geri Yükleme Yardımcı Programı'nın yürütülebilir dosyasının kaydedileceği klasör yolunu elle girin veya **Gözat** düğmesine tıklayın.
6. **Bağımsız Geri Yükleme Yardımcı Programı Oluşturma** penceresinde **Tamam**'a tıklayın.

   Geri Yükleme Yardımcı Programı'nın yürütülebilir dosyası (fdert.exe) seçilen klasöre kaydedilir.

Geri Yükleme Yardımcı Programını kullanarak şifreli aygıtlara erişimi geri yükleme

Bu talimatlar, Kaspersky Endpoint Security'nin yüklü olduğu istemci bilgisayarların kullanıcılarına yöneliktir.

Geri Yükleme Yardımcı Programını kullanarak şifreli aygıtlara erişimi geri yüklemek için:

1. Geri Yükleme Yardımcı Programını aşağıdaki yollardan birini kullanarak çalıştırın:

   - Kaspersky Endpoint Security'nin ana penceresinde düğmesine tıklayarak **Destek** penceresini açın ve **Şifrelenmiş aygıtı geri yükle** düğmesine tıklayın.
   - Geri Yükleme Yardımcı Programının fdert.exe yürütülebilir dosyasını çalıştırın. Bu dosya, Kaspersky Endpoint Security tarafından oluşturulur.
2. Geri Yükleme Yardımcı Programını penceresinde **Aygıtı seçin** açılır listesinden erişimi geri yüklemek istediğiniz bir şifrelenmiş aygıt seçin.
3. **Tara** düğmesine tıklandığında yardımcı program aygıtta hangi eylemlerin gerçekleştirilmesi gerektiğini; kilitsiz veya şifresiz olup olmaması gerektiğini belirler.

Bilgisayarın Kaspersky Endpoint Security şifreleme işlevselliğine erişimi varsa, Geri Yükleme Yardımcı Programı aygıtın kilidini açmanızı ister. Aygıtın kilidinin açılması şifresini çözmese de, kilidinin açılmasından dolayı aygıt doğrudan erişilebilir hale gelir. Bilgisayarın Kaspersky Endpoint Security şifreleme işlevselliğine erişimi yoksa Geri Yükleme Yardımcı Programı aygıtın şifresini çözmenizi ister.

4. Şifrelenmiş sistem sabit sürücüsünün tanılaması, aygıtın ana önyükleme kaydı (MBR) ile ilgili sorunlar hakkında bir mesaj verdiyse **MBR'yi düzelt** düğmesine tıklayın.

   Cihazın ana önyükleme kaydının düzeltilmesi, cihaz kilidini açmak veya şifresini çözmek için gereken bilgileri toplama işlemini hızlandırabilir.

5. Teşhis sonuçlarına göre **Kilit aç** veya **Şifre çöz** düğmesine tıklayın.

   Aygıt kilit açma ayarları veya **Aygıt şifre çözme ayarları** penceresi açılır.

6. Bir Kimlik Doğrulama Aracısı hesabı kullanarak verileri geri yüklemek isterseniz:

   a. **Kimlik Doğrulama Aracısı hesabı ayarlarını kullan** seçeneğini seçin.

   b. **Ad** ve **Parola** alanlarında Kimlik Doğrulama Aracısı hesap kimlik bilgilerini belirleyin.

   Bu yöntem, yalnızca bir sistem sabit sürücüsündeki verileri geri yüklerken mümkündür. Sistem sabit sürücüsü bozuksa ve Kimlin Doğrulama Aracısı hesabı verileri kaybolduysa, şifrelenmiş bir aygıttaki verileri geri yüklemek için kurumsal LAN yöneticinizden bir erişim anahtarı edinmelisiniz.

7. Verileri geri yüklemek için bir erişim anahtarı kullanmak istiyorsanız:

   a. **Ayıt erişim anahtarını elle belirle** seçeneğini seçin.

   b. **Erişim anahtarını al** düğmesine tıklayın.

   c. **Aygıt erişim anahtarı al** penceresi açılır.

   d. **Kaydet** düğmesine tıklayın ve fdertc uzantılı istek erişim dosyasını kaydedeceğiniz klasörü seçin.

   e. İstek erişim dosyasını kurumsal LAN yöneticisine gönderin.

   > Erişim anahtarını almayana kadar **Aygıt erişim anahtarı al** penceresini kapatmayın. Bu pencere tekrar açıldığında, yönetici tarafından daha önce oluşturulmuş olan erişim anahtarını uygulayamazsınız.

   f. Kurumsal LAN yöneticisi tarafından oluşturulan ve size sağlanan erişim anahtarı dosyasını alın ve kaydedin.

   g. Açılan pencereden **Yükle** düğmesine tıklayın ve fdertr uzantılı erişim anahtarı dosyasını seçin.

8. Bir aygıtın şifresini çözüyorsanız, **Cihaz şifre çözme ayarları** penceresindeki diğer şifre çözme ayarların belirtmelisiniz. Bunun için:

   - Şifresini çözmek için alanı belirtin:
     - Tüm aygıtın şifresini çözmek istiyorsanız, **Tüm aygıtın şifresini çöz** seçeneğini seçin.
     - Bir aygıttaki verilerin bir kısmının şifresini çözmek istiyorsanız **Bağımsız aygıt alanlarının şifresini çöz** seçeneğini seçin ve şifresi çözülecek alanın sınırlarını belirlemek için **Başlat** ve **Bitir** alanlarını kullanın.
   - Şifresi çözülmüş verileri yazmak için konumu seçin:

- Orijinal aygıttaki verilerin şifresi çözülmüş verilerle yeniden yazılmasını istiyorsanız **Şifre çözüldükten sonra verileri dosyaya kaydet** onay kutsununun işaretini kaldırın.

- Şifres çözülmüş verilerin orijinal şifreli verilerden ayrı olarak kaydedilmesini istiyorsanız **Şifre çözüldükten sonra verileri dosyaya kaydet** onay kutusunu seçin ve verileri kaydetmek için yolu belirtmek üzere **Gözat** düğmesini kullanın.

9. **Tamam**'a tıklayın.

Aygıt kilit açma / şifre çözme işlemi başlar.

Şifrelenmiş aygıtlardaki verileri geri yüklemek için bir kullanıcı isteğine yanıtlama

Şifrelenmiş aygıta erişim amacıyla bir anahtar dosyası oluşturmak ve kullanıcıya sağlamak için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacında, **Diğer → Şifreleme ve veri koruma → Şifrelenmiş aygıtlar** klasörünü seçin.

3. Çalışma alanında, bir erişim anahtarı oluşturmak istediğiniz şifreli aygıtı seçin ve aygıt içerik menüsünden **Belirli şifreli aygıt için erişim anahtarı al** öğesini seçin.

   İstek erişim dosyasının hangi bilgisayar için üretildiğinden emin değilseniz, Yönetici Konsolu ağacından **Diğer → Şifrelenmiş veri koruma** klasörünü seçin ve çalışma alanında **Cihaz şifreleme anahtarını al** bağlantısını tıklayın.

   Aygıta erişime izin ver penceresi açılır.

4. Kullanılan şifreleme algoritmasını seçin. Bunun için aşağıdaki seçeneklerden birini seçin:

   - **AES256**, Kaspersky Endpoint Security cihazın şifrelendiği bilgisayardaki aes256 klasöründe bulunan bir dağıtım paketinden yüklenmişse;

   - **AES56**, Kaspersky Endpoint Security cihazın şifrelendiği bilgisayardaki aes56 klasöründe bulunan bir dağıtım paketinden yüklenmişse;

5. **Gözat** düğmesine tıklayın.

   Standart **İstek dosyasını seç** Microsoft Windows iletişim kutusu açılır.

6. **İstek erişim dosyayı seç** penceresinde, kullanıcıdan aldığınız fdertc uzantılı istek dosyasının yolunu belirtin.

7. **Aç** düğmesine tıklayın.

   Kaspersky Security Center şifrelenmiş cihaza erişim için fdertr uzantılı bir erişim anahtarı dosyası üretir.

8. Aşağıdakilerden birini yapın:

   - Oluşturulan erişim anahtarı dosyasını kullanıcıya e-posta ile göndermek için **E-posta ile gönder** düğmesine tıklayın.

   - Şifrelenmiş aygıtın erişim anahtarı dosyasını kaydetmek ve başka bir yöntemle kullanıcıya göndermek için **Kaydet** düğmesine tıklayın.

İşletim sistemi hatasının ardından şifrelenmiş verilere yeniden erişim sağlama

İşletim sistemi hatasının ardından verilere erişimi sadece dosya düzeyinde şifreleme (FLE) için geri yükleyebilirsiniz. Tam disk şifreleme (FDE) kullanılıyorsa verilere erişimi geri yükleyemezsiniz.

İşletim sistemi hatasının ardından şifrelenmiş verilere erişimi geri yüklemek için:

1. Sabit sürücüyü biçimlendirmeden işletim sistemini yeniden yükleyin.
2. Kaspersky Endpoint Security'yi yükleyin.
3. Verilerin şifrelenmesi sırasında, bilgisayar ile bilgisayarı denetleyen Kaspersky Security Center Yönetim Sunucusu arasında bir bağlantı kurun.

Şifrelenmiş verilere erişim, işletim sistemi hatasından önce uygulanan aynı koşullarda sağlanır.

İşletim sistemi kurtarma diskini oluşturma

İşletim sistemi kurtarma diski, şifrelenmiş bir sabit sürücüye herhangi bir nedenle erişilemediğinde ve işletim sistemi yüklenemediğinde kullanışlı olabilir.

Kurtarma diskini kullanarak Windows işletim sisteminin bir görüntüsünü yükleyebilir ve işletim sistemi görüntüsünde bulunan Geri Yükleme Yardımcı Programını kullanarak şifrelenmiş sabit sürücüye erişimi geri yükleyebilirsiniz.

Bir işletim sistemi kurtarma diski oluşturmak için:

1. Şifreli Aygıt Geri Yükleme Yardımcı Program için bir yürütülebilir dosyası oluşturun.
2. Windows önyükleme öncesi ortamının özel bir görüntüsünü oluşturun. Windows önyükleme öncesi ortamının özel bir görüntüsünü oluştururken, görüntüye Geri yükleme Yardımcı Programı'nın yürütülebilir dosyasını ekleyin.
3. Windows önyükleme ortamının özel görüntüsünü, CD veya çıkarılabilir sürücü gibi önyüklenebilir bir ortama kaydedin.

   Windows önyükleme öncesi ortamının özel bir görüntüsünü oluşturma konusunda Microsoft yardım dosyalarına başvurun (örn. Microsoft TechNet kaynağı).

Ağ Koruması

Bu bölümde ağ trafiğini izleme hakkında bilgiler ve izlenen ağ bağlantı noktalarının ayarlarını yapılandırma talimatları bulunmaktadır.

Ağ Koruması Hakkında

Kaspersky Endpoint Security'nin çalışması sırasında, Posta Koruması, İnternet Koruması ve IM Koruması belirli iletişim kurallarından aktarılan ve bilgisayarınızda TCP ve UDP gibi belirli açık bağlantı noktalarından iletilen veri akışlarını izler. Örneğin Posta Koruması, SMTP üzerinden aktarılan verileri tararken, İnternet Koruması; HTTP ve FTP üzerinden aktarılan verileri tarar.

Kaspersky Endpoint Security, işletim sisteminin TCP ve UDP bağlantı noktalarını riskten etkilenme olasılığına bağlı olarak birkaç gruba ayırır. Bazı ağ bağlantı noktaları, hassas olabilecek hizmetlere ayrılmıştır. Saldırıya maruz kalma olasılığı daha yüksek olduğundan bu bağlantı noktalarını daha kapsamlı olarak izlemeniz tavsiye edilir. Standart olmayan ağ bağlantı noktalarından yararlanan standart olmayan hizmetler kullanıyorsanız, bu ağ bağlantı noktaları da saldıran bilgisayar tarafından hedeflenebilir. Ağa erişim isteyen ağ bağlantı noktalarının listesini ve uygulamaların listesini de belirtebilirsiniz. Ağ trafiğini izleyen Posta Koruması, İnternet Koruması ve IM Koruması bileşenleri bu bağlantı noktaları ve uygulamalara özellikle dikkat eder.

Ağ trafiğini izleme ayarlarını yapılandırma

Ağ trafiğini izleme ayarlarını yapılandırmak için aşağıdaki işlemleri yapabilirsiniz:

- Tüm ağ bağlantı noktalarını izlemeyi etkinleştirebilirsiniz.
- İzlenen ağ bağlantı noktalarının listesini oluşturabilirsiniz.
- Tüm ağ bağlantı noktalarının izlendiği uygulamaların listesini oluşturabilirsiniz.

Tüm ağ bağlantı noktalarını izlemeyi etkinleştirme

Tüm ağ bağlantı noktalarını izlemeyi etkinleştirmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünü seçin.
   Virüse karşı koruma ayarları, pencerenin sağında görüntülenir.
3. **İzlenen bağlantı noktaları** bölümünde, **Tüm ağ bağlantı noktalarını izle**'yi seçin.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

İzlenen ağ bağlantı noktalarının listesini oluşturma

İzlenen ağ bağlantı noktalarının listesini oluşturmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünü seçin.

   Virüse karşı koruma ayarları, pencerenin sağında görüntülenir.
3. **İzlenen bağlantı noktaları** bölümünde, **Yalnızca seçilen bağlantı noktalarını izle** seçeneğini seçin.
4. **Ayarlar** düğmesine tıklayın.

   Ağ bağlantı noktaları penceresi açılır. **Ağ bağlantı noktaları** penceresinde, normalde e-posta ve ağ trafiğinin aktarımı için kullanılan ağ bağlantı noktalarının listesi görüntülenir. Ağ bağlantı noktalarının listesi, Kaspersky Endpoint Security paketinde yer alır.
5. Ağ bağlantı noktalarının listesinde aşağıdakileri gerçekleştirin:

   - İzlenen ağ bağlantı noktalarının listesine eklemek istediğiniz ağ bağlantı noktalarının karşısındaki onay kutularını işaretleyin.

     Varsayılan olarak **Ağ bağlantı noktaları** penceresinde belirtilen tüm ağ bağlantı noktalarının karşısındaki onay kutuları seçilir.
   - İzlenen ağ bağlantı noktalarının listesinin dışında tutmak istediğiniz ağ bağlantı noktalarının karşısındaki onay kutularının işaretini kaldırın.
6. Ağ bağlantı noktalarının listesinde bir ağ bağlantı noktası görülmüyorsa aşağıdaki işlemleri yaparak ekleyin:

   a. Ağ bağlantı noktalarının listesinde **Ekle** bağlantısına tıklayarak **Ağ bağlantı noktası** penceresini açın.

   b. **Bağlantı noktası** alanına ağ bağlantı noktası numarasını girin.

   c. **Açıklama** alanına ağ bağlantı noktasının adını girin.

   d. **Tamam**'a tıklayın.

   Ağ bağlantı noktası penceresi kapanır. Yeni eklenen ağ bağlantı noktası, ağ bağlantı noktalarının listesinin sonuna eklenir.
7. **Ağ bağlantı noktaları** penceresinde **Tamam**'a tıklayın.
8. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

FTP iletişim kuralı pasif modda çalıştığında, izlenen ağ bağlantı noktalarının listesine eklenmeyen rastgele bir ağ bağlantı noktası üzerinden bağlantı kurulur. Bu bağlantıları korumak için **İzlenen bağlantı noktaları** bölümünde **Tüm ağ bağlantı noktalarını izle** onay kutusunu işaretleyin veya FTP bağlantısını kuran uygulamaların tüm bağlantı noktalarının izlenmesini yapılandırın.

Tüm ağ bağlantı noktalarının izlendiği uygulamaların listesini oluşturma

Kaspersky Endpoint Security'nin tüm ağ bağlantı noktalarını izlediği uygulamaların bir listesini oluşturabilirsiniz.

FTP iletişim kuralı üzerinden veri alan veya ileten uygulamaların, Kaspersky Endpoint Security'nin tüm ağ bağlantı noktalarını izlediği uygulamalar listesine eklenmesini öneririz.

Tüm ağ bağlantı noktalarının izlendiği uygulamaların listesini oluşturmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünü seçin.

   Virüse karşı koruma ayarları, pencerenin sağında görüntülenir.
3. **İzlenen bağlantı noktaları** bölümünde, **Yalnızca seçilen bağlantı noktalarını izle** seçeneğini seçin.
4. **Ayarlar** düğmesine tıklayın.

   Ağ bağlantı noktaları penceresi açılır.
5. **Belirtilen uygulamalar için tüm bağlantı noktalarını izle** onay kutusunu işaretleyin.
6. **Belirtilen uygulamalar için tüm bağlantı noktalarını izle** onay kutusu altındaki uygulamalar listesinde, aşağıdakileri yapın:

   - Tüm ağ bağlantı noktalarını izlemek istediğiniz uygulama adlarının karşısındaki onay kutularını işaretleyin.

     Varsayılan olarak **Ağ bağlantı noktaları** penceresinde belirtilen tüm uygulamaların karşısındaki onay kutuları seçilir.
   - Tüm ağ bağlantı noktalarını izlemek istemediğiniz uygulama adlarının karşısındaki onay kutularının işaretini kaldırın.
7. Bir uygulama, uygulamalar listesinde yer almıyorsa aşağıdaki şekilde ekleyin:

   a. Uygulamalar listesi altında **Ekle** bağlantısına tıklayın ve içerik menüsünü açın.

   b. İçerik menüsünde, uygulamalar listesine uygulamayı nasıl eklemek istediğinizi seçin:

      - Bilgisayarda yüklü uygulamalar listesinden bir uygulama seçmek için **Uygulamalar** komutunu seçin. Uygulama adını belirtmenize imkan tanıyan **Uygulama seç** penceresi açılır.
      - Uygulamanın yürütülebilir dosyasının konumunu belirtmek için **Gözat** komutunu seçin. Uygulamanın yürütülebilir dosyasının adını belirtmenizi sağlayan Microsoft Windows'taki standart **Aç** penceresi açılır.

     Uygulamayı seçtikten sonra **Uygulama** penceresi açılır.

   c. **Ad** alanına, seçilen uygulamanın adını girin.

   d. **Tamam**'a tıklayın.

     Uygulama penceresi kapanır. Eklediğiniz uygulama, uygulamalar listesinin sonunda görülür.
8. **Ağ bağlantı noktaları** penceresinde **Tamam**'a tıklayın.
9. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Veritabanlarını ve uygulama yazılım modüllerini güncelleme

Bu bölümde, veritabanı ve uygulama modülü güncellemeleri ("güncellemeler" olarak da adlandırılır) hakkında bilgiler ve güncelleme ayarlarını yapılandırma talimatları bulunmaktadır.

Veritabanı ve uygulama modülü güncellemeleri hakkında

Kaspersky Endpoint Security'nin veritabanlarının ve uygulama modüllerinin güncellenmesi, bilgisayarınızdaki korumanın güncel olmasını sağlar. Dünya genelinde her gün yeni virüsler ve diğer zararlı yazılım türleri ortaya çıkmaktadır. Kaspersky Endpoint Security veritabanları, tehditler ve bunların etkisiz hale getirilmesiyle ilgili bilgi içermektedir. Tehditleri hızlı bir şekilde tespit etmek için, veritabanlarını ve uygulama modüllerini düzenli olarak güncellemeniz tavsiye edilir.

Düzenli güncellemeler için geçerli bir lisans gerekir. Geçerli bir lisans yoksa, güncellemeyi günde sadece bir kez gerçekleştirebilirsiniz.

Kaspersky Endpoint Security'nin ana güncelleme kaynağı, Kaspersky güncelleme sunucularıdır.

Kaspersky güncelleme sunucularından güncelleme paketini başarılı bir şekilde indirmek için bilgisayarınız İnternet'e bağlı olmalıdır. Varsayılan olarak İnternet bağlantısı ayarları otomatik olarak tespit edilir. Proxy sunucusu kullanıyorsanız bağlantı ayarlarını yapmanız gerekir.

Güncelleme gerçekleştirirken aşağıdaki nesneler bilgisayarınıza indirilir ve yüklenir:

- Kaspersky Endpoint Security veritabanları. Bilgisayar koruması, virüslerin ve diğer tehditlerin imzalarını ve bunların nasıl etkisiz hale getirileceği hakkında bilgi içeren veritabanlarını kullanarak sağlanır. Koruma bileşenleri, bilgisayarınızdaki virüslü dosyaları ararken ve etkisiz hale getirirken bu bilgileri kullanır. Veritabanları, yeni tehditlerin kayıtları ve bunlara karşı koyma yöntemleri ile sürekli olarak güncellenmektedir. Bu nedenle veritabanlarını düzenli olarak güncellemenizi öneririz.

  Kaspersky Endpoint Security veritabanlarına ek olarak uygulamanın ağ trafiğini yakalamasına imkan tanıyan ağ sürücüleri de güncellenir.

- Uygulama modülleri. Kaspersky Endpoint Security'nin veritabanlarına ek olarak uygulama modüllerini de güncelleyebilirsiniz. Uygulama modüllerinin güncellenmesi, Kaspersky Endpoint Security'deki zayıf noktaları düzeltir, yeni işlevler ekler veya mevcut işlevleri geliştirir.

Güncelleme sırasında bilgisayarınızdaki uygulama modülleri ve veritabanları, güncelleme kaynağındaki güncel sürümle karşılaştırılır. Geçerli veritabanları ve uygulama modülleri ilgili güncel sürümlerden farklıysa güncellemelerin eksik kısmı bilgisayarınıza yüklenir.

İçerik yardım dosyaları, uygulama modülü güncellemeleri ile birlikte güncellenebilir.

Veritabanları eskiyse, güncelleme paketi çok büyük olabilir ve ek İnternet trafiğine (onlarca MB) neden olabilir.

Kaspersky Endpoint Security veritabanlarının geçerli durumlarıyla ilgili bilgiler ana uygulama penceresinin **Koruma ve Denetim** sekmesinde **Görevler** kısmında **Güncelleme** bölümünde görüntülenir.

Güncelleme sonuçları ve güncelleme görevinin gerçekleştirilmesi sırasında gerçekleşen tüm olaylarla ilgili bilgiler Kaspersky Endpoint Security raporuna kaydedilir.

Güncelleme kaynakları hakkında

Güncelleme kaynağı, Kaspersky Endpoint Security'nin veritabanları ve uygulama modülleri için güncellemeler içeren bir kaynaktır.

Güncelleme kaynakları arasında Kaspersky Security Center, Kaspersky güncelleme sunucuları ve ağ klasörleri veya yerel klasörler sayılabilir.

Güncelleme ayarları yapılandırması

Güncelleme ayarlarını yapılandırmak için aşağıdaki eylemleri gerçekleştirebilirsiniz:

- Yeni güncelleme kaynakları ekleyebilirsiniz.

  Varsayılan güncelleme kaynaklarının listesi, Kaspersky Security Center ve Kaspersky güncelleme sunucularını içerir. Listeye başka güncelleme kaynakları da ekleyebilirsiniz. HTTP/FTP sunucuları ve paylaşım klasörlerini güncelleme kaynakları olarak belirtebilirsiniz.

  Güncelleme kaynakları olarak birkaç kaynak seçilirse Kaspersky Endpoint Security, listenin en üstünden başlayarak bunları sırayla bağlamaya çalışır ve güncelleme görevini, mevcut ilk kaynaktan güncelleme paketini indirerek gerçekleştirir.

  > Güncelleme kaynağı olarak LAN dışında bir kaynak seçerseniz güncellemeyi gerçekleştirmek için İnternet bağlantınız olmalıdır.

- Kaspersky güncelleme sunucusunun bölgesini seçebilirsiniz.

  Güncelleme kaynağı olarak Kaspersky güncelleme sunucularını seçerseniz güncelleme paketini indirmek için kullanılan Kaspersky güncelleme sunucusunun konumunu seçebilirsiniz. Kaspersky güncelleme sunucuları birkaç ülkede bulunmaktadır. En yakın Kaspersky güncelleme sunucularının kullanılması, bir güncelleme paketini indirmek ve güncellemek için geçen süreyi azaltmaya yardımcı olur.

  Varsayılan olarak uygulama, işletim sisteminin kayıt defterinden mevcut bölge hakkındaki bilgiyi kullanır.

- Kaspersky Endpoint Security'nin bir paylaşım klasöründen güncellemesini yapılandırabilirsiniz.

  İnternet trafiğini rahatlatmak amacıyla yerel ağınızda yer alan bilgisayarların güncellemeleri paylaşılmış bir klasörden almasını sağlayacak şekilde Kaspersky Endpoint Security güncellemelerini yapılandırabilirsiniz. Bu amaçla, LAN ağınızdaki bilgisayarlardan biri Kaspersky Security Center sunucusundan veya Kaspersky güncelleme sunucularından güncel bir güncelleme paketi alır ve alınan güncelleme paketini bir paylaşım klasörüne kopyalar. Ardından yerel ağdaki diğer bilgisayarlar bu paylaşım klasöründen güncelleme paketini alabilir.

- Güncelleme görevinin çalışma modunu seçebilirsiniz.

  Güncelleme görevini herhangi bir nedenle çalıştırmak mümkün değilse (örneğin bilgisayar o sırada açık değilse) atlanan görevi mümkün olur olmaz otomatik olarak başlayabilecek şekilde yapılandırabilirsiniz.

  Zamanlamaya göre güncelleme görevi çalışma modunu seçerseniz ve Kaspersky Endpoint Security güncelleme görevi başlatma zamanlamasıyla eşleşiyorsa güncelleme görevini başlatmayı, uygulamanın başlatılmasından sonraya erteleyebilirsiniz. Güncelleme görevi yalnızca Kaspersky Endpoint Security'nin başlatılmasından sonra belirlenen süre geçtikten sonra çalıştırılabilir.

- Güncelleme görevini farklı bir kullanıcı hesabının hakları altında çalışacak şekilde yapılandırabilirsiniz.

Güncelleme kaynağı ekleme

Bir güncelleme kaynağı eklemek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Zamanlanmış görevler** bölümünde **Güncelle**'yi seçin.
   Pencerenin sağında, Uygulama Güncelleme Ayarları görüntülenir.
3. **Çalışma modu ve güncelleme kaynağı** bölümünde **Güncelleme kaynağı** düğmesine tıklayın.
   Güncelleme penceresinin **Kaynak** sekmesi açılır.
4. **Kaynak** sekmesinde **Ekle** düğmesine tıklayın.
   Güncelleme kaynağını seçin penceresi açılır.
5. **Güncelleme kaynağını seçin** penceresinde güncelleme paketini içeren bir klasör seçin veya **Kaynak** alanında tam yolu klasöre girin.
6. **Tamam**'a tıklayın.
7. **Güncelleme** penceresinde **Tamam**'a tıklayın.
8. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Güncelleme sunucusu bölgesini seçme

Güncelleme sunucusu bölgesini seçmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Zamanlanmış görevler** bölümünde **Güncelle**'yi seçin.
   Pencerenin sağında, Uygulama Güncelleme Ayarları görüntülenir.
3. **Çalışma modu ve güncelleme kaynağı** bölümünde **Güncelleme kaynağı** düğmesine tıklayın.
   Güncelleme penceresinin **Kaynak** sekmesi açılır.
4. **Bölgesel ayarlar** bölümünde, **Kaynak** sekmesinde **Listeden seç**'i seçin.
5. Açılır listede, mevcut yerleşim yerinize en yakın ülkeyi seçin.
6. **Tamam**'a tıklayın.
7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Paylaşım klasöründen güncellemeleri yapılandırma

Bir paylaşım klasöründen Kaspersky Endpoint Security'nin güncellemelerinin yapılandırılması aşağıdaki adımlardan oluşur:

1. Yerel ağ üzerindeki bilgisayarlardan birindeki bir paylaşım klasörüne bir güncelleme paketinin kopyalanmasını etkinleştirme.
2. Belirtilen paylaşım klasöründen yerel alan ağı üzerinde kalan bilgisayarlara kadar Kaspersky Endpoint Security güncellemelerini yapılandırma.

Güncelleme paketinin paylaşım klasörüne kopyalanmasını etkinleştirmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Zamanlanmış görevler** bölümünde **Güncelle**'yi seçin.

   Pencerenin sağında, Uygulama Güncelleme Ayarları görüntülenir.
3. **Diğer** bölümünde **Güncellemelerin kopyalanacağı klasör** onay kutusunu seçin.
4. Güncelleme paketinin yerleştirileceği paylaşım klasörünün yolunu belirleyin. Bunu aşağıdaki yollardan biriyle yapabilirsiniz:
   - **Güncellemelerin kopyalanacağı klasör** onay kutusunun altındaki alanda paylaşım klasörü yolunu girin.
   - **Gözat** düğmesine tıklayın. Daha sonra, açılan **Klasör seçin** penceresinde gerekli klasörü seçin ve **Tamam**'a tıklayın.
5. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Kaspersky Endpoint Security'nin bir paylaşım klasöründen güncellemesini yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Zamanlanmış görevler** bölümünde **Güncelle**'yi seçin.

   Pencerenin sağında, Uygulama Güncelleme Ayarları görüntülenir.
3. **Çalışma modu ve güncelleme kaynağı** bölümünde **Güncelleme kaynağı** düğmesine tıklayın.

   Güncelleme penceresinin **Kaynak** sekmesi açılır.
4. **Kaynak** sekmesinde **Ekle** düğmesine tıklayın.

   Güncelleme kaynağını seçin penceresi açılır.
5. **Güncelleme kaynağını seçin** penceresinde, güncelleme paketini içeren paylaşım klasörünü seçin ya da paylaşım klasörünün tam yolunu **Kaynak** alanına girin.
6. **Tamam**'a tıklayın.
7. **Kaynak** sekmesinde, paylaşım klasörü olarak belirtmediğiniz güncelleme kaynaklarının adlarının yanındaki onay kutularını temizleyin.
8. **Tamam**'a tıklayın.

9. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Güncelleme görevinin çalışma modunu seçme

Güncelleme görevinin çalışma modunu seçmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Zamanlanmış görevler** bölümünde **Güncelle**'yi seçin.

   Pencerenin sağında, Uygulama Güncelleme Ayarları görüntülenir.
3. **Çalışma modu** düğmesine tıklayın.

   Güncelle penceresinde **Çalışma modu** sekmesi açılır.
4. **Çalışma modu** bölümünde, güncelleme görevini başlatmak için aşağıdaki seçeneklerden birini seçin:

   - Kaspersky Endpoint Security'nin güncelleme kaynağından bir güncelleme paketi bulunup bulunmadığına göre güncelleme görevini gerçekleştirmesini istiyorsanız **Otomatik** seçeneğini seçin. Kaspersky Endpoint Security'nin güncelleme paketlerini denetleme sıklığı virüs salgınları sırasında artar ve diğer zamanlarda azalır.
   - Güncelleme görevini elle başlatmak isterseniz **Elle** seçeneğini seçin.
   - Güncelleme görevi için bir başlangıç zamanlaması yapılandırmak isterseniz **Zamanlamaya göre**'yi seçin.
5. Aşağıdakilerden birini yapın:

   - **Otomatik** veya **Elle** seçeneğini seçtiyseniz bu talimatların 6. adımına gidin.
   - **Zamanlamaya göre** seçeneğini seçtiyseniz güncelleme görevi çalışma zamanlaması ayarlarını belirtin. Bunun için:

     a. **Sıklık** açılır menüsünde güncelleme görevinin ne zaman başlatılacağını belirtin. Şu seçeneklerden birini seçin: **Dakika**, **Saat**, **Gün**, **Her hafta**, **Belirtilen saatte**, **Her ay** veya **Uygulama başlatıldıktan sonra**.

     b. **Sıklık** açılır listesinde seçilen öğeye bağlı olarak, güncelleme görevinin başlangıç zamanını tanımlayan ayarların değerlerini belirtin.

     c. **Uygulama başladıktan sonra çalışmayı şu kadar ertele** alanında, Kaspersky Endpoint Security başlatıldıktan sonra güncelleme görevinin başlatılmasının ne kadar ertelenmesi gerektiğini belirtin.

     > **Sıklık** açılır listesinden **Uygulama başlatıldıktan sonra** öğesi seçilirse **Uygulama başladıktan sonra çalışmayı şu kadar ertele** alanı etkin değildir.

     d. Kaspersky Endpoint Security'nin atlanmış tarama görevlerini hemen başlatmasını isterseniz **Atlanmış görevleri çalıştır** onay kutusunu işaretleyin.

     > **Sıklık** açılır listesinden **Saat**, **Dakika** veya **Uygulama başlatıldıktan sonra** seçilirse **Atlanmış görevleri çalıştır** onay kutusu etkin değildir.
6. **Tamam**'a tıklayın.

7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Farklı bir kullanıcı hesabının hakları altında bir güncelleme görevi başlatma

Varsayılan olarak Kaspersky Endpoint Security güncelleme görevi, işletim sisteminde oturum açmak için hesabını kullandığınız kullanıcı adına başlatılır. Ancak Kaspersky Endpoint Security, gerekli hakların olmaması veya yetkili bir proxy sunucusu kullanıcısının haklarına sahip olmama nedeniyle kullanıcının erişemediği bir güncelleme kaynağından (örneğin bir güncelleme paketi içeren bir paylaşım klasöründen) güncellenemez. Kaspersky Endpoint Security ayarlarında, bu haklara sahip bir kullanıcı belirtebilir ve Kaspersky Endpoint Security güncelleme görevini o kullanıcı hesabı altında başlatabilirsiniz.

Farklı bir kullanıcı hesabı altında bir güncelleme görevi başlatmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Zamanlanmış görevler** bölümünde **Güncelle**'yi seçin.
   Pencerenin sağında, Uygulama Güncelleme Ayarları görüntülenir.
3. **Çalışma modu ve güncelleme kaynağı** bölümünde, **Çalışma modu** düğmesine tıklayın.
   Güncelle penceresinde **Çalışma modu** sekmesi açılır.
4. **Çalışma modu** sekmesinde, **Kullanıcı** bölümünde, **Görevi farklı çalıştır** onay kutusunu işaretleyin.
5. **Ad** alanına, güncelleme kaynağına erişim için hakları gerekli kullanıcı hesabının adını girin.
6. **Parola** alanına, güncelleme kaynağına erişim için hakları gerekli kullanıcının parolasını girin.
7. **Tamam**'a tıklayın.
8. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Uygulama modülü güncellemelerini yapılandırma

Uygulama modülü güncellemelerini yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Zamanlanmış görevler** bölümünde **Güncelle**'yi seçin.
   Pencerenin sağında, Uygulama Güncelleme Ayarları görüntülenir.
3. **Diğer** bölümünde aşağıdakilerden birini yapın:
   - Uygulamanın güncelleme paketlerinde uygulama modülü güncellemelerinin bulunmasını istiyorsanız **Uygulama modüllerinin güncellemelerini indir** onay kutusunu işaretleyin.
   - İstemiyorsanız **Uygulama modüllerinin güncellemelerini indir** onay kutusunu işaretlemeyin.

4. **Uygulama modüllerinin güncellemelerini indir** onay kutusu önceki adımda seçildiyse uygulamanın hangi koşullarda uygulama modülü güncellemelerini yükleyeceğini belirtin:

   - Uygulamanın uygulama modüllerinin kritik güncellemelerini otomatik olarak, diğer güncellemeleri de kurulumları onaylandıktan sonra uygulama arabirimi üzerinden yerel olarak veya Kaspersky Security Center'ı kullanarak yüklemesini istiyorsanız **Kritik ve onaylı güncelleştirmeleri yükle** seçeneğini seçin.

   - Uygulamanın uygulama modülü güncellemelerini yalnızca kurulumları onaylandıktan sonra uygulama arabirimi üzerinden yerel olarak veya Kaspersky Security Center'ı kullanarak yüklemesini istiyorsanız **Yalnızca onaylı güncelleştirmeleri yükle** seçeneğini seçin.

5. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Güncelleme görevini başlatma veya durdurma

Seçilen güncelleme görevi çalışma modundan bağımsız olarak, herhangi bir zamanda bir Kaspersky Endpoint Security güncelleme görevini başlatabilir ya da durdurabilirsiniz.

Kaspersky sunucularından bir güncelleme paketi indirmek için İnternet bağlantısı gereklidir.

Bir güncelleme görevini başlatmak veya durdurmak için:

1. Ana uygulama penceresinin alt kısmındaki **Görevler** düğmesine tıklayın.
   Görevler penceresi açılır.

2. Güncelleme görevinin adını içeren bölüme tıklayın.
   Seçilen bölüm genişletilir.

3. Aşağıdakilerden birini yapın:

   - Güncelleme görevini başlatmak istiyorsanız menüden **Başlat** seçeneğini belirleyin.
     Güncelleme görevinin adının altında görüntülenen görev ilerleme durumu *Çalışıyor* olarak değişir.

   - Güncelleme görevini durdurmak istiyorsanız menüden **Durdur** seçeneğini belirleyin.
     Güncelleme görevinin adının altında görüntülenen görev ilerleme durumu *Durduruldu* olarak değişir.

Basitleştirilmiş uygulama arabirimi görüntülendiğinde güncelleme görevini başlatmak veya durdurmak için:

1. Sağ tıklayarak görev çubuğu bildirim alanındaki uygulama simgesinin içerik menüsünü açın.

2. İçerik menüsündeki **Görevler** açılır listesinde aşağıdakilerden birini yapın:

   - çalışmayan bir güncelleme görevini seçerek başlatın

   - çalışan bir güncelleme görevini seçerek durdurun

   - duraklatılmış bir güncelleme görevini seçerek sürdürün veya yeniden başlatın

Son güncellemeyi geri alma

Veritabanları ve uygulama modülleri ilk kez güncellendikten sonra, veritabanları ve uygulama modüllerini önceki sürümlere geri alma işlevi mevcut olur.

Kullanıcı güncelleme işlemine her başladığında Kaspersky Endpoint Security, mevcut veritabanları ve uygulama modüllerinin bir yedek kopyasını oluşturur. Bu, gerektiğinde veritabanlarını ve uygulama modüllerini önceki sürümlerine geri almanıza olanak tanır. Son güncellemeyi geri almak, örneğin yeni veritabanı Kaspersky Endpoint Security'nin güvenli bir uygulamayı engellemesine neden olan geçersiz bir imza içerdiğinde faydalı olabilir.

Son güncellemeyi geri almak için:

1. Ana uygulama penceresini açın.
2. **Koruma ve Denetim** sekmesini seçin.
3. **Görevler** bölümüne tıklayın.
   Görevler bölümü açılır.
4. **Güncelleme** görevinin içerik menüsünü görüntülemek için sağ tıklayın.
5. **Güncellemeyi geri al**'a tıklayın.

Proxy sunucusu ayarlarını yapılandırma

Proxy sunucusu ayarlarını yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Zamanlanmış görevler** bölümünde **Güncelle**'yi seçin.
   Pencerenin sağında, Uygulama Güncelleme Ayarları görüntülenir.
3. **Proxy sunucu** bölümünde, **Ayarlar** düğmesine tıklayın.
   Proxy Sunucu Ayarları penceresi açılır.
4. **Proxy Sunucu Ayarları** penceresinde, **Proxy sunucu kullan** onay kutusunu işaretleyin.
5. Proxy sunucusu ayarlarını belirtin.
6. **Tamam**'a tıklayın.
7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Ana uygulama penceresinde proxy sunucusu ayarlarını **Gelişmiş ayarlar** bölümünde **Ayarlar** sekmesinden de yapılandırabilirsiniz.

Bilgisayarı tarama

Virüs taraması, bilgisayar güvenliği için hayati önem taşır. Düzenli yapılan virüs taramaları, düşük güvenlik düzeyi ayarı veya başka nedenlerle koruma bileşenleri tarafından tespit edilmeyen zararlı yazılımların yayılması olasılığı ortadan kaldırır.

Bu bölümde tarama görevlerinin, güvenlik düzeylerinin, tarama yöntemlerinin ve teknolojilerinin özellikleri ve ayarları ile Kaspersky Endpoint Security'nin virüs taraması sırasında işlemediği dosyaları işleme talimatları açıklanmaktadır.

Tarama görevleri hakkında

Virüsler ve diğer tür zararlı yazılımları bulmak ve uygulama modüllerinin bütünlüğünü denetlemek için Kaspersky Endpoint Security aşağıdaki görevleri kapsar:

- **Tam Tarama**. Tüm bilgisayarda gerçekleştirilen kapsamlı bir taramadır. Varsayılan olarak Kaspersky Endpoint Security aşağıdaki nesneleri tarar:
  - Sistem belleği
  - İşletim sistemi açılışında yüklenen nesneler
  - Önyükleme sektörleri
  - İşletim sistemi yedekleme
  - Tüm sabit ve çıkarılabilir sürücüler
- **Kritik Alanları Tarama**. Varsayılan olarak, Kaspersky Endpoint Security, çekirdek belleğini, çalışan işlemleri ve disk önyükleme kesimlerini tarar.
- **Özel Tarama**. Kaspersky Endpoint Security kullanıcı tarafından seçilen nesneleri tarar. Aşağıdaki listeden herhangi bir nesneyi tarayabilirsiniz:
  - Sistem belleği
  - İşletim sistemi açılışında yüklenen nesneler
  - İşletim sistemi yedekleme
  - Outlook posta kutusu
  - Tüm sabit, çıkarılabilir sürücüler ve ağ sürücüleri
  - Seçilen herhangi bir dosya
- **Bütünlük Denetimi**. Kaspersky Endpoint Security, uygulama modüllerinde bozukluk veya değişiklik olup olmadığını denetler.

Tam Tarama ve Kritik Alanları Tarama görevleri diğerlerinden biraz farklıdır. Bu görevler için tarama kapsamının düzenlenmesi önerilmez.

Tarama görevleri başlatıldıktan sonra, tamamlama durumu tarama yapılıyor görevinin adının yanındaki alanda, Kaspersky Endpoint Security'nin ana penceresinin **Koruma ve Denetim** sekmesinde **Görevler** bölümünde görüntülenir.

Tarama sonuçları ve tarama görevlerinin gerçekleştirilmesi sırasında gerçekleşen olaylarla ilgili bilgiler, Kaspersky Endpoint Security raporuna kaydedilir.

Tarama görevini başlatma veya durdurma

Seçilen tarama görevi çalışma modundan bağımsız olarak, herhangi bir zamanda bir tarama görevini başlatabilir ya da durdurabilirsiniz.

Bir tarama görevini başlatmak veya durdurmak için:

1. Ana uygulama penceresini açın.
2. **Koruma ve Denetim** sekmesini seçin.
3. **Görevler** bölümüne tıklayın.

   Görevler bölümü açılır.
4. Sağ tıklayarak tarama görevi adını içeren satırın içerik menüsünü açın.

   Tarama görevi eylemlerini içeren bir menü açılır.
5. Aşağıdakilerden birini yapın:

   - Tarama görevini başlatmak isterseniz, menüden **Taramayı başlat**'ı seçin.

     Bu görevin adını içeren düğmenin sağında görüntülenen görev ilerleme durumu *Çalışıyor* olarak değişir.
   - Tarama görevini durdurmak isterseniz, menüden **Taramayı durdur**'u seçin.

     Bu görevin adını içeren düğmenin sağında görüntülenen görev ilerleme durumu *Durduruldu* olarak değişir.

Tarama görevi ayarlarını yapılandırma

Tarama görevi ayarlarını yapılandırmak için aşağıdakileri yapabilirsiniz:

- Güvenlik düzeyini değiştirebilirsiniz.

  Ön tanımlı güvenlik düzeylerinden birini seçebilir veya güvenlik düzeyi ayarlarını elle yapılandırabilirsiniz. Güvenlik düzeyi ayarlarını değiştirirseniz önerilen güvenlik düzeyi ayarlarına her zaman geri dönebilirsiniz.
- Kaspersky Endpoint Security'nin virüslü bir dosya algıladığında gerçekleştirdiği eylemi değiştirebilirsiniz.
- Tarama kapsamını düzenleyebilirsiniz.

  Tarama kapsamını tarama nesneleri ekleyip kaldırarak veya taranacak dosya türlerini değiştirerek genişletebilir ya da kısıtlayabilirsiniz.
- Taramayı optimize edebilirsiniz.

Dosya taramayı optimize edebilirsiniz: tarama zamanını azaltın ve Kaspersky Endpoint Security'nin çalışma hızını arttırın. Sadece yeni dosyaları tarayarak ve önceki taramadan bu yana değiştirilmiş dosyaları tarayarak bunu sağlayabilirsiniz. Bu mod hem basit hem bileşik dosyalara uygulanır. Tek bir dosyanın taranması için bir sınır da belirleyebilirsiniz. Belirlenen zaman aralığı sona erdiğinde Kaspersky Endpoint Security, dosyayı (arşivler ve birkaç dosya içeren nesneler hariç) mevcut taramanın dışında tutar.

iChecker ve iSwift teknolojilerinin kullanımını da etkinleştirebilirsiniz. Bu teknolojiler, en son taramadan beri değiştirilmemiş dosyaları hariç tutarak dosyaları taramanın hızını optimize edebilir.

- Bileşik dosyaların taranmasını yapılandırabilirsiniz.
- Tarama yöntemlerinin kullanımını yapılandırabilirsiniz.

  Aktif olduğunda Kaspersky Endpoint Security imza analizini kullanır. İmza analizi sırasında Kaspersky Endpoint Security, algılanan nesneyi veritabanındaki kayıtlarla eşleştirir. Kaspersky uzmanlarının önerilerine uygun olarak imza analizi her zaman etkindir.

  Koruma etkinliğini artırmak için sezgisel analizi kullanabilirsiniz. Sezgisel analiz sırasında Kaspersky Endpoint Security, işletim sistemindeki nesnelerin etkinliğini analiz eder. Sezgisel analiz, şu anda Kaspersky Endpoint Security veritabanında kaydı olmayan zararlı nesneler algılayabilir.
- Tarama görevinin çalışma modunu seçebilirsiniz.

  Tarama görevini herhangi bir nedenle çalıştırmak mümkün değilse (örneğin bilgisayar o sırada kapalıysa) atlanan görevi mümkün olur olmaz otomatik olarak çalışacak şekilde yapılandırabilirsiniz.

  Zamanlamaya göre güncelleme görevi çalışma modunu seçtiyseniz ve Kaspersky Endpoint Security başlatma zamanı tarama görevi çalıştırma zamanlamasıyla eşleşiyorsa tarama görevinin başlatılmasını uygulamanın başlatılmasından sonraya erteleyebilirsiniz. Tarama görevi yalnızca Kaspersky Endpoint Security'nin başlatılmasından sonra belirlenen süre geçtikten sonra çalıştırılabilir.
- Tarama görevini farklı bir kullanıcı hesabı altında çalışacak şekilde yapılandırabilirsiniz.
- Çıkarılabilir sürücüler bağlıyken tarama ayarlarını belirleyebilirsiniz.

Güvenlik düzeyini değiştirme

Tarama görevlerini gerçekleştirmek için Kaspersky Endpoint Security çeşitli ayar kombinasyonları kullanır. Uygulamaya kaydedilen bu ayar kombinasyonlarına *dosya güvenlik düzeyleri* denir. Üç adet ön tanımlı güvenlik düzeyi vardır: **Yüksek**, **Önerilen** ve **Düşük**. **Önerilen** güvenlik düzeyi ayarlarının ideal olduğu değerlendirilir. Kaspersky uzmanları tarafından tavsiye edilmektedir.

Güvenlik düzeyini değiştirmek için:

1. Ana uygulama penceresinde **Ayarlar** düğmesine tıklayın.
2. Pencerenin solunda, **Görevler** bölümünde, gereken tarama görevinin (**Tam Tarama**, **Kritik Alanları Tarama** veya **Özel Tarama**) adının bulunduğu alt bölümü seçin.

   Pencerenin sağ kısmında, seçilen tarama görevinin ayarları görüntülenir.
3. **Güvenlik düzeyi** bölümünde aşağıdakilerden birini yapın:

   - Ön tanımlı güvenlik düzeylerinden birini uygulamak isterseniz (**Yüksek**, **Önerilen**, veya **Düşük**), kaydırma çubuğuyla seçin.
   - Özel bir güvenlik düzeyi yapılandırmak isterseniz **Ayarlar** düğmesine tıklayın ve açılan pencerede tarama görevinin adıyla ayarları belirleyin.

Özel bir güvenlik düzeyi yapılandırdıktan sonra **Güvenlik düzeyi** bölümündeki güvenlik düzeyinin adı **Özel** olarak değişir.

- Güvenlik düzeyini **Önerilen** olarak değiştirmek için **Varsayılan olarak** düğmesine tıklayın.

4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Virüslü dosyalara uygulanacak eylemi değiştirme

Virüslü dosyalara uygulanacak eylemi değiştirmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin solunda, **Zamanlanmış görevler** bölümünde, gereken tarama görevinin adının bulunduğu alt bölümü seçin (**Tam Tarama**, **Kritik Alanları Tarama** veya **Özel Tarama**).

   Pencerenin sağ kısmında, seçilen tarama görevinin ayarları görüntülenir.
3. **Tehdit algılandığında uygulanacak eylem** bölümünde gereken seçeneği seçin:
   - **Eylemi otomatik olarak seç**.
   - **Eylemi gerçekleştir**.
4. Önceki adımda **Eylemi gerçekleştir** seçeneğini seçtiyseniz aşağıdaki onay kutularını işaretleyin:
   - Kaspersky Endpoint Security'nin tespit edilen tehditlerdeki nesneleri temizlemesini isterseniz **Temizle** onay kutusunu işaretleyin.

     Bu seçenek seçilse bile Kaspersky Endpoint Security, Windows Store uygulamasının parçası olan dosyalara **Kaldır** eylemini uygular.
   - Kaspersky Endpoint Security'nin tehdit tespit edilen nesneleri silmesini isterseniz **Sil** onay kutusunu işaretleyin.
   - Kaspersky Endpoint Security'nin tehdit tespit edilen nesneleri temizlemesini ve temizlenemeyen nesneleri silmesini isterseniz hem **Temizle** hem de **Sil** onay kutularını işaretleyin.
   - Kaspersky Endpoint Security'nin tehdit tespit edilen nesnelerde herhangi bir işlem gerçekleştirmemesini, sadece kullanıcıya bu nesneleri taramanın sonucunu bildirmesini isterseniz hem **Temizle** hem de **Sil** onay kutularının işaretini kaldırın.
5. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Taranacak nesnelerin bir listesinin üretilmesi

Taramak için bir nesne listesi oluşturmak için aşağıdaki iki yöntemden birini kullanabilirsiniz:

- Ana uygulama penceresinde **Koruma ve Denetim** sekmesinde

- Uygulama ayarları penceresinden.

> Bu yöntem sadece **Tam Tarama** ve **Kritik Bölge Tarama** görevlerinde kullanılabilir. **Özel Tarama** görevi için taranacak nesnelerin listesi sadece **Koruma ve Kontrol** sekmesinden oluşturulabilir.

Ana uygulama penceresinin Koruma ve Denetim sekmesinde taranacak nesnelerin bir listesini oluşturmak için:

1. Ana uygulama penceresini açın.
2. **Koruma ve Denetim** sekmesini seçin.
3. **Görevler** bölümüne tıklayın.
   Görevler bölümü açılır.
4. Görev adını içeren satırın içerik menüsünü açmak için sağ tıklayın ve **Tarama kapsamı** öğesini seçin.
   Tarama kapsamı penceresi açılır.
5. Tarama kapsamına yeni bir nesne eklemek isterseniz:
   a. **Ekle** düğmesine tıklayın.
      Tarama kapsamını seç penceresi açılır.
   b. Nesneyi seçin ve **Ekle** düğmesine tıklayın.
      Tarama kapsamını seç penceresinde seçilen tüm nesneler **Tarama kapsamı** listesinde gösterilir.
   c. **Tamam**'a tıklayın.
6. Tarama kapsamındaki nesnenin yolunu değiştirmek istiyorsanız:
   a. Tarama kapsamındaki nesneyi seçin.
   b. **Düzenle** düğmesine tıklayın.
      Tarama kapsamını seç penceresi açılır.
   c. Tarama kapsamındaki nesnenin yeni yolunu girin.
   d. **Tamam**'a tıklayın.
7. Tarama kapsamından bir nesneyi kaldırmak isterseniz:
   a. Tarama kapsamından kaldırmak istediğiniz nesneyi seçin.
      Çok sayıda nesne seçmek için **CTRL** tuşunu basılı tutarak seçin.
   b. **Kaldır** düğmesine tıklayın.
      Silmeyi onaylama penceresi açılır.
   c. Kaldırma onayı penceresinde **Evet** düğmesine tıklayın.

> Varsayılan tarama kapsamına dahil edilen nesneleri kaldırabilir veya düzenleyebilirsiniz.

8. Bir nesneyi tarama kapsamı dışında tutmak için **Tarama kapsamı** penceresindeki nesnenin karşısındaki onay kutusunun işaretini kaldırın.

   Nesne, tarama kapsamındaki nesnelerin listesinde kalır ama tarama görevi gerçekleştirildiğinde taranmaz.

9. **Tamam**'a tıklayın.

10. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Uygulama ayarları penceresinden taranacak nesnelerin bir listesini oluşturmak için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin solunda, **Zamanlanmış görevler** bölümünde, gereken tarama görevinin adının bulunduğu alt bölümü seçin: **Tam Tarama**, **Kritik Alanları Tarama**.

   Pencerenin sağ kısmında, seçilen tarama görevinin ayarları görüntülenir.

3. **Tarama kapsamı** düğmesine tıklayın.

   Tarama kapsamı penceresi açılır.

4. Önceki talimatların 5-10 adımlarına göre taranacak nesnelerin bir listesini oluşturun.

Taranacak dosya türlerinin seçimi

Taranacak dosyaların türünü seçmek için aşağıdaki iki yöntemi kullanabilirsiniz:

- Ana uygulama penceresinde **Koruma ve Denetim** sekmesinde
- Uygulama ayarları penceresinden.

> Bu yöntem sadece **Tam Tarama** ve **Kritik Bölge Tarama** görevlerinde kullanılabilir. **Özel Tarama** görevi için taranacak dosyaların türü sadece **Koruma ve Kontrol** sekmesinden seçilebilir.

Ana uygulama penceresinin Koruma ve Denetim sekmesinde taranacak dosya türlerini seçmek için:

1. Ana uygulama penceresini açın.

2. **Koruma ve Denetim** sekmesini seçin.

3. **Görevler** bölümüne tıklayın.

   Görevler bölümü açılır.

4. Görev adını içeren satırın içerik menüsünü açmak için sağ tıklayın ve **Ayarlar** öğesini seçin.

   Seçilen tarama görevinin adının bulunduğu bir pencere açılır.

5. Seçilen tarama görevinin adının bulunduğu pencerede, **Kapsam** sekmesini seçin.

6. **Dosya türleri** bölümünde, seçilen tarama görevi çalıştığında taramak istediğiniz dosya türünü belirtin:

   - Tüm dosyaları taramak istiyorsanız **Tüm dosyalar**'ı seçin.

- Virüs bulaşmasına en hassas biçimdeki dosyaları taramak istiyorsanız **Biçime göre taranan dosyalar**'ı seçin.
- Virüs bulaşmasına karşı genellikle en hassas uzantılara sahip dosyaları taramak istiyorsanız **Uzantısına göre taranan dosyalar**'ı seçin.

Taranacak dosya türünü seçerken aşağıdakileri unutmayın:

- Kötü amaçlı kod içerme ve sonradan etkinleştirme olasılığı oldukça düşük olan bazı dosya biçimleri (.txt gibi) bulunmaktadır. Aynı zamanda yürütülebilir kod içeren veya içerebilecek dosya biçimleri de (.exe, .dll ve .doc gibi) bulunmaktadır. Bu tür dosyaların kötü amaçlı kod içerme ve etkinleştirme riski oldukça yüksektir.
- Bir saldırgan .txt uzantılı olarak yeniden adlandırılmış yürütülebilir bir dosya şeklinde bir virüs veya kötü amaçlı programı bilgisayarınıza gönderebilir. Uzantıya göre dosyaların taranmasını seçerseniz tarama sırasında uygulama bu dosyayı atlar. Biçime göre dosya taraması seçilirse, Dosya Koruması uzantıdan bağımsız olarak dosya üst-bilgisini analiz eder. Bu analiz dosyanın EXE biçimine sahip olduğunu ortaya çıkarırsa uygulama dosyayı tarar.

7. Tarama görevinin adının yer aldığı pencerede **Tamam**'a tıklayın.
8. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Uygulama ayarları penceresinden taranacak dosyaların türünü seçmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin solunda, **Zamanlanmış görevler** bölümünde, gereken tarama görevinin adının bulunduğu alt bölümü seçin: **Tam Tarama**, **Kritik Alanları Tarama**.

   Pencerenin sağ kısmında, seçilen tarama görevinin ayarları görüntülenir.
3. **Güvenlik düzeyi** bölümünde, **Ayarlar** düğmesine tıklayın.

   Seçilen tarama görevinin adının bulunduğu bir pencere açılır.
4. Seçilen tarama görevinin adının bulunduğu pencerede, **Kapsam** sekmesini seçin.
5. Önceki talimatlarda 5-7 adımlarını tamamlayın.

Dosya taramasını optimize etme

Dosya taramasını optimize etmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin solunda, **Zamanlanmış görevler** bölümünde, gereken tarama görevinin adının bulunduğu alt bölümü seçin (**Tam Tarama**, **Kritik Alanları Tarama** veya **Özel Tarama**).

   Pencerenin sağ kısmında, seçilen tarama görevinin ayarları görüntülenir.
3. **Güvenlik düzeyi** bölümünde, **Ayarlar** düğmesine tıklayın.

   Seçilen tarama görevinin adının bulunduğu bir pencere açılır.
4. Açılan pencerede **Kapsam** sekmesini seçin.
5. **Tarama optimizasyonu** bölümünde aşağıdaki işlemleri gerçekleştirin:

- **Sadece yeni ve değiştirilmiş dosyaları tara** onay kutusunu işaretleyin.
- **Şundan uzun süreyle taranan dosyaları atla** onay kutusunu işaretleyin ve tek bir dosyayı tarama süresini (saniye olarak) belirtin.

6. **Tamam**'a tıklayın.
7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Bileşik dosyaları tarama

Virüsleri ve diğer zararlı yazılımları gizlemenin yaygın bir tekniği, bunları arşivler veya veritabanları gibi bileşik dosyaların içine yerleştirmektir. Bu şekilde gizlenen virüsleri ve diğer zararlı yazılımları tespit etmek için bileşik dosyanın paketinin açılması gerekir ve bu da taramayı yavaşlatabilir. Taranacak bileşik dosya türlerini sınırlayarak, taramayı hızlandırabilirsiniz.

Bileşik dosyaların taranmasını yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin solunda, **Zamanlanmış görevler** bölümünde, gereken tarama görevinin adının bulunduğu alt bölümü seçin (**Tam Tarama**, **Kritik Alanları Tarama** veya **Özel Tarama**).

   Pencerenin sağ kısmında, seçilen tarama görevinin ayarları görüntülenir.
3. **Güvenlik düzeyi** bölümünde, **Ayarlar** düğmesine tıklayın.

   Seçilen tarama görevinin adının bulunduğu bir pencere açılır.
4. Açılan pencerede **Kapsam** sekmesini seçin.
5. **Bileşik dosya taraması** bölümünde taramak istediğiniz bileşik dosyaları belirleyin: arşivler, yükleme paketleri, office biçiminde dosyalar, e-posta biçiminde dosyalar ve parola korumalı arşivler.
6. **Tarama optimizasyonu** bölümünde **Sadece yeni ve değiştirilmiş dosyaları tara** onay kutusu işaretlenmezse her bir bileşik dosya türünün, bu türdeki tüm dosyaları mı yoksa yalnızca bu türden yeni dosyaları mı tarayıp taramayacağını belirtmek isterseniz bileşik dosya türü adının yanındaki **tümü / yeni** bağlantısına tıklayın.

   Tıklandığında bu bağlantının değeri değişir.

   Sadece yeni ve değiştirilmiş dosyaları tara onay kutusu işaretlenirse sadece yeni dosyalar taranır.
7. **Diğer** düğmesine tıklayın.

   Bileşik dosyalar penceresi açılır.
8. **Boyut sınırı** bölümünde aşağıdakilerden birini yapın:
   - Büyük bileşik dosyaları açmak istemezseniz **Büyük bileşik dosyaları açma** onay kutusunu işaretleyin ve **En büyük dosya boyutu** alanında gereken değeri belirtin.
   - Büyük bileşik dosyaları boyutlarına bakmaksızın açmak isterseniz **Büyük bileşik dosyaları açma** onay kutusunu işaretlemeyin.

Kaspersky Endpoint Security, **Büyük bileşik dosyaları açma** onay kutusunun işaretlenip işaretlenmediğine bakılmaksızın, arşivlerden çıkarılan büyük dosyaları tarar.

9. **Tamam**'a tıklayın.
10. Tarama görevi adının yer aldığı pencerede **Tamam**'a tıklayın.
11. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Tarama yöntemlerini kullanma

Tarama yöntemlerini kullanmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin solunda, **Zamanlanmış görevler** bölümünde, gereken tarama görevinin adının bulunduğu alt bölümü seçin (**Tam Tarama**, **Kritik Alanları Tarama** veya **Özel Tarama**).

   Pencerenin sağ kısmında, seçilen tarama görevinin ayarları görüntülenir.
3. **Güvenlik düzeyi** bölümünde, **Ayarlar** düğmesine tıklayın.

   Seçilen tarama görevinin adının bulunduğu bir pencere açılır.
4. Açılan pencerede **Diğer** sekmesini seçin.
5. Tarama görevini çalıştırırken uygulamanın sezgisel analizi kullanmasını isterseniz **Tarama yöntemleri** bölümünde, Sezgisel analiz onay kutusunu seçin. Sonra sezgisel analiz düzeyini ayarlamak için kaydırma çubuğunu kullanın: **Hızlı tarama**, **Normal tarama** ya da **Ayrıntılı tarama**.
6. **Tamam**'a tıklayın.
7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Tarama teknolojilerini kullanma

Tarama teknolojilerini kullanmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin solunda, **Zamanlanmış görevler** bölümünde, gereken tarama görevinin adının bulunduğu alt bölümü seçin (**Tam Tarama**, **Kritik Alanları Tarama** veya **Özel Tarama**).

   Pencerenin sağ kısmında, seçilen tarama görevinin ayarları görüntülenir.
3. **Güvenlik düzeyi** bölümünde, **Ayarlar** düğmesine tıklayın.

   Seçilen tarama görevinin adının bulunduğu bir pencere açılır.
4. Açılan pencerede **Diğer** sekmesini seçin.

5. **Tarama teknolojileri** bölümünde, tarama sırasında kullanmak istediğiniz teknolojilerin adının yanındaki onay kutularını seçin.

6. **Tamam**'a tıklayın.

7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Tarama görevinin çalışma modunu seçme

Tarama görevinin çalışma modunu seçmek için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin solunda, **Zamanlanmış görevler** bölümünde, gereken görevinin adının bulunduğu alt bölümü seçin (**Tam Tarama**, **Kritik Alanları Tarama** veya **Özel Tarama**).

   Pencerenin sağ kısmında, seçilen tarama görevinin ayarları görüntülenir.

3. **Çalışma modu** düğmesine tıklayın.

   Çalışma modu sekmesinde, seçilen görevin özelliklerinin bulunduğu bir pencere açılır.

4. **Çalışma modu** bölümünde, görevin çalışma modunu seçin: **Elle** veya **Zamanlamaya göre**.

5. **Zamanlamaya göre** seçeneğini seçtiyseniz, zamanlama ayarlarını belirtin. Bunun için:

   a. **Sıklık** açılır listesinde, görev yürütme sıklığını seçin (**Dakika**, **Saat**, **Gün**, **Her hafta**, **Belirtilen saatte**, **Her ay** veya **Uygulama başlatıldıktan sonra**, **Her güncelleme sonrası**).

   b. Seçilen sıklığa bağlı olarak görev çalışma zamanlamasını belirten gelişmiş ayarları yapılandırın.

   c. Kaspersky Endpoint Security'nin atlanmış tarama görevlerini hemen başlatmasını isterseniz, **Atlanmış görevleri çalıştır** onay kutusunu işaretleyin.

   > **Sıklık** açılır listesinde **Dakika**, **Saat**, **Uygulama başlatıldıktan sonra** veya **Her güncelleme sonrası** öğesi seçilirse, **Atlanmış görevleri çalıştır** onay kutusu etkin değildir.

   a. Bilgisayar kaynakları sınırlı olduğunda Kaspersky Endpoint Security'nin bir görevi askıya almasını istiyorsanız **Ekran koruyucu kapalı olduğunda ve bilgisayarın kilidi açıldığında zamanlanmış taramayı askıya al** onay kutusunu işaretleyin.

   Bu zamanlama seçeneği, bilgisayar kaynaklarını dönüştürmenize yardımcı olur.

6. **Tamam**'a tıklayın.

7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Farklı bir kullanıcı hesabıyla bir tarama görevi başlatma

Varsayılan olarak tarama görevi, kullanıcının işletim sisteminde oturum açtığı hesabın izinleriyle gerçekleştirilir. Ancak farklı bir kullanıcı hesabı ile tarama görevini yürütmeniz gerekebilir. Tarama görevinin ayarlarında uygun haklara sahip kullanıcıyı belirtebilir ve tarama görevini bu kullanıcı hesabı ile gerçekleştirebilirsiniz.

Farklı bir kullanıcı hesabıyla tarama görevini başlatmayı yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin solunda, **Zamanlanmış görevler** bölümünde, gereken görevinin adının bulunduğu alt bölümü seçin (**Tam Tarama**, **Kritik Alanları Tarama** veya **Özel Tarama**).

   Pencerenin sağ kısmında, seçilen tarama görevinin ayarları görüntülenir.
3. **Çalışma modu** düğmesine tıklayın.

   Çalışma modu sekmesinde, seçilen görevin özelliklerinin bulunduğu bir pencere açılır.
4. **Çalışma modu** sekmesinde, **Kullanıcı** bölümünde, **Görevi farklı çalıştır** onay kutusunu işaretleyin.
5. **Ad** alanına, tarama görevini başlatmak için hakları gerekli olan kullanıcı hesabının adını girin.
6. **Parola** alanına, tarama görevini başlatmak için hakları gerekli olan kullanıcının parolasını girin.
7. **Tamam**'a tıklayın.
8. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Bilgisayara bağlandığında çıkarılabilir sürücüleri tarama

Bazı kötü amaçlı programlar, yerel ağlar ve çıkarılabilir sürücüler üzerinden kendilerini çoğaltmak için işletim sistemi zayıf noktalarından yararlanır. Kaspersky Endpoint Security, bilgisayarınıza bağlanan çıkarılabilir sürücülerde virüs ve diğer zararlı yazılımları taramanıza olanak tanır.

Bağlandığı zaman çıkarılabilir sürücülerin taranmasını yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Gelişmiş Ayarlar** bölümünü seçin.

   Görev ayarları, pencerenin sağ kısmında görüntülenir.
3. **Çıkarılabilir sürücüleri bağlandıklarında tara** bölümünde **Çıkarılabilir sürücü bağlantısı üzerindeki eylem** açılır listesinde, gereken işlemi seçin:

   - **Tarama**
   - **Ayrıntılı Tarama**

     Bu modda Kaspersky Endpoint Security, bileşik nesneleri içeren dosyalar dahil olmak üzere çıkarılabilir sürücüde bulunan tüm dosyaları tarar.
   - **Hızlı Tarama**

     Bu modda, Kaspersky Endpoint Security sadece potansiyel olarak virüs bulaşabilecek dosyaları tarar ve bileşik nesneleri açmaz.

4. Kaspersky Endpoint Security'nin sadece boyutu belirtilen değeri aşmayan çıkarılabilir sürücüleri taramasını istiyorsanız, **Maksimum çıkarılabilir sürücü boyutu** onay kutusunu işaretleyin ve karşısındaki alana megabayt olarak bir değer belirtin.

5. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

İşlenmemiş dosyaları yönetme

Bu bölümde, bilgisayarda virüs ve diğer tehditleri tararken Kaspersky Endpoint Security'nin işlemediği virüslü ve büyük olasılıkla virüslü dosyaların nasıl yönetileceğiyle ilgili talimatlar yer almaktadır.

Korumasız dosyalar hakkında

Kaspersky Endpoint Security bazı nedenlerle işlemediği dosyalar hakkında bilgi kaydeder. Bu bilgiler, işlenmemiş dosyaların listesine olaylar biçiminde kaydedilir.

Kaspersky Endpoint Security bilgisayarda virüs ve diğer tehditlerin taramasını yaparken belirtilen uygulama ayarlarına göre bir virüslü dosyada aşağıdaki işlemlerden birini gerçekleştirirse bu dosya *işlenmiş* olarak değerlendirilir:

- Temizle.
- Kaldır.
- Temizleme başarısız olursa sil.

Kaspersky Endpoint Security bilgisayarda virüs ve diğer tehditlerin taramasını yaparken herhangi bir nedenle belirtilen uygulama ayarlarına göre bir virüslü dosyada bir işlem gerçekleştiremezse bu dosya *işlenmemiş* olarak değerlendirilir.

Bu durumla aşağıdaki örneklerde karşılaşılabilir:

- Taranan dosya erişilemez durumdadır (örneğin bir ağ sürücüsünde veya yazma ayrıcalığı bulunmayan bir çıkarılabilir sürücüde bulunmaktadır).
- Tarama görevleri için **Tehdit algılandığında uygulanacak eylem** bölümünde seçilen eylem **Bildir**'dir ve kullanıcı virüslü dosya hakkında bir bildirim görüntülendiğinde **Atla** eylemini seçer.

Veritabanları ve uygulama modüllerini güncelledikten sonra işlenmemiş dosyalar listesindeki dosyalar için Özel Tarama görevini elle başlatabilirsiniz. Taramanın ardından dosya durumu değişebilir. Durumuna bağlı olarak dosyalarda gereken eylemleri gerçekleştirebilirsiniz.

Örneğin aşağıdaki eylemleri gerçekleştirebilirsiniz:

- *Virüslü* durumdaki dosyaları silebilirsiniz.
- Önemli bilgiler içeren virüslü dosyaları geri yükleyebilir ve *Temizlendi* veya *Virüslü değil* olarak işaretlenen dosyaları geri yükleyebilirsiniz.
- *Büyük olasılıkla virüslü* durumdaki dosyaları karantinaya alabilirsiniz.

İşlenmemiş dosyaların listesini yönetme

İşlenmemiş dosyaların listesi bir tablo şeklinde görüntülenir.

Aşağıdaki işlemleri işlenmemiş dosyalarla gerçekleştirebilirsiniz:

- İşlenmemiş dosyaların listesini görüntüleyebilirsiniz.
- Kaspersky Endpoint Security veritabanları ve modüllerinin güncel sürümünü kullanarak işlenmemiş dosyaları tarayabilirsiniz.
- İşlenmemiş dosyaların listesindeki dosyaları orijinal klasörlerine veya (orijinal klasöre yazılamadığında) tercih ettiğiniz farklı bir klasöre geri yükleyebilirsiniz.
- İşlenmemiş dosyaların listesinden dosyaları silebilirsiniz.
- İşlenmemiş dosyaların bulunduğu asıl klasörü açabilirsiniz.

Tablodaki verileri yönetirken aşağıdaki eylemleri de gerçekleştirebilirsiniz:

- İşlenmemiş dosya olaylarını sütun adına veya özel filtre koşullarına göre filtreleyebilirsiniz.
- İşlenmemiş dosya olayı arama işlevini kullanabilirsiniz.
- İşlenmemiş dosya olaylarını sıralayabilirsiniz.
- İşlenmemiş dosyalar listesinde görüntülenen sütunları ve sırasını değiştirebilirsiniz.
- İşlenmemiş dosya olaylarını gruplayabilirsiniz.

Gerekirse seçilen işlenmemiş dosya olaylarını panoya kopyalayabilirsiniz.

İşlenmemiş dosyalar için Özel Tarama görevini başlatma

İşlenmemiş dosyalar için Özel Tarama görevini elle başlatabilirsiniz. Son tarama bazı nedenlerle yarıda kesildiyse veya veritabanı ve güncelleme modüllerindeki en son güncellemenin ardından işlenmemiş dosyaları yeniden taramak isterseniz taramayı başlatabilirsiniz.

İşlenmemiş dosyaların Özel Tarama işlemini başlatmak için:

1. Ana uygulama penceresini açın.
2. Ana uygulama penceresinin üst kısmında, **Karantina** bağlantısına tıklayarak **Depolama Alanları** penceresini açın.
3. **Depolama Alanları** penceresinde, **İşlenmemiş dosyalar** sekmesini seçin.
4. **İşlenmemiş dosyalar** sekmesinde, taramak istediğiniz dosyalarla ilişkili bir veya daha fazla olay seçin.
   Çok sayıda olay seçmek için **CTRL** tuşunu basılı tutarak seçin.
5. Özel Tarama görevini aşağıdaki yollardan biriyle başlatın:

- **Yeniden tara** düğmesine tıklayın.
- İçerik menüsünü açmak için sağ tıklayın ve **Yeniden tara** seçeneğini seçin.

İşlenmemiş dosyaların listesinden dosyaları silme

İşlenmemiş dosyaların listesinden dosyaları silmek için:

1. Ana uygulama penceresini açın.
2. Ana uygulama penceresinin üst kısmında, **Karantina** bağlantısına tıklayarak **Depolama Alanları** penceresini açın.
3. **Depolama Alanları** penceresinde, **İşlenmemiş dosyalar** sekmesini seçin.
4. **İşlenmemiş dosyalar** sekmesindeki tabloda, silmek istediğiniz dosyalarla ilişkili bir veya daha fazla olay seçin. Çok sayıda olay seçmek için **CTRL** tuşunu basılı tutarak seçin.
5. Dosyaları şu yollardan birini kullanarak silin:
   - **Kaldır** düğmesine tıklayın.
   - İçerik menüsünü görüntülemek için sağ tıklayın ve **Sil** seçeneğini seçin.

Zayıf Nokta Taraması

Bu bölümde, Zayıf Nokta Taraması görevinin özellikleri ve ayarları hakkında bilgi ve Zayıf Nokta Taraması görevini çalıştırırken Kaspersky Endpoint Security tarafından algılanan zayıf noktaların listesini yönetme talimatları bulunmaktadır.

Çalışan uygulamaların zayıf noktaları hakkında bilgi görüntüleme

Çalışan uygulamaların zayıf noktaları hakkında bilgi, Kaspersky Endpoint Security'nin iş istasyonları için Microsoft Windows kurulu bir bilgisayara yüklenmiş olması durumunda görüntülenebilir. Bu bilgi, Kaspersky Endpoint Security'nin Dosya sunucuları için Microsoft Windows'un kurulu olduğu bir bilgisayara yüklenmiş olması duurmunda kullanılamaz.

Çalışan uygulamaların zayıf noktaları hakkında bilgi görüntülemek için:

1. Ana uygulama penceresini açın.
2. **Koruma ve Denetim** sekmesini seçin.
3. **Uç nokta denetimi** bölümünü açın.
4. **Uygulama Etkinlik İzleyicisi** düğmesine tıklayın.

   Uygulama Etkinlik İzleyicisi sekmesinde **Uygulama Ayrıcalığı Denetimi** penceresi açılır. **Uygulama Etkinlik İzleyicisi** tablosunda, işletim sisteminde çalışan uygulamaların etkinliği hakkında özet bilgi yer alır. Zayıf Nokta İzleyicisi bileşeni tarafından belirlendiği gibi çalışan uygulamaların zayıf nokta önem düzeyi **Zayıf nokta önem düzeyi** sütununda yer alır.

Zayıf Nokta Taraması görevi hakkında

İşletim sistemindeki zayıf noktalar, örneğin programlama ya da tasarımdaki hatalar, zayıf parolalar veya zararlı yazılım etkinliğinden kaynaklanıyor olabilir. Zayıf noktaları tararken uygulama, işletim sistemini analiz eder ve Microsoft ve diğer satıcıların uygulamalarının anomalilerini ve zarar görmüş ayarlarını araştırır.

Zayıf nokta taraması, işletim sisteminin güvenlik tanılamasını gerçekleştirir ve saldırganların zararlı nesneler yaymak ve kişisel bilgilere erişmek için kullanabileceği yazılım özelliklerini algılar.

Zayıf Nokta Taraması görevi başladıktan sonra tamamlama durumu, Kaspersky Endpoint Security'nin ana penceresinin **Koruma ve Denetim** sekmesinde **Görevler** bölümündeki **Zayıf Nokta Taraması** görevinin adının yanındaki alanda görüntülenir.

Zayıf Nokta Taraması görevinin sonuçları raporlar'a kaydedilir.

Zayıf Nokta Taraması görevini başlatma veya durdurma

Zayıf Nokta Taraması görevi için seçilen çalışma modundan bağımsız olarak herhangi bir zamanda başlatabilir veya durdurabilirsiniz.

Zayıf Nokta Taraması görevini başlatmak veya durdurmak için:

1. Ana uygulama penceresini açın.
2. **Koruma ve Denetim** sekmesini seçin.
3. **Görevler** bölümüne tıklayın.

   Görevler bölümü açılır.
4. Zayıf Nokta Taraması görevinin adını içeren satırın içerik menüsünü görüntülemek için sağ tıklayın.

   Zayıf Nokta Taraması görevi işlemlerini içeren bir menü açılır.
5. Aşağıdakilerden birini yapın:

   - Zayıf Nokta Taraması görevini başlatmak için menüden **Taramayı başlat**'ı seçin.

     Zayıf Nokta Taraması görevinin adını içeren düğmenin sağında görüntülenen görev ilerleme durumu *Çalışıyor* olarak değişir.
   - Zayıf Nokta Taraması görevini durdurmak için menüden **Taramayı durdur**'u seçin.

     Zayıf Nokta Taraması görevinin adını içeren düğmenin sağında görüntülenen görev ilerleme durumu *Durduruldu* olarak değişir.

Zayıf Nokta taraması ayarlarını yapılandırma

Zayıf Nokta Taraması ayarlarını yapılandırmak için aşağıdaki eylemleri yapabilirsiniz:

- Zayıf Nokta Taraması kapsamı oluşturabilirsiniz.

  Zayıf nokta taraması yapılacak uygulamaları ekleyerek veya kaldırarak tarama kapsamını genişletebilir veya daraltabilirsiniz.
- Zayıf Nokta Taraması görevinin çalışma modunu seçin

  Görevi herhangi bir nedenle çalıştırmak mümkün değilse (örneğin bilgisayar kapalıysa), atlanan görevi mümkün olur olmaz otomatik olarak çalışacak şekilde yapılandırabilirsiniz.
- Görevi farklı bir kullanıcı hesabının hakları altında çalışması için yapılandırabilirsiniz.

  Varsayılan olarak tarama görevi, kullanıcının işletim sisteminde oturum açtığı hesabın izinleriyle gerçekleştirilir. Ancak farklı bir kullanıcı hesabı ile tarama görevini yürütmeniz gerekebilir. Görevin ayarlarında uygun haklara sahip bir kullanıcı belirtebilir ve görevi bu kullanıcı hesabı ile çalıştırabilirsiniz.

Zayıf nokta taraması kapsamını oluşturma

Zayıf nokta taraması kapsamı bir yazılım satıcısı veya yazılımın yüklendiği klasörün yoludur (örneğin Program Files klasörüne yüklenen tüm Microsoft uygulamaları).

Bir zayıf nokta taraması kapsamı oluşturmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol tarafında, **Zamanlanmış görevler** bölümünde **Zayıf Nokta Taraması**'nı seçin.

Pencerenin sağ tarafında, Zayıf Nokta Taraması görevinin ayarları görüntülenir.

3. **Tarama kapsamı** bölümünde:

   a. Bilgisayarda yüklü Microsoft uygulamalarındaki zayıf noktaları aramak için Kaspersky Endpoint Security'yi kullanmak amacıyla **Microsoft** onay kutusunu işaretleyin.

   b. Bilgisayarda yüklü Microsoft dışındaki tüm uygulamalarda zayıf noktaları aramak için Kaspersky Endpoint Security'yi kullanmak amacıyla **Diğer satıcılar** onay kutusunu işaretleyin.

   c. **Ek zayıf nokta tarama alanı** penceresinde **Ayarlar** düğmesine tıklayın.

   Zayıf nokta taraması kapsamı penceresi açılır.

   d. Zayıf nokta taraması kapsamını oluşturun. Bunun için **Ekle** ve **Kaldır** düğmelerini kullanın.

   e. **Zayıf nokta taraması kapsamı** penceresinde **Tamam**'a tıklayın.

4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Zayıf Nokta Taraması görevinin çalışma modunu seçme

Zayıf Nokta Taraması görevi çalışma modunu seçmek için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol tarafında, **Zamanlanmış görevler** bölümünde **Zayıf Nokta Taraması**'nı seçin.

   Pencerenin sağ tarafında, Zayıf Nokta Taraması görevinin ayarları görüntülenir.

3. **Çalışma modu** düğmesine tıklayın.

   Zayıf Nokta Taraması penceresinin **Çalışma modu** sekmesi açılır.

4. **Çalışma modu** bölümünde, Zayıf Nokta Taraması görevini başlatmak için aşağıdaki çalışma modu seçeneklerinden birini seçin:

   - Zayıf Nokta Taraması görevini elle başlatmak isterseniz **Elle** seçeneğini seçin.
   - Zayıf Nokta Taraması görevi için bir başlangıç zamanlaması yapılandırmak isterseniz **Zamanlamaya göre**'yi seçin.

5. Aşağıdakilerden birini yapın:

   - **Elle** seçeneğini seçtiyseniz bu talimatların 6. adımına gidin.
   - **Zamanlamaya göre** seçeneğini seçtiyseniz Zayıf Nokta Taraması görevi için başlangıç ayarlarını belirtin. Bunun için:

     a. **Sıklık** açılır menüsünde Zayıf Nokta Taraması görevinin ne zaman başlatılacağını belirtin. Aşağıdaki seçeneklerden birini seçin: **Gün**, **Her hafta**, **Belirtilen saatte**, **Her ay**, **Uygulama başlatıldıktan sonra** veya **Her güncelleme sonrası**.

     b. **Sıklık** açılır listesinde seçilen öğeye bağlı olarak, Zayıf Nokta Taraması görevinin başlangıç zamanını tanımlayan ayarların değerlerini belirtin.

c. Kaspersky Endpoint Security'nin atlanmış Zayıf Nokta Taraması görevlerini hemen başlatmasını isterseniz **Atlanmış görevleri çalıştır** onay kutusunu işaretleyin.

> **Sıklık** açılır listesinden **Uygulama başlatıldıktan sonra** veya **Her güncelleme sonrası** seçilirse **Atlanmış görevleri çalıştır** onay kutusu mevcut değildir.

6. **Tamam**'a tıklayın.
7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Zayıf Nokta Taraması görevini farklı bir kullanıcı hesabının haklarını kullanarak başlatma

Varsayılan olarak, Zayıf Nokta Taraması görevi kullanıcının işletim sistemine oturum açtığı hesap altında başlatılır. Ancak farklı bir kullanıcı hesabı ile Zayıf Nokta Taraması görevini başlatmanız gerekebilir. Zayıf Nokta Taraması görevinin ayarlarında bu haklara sahip bir kullanıcı belirtebilir ve Zayıf Nokta Taraması görevini bu kullanıcının hesabı altında başlatabilirsiniz.

Zayıf Nokta Taraması görevinin farklı bir kullanıcı hesabı altında başlatılmasını yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol tarafında, **Zamanlanmış görevler** bölümünde **Zayıf Nokta Taraması**'nı seçin.
   Pencerenin sağ tarafında, Zayıf Nokta Taraması görevinin ayarları görüntülenir.
3. **Çalışma modu** düğmesine tıklayın.
   Zayıf Nokta Taraması penceresinin **Çalışma modu** sekmesi açılır.
4. **Çalışma modu** sekmesinde, **Kullanıcı** bölümünde, **Görevi farklı çalıştır** onay kutusunu işaretleyin.
5. **Ad** alanına, Zayıf Nokta Taraması görevini başlatmak için hakları gerekli kullanıcının hesap adını girin.
6. **Parola** alanına, Zayıf Nokta Taraması görevini başlatmak için hakları gerekli kullanıcının parolasını girin.
7. **Tamam**'a tıklayın.
8. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Zayıf nokta listesini yönetme

Zayıf noktaların listesini yönetirken aşağıdaki eylemleri yapabilirsiniz:

- Zayıf noktaların listesini görebilirsiniz.
- Veritabanlarını ve uygulama modüllerini güncelledikten sonra Zayıf Nokta Taraması görevini yeniden başlatabilirsiniz.
- Zayıf nokta ve düzeltme konusunda tavsiyeleri ayrı bir bölümde görebilirsiniz.

- Zayıf noktalar listesinde seçilen girişleri gizleyebilirsiniz.
- Zayıf noktalar listesini önem düzeyine göre filtreleyebilirsiniz.
- Zayıf noktalar listesini *Düzeltildi* ve *Gizli* durum değerlerine göre filtreleyebilirsiniz.

Tablodaki verileri yönetirken aşağıdaki eylemleri de gerçekleştirebilirsiniz:

- Zayıf noktalar listesini sütun değerleri veya özel filtre koşullarına göre filtreleyebilirsiniz.
- Zayıf nokta arama işlevini kullanabilirsiniz.
- Zayıf noktalar listesindeki girişleri sıralayabilirsiniz.
- Zayıf noktalar listesinde gösterilen sütunların sırasını ve düzenlemesini değiştirebilirsiniz.
- Zayıf noktalar listesinde girişleri gruplandırabilirsiniz.

Zayıf noktaların listesi hakkında

Kaspersky Endpoint Security, Zayıf Nokta Taraması görevinin sonuçlarını zayıf noktaların listesine kaydeder.

Belirli zayıf noktaları gözden geçirdikten ve bunları düzeltmek için önerilen eylemleri gerçekleştirdikten sonra Kaspersky Endpoint Security, zayıf noktaların durumunu *Düzeltildi* olarak değiştirir.

Zayıf noktaların listesinde belirli zayıf noktalarla ilgili girişleri görüntülemek istemiyorsanız bu girişleri gizlemeyi tercih edebilirsiniz. Kaspersky Endpoint Security, bu zayıf noktalar *Gizli* durumunu atar.

Zayıf noktaların listesi bir tablo şeklinde görüntülenir. Her bir tablo satırında aşağıdaki bilgiler yer alır:

- Zayıf nokta önem düzeyini belirten bir simge. Zayıf noktaların aşağıdaki önem düzeyleri mevcuttur:
  - simgesi. **Kritik**. Bu önem düzeyi, ertelemeksizin düzeltilmesi gereken çok tehlikeli zayıf noktalar için geçerlidir. Saldırganlar bilgisayarın işletim sistemine virüs bulaştırmak veya kullanıcının kişisel verilerine erişim sağlamak amacıyla bu düzeyin zayıf noktalarından etkin olarak yararlanır. Kaspersky, "Kritik" önem düzeyindeki zayıf noktaları düzeltmek için gereken tüm adımları derhal atmanızı önerir.
  - simgesi. **Önemli**. Bu önem düzeyi yakında düzeltilmesi gereken önemli zayıf noktalar için geçerlidir. Saldırganlar bu düzeydeki zayıf noktalardan etkin olarak yararlanabilir. Saldırganlar şu anda "Önemli" önem düzeyindeki zayıf noktalardan etkin olarak yararlanmamaktadır. Kaspersky, "Önemli" önem düzeyindeki zayıf noktaları düzeltmek için gereken tüm adımları derhal atmanızı önerir.
  - simgesi. **Uyarı**. Bu önem düzeyi, düzeltmenin ertelenebileceği zayıf noktalar için geçerlidir. Ancak bu zayıf noktalar gelecekte bilgisayarın güvenliğini tehdit edebilir.
- Zayıf nokta kimliği
- Zayıf nokta tespit edilen uygulamanın adıdır.
- Zayıf noktanın kısa açıklaması.
- Dijital imzada belirtilen şekilde yazılım yayınlayıcı hakkında bilgi.
- Zayıf noktayı düzeltmek için uygulanan işlemin sonucu.

Zayıf Nokta Taraması görevini yeniden başlatma

Önceden tespit edilen zayıf noktalarla ilgili bilgileri güncellemek için Zayıf Nokta Taraması görevini yeniden başlatabilirsiniz. Zayıf nokta taraması herhangi bir nedenle yarıda kesildiyse veya veritabanı ve uygulama modüllerindeki en son güncellemenin ardından bilgisayarda zayıf noktaları yeniden taramak isterseniz tarama görevini yeniden başlatmanız gerekebilir.

Zayıf Nokta Taraması görevini yeniden başlatmak için:

1. Ana uygulama penceresini açın.
2. Ana uygulama penceresinin üst kısmında, **Karantina** bağlantısına tıklayarak **Depolama Alanları** penceresini açın.
3. **Depolama Alanları** penceresinde, **Zayıf noktalar** sekmesini seçin.

   Zayıf Noktalar sekmesi, Zayıf Nokta Taraması sırasında Kaspersky Endpoint Security'nin tespit ettiği zayıf noktaların listesini içerir.
4. **Depolama Alanları** penceresinin sağ alt kısmında, **Yeniden tara** düğmesine tıklayın.

Kaspersky Endpoint Security, zayıf noktaların listesindeki zayıf noktalar hakkında ayrıntılı bilgileri günceller.

Önerilen bir yamanın yüklenmesiyle düzeltilen bir zayıf noktanın durumu, başka bir zayıf nokta taramasından sonra değişmez.

Zayıf noktayı düzeltme

Bir işletim sistemi güncellemesini yükleyerek, uygulama yapılandırmasını değiştirerek veya bir uygulama yaması yükleyerek bir zayıf noktayı düzeltebilirsiniz.

Tespit edilen zayıf noktalar yüklü uygulamalar için geçerli olmayabilir ama kopyaları için geçerli olabilir. Bir yama, zayıf noktayı sadece uygulama yüklenmişse düzeltebilir.

Bir zayıf noktayı düzeltmek için:

1. Ana uygulama penceresini açın.
2. Ana uygulama penceresinin üst kısmında, **Karantina** bağlantısına tıklayarak **Depolama Alanları** penceresini açın.
3. **Depolama Alanları** penceresinde, **Zayıf noktalar** sekmesini seçin.

   Zayıf Noktalar sekmesi, Zayıf Nokta Taraması sırasında Kaspersky Endpoint Security'nin tespit ettiği zayıf noktaların listesini içerir.
4. Zayıf noktaların listesinde ilgili zayıf noktayı belirten girişi seçin.

   Bu zayıf nokta ve nasıl düzeltileceğiyle ilgili bilgi içeren bir bölüm zayıf noktaların listesinin en altında açılır.

   Seçilen her bir zayıf nokta için aşağıdaki bilgiler mevcuttur:

- Zayıf nokta tespit edilen uygulamanın adıdır.
- Zayıf nokta tespit edilen uygulamanın sürümü.
- Zayıf noktanın önem düzeyi.
- Zayıf nokta kimliği
- Zayıf noktanın en son tespit edildiği tarih ve saat.
- Zayıf noktayı düzeltme önerileri (örneğin işletim sistemi güncellemesinin veya uygulama yamasının bulunduğu web sitesinin bağlantısı).
- Zayıf noktanın açıklamasını içeren bir İnternet sitesinin bağlantısı.

5. Zayıf noktanın ayrıntılı bir açıklamasını görüntülemek için **Ek bilgiler** bağlantısına tıklayarak, seçilen zayıf nokta ile ilişkili tehdidin açıklamasının yer aldığı İnternet sayfasını açın. www.secunia.com web sitesi, uygulamanın geçerli sürümü için gerekli güncelleştirmeyi indirmenize ve yüklemenize olanak tanır.
6. Zayıf noktayı düzeltmek için aşağıdaki yöntemlerden birini seçin:
   - Uygulama için bir veya daha fazla yama mevcutsa yama adının yanındaki talimatları uygulayarak gereken yamayı yükleyin.
   - Bir işletim sistemi güncellemesi mevcutsa, güncelleme adının yanındaki talimatları uygulayarak gereken yamayı yükleyin.

   Yama veya güncellemeyi yükledikten sonra zayıf nokta düzeltilir. Kaspersky Endpoint Security bu zayıf noktaya, zayıf noktanın düzeltildiğini belirten bir durum atar. Düzeltilen zayıf noktayla ilgili giriş, zayıf noktalar listesinde gri renklidir.
7. Pencerenin altı bölümünde zayıf noktanın nasıl düzeltileceğiyle ilgili herhangi bir bilgi yer almıyorsa Kaspersky Endpoint Security veritabanlarını ve modülleri güncelledikten sonra Zayıf Nokta Taraması görevini yeniden başlatabilirsiniz. Kaspersky Endpoint Security'nin sistemi zayıf noktaların veritabanındaki zayıf noktalara göre taramasından dolayı uygulama güncellendikten sonra düzeltilen bir zayıf noktayla ilgili bir giriş görülebilir.

Zayıf noktalar listesinde girişleri gizleme

Seçilen zayıf nokta girişini gizleyebilirsiniz. Kaspersky Endpoint Security, zayıf noktalar listesinde seçilen ve gizli olarak işaretlenen girişlere *Gizli* durumunu atar. Ardından zayıf noktaların listesini *Gizli* durum değerine göre filtreleyebilirsiniz.

Zayıf noktaların listesindeki bir girişi gizlemek için:

1. Ana uygulama penceresini açın.
2. Ana uygulama penceresinin üst kısmında, **Karantina** bağlantısına tıklayarak **Depolama Alanları** penceresini açın.
3. **Depolama Alanları** penceresinde, **Zayıf noktalar** sekmesini seçin.

   Zayıf Noktalar sekmesi, Zayıf Nokta Taraması sırasında Kaspersky Endpoint Security'nin tespit ettiği zayıf noktaların listesini içerir.
4. Zayıf noktaların listesinde gizlemek istediğiniz zayıf noktayla ilgili girişi seçin.

Bu zayıf nokta ve nasıl düzeltileceğiyle ilgili bilgi içeren bir bölüm zayıf noktaların listesinin en altında açılır.

5. **Gizle** düğmesine tıklayın.

   Kaspersky Endpoint Security seçilen zayıf noktaya *Gizli* durumunu atar. *Gizli* durumuna sahip zayıf noktalarla ilgili girişler, zayıf noktaların listesinde sona taşınır ve gri olur.

6. Zayıf noktaların listesinde bir zayıf noktayla ilgili girişi gizlemek için listenin başındaki **Gizli** onay kutusunu işaretleyin.

Zayıf noktalar listesini önem düzeyine göre filtreleme

Zayıf noktalar listesini önem düzeyine göre filtrelemek için:

1. Ana uygulama penceresini açın.

2. Ana uygulama penceresinin üst kısmında, **Karantina** bağlantısına tıklayarak **Depolama Alanları** penceresini açın.

3. **Depolama Alanları** penceresinde, **Zayıf noktalar** sekmesini seçin.

   Zayıf Noktalar sekmesi, Zayıf Nokta Taraması sırasında Kaspersky Endpoint Security'nin tespit ettiği zayıf noktaların listesini içerir. Zayıf nokta önem düzeyi ile ilgili üç simge (Uyarı, Önemli, Kritik), zayıf noktalar listesinde **Önem düzeyini göster** satırının üst kısmında görülür. Bu simgelere tıklayarak zayıf noktalar listesini önem düzeyine göre filtreleyebilirsiniz.

4. Zayıf nokta önem düzeyinin bir, iki veya üç simgesine tıklayın. Seçilen önem düzeyleriyle eşleşen zayıf noktalar listede görüntülenir. Belirli bir önem düzeyi ile eşleşen zayıf noktaları görüntülemeyi durdurmak için ilgili önem düzeyi seviyesinin simgesine tekrar tıklayın. Tek bir önem düzeyi seçilmediyse zayıf noktalar listesi boştur.

Belirtilen önem düzeyi giriş filtreleme koşulları, **Depolama Alanları** penceresi kapatıldıktan sonra kaydedilir.

Zayıf noktaların listesini Düzeltildi ve Gizli durum değerlerine göre filtreleme

Zayıf noktaların listesini Düzeltildi ve Gizli durum değerlerine göre filtrelemek için:

1. Ana uygulama penceresini açın.

2. Ana uygulama penceresinin üst kısmında, **Karantina** bağlantısına tıklayarak **Depolama Alanları** penceresini açın.

3. **Depolama Alanları** penceresinde, **Zayıf noktalar** sekmesini seçin.

   Zayıf Noktalar sekmesi, Zayıf Nokta Taraması sırasında Kaspersky Endpoint Security'nin tespit ettiği zayıf noktaların listesini içerir.

4. **Zayıf noktaları göster** değerinin karşısında zayıf noktaların durumunu belirten onay kutuları görüntülenir. Zayıf noktaların listesini *Düzeltildi* durumuna göre filtrelemek için aşağıdakilerden birini yapın:

   - Zayıf noktaların listesindeki düzeltilen zayıf noktalarla ilgili girişleri görüntülemek için **Düzeltildi** onay kutusunu işaretleyin. Düzeltilen zayıf noktalarla ilgili girişler, zayıf noktaların listesinde gri renklidir.

   - Zayıf noktaların listesindeki düzeltilen zayıf noktalarla ilgili girişleri gizlemek için **Düzeltildi** onay kutusunu işaretleyin.

5. Zayıf noktaların listesini *Gizli* durumuna göre filtrelemek için aşağıdakilerden birini yapın:

- Zayıf noktaların listesindeki gizlenen zayıf noktalarla ilgili girişleri görüntülemek için **Gizli** onay kutusunu işaretleyin. Gizli zayıf noktalar hakkındaki girişler, zayıf noktalar listesinde gri renklidir.

- Gizlenen zayıf noktalarla ilgili girişleri zayıf noktaların listesinden gizlemek için **Gizli** onay kutusunu işaretleyin.

Belirtilen zayıf nokta girişi filtreleme koşulları, **Depolama Alanları** penceresi kapatıldıktan sonra kaydedilmez.

Uygulama modüllerinin bütünlüğünü kontrol etme

Bu bölümde bütünlük denetimi görevinin özellikleri ve ayarları hakkında bilgiler bulunmaktadır.

Bütünlük denetimi görevi hakkında

Kaspersky Endpoint Security, uygulama yükleme klasöründeki uygulama modüllerinde bozulma veya değişiklik olup olmadığını denetler. Bir uygulama modülünün yanlış bir dijital imzası varsa modül bozuk olarak değerlendirilir.

Bütünlük denetimi görevi başladıktan sonra, tamamlanma süreci Kaspersky Endpoint Security ana penceresinin **Koruma ve Denetim** sekmesindeki **Görevler** bölümünde görevin adının yanındaki alanda görüntülenir.

Bütünlük denetimi görevinin sonuçları raporlara kaydedilir.

Bütünlük denetimi görevini başlatma veya durdurma

Seçilen çalışma modundan bağımsız olarak herhangi bir zamanda bir bütünlük denetimi görevini başlatabilir ya da durdurabilirsiniz.

Bütünlük denetimi görevini başlatmak veya durdurmak için:

1. Ana uygulama penceresini açın.
2. **Koruma ve Denetim** sekmesini seçin.
3. **Görevler** bölümünü açın.
4. Bütünlük denetimi görev adı olan satırın içerik menüsünü çıkarmak için sağ tıklayın.
5. Aşağıdakilerden birini yapın:
   - Bütünlük denetimi görevini başlatmak için içerik menüsünden **Taramayı başlat**'ı seçin.
     Düğmenin sağında bu görev adını taşıyan görev ilerleme durumu, *Çalışıyor* olarak değişir.
   - Bütünlük denetimi görevini durdurmak isterseniz içerik menüsünden **Taramayı durdur**'u seçin.
     Düğmenin sağında bu görev adını taşıyan görev ilerleme durumu, *Durduruldu* olarak değişir.

Bütünlük Denetimi görevi için çalışma modunu seçme

Bütünlük denetimi görevinin çalışma modunu seçmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol tarafında, **Zamanlanmış görevler** bölümünde **Bütünlük denetimi**'ni seçin.
   Pencerenin sağ tarafında, bütünlük denetimi görevinin ayarları görüntülenir.

3. **Çalışma modu** bölümünde aşağıdaki seçeneklerden birini seçin:

   - Bütünlük denetimi görevini elle olarak başlatmak isterseniz **Elle** seçeneğini seçin.
   - Bütünlük denetimi görevi için bir başlangıç zamanlaması yapılandırmak isterseniz **Zamanlamaya göre**'yi seçin.

4. Bir önceki adımda **Zamanlamaya göre** seçeneğini seçtiyseniz görev çalıştırma zamanlamasının ayarlarını belirleyin. Bunun için:

   a. **Sıklık** açılır listesinde, bütünlük denetimi görevinin ne zaman başlatılacağını belirtin. Şu seçeneklerden birini seçin: **Dakika**, **Saat**, **Gün**, **Her hafta**, **Belirtilen saatte**, **Her ay** veya **Uygulama başlatıldıktan sonra**.

   b. **Sıklık** açılır listesinden seçilen öğeye bağlı olarak, görevi başlatma zamanını tanımlayan ayarların değerini belirtin.

   c. Kaspersky Endpoint Security'nin atlanmış bütünlük denetimi görevlerini hemen başlatmasını isterseniz, **Atlanmış görevleri çalıştır** onay kutusunu işaretleyin,.

   > **Sıklık** açılır listesinden **Uygulama başlatıldıktan sonra**, **Dakika** veya **Saat** seçilirse **Atlanmış görevleri çalıştır** onay kutusu mevcut değildir.

   d. Bilgisayar kaynakları sınırlı olduğunda Kaspersky Endpoint Security'nin bir görevi askıya almasını istiyorsanız **Ekran koruyucu kapalı olduğunda ve bilgisayarın kilidi açıldığında zamanlanmış taramayı askıya al** onay kutusunu işaretleyin.

   Bu zamanlama seçeneği, bilgisayar kaynaklarını dönüştürmenize yardımcı olur.

5. **Tamam**'a tıklayın.

6. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Raporları yönetme

Bu bölümde, rapor ayarlarının nasıl yapılandırılacağı ve raporların nasıl yönetileceği açıklanmaktadır.

Raporlar hakkında

Her bir Kaspersky Endpoint Security bileşeninin çalışmasına dair bilgiler, veri şifreleme olayları, her bir tarama görevi, güncelleme görevi ve bütünlük denetimi görevinin performans sonuçları ve uygulamanın genel çalışma bilgileri raporlara kaydedilir.

Raporlar, ProgramData\Kaspersky Lab\KES\Report klasöründe saklanır.

Raporlar aşağıdaki kullanıcı verilerini içerebilir:

- Kaspersky Endpoint Security tarafından taranan dosya yolları
- Kayıt defterlerine yönelik yollar, Kaspersky Endpoint Security'nin çalışması sırasında değiştirilir
- Microsoft Windows kullanıcı adı
- Kullanıcı tarafından açılan İnternet sayfası adresleri.

Rapor verileri, olayların listesini içeren bir tablo şeklinde sunulur. Her bir tablo satırı, ayrı bir olayla ilgili bilgi içerir. Olay öznitelikleri tablo sütunlarında yer alır. Belirli sütunlar, ek özniteliklere sahip iç içe geçmiş sütunlar içeren bileşik sütunlardır. Ek öznitelikleri görüntülemek için sütun adının karşısındaki ⊞ düğmesine tıklamalısınız. Çeşitli bileşenlerin çalışması ve çeşitli görevlerin gerçekleştirilmesi sırasında kaydedilen olaylar farklı öznitelik kümelerine sahiptir.

Aşağıdaki raporlar mevcuttur:

- **Sistem Denetimi** raporu. Kullanıcı ile uygulama etkileşimi sırasında ortaya çıkan olaylar ve herhangi bir Kaspersky Endpoint Security bileşeni veya görevi ile ilgili olmayan genel olarak uygulama çalışması sırasında ortaya çıkan olaylarla ilgili bilgi içerir.
- Kaspersky Endpoint Security bileşeninin çalışması ve görevin gerçekleştirilmesi ile ilgili rapor.
- **Şifreleme** raporu. Veri şifreleme ve şifre çözme sırasında oluşan olaylarla ilgili bilgi içerir.

Raporlarda aşağıdaki olay önem düzeyleri kullanılır:

- **Bilgilendirici mesajlar**. simgesi. Normalde önemli bilgi içermeyen resmi olaylardır.
- **Uyarılar**. simgesi. Kaspersky Endpoint Security'nin çalışmasında önemli durumları yansıttığı için dikkat edilmesi gereken olaylardır.
- **Kritik olaylar**. simgesi. Kaspersky Endpoint Security'nin çalışmasında sorun olduğunu gösteren hatalar veya kullanıcı bilgisayarının korunmasında zayıf noktalar olduğunu gösteren kritik öneme sahip olaylardır.

Raporların rahat işlenmesi için ekrandaki veri sunumunu aşağıdaki şekillerde değiştirebilirsiniz:

- Olay listesini çeşitli kriterlere göre filtreleyebilirsiniz.
- Belirli bir olayı bulmak için arama işlevini kullanabilirsiniz.

- Seçilen olayı ayrı bir bölümde görüntüleyebilirsiniz.
- Olayların listesini her bir rapor sütununa göre sıralayabilirsiniz.
- Olay filtresine göre gruplanan olayları görüntüleyebilir ve gizleyebilirsiniz.
- Raporda görüntülenen sütunların sırasını ve düzenlemesini değiştirebilirsiniz.

Gerekirse üretilen raporu bir metin dosyasına kaydedebilirsiniz.

Gruplar halinde birleştirilen Kaspersky Endpoint Security bileşenleri ve görevleriyle ilgili rapor bilgilerini de silebilirsiniz. Kaspersky Endpoint Security, geçerli saate en yakın girişten başlayarak seçilen raporların tüm girişlerini siler.

Kaspersky Endpoint Security, Kaspersky Security Center yönetimi altında çalışıyorsa olaylar hakkındaki bilgiler Kaspersky Security Center Yönetim Sunucusu'na iletilebilir. Kaspersky Security Center'da raporları yönetme hakkında daha ayrıntılı bilgi için lütfen Kaspersky Security Center Yardım sistemine bakın.

Raporlar ayarlarını yapılandırma

Rapor ayarlarını aşağıdaki şekillerde yapılandırabilirsiniz:

- Maksimum rapor depolama süresini yapılandırabilirsiniz.

  Kaspersky Endpoint Security tarafından kaydedilen olaylar hakkındaki raporların varsayılan maksimum depolama süresi 30 gündür. Bu süre dolduktan sonra Kaspersky Endpoint Security, en eski kayıtları rapor dosyasından otomatik olarak siler. Süreye dayalı kısıtlamayı iptal edebilir ya da maksimum rapor depolama süresini değiştirebilirsiniz.

- Rapor dosyasının maksimum boyutunu yapılandırabilirsiniz.

  Raporu içeren dosyanın maksimum boyutunu belirtebilirsiniz. Varsayılan olarak maksimum rapor dosyası boyutu 1024 MB'dir. Maksimum rapor dosyası boyutunu aşmamak için Kaspersky Endpoint Security, maksimum rapor dosyası boyutuna ulaşıldığında en eski kayıtları rapor dosyasından otomatik olarak siler. Rapor dosyasının büyüklüğü üzerindeki kısıtlamayı iptal edebilirsiniz ya da farklı bir değer ayarlayabilirsiniz.

Maksimum rapor depolama süresini yapılandırma

Maksimum rapor depolama süresini yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Gelişmiş ayarlar** bölümünde, **Raporlar ve Depolama Alanları** alt bölümünü seçin.
3. Pencerenin sağ tarafında, **Rapor parametreleri** bölümünde aşağıdakilerden birini yapın:

   - Rapor depolama süresini sınırlandırmak için **Raporları şu süreden fazla depolama** onay kutusunu seçin. **Raporları şu süreden fazla depolama** onay kutusunun yanındaki alanda, maksimum rapor depolama süresini belirtin.

     Raporlar için varsayılan maksimum depolama süresi 30 gündür.

   - Rapor depolama süresinin sınırını iptal etmek için **Raporları şu süreden fazla depolama** onay kutusunun işaretini kaldırın.

Rapor depolama süresinin sınırı varsayılan olarak etkindir.

4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Rapor dosyasının maksimum boyutunu yapılandırma

Maksimum rapor dosyası boyutunu yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Gelişmiş ayarlar** bölümünde, **Raporlar ve Depolama Alanları** alt bölümünü seçin.
3. Pencerenin sağ tarafında, **Rapor parametreleri** bölümünde aşağıdakilerden birini yapın:
   - Rapor dosyası boyutunu sınırlandırmak için **Maksimum dosya boyutu** onay kutusunu seçin. **Maksimum dosya boyutu** onay kutusunun sağındaki alanda maksimum dosya boyutunu belirtin.

     Varsayılan olarak rapor dosyası boyutu 1024 MB'tır.
   - Rapor dosyası boyutu üzerindeki kısıtlamayı kaldırmak için **Maksimum dosya boyutu** onay kutusunun işaretini kaldırın.

   Rapor dosyası boyutu sınırı varsayılan olarak etkindir.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Raporların görüntülenmesi

Raporları görüntülemek için:

1. Ana uygulama penceresini açın.
2. Ana uygulama penceresinin üst kısmında, **Raporlar** bağlantısına tıklayarak **Raporlar** penceresini açın.
3. Tüm Koruma Bileşenleri raporunu oluşturmak için **Raporlar** penceresinin sol kısmında, bileşenler ve görevler listesindeki **Tüm koruma bileşenleri** öğesini seçin.

   Pencerenin sağında, Kaspersky Endpoint Security'nin tüm koruma bileşenlerinin çalışması sırasındaki olayların listesini içeren Tüm Koruma Bileşenleri raporu görüntülenir.
4. Bir bileşenin veya görevin çalışmasıyla ilgili bir rapor oluşturmak için **Raporlar** penceresinin sol kısmında bileşenler ve görevler listesinde bir bileşen veya görev seçin.

   Pencerenin sağında, Kaspersky Endpoint Security'nin seçilen bileşen veya görevinin çalışması sırasındaki olayların listesini içeren bir rapor görüntülenir.

Varsayılan olarak rapor olayları, **Olay tarihi** sütununda değerlerin artan sırasına göre sıralanır.

Olay bilgilerini raporda görüntüleme

Her bir olayın ayrıntılı özetini raporda görüntüleyebilirsiniz.

Bir olayın ayrıntılı özetini raporda görüntülemek için:

1. Ana uygulama penceresini açın.
2. Ana uygulama penceresinin üst kısmında, **Raporlar** bağlantısına tıklayarak **Raporlar** penceresini açın.
3. Pencerenin sol kısmında, bileşen veya görevle ilgili raporu seçin.

   Rapor kapsamına giren olaylar, pencerenin sağ kısmındaki tabloda görüntülenir. Rapordaki belirli olayları bulmak için filtre, arama ve sıralama işlevlerini kullanın.
4. Rapordaki ilgili olayı seçin.

Pencerenin sol alt kısmında olay özetini içeren bir bölüm görüntülenir.

Raporu dosya olarak kaydetme

Oluşturduğunuz raporu, salt metin (TXT) veya CSV dosyası olarak kaydedebilirsiniz.

Kaspersky Endpoint Security, olayları rapora ekranda görüntülendiği gibi kaydeder: yani aynı olay özniteliği kümesi ve dizisi ile kaydeder.

Raporu dosya olarak kaydetmek için:

1. Ana uygulama penceresini açın.
2. Ana uygulama penceresinin üst kısmında, **Raporlar** bağlantısına tıklayarak **Raporlar** penceresini açın.
3. Aşağıdakilerden birini yapın:
   - "Tüm koruma bileşenleri" raporunu oluşturmak için bileşenler ve görevler listesinde **Tüm koruma bileşenleri**'ni seçin.

     Pencerenin sağında, tüm koruma bileşenlerinin çalışması sırasındaki olayların listesini içeren "Tüm koruma bileşenleri" raporu görüntülenir.
   - Belirli bir bileşen veya görevin çalışmasıyla ilgili bir rapor oluşturmak için bileşenler ve görevler listesinde bu bileşeni veya görevi seçin.

     Pencerenin sağında, seçilen bileşen veya görevin çalışması sırasındaki olayların listesini içeren bir rapor görüntülenir.
4. Gerekirse rapordaki veri sunumunu aşağıdaki yöntemlerle değiştirebilirsiniz:
   - Olayları filtreleyerek
   - Olay araması yaparak
   - Sütunları yeniden düzenleyerek
   - Olayları sıralayarak
5. Pencerenin sağ üst kısmındaki **Raporu kaydet** düğmesine tıklayın.

   İçerik menüsü açılır.

6. İçerik menüsünden rapor dosyasının kaydedileceği kodlamayı seçin: **ANSI olarak Kaydet** veya **Unicode olarak Kaydet**.

   Microsoft Windows'ta standart **Farklı kaydet** penceresi açılır.

7. **Farklı kaydet** penceresinde, rapor dosyasının hedef klasörünü belirtin.

8. **Dosya adı** alanına rapor dosyası adını yazın.

9. **Dosya türü** alanında gereken rapor dosyası biçimini seçin: TXT veya CSV.

10. **Kaydet** düğmesine tıklayın.

Raporları temizleme

Raporlardan bilgi çıkarmak için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol kısmında, **Gelişmiş ayarlar** bölümünde, **Raporlar ve Depolama Alanları** alt bölümünü seçin.

3. Pencerenin sağ tarafında, **Rapor parametreleri** bölümünde, **Raporları sil** düğmesine tıklayın.

   Raporları temizleme penceresi açılır.

4. Bilgi silmek istediğiniz raporların karşısındaki onay kutularını işaretleyin:

   - **Tüm raporlar**.
   - **Genel koruma raporu**. Aşağıdaki Kaspersky Endpoint Security bileşenlerinin çalışması hakkında bilgi içerir:
     - Dosya Koruması
     - Posta Koruması.
     - İnternet Koruması.
     - IM Koruması.
     - Sistem İzleyici.
     - Güvenlik Duvarı.
     - Ağ Saldırısı Engelleyici.
     - BadUSB Saldırısı Önleme.
   - **Tarama görevleri raporu**. Tamamlanan tarama görevleriyle ilgili bilgi içerir:
     - Tam Tarama
     - Kritik Alanları Tarama
     - Özel Tarama

- Bütünlük Denetimi.

- **Güncelleme görevi raporu**. Tamamlanan güncelleme görevleriyle ilgili bilgi içerir:
- **Güvenlik duvarı raporu**. Güvenlik Duvarı'nın çalışmasıyla ilgili bilgi içerir.
- **Denetim bileşenleri raporu**. Aşağıdaki Kaspersky Endpoint Security bileşenlerinin çalışması hakkında bilgi içerir:
  - Uygulama Başlatma Denetimi.
  - Uygulama Ayrıcalığı Denetimi.
  - Zayıf Nokta İzleyicisi.
  - Aygıt Denetimi.
  - İnternet Denetimi.
- **Veri şifreleme raporu**.

5. **Tamam**'a tıklayın.

Bildirim hizmeti

Bu bölüm, kullanıcıyı Kaspersky Endpoint Security'nin çalışması sırasındaki olaylar hakkında uyaran bildirim hizmeti hakkında bilgi ve bildirimlerin iletilmesini yapılandırmayla ilgili talimatlar içerir.

Kaspersky Endpoint Security bildirimleri hakkında

Kaspersky Endpoint Security'nin çalışması sırasında her tür olay gerçekleşir. Bu olayların bildirimleri tamamen bilgilendirme amaçlı olabilir ya da kritik bilgiler de içerebilir. Örnek olarak, bildirimler başarılı bir veri tabanı ve uygulama modülü güncellemesi veya düzeltilmesi gereken bileşen hataları kaydı bilgilerini verebilir.

Kaspersky Endpoint Security, Microsoft Windows uygulama günlüğünün ve / veya Kaspersky Endpoint Security olay günlüğünün çalışması olaylarıyla ilgili bilgi günlüğünü desteklemektedir.

Kaspersky Endpoint Security, bildirimleri aşağıdaki şekillerde iletir:

- Microsoft Windows görev çubuğu bildirim alanında açılır pencere bildirimlerini kullanma;
- e-posta ile.

Olay bildirimlerinin iletilmesini yapılandırabilirsiniz. Bildirim iletilme yöntemi, her bir olay türü için yapılandırılır.

Bildirim hizmetini yapılandırma

Bildirim hizmetini yapılandırmak için aşağıdaki eylemleri gerçekleştirebilirsiniz:

- Kaspersky Endpoint Security'nin olayları kaydettiği olay günlüklerinin ayarlarını yapılandırabilirsiniz.
- Ekran üzeri bildirimlerin nasıl görüntüleneceğini yapılandır.
- E-posta bildirimlerinin iletilmesini yapılandırabilirsiniz.

Bildirim hizmetini yapılandırmak için olaylar tablosunu kullanırken aşağıdaki işlemleri gerçekleştirebilirsiniz:

- Bildirim hizmeti olaylarını sütun değerlerine veya özel filtre koşullarına göre filtreleyebilirsiniz.
- Bildirim hizmeti olayları için arama işlevini kullanabilirsiniz.
- Bildirim hizmeti olaylarını sıralayabilirsiniz.
- Bildirim hizmeti olaylarının listesinde görüntülenen sütunları ve sırasını değiştirebilirsiniz.

Olay günlüğü ayarlarını yapılandırma

Olay günlüğü ayarlarını yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Gelişmiş ayarlar** bölümünde, **Raporlar ve Depolama Alanları** alt bölümünü seçin.

Pencerenin sağ kısmında, raporlar ve depolama alanlarının ayarları görüntülenir.

3. **Bildirimler** bölümünde **Ayarlar** düğmesine tıklayın.

   Bildirimler penceresi açılır.

   Kaspersky Endpoint Security bileşenleri ve görevleri pencerenin sol kısmında yer alır. Pencerenin sağ kısmında, seçilen bileşen veya görev için üretilen olaylar listelenir.

4. Pencerenin sol kısmında, olay günlüğü ayarlarını yapılandırmak istediğiniz bileşeni veya görevi seçin.

5. **Yerel günlüğe kaydet** ve **Windows Olay Günlüğüne kaydet** sütunlarında ilgili olayların karşısındaki onay kutularını işaretleyin.

   Yerel günlüğe kaydet sütununda onay kutuları seçilen olaylar, **Kaspersky Olay Günlüğü** bölümünde **Uygulamaların ve hizmetlerin günlüğü** kısmında görüntülenir. **Windows Olay Günlüğüne kaydet** sütununda onay kutuları seçilen olaylar, **Uygulama** bölümünde **Windows günlükleri**'nde görüntülenir. Olay günlüklerini açmak için **Başlat** → **Denetim Masası** → **Yönetim** → **Olay Görüntüleyicisi**'ni seçin.

6. **Tamam**'a tıklayın.

7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Bildirimlerin görüntülenmesini ve iletilmesini yapılandırma

Bildirimlerin görüntülenmesini ve iletilmesini yapılandırmak için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol kısmında, **Gelişmiş ayarlar** bölümünde, **Raporlar ve Depolama Alanları** alt bölümünü seçin.

   Pencerenin sağ kısmında, raporlar ve depolama alanlarının ayarları görüntülenir.

3. **Bildirimler** bölümünde **Ayarlar** düğmesine tıklayın.

   Bildirimler penceresi açılır.

   Kaspersky Endpoint Security bileşenleri ve görevleri pencerenin sol kısmında yer alır. Pencerenin sağ kısmında seçilen bileşen veya seçilen görev için üretilen olaylar listelenir.

4. Pencerenin sol tarafında bildirimlerin iletimini yapılandırmak istediğiniz bileşeni veya görevi seçin.

5. **Ekran üzerinde bildir** sütununda gerekli olayların yanındaki onay kutularını işaretleyin.

   Seçilen olaylar hakkında bilgiler Microsoft Windows görev çubuğu bildirim alanında açılır mesajlar olarak görüntülenir.

6. **E-posta ile bildir** sütununda gerekli olayların yanındaki onay kutularını işaretleyin.

   E-posta bildirimi iletim ayarları yapılandırıldıysa seçilen olaylar hakkında bilgiler e-posta ile iletilir.

7. **E-posta bildirim ayarları** düğmesine tıklayın.

   E-posta bildirim ayarları penceresi açılır.

8. **E-posta ile bildir** sütununda seçilen Kaspersky Endpoint Security olayları hakkındaki bilgilerin iletimini etkinleştirmek için **Olay bildirimlerini gönder** onay kutusunu işaretleyin.

9. E-posta bildirimi iletim ayarlarını belirleyin.

10. **Tamam**'a tıklayın.

11. **E-posta bildirim ayarları** penceresinde **Tamam** düğmesine tıklayın.

12. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Bildirim alanında uygulama durumu hakkında uyarıların görüntülenmesini yapılandırma

Bildirim alanında uygulama durumu uyarılarının görüntülenmesini yapılandırmak için:

1. Ana uygulama penceresinde **Ayarlar** düğmesine tıklayın.

2. Pencerenin sol kısmında, **Genel Ayarlar** bölümünde **Arabirim** seçeneğini belirleyin.

   Kaspersky Endpoint Security arabiriminin ayarları, pencerenin sağ kısmında görüntülenir.

3. **Uyarılar** bölümünde, Microsoft Windows'un bildirim alanında bildirimlerini görmek istediğiniz olay kategorilerinin karşısındaki onay kutularını işaretleyin.

4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Seçilen kategoriyle ilişkili bir olay gerçekleşirse bildirim alanında uygulama simgesi uyarının önem düzeyine bağlı olarak hata oluştu simgesine veya yeniden başlatma gerekiyor simgesine değişir.

Karantina ve Yedeklemeyi Yönetme

Bu bölümde, Karantina ve Yedekleme'nin nasıl yapılandırılacağı ve yönetileceği açıklanmaktadır.

Karantina ve Yedekleme Hakkında

Karantina büyük olasılıkla virüslü dosyaların listesidir. *Büyük olasılıkla virüslü dosyalar*, virüsler ve başka tehditleri veya bu tehditlerin çeşitlerini içerebilecek dosyalardır.

Kaspersky Endpoint Security büyük olasılıkla virüslü bir dosyayı karantinaya aldığında dosyayı kopyalamaz, taşır: uygulama, dosyayı sabit sürücü veya e-posta mesajından siler ve dosyayı özel bir veri deposuna kaydeder. Karantinadaki dosyalar özel bir biçimde saklanır ve bir tehdit oluşturmaz.

Kaspersky Endpoint Security, virüs taraması yürütürken ve ayrıca Dosya Koruması, Posta Koruması ve Sistem İzleyici bileşenlerinin çalışması sırasında büyük olasılıkla virüslü bir dosyayı tespit edebilir ve karantinaya alabilir.

Kaspersky Endpoint Security aşağıdaki durumlarda dosyaları Karantina'ya alır:

- Dosya kodu bilinen veya kısmen değiştirilmiş bir kötü amaçlı programa benziyorsa ve zararlı yazılıma benzer bir yapıya sahipse ve Kaspersky Endpoint Security veritabanında yer almıyorsa. Bu durumda dosya, Dosya Koruması ve Posta Koruması tarafından sezgisel analizin ardından veya virüs taraması sırasında Karantina'ya alınır. Sezgisel analiz nadiren hatalı pozitif durumlara neden olur.

- Bir dosyanın gerçekleştirdiği işlem dizisi tehlikelidir. Bu durumda dosya, Sistem İzleyici'nin davranışını analiz etmesinin ardından Karantina'ya alınır.

Yedekleme, temizleme işlemi sırasında silinen veya değiştirilen dosyaların yedek kopyalarının listesidir. *Yedekleme kopyası*, ilk defa bu dosyayı temizlemeye veya silmeye çalıştığınızda oluşturulan dosya kopyasıdır. Dosyaların yedekleme kopyaları, özel bir biçimde saklanır ve bir tehdit oluşturmaz.

Bazen temizleme işlemi sırasında dosyaların bütünlüğünü korumak mümkün değildir. Temizleme işlemini ardından temizlenen dosyadaki önemli bilgilere kısmen veya tamamen erişimi kaybederseniz, dosyanın temizlenen kopyasını orijinal klasöre geri yüklemeyi deneyebilirsiniz.

Başka bir veritabanı veya uygulama yazılım modülü güncellemesinin ardından Kaspersky Endpoint Security'nin bunları kesin olarak tespit etmesi ve etkisiz hale getirmesi mümkündür. Bu nedenle her bir veritabanı ve uygulama yazılım modülü güncellemesinin ardından karantinaya alınan nesnelerin taranması önerilir.

Karantina ve Yedekleme Ayarlarını Yapılandırma

Veri deposu, Karantina ve Yedekleme'den oluşur. Karantina ve Yedekleme ayarlarını aşağıdaki şekilde yapılandırabilirsiniz:

- Karantina'daki dosyalar ve Yedekleme konumundaki dosya kopyaları için maksimum depolama süresini yapılandırın.

  Karantina'daki dosyalar ve Yedekleme konumundaki dosya kopyaları için varsayılan maksimum depolama süresi 30 gündür. Maksimum depolama süresi sona erdiğinde Kaspersky Endpoint Security, en eski dosyaları veri depolamadan siler. Süreye dayalı kısıtlamayı iptal edebilir ya da maksimum dosya depolama süresini değiştirebilirsiniz.

- Karantina ve Yedekleme için maksimum boyutu yapılandırabilirsiniz.

Varsayılan olarak maksimum Karantina ve Yedekleme boyutu 100 MB'dir. Veri depolama limite ulaştığında Kaspersky Endpoint Security, maksimum veri depolama boyutunun aşılmaması için Karantina ve Yedekleme konumundan en eski dosyaları otomatik olarak siler. Karantina ve Yedekleme boyut limitini iptal edebilir veya maksimum boyutu değiştirebilirsiniz.

Karantina'daki dosyalar ve Yedekleme konumundaki dosya kopyaları için maksimum depolama süresini yapılandırma

Karantina'daki dosyalar ve Yedekleme konumundaki dosya kopyalarının maksimum depolama süresini yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Gelişmiş ayarlar** bölümünde, **Raporlar ve Depolama Alanları** alt bölümünü seçin.
3. Aşağıdakilerden birini yapın:
   - Karantina ve Yedekleme dosya depolama süresini sınırlamak için pencerenin sağ kısmındaki **Karantina ve Yedekleme Ayarları** bölümünde, **Nesneleri şu süreden fazla depolama** onay kutusunu işaretleyin. **Nesneleri şu süreden fazla depolama** onay kutusunun sağındaki alanda, Karantina konumundaki dosyaların ve Yedekleme konumundaki dosya kopyalarının maksimum depolama süresini belirtin. Karantina konumundaki dosyalar ve Yedekleme konumundaki dosya kopyaları için maksimum depolama süresi varsayılan olarak 30 gündür.
   - Karantina ve Yedekleme dosya depolama süresi sınırlamasını iptal etmek için pencerenin sağ kısmındaki **Karantina ve Yedekleme Ayarları** bölümünde, **Nesneleri şu süreden fazla depolama** onay kutusunu işaretleyin.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Karantina ve Yedekleme için maksimum boyutu yapılandırma

Maksimum Karantina ve Yedekleme boyutunu yapılandırmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Gelişmiş ayarlar** bölümünde, **Raporlar ve Depolama Alanları** alt bölümünü seçin.
3. Aşağıdakilerden birini yapın:
   - Karantina ve Yedekleme'nin toplam boyutunu sınırlamak isterseniz, **Karantina ve Yedekleme Ayarları** bölümündeki pencerenin sağ kısmında **Maksimum depolama boyutu** onay kutusunu işaretleyin ve **Maksimum depolama boyutu** onay kutusunun sağında Karantina ve Yedekleme maksimum boyutunu belirtin.

     Varsayılan olarak Karantina dizini ve dosyaların yedek kopyalarından oluşan verilerin maksimum depolama boyutu 100 MB'dir.
   - Karantina ve Yedekleme boyutunun üzerindeki sınırlamayı kaldırmak isterseniz, **Karantina ve Yedekleme Ayarları** bölümündeki pencerenin sağ kısmında **Maksimum depolama boyutu** onay kutusunun işaretini kaldırın.

Karantina ve Yedekleme boyutu varsayılan olarak sınırsızdır.

4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Karantinayı Yönetme

Kaspersky Endpoint Security, gelişmiş ayarlar bölümünde yapılandırılan depolama süresi geçtikten sonra Karantina durumdaki tüm dosyaları otomatik olarak siler.

Karantinayı yönetirken aşağıdaki dosya işlemleri kullanılabilir:

- Kaspersky Endpoint Security tarafından karantinaya alınan dosyaları görüntüle.
- Kaspersky Endpoint Security veritabanları ve modüllerinin güncel sürümünü kullanarak büyük olasılıkla virüslü dosyaları tarama.
- Karantina konumundan orijinal klasörlerine dosyaları geri yükleme.
- Karantina konumundan dosyaları kaldırma.
- Dosyaların orijinal konumundaki klasörleri açma.

Karantinaya alınan dosyaların grubu bir tablo olarak sunulmuştur.

Tablodaki verileri yönetirken aşağıdaki eylemleri de gerçekleştirebilirsiniz:

- Sütun ve özel filtre koşullarına dayalı olarak karantinaya alınmış nesneleri filtreleyebilirsiniz.
- Karantinaya alınan dosya arama işlevini kullanan.
- Karantinaya alınan dosyaları sırala.
- Karantinaya alınan dosyalar tablosunda görüntülenen sütunları ve sırasını değiştir.

Seçilen Karantina olaylarını panoya kopyalayabilirsiniz. Çok sayıda karantinaya alınmış nesne seçmek için herhangi bir dosyanın içerik menüsüne sağ tıklayın ve **Tümünü seç**'i seçin. Taramak istemediğiniz dosyaların seçimini kaldırmak için **CTRL** tuşunu basılı tutarak tıklayın.

Güncellemenin ardından Karantina'daki dosyaların taranmasını etkinleştirme ve devre dışı bırakma

Kaspersky Endpoint Security bir dosyayı tararken virüs belirtileri tespit ederse ancak hangi kötü amaçlı programların buna neden olduğunu belirleyemezse Kaspersky Endpoint Security bu dosyayı Karantina'ya taşır. Veritabanı ve uygulama modülleri güncellendikten sonra Kaspersky Endpoint Security tehditleri kesin olarak tespit edebilir ve etkisiz hale getirebilir. Veritabanları ve uygulama modüllerinin her bir güncellemesinin ardından Karantina'daki dosyaların otomatik olarak taranmasını etkinleştirebilirsiniz.

Karantina'daki dosyaları düzenli olarak taramanızı öneririz. Tarama, dosyaların durumunu değiştirebilir. Kullanmaya devam edebilmeniz için bazı dosyalar temizlenebilir ve orijinal konumlarına geri yüklenebilir.

Güncellemelerin ardından karantinaya alınmış nesnelerin taranmasını etkinleştirmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Gelişmiş ayarlar** bölümünde, **Raporlar ve Depolama Alanları** alt bölümünü seçin.

   Pencerenin sağ kısmında, raporlar ve depolama alanlarının yönetim ayarları görüntülenir.
3. **Karantina ve Yedekleme Ayarları** bölümünde aşağıdakilerden birini yapın:

   - Kaspersky Endpoint Security'nin her bir güncellemesinin ardından karantinaya alınmış nesnelerin taranmasını etkinleştirmek için **Güncellemeden sonra Karantina'yı yeniden tara** onay kutusunu işaretleyin.
   - Kaspersky Endpoint Security'nin her bir güncellemesinin ardından karantinaya alınmış nesnelerin taranmasını devre dışı bırakmak için **Güncellemeden sonra Karantina'yı yeniden tara** onay kutusunu işaretleyin.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Karantina'daki dosyalar için Özel Tarama görevini başlatma

Veritabanlarının ve uygulama yazılım modüllerinin güncellenmesinin ardından Kaspersky Endpoint Security, karantinaya alınmış nesnelerdeki tehditleri kesin olarak tespit edebilir ve etkisiz hale getirebilir. Uygulama, veritabanlarının ve uygulama modüllerinin her bir güncellemesinin ardından karantinaya alınmış nesneleri otomatik olarak tarayacak şekilde yapılandırılmamışsa karantinaya alınmış nesneler için Özel Tarama görevini elle başlatabilirsiniz.

Karantinaya alınmış nesneler için Özel Tarama görevini başlatmak amacıyla:

1. Ana uygulama penceresini açın.
2. Ana uygulama penceresinin üst kısmında, **Karantina** bağlantısına tıklayarak **Depolama Alanları** penceresini açın.

   Depolama Alanları penceresinin **Karantina** sekmesi açılır.
3. **Karantina** sekmesinde taramak istediğiniz büyük olasılıkla virüslü dosyalardan birini veya birkaçını seçin.

   Çok sayıda karantinaya alınmış nesne seçmek için herhangi bir dosyanın içerik menüsüne sağ tıklayın ve **Tümünü seç**'i seçin. Taramak istemediğiniz dosyaların seçimini kaldırmak için **CTRL** tuşunu basılı tutarak tıklayın.
4. Özel Tarama görevini aşağıdaki yollardan biriyle başlatın:

   - **Yeniden tara** düğmesine tıklayın.
   - İçerik menüsünü açmak için sağ tıklayın ve **Yeniden tara** seçeneğini seçin.

Tarama tamamlandığında taranan dosya sayısı ve tespit edilen tehdit sayısının olduğu bir bildirim görülür.

Karantina konumundan dosyaları geri yükleme

Karantina konumundan dosyaları geri yüklemek için:

1. Ana uygulama penceresini açın.
2. Ana uygulama penceresinin üst kısmında, **Karantina** bağlantısına tıklayarak **Depolama Alanları** penceresini açın.

   Depolama Alanları penceresinin **Karantina** sekmesi açılır.

3. Karantinaya alınmış nesnelerin tamamını geri yüklemek isterseniz herhangi bir dosyanın içerik menüsünden **Tümünü geri yükle** seçeneğini seçin.

   Kaspersky Endpoint Security, Karantina konumundan tüm dosyaları orijinal klasörlerine geri yükler.

4. Bir veya daha fazla karantinaya alınmış nesneyi geri yüklemek için:

   a. **Karantina** sekmesinde, Karantina konumundan geri yüklemek istediğiniz bir veya daha fazla dosya seçin.

      Çok sayıda karantinaya alınmış nesne seçmek için herhangi bir dosyanın içerik menüsüne sağ tıklayın ve **Tümünü seç**'i seçin. Taramak istemediğiniz dosyaların seçimini kaldırmak için **CTRL** tuşunu basılı tutarak tıklayın.

   b. Dosyaları aşağıdaki yollardan biriyle geri yükleyebilirsiniz:

      - **Geri yükle** düğmesine tıklayın.
      - İçerik menüsünü görüntülemek için sağ tıklayın ve **Geri yükle** seçeneğini seçin.

Kaspersky Endpoint Security, seçilen dosyaları orijinal klasörlerine geri yükler.

Karantina konumundan dosyaları silme

Karantina konumundan dosyaları silmek için:

1. Ana uygulama penceresini açın.
2. Ana uygulama penceresinin üst kısmında, **Karantina** bağlantısına tıklayarak **Depolama Alanları** penceresini açın.

   Depolama Alanları penceresinin **Karantina** sekmesi açılır.

3. Karantina konumundan tüm nesneleri silmek isterseniz herhangi bir dosyanın içerik menüsünden **Tümünü sil** seçeneğini seçin.

   Kaspersky Endpoint Security, Karantina konumundan tüm dosyaları siler.

4. Bir veya daha fazla karantinaya alınmış dosyayı silmek için:

   a. **Karantina** sekmesindeki tabloda, Karantina konumundan silmek istediğiniz bir veya daha fazla büyük olasılıkla virüslü dosyayı seçin.

      Çok sayıda karantinaya alınmış nesne seçmek için herhangi bir dosyanın içerik menüsüne sağ tıklayın ve **Tümünü seç**'i seçin. Taramak istemediğiniz dosyaların seçimini kaldırmak için **CTRL** tuşunu basılı tutarak tıklayın.

   b. Dosyaları şu yollardan birini kullanarak silin:

      - **Kaldır** düğmesine tıklayın.
      - İçerik menüsünü görüntülemek için sağ tıklayın ve **Sil** seçeneğini seçin.

Kaspersky Endpoint Security, seçilen dosyaları Karantina konumundan siler.

Yedeklemeyi Yönetme

Dosyada kötü amaçlı kod tespit edilirse Kaspersky Endpoint Security dosyayı engeller, orijinal klasöründen kaldırır, kopyasını Yedekleme konumuna yükler ve temizlemeye çalışır. Dosya temizleme işlemi başarılı olursa dosyanın yedekleme kopyasının durumu *Temizlendi* olarak değişir. Dosya kendi özgün klasöründe kullanılabilir hale gelir. Bir dosya temizlenemezse, Kaspersky Endpoint Security dosyayı özgün klasöründen siler. Temizlenen yedekleme kopyasından dosyayı orijinal klasörüne geri yükleyebilirsiniz.

Windows Store uygulamasının parçası olan dosyadaki kötü amaçlı kod tespit edildiğinde Kaspersky Endpoint Security, Yedekleme konumuna taşımadan dosyayı hemen siler. Microsoft Windows 8 işletim sisteminin araçlarını kullanarak Windows Store uygulamasının bütünlüğünü geri yükleyebilirsiniz (Windows Store uygulamalarının geri yüklenmesiyle ilgili ayrıntılar için *Microsoft Windows 8 yardım dosyaları* bölümüne bakınız).

Kaspersky Endpoint Security, gelişmiş ayarlar bölümünde yapılandırılan depolama süresi geçtikten sonra Yedekleme konumundan tüm durumdaki dosyaların yedekleme kopyalarını otomatik olarak siler.

Ayrıca bir dosyanın herhangi bir kopyasını Yedekten el ile de silebilirsiniz.

Dosyaların yedek kopyalarının grubu bir tablo olarak sunulmuştur.

Yedekleme konumunu yönetirken dosyaların yedekleme kopyaları ile aşağıdaki eylemleri yapabilirsiniz:

- Dosyaların yedekleme kopyalarının listesini görüntüleyebilirsiniz.
- Yedekleme konumundan dosyaları orijinal klasörlerine geri yükleyebilirsiniz.
- Yedekleme konumundan dosyaların yedekleme kopyalarını silebilirsiniz.

Tablodaki verileri yönetirken aşağıdaki eylemleri de gerçekleştirebilirsiniz:

- Yedekleme olaylarını sütun değerine veya özel filtre koşullarına göre filtreleyebilirsiniz.
- Yedek kopya arama işlevini kullan.
- Yedek kopyalarını sırala.
- Yedek kopyalar tablosunda görüntülenen sütunları ve sırasını değiştir.

Seçilen Yedekleme olaylarını panoya kopyalayabilirsiniz. Çok sayıda Yedekleme dosyası seçmek için herhangi bir dosyanın içerik menüsüne sağ tıklayın ve **Tümünü seç**'i seçin. Taramak istemediğiniz dosyaların seçimini kaldırmak için **CTRL** tuşunu basılı tutarak tıklayın.

Yedekleme konumundan dosyaları geri yükleme

Yedekleme konumundan dosyaları geri yüklemek için:

1. Ana uygulama penceresini açın.
2. Ana uygulama penceresinin üst kısmında, **Karantina** bağlantısına tıklayarak **Depolama Alanları** penceresini açın.
3. **Depolama Alanları** penceresinde, **Yedekleme** sekmesini seçin.
4. Yedekleme konumundan tüm dosyaları geri yüklemek isterseniz herhangi bir dosyanın içerik menüsünden **Tümünü geri yükle** seçeneğini seçin.

Kaspersky Endpoint Security, yedekleme kopyalarından tüm dosyaları orijinal klasörlerine geri yükler.

5. Yedekleme konumundan bir veya daha fazla dosyayı geri yüklemek için:

   a. **Yedekleme** sekmesindeki tabloda, bir veya daha fazla Yedekleme dosyası seçin.

   Çok sayıda karantinaya alınmış nesne seçmek için herhangi bir dosyanın içerik menüsüne sağ tıklayın ve **Tümünü seç**'i seçin. Taramak istemediğiniz dosyaların seçimini kaldırmak için **CTRL** tuşunu basılı tutarak tıklayın.

   b. Dosyaları aşağıdaki yollardan biriyle geri yükleyebilirsiniz:

   - **Geri yükle** düğmesine tıklayın.
   - İçerik menüsünü görüntülemek için sağ tıklayın ve **Geri yükle** seçeneğini seçin.

Kaspersky Endpoint Security, seçilen yedekleme kopyalarını orijinal klasörlerine geri yükler.

Yedekleme konumundan dosyaların yedekleme kopyalarını silme

Yedekleme konumundan dosyaların yedekleme kopyalarını silmek için:

1. Ana uygulama penceresini açın.
2. Ana uygulama penceresinin üst kısmında, **Karantina** bağlantısına tıklayarak **Depolama Alanları** penceresini açın.
3. **Depolama Alanları** penceresinde, **Yedekleme** sekmesini seçin.
4. Tüm dosyaları Yedekten silmek istioyrsanız aşağıdaki eylemlerden irini gerçekleştirin:
   - Herhangi bir dosyanın içerik menüsünden **Tümünü sil** öğesini seçin.
   - **Depolamayı temizle** düğmesine tıklayın.

   Kaspersky Endpoint Security, Yedekleme konumundan yedekleme dosyalarının tüm kopyalarını siler.
5. Yedekleme konumundan bir veya daha fazla dosyayı silmek istiyorsanız:

   a. **Yedekleme** sekmesindeki tabloda, bir veya daha fazla Yedekleme dosyası seçin.

   Çok sayıda Yedekleme dosyası seçmek için herhangi bir dosyanın içerik menüsüne sağ tıklayın ve **Tümünü seç**'i seçin. Taramak istemediğiniz dosyaların seçimini kaldırmak için **CTRL** tuşunu basılı tutarak tıklayın.

   b. Dosyaları şu yollardan birini kullanarak silin:

   - **Kaldır** düğmesine tıklayın.
   - İçerik menüsünü görüntülemek için sağ tıklayın ve **Sil** seçeneğini seçin.

Kaspersky Endpoint Security, Yedekleme konumundan seçilen dosyaların yedekleme kopyalarını siler.

Gelişmiş uygulama ayarları

Bu bölümde, Kaspersky Endpoint Security'nin gelişmiş ayarları ve nasıl yapılandırılabilecekleri açıklanmaktadır.

Yapılandırma dosyası oluşturma ve kullanma

Kaspersky Endpoint Security ayarlarını içeren bir yapılandırma dosyası ile aşağıdaki görevleri yapabilirsiniz:

- Önceden tanımlanmış ayarların bulunduğu komut satırı aracılığıyla Kaspersky Endpoint Security'nin yerel kurulumunu yapabilirsiniz.

  Bunu yapabilmek için yapılandırma dosyasını, dağıtım kitinin bulunduğu aynı klasöre kaydetmelisiniz.

- Önceden tanımlanmış ayarlarla Kaspersky Security Center aracılığıyla Kaspersky Endpoint Security'nin uzaktan kurulumunu yapabilirsiniz.

- Kaspersky Endpoint Security ayarlarını bir bilgisayardan diğerine taşıyabilirsiniz.

Bir yapılandırma dosyası oluşturmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Gelişmiş Ayarlar** sekmesini seçin.

   Gelişmiş uygulama ayarları, pencerenin sağında görüntülenir.
3. **Ayarları Yönet** bölümünde, **Kaydet** düğmesine tıklayın.

   Microsoft Windows'un standart **Lütfen bir yapılandırma dosyası seçin** penceresi açılır.
4. Yapılandırma dosyasını kaydetmek istediğiniz yolu belirtin ve adını girin.

   > Yapılandırma dosyasını Kaspersky Endpoint Security'nin yerel veya uzaktan kurulumunda kullanmak için install.cfg olarak adlandırmalısınız.

5. **Kaydet** düğmesine tıklayın.

Kaspersky Endpoint Security ayarlarını bir yapılandırma dosyasından içe aktarmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Gelişmiş Ayarlar** sekmesini seçin.

   Gelişmiş uygulama ayarları, pencerenin sağında görüntülenir.
3. **Ayarları Yönet** bölümünde, **Yükle** düğmesine tıklayın.

   Microsoft Windows'un standart **Lütfen bir yapılandırma dosyası seçin** penceresi açılır.
4. Yapılandırma dosyasının yolunu belirtin.
5. **Aç** düğmesine tıklayın.

Kaspersky Endpoint Security ayarlarının bütün değerleri, seçilen yapılandırma dosyasına göre ayarlanacaktır.

Güvenilir bölge

Bu bölümde güvenilir bölge ile ilgili bilgiler, tarama istisnalarının yapılandırılması ve güvenilir uygulamaların listesinin oluşturulmasıyla ilgili talimatlar yer almaktadır.

Güvenilir bölge hakkında

Güvenilir bölge, Kaspersky Endpoint Security'nin etkin olduğunda izlemediği nesnelerin ve uygulamaların sistem yöneticisi tarafından yapılandırılan listesidir. Başka bir ifadeyle tarama istisnaları kümesidir.

Yönetici, işlenen nesnelerin özelliklerini ve bilgisayarda yüklü uygulamaları göz önünde bulundurarak güvenilir bölgeyi bağımsız olarak oluşturur. Kaspersky Endpoint Security belirli nesne ve uygulamalara erişimi engellediğinde nesne veya uygulamanın zararsız olup olmadığından emin değilseniz nesne ve uygulamaların güvenilir bölgeye eklenmesi gerekebilir.

Aşağıdaki nesneleri tarama dışında tutabilirsiniz:

- Belirli biçimlerdeki dosyalar
- Maske ile seçilen dosyalar
- Seçilen dosyalar
- Klasörler
- Uygulama süreçleri

Tarama istisnaları

Tarama istisnası, Kaspersky Endpoint Security'nin belirli bir nesnede virüsleri ve diğer tehditleri taramaması için karşılanması gereken koşullar kümesidir.

Tarama istisnaları, saldırganlar tarafından bilgisayar veya kullanıcı verilerine zarar vermek amacıyla kullanılabilecek meşru yazılımın güvenli bir şekilde kullanılabilmesine imkan tanır. Kötü amaçlı işlevler içermese bile bu uygulamalar zararlı yazılımda yardımcı bileşen olarak kullanılabilir. Uzaktan yönetim araçları, IRC istemcileri, FTP sunucuları, işlemleri gizlemek veya askıya almak için kullanılan çeşitli araçlar, tuş kaydediciler, parola kırıcılar ve otomatik çeviriciler bu uygulamalara örnek gösterilebilir. Bu uygulamalar virüs olarak kategorize edilmez. Suçlular tarafından bir kullanıcının bilgisayarına veya kişisel verilerine zarar vermek amacıyla kullanılabilecek yasal yazılımlarla ilgili ayrıntılar için lütfen Kaspersky Virüs Ansiklopedisi'nin www.securelist.com/threats/riskware adresindeki İnternet sitesini ziyaret edin.

Bu uygulamalar, Kaspersky Endpoint Security tarafından engellenebilir. Uygulamaların engellenmesini önlemek için kullanılan uygulamaların tarama istisnalarını yapılandırabilirsiniz. Bunun için Kaspersky Virüs Ansiklopedisi'nde belirtilen adı veya ad maskesini güvenilir bölgeye ekleyin. Örneğin bilgisayarların uzaktan yönetimi için genellikle Radmin uygulamasını kullanırsınız. Kaspersky Endpoint Security bu etkinliği şüpheli olarak değerlendirir ve engelleyebilir. Uygulamanın engellenmesini önlemek için Kaspersky Virüs Ansiklopedisi'nde belirtilen ada veya ad maskesine sahip bir tarama istisnası oluşturun.

Bilgileri toplayan ve işlenmek üzere gönderen bir uygulama bilgisayarınızda yüklü ise Kaspersky Endpoint Security bu uygulamayı zararlı yazılım olarak sınıflandırabilir. Bunu önlemek amacıyla Kaspersky Endpoint Security'yi bu belgede açıklanan şekilde yapılandırarak uygulamayı taramadan istisna tutabilirsiniz.

Tarama istisnaları, sistem yöneticileri tarafından yapılandırılan uygulama bileşenlerini ve görevlerini izleyerek kullanılabilir.

- Davranış Tespiti.
- Exploit Önleme.
- Sunucu Yetkisiz Erişim Önleme.
- Dosya Tehdidi Koruması.
- Web Tehdidi Koruması.
- Posta Tehdidi Koruması.
- Tarama görevleri.

Güvenilir uygulamaların listesi

Güvenilir uygulamaların listesi, dosya ve ağ etkinliği (kötü amaçlı etkinlik dahil) ve sistem kayıt defterine erişimi Kaspersky Endpoint Security tarafından izlenmeyen uygulamaların listesidir. Varsayılan olarak Kaspersky Endpoint Security, herhangi bir program işlemi tarafından açılan, yürütülen veya kaydedilen nesneleri tarar ve bunlar tarafından oluşturulan tüm uygulamaların ve ağ trafiğinin etkinliğini denetler. Kaspersky Endpoint Security, güvenilir uygulamaların listesini tarama dışında tutar.

Örneğin standart Microsoft Windows Not defteri uygulaması tarafından kullanılan nesnelerin tarama yapmadan güvenli olduğunu düşünüyorsanız yani bu uygulamaya güveniyorsanız Microsoft Windows Not Defteri'ni güvenilir uygulamaların listesine ekleyebilirsiniz. Ardından tarama, bu uygulama tarafından kullanılan nesneleri atlar.

Ayrıca Kaspersky Endpoint Security tarafından şüpheli olarak sınıflandırılan belirli eylemler, bir dizi uygulamanın işlevleri bağlamında güvenli olabilir. Örneğin klavyeden yazılan metne erişim, otomatik klavye düzeni değiştiriciler (Punto Switcher gibi) için rutin bir işlemdir. Bu uygulamaların özelliklerini göz önünde bulundurmak ve etkinliklerini izleme kapsamı dışında tutmak için bu uygulamaları güvenilir uygulamalar listesine eklemenizi öneririz.

Bu uygulamaların tarama dışında tutulması, Kaspersky Endpoint Security ile diğer programlar arasında uyumsuzlukların önlenmesine olanak tanır (örneğin üçüncü taraf bilgisayarın ağ trafiğinin Kaspersky Endpoint Security ve başka bir anti-virüs uygulaması tarafından iki kez taranması sorunu) ve sunucu uygulamalarını kullanırken kritik olan bilgisayar performansını da yükseltir.

Aynı zamanda güvenilir uygulamaların yürütülebilir dosyaları ve işleminde de virüsler ve diğer zararlı yazılımlar taranır. Bir uygulama, tarama istisnaları ile Kaspersky Endpoint Security taramasının tamamen dışında tutulabilir.

Tarama istisnası oluşturma

Bir nesne, bu nesneyi içeren sürücü veya klasör tarama görevlerinden birinin başlangıcında tarama kapsamına dahil edilmişse Kaspersky Endpoint Security bu nesneyi taramaz. Ancak özellikle bu nesne için özel tarama görevi başlatıldığında tarama istisnası uygulanmaz.

Bir tarama istisnası oluşturmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Genel Ayarlar** bölümünde **İstisnalar** seçeneğini belirleyin.

İstisnalar ayarları, pencerenin sağ kısmında görüntülenir.

3. **Tarama istisnaları ve güvenilir uygulamalar** bölümünde, **Ayarlar** düğmesine tıklayın.

   Tarama istisnaları sekmesinde **Güvenilir bölge** penceresi açılır.

4. **Ekle** düğmesine tıklayın.

   Tarama istisnası penceresi açılır. Bu pencerede, **Özellikler** bölümünden bir veya her iki kriteri kullanarak bir tarama istisnası oluşturabilirsiniz.

5. Bir dosya veya klasörü tarama dışında tutmak için:

   a. **Özellikler** bölümünde **Dosya veya klasör** onay kutusunu işaretleyin.

   b. **Dosya veya klasör adı** penceresinde **Tarama istisnası açıklaması** bölümünde **dosya veya klasör seçin** bağlantısına tıklayın.

   c. Dosya veya klasör adını veya dosya veya klasör adı maskesini girin veya **Gözat** düğmesine tıklayarak klasör ağacındaki dosya veya klasörü seçin.

   Bir dosya veya klasör adı maskesinde, dosya adındaki herhangi bir karakter kümesinin yerine geçmesi için yıldız karakterini (*) kullanabilirsiniz.

   Örneğin aşağıdaki yolları eklemek için maskeler kullanabilirsiniz:

   - Herhangi bir klasörde bulunan dosya yolları:
     - "`*.exe`" maskesi, EXE uzantısı olan tüm dosya yollarını içerir.
     - `Örnek` maskesi, ÖRNEK adlı tüm dosya yollarını içerir.
   - Belirtilen bir klasörde bulunan dosya yolları:
     - "C:\dir*.*" maskesi, C:\dir\ klasöründe bulunan tüm dosya yollarını içerir ancak C:\dir\ alt klasörlerindekileri içermez.
     - "C:\dir*" maskesi, C:\dir\ klasöründe bulunan tüm dosya yollarını içerir ancak C:\dir\ alt klasörlerindekileri içermez.
     - "C:\dir\" maskesi, C:\dir\ klasöründe bulunan tüm dosya yollarını içerir ancak C:\dir\ alt klasörlerindekileri içermez.
     - "C:\dir*.exe" maskesi, C:\dir\ klasöründe bulunan EXE uzantılı tüm dosya yollarını içerir ancak C:\dir\ alt klasörlerindekileri içermez.
     - "C:\dir\test" maskesi, C:\dir\ klasöründe bulunan "test" adlı tüm dosya yollarını içerir ancak C:\dir\ alt klasörlerindekileri içermez.
     - "C:\dir*\test" maskesi, C:\dir\ klasöründe bulunan "test" adlı tüm dosya yollarını içerir ancak C:\dir\ alt klasörlerindekileri içermez.
   - Belirtilen ada sahip tüm klasörlerde bulunan dosya yolları:
     - "dir*.*" maskesi, "dir" adlı klasörlerdeki tüm dosya yollarını içerir ancak bu klasörlerin alt klasörlerindekileri içermez.
     - "dir*" maskesi, "dir" adlı klasörlerdeki tüm dosya yollarını içerir ancak bu klasörlerin alt klasörlerindekileri içermez.

- "dir\" maskesi, "dir" adlı klasörlerdeki tüm dosya yollarını içerir ancak bu klasörlerin alt klasörlerindekileri içermez.
- "dir*.exe" maskesi, "dir" adlı klasörlerde bulunan EXE uzantılı tüm dosya yollarını içerir ancak bu klasörlerin alt klasörlerindekileri içermez.
- "dir\test" maskesi, "dir" adlı klasörlerdeki "test" adlı tüm dosya yollarını içerir ancak bu klasörlerin alt klasörlerindekileri içermez.

d. **Dosya veya klasör adı** penceresinde **Tamam**'a tıklayın.

Tarama istisnası penceresinin **Tarama istisnası açıklaması** bölümünde eklenen dosya veya klasörün bağlantısı görülür.

6. Belirli bir ada sahip nesneleri tarama dışında tutmak için:

a. **Özellikler** bölümünde **Nesne adı** onay kutusunu işaretleyin.

b. **Nesne adı** penceresinde **Tarama istisnası açıklaması** bölümünde **nesne adını girin** bağlantısına tıklayın.

c. Kaspersky Virüs Ansiklopedisinin sınıflandırmasına göre nesne adı veya ad maskesini girin:

d. **Nesne adı** penceresinde **Tamam**'a tıklayın.

Tarama istisnası penceresinin **Tarama istisnası açıklaması** bölümünde eklenen nesne adı bağlantısı görülür.

7. Gerekirse **Yorum** alanına, oluşturduğunuz tarama istisnasıyla ilgili kısa bir açıklama girin.

8. Tarama istisnasını kullanması gereken Kaspersky Endpoint Security bileşenlerini belirtin:

a. **Bileşenleri seç** bağlantısını etkinleştirmek için **Tarama istisnası açıklaması** bölümünde **herhangi** bağlantısına tıklayın.

b. **Bileşenleri seç** bağlantısına tıklayarak **Koruma bileşenleri** penceresini açın.

c. Tarama istisnasının uygulanması gereken bileşenlerin karşısındaki onay kutularını işaretleyin.

d. **Koruma bileşenleri** penceresinde **Tamam**'a tıklayın.

Bileşenler tarama istisnası ayarlarında belirtilirse bu istisna sadece Kaspersky Endpoint Security tarafından bu bileşenlerin taraması sırasında uygulanır.

Bileşenler tarama istisnası ayarlarında belirtilmezse bu istisna, Kaspersky Endpoint Security tarafından tüm bileşenlerin taranması sırasında uygulanır.

9. **Tarama istisnası** penceresinde **Tamam**'a tıklayın.

Eklediğiniz tarama istisnası, **Güvenilir bölge** penceresinin **Tarama istisnaları** sekmesindeki tabloda görülür. Bu tarama istisnasının yapılandırılan ayarları **Tarama istisnası açıklaması** bölümünde görülür.

10. **Güvenilir bölge** penceresinde **Tamam**'a tıklayın.

11. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Tarama istisnasını değiştirme

Tarama istisnasını değiştirmek için:

1. Uygulama Ayarları penceresini açın.
2. Soldaki **Virüse karşı koruma** bölümünü seçin.
   Virüse karşı koruma ayarları, pencerenin sağında görüntülenir.
3. **Tarama istisnaları ve güvenilir uygulamalar** bölümünde, **Ayarlar** düğmesine tıklayın.
   Tarama istisnaları sekmesinde **Güvenilir bölge** penceresi açılır.
4. Değiştirmek istediğiniz tarama istisnasını listeden seçin.
5. Aşağıdaki yöntemlerden birini kullanarak tarama istisnası ayarlarını değiştirin.
   - **Düzenle** düğmesine tıklayın.
     Tarama istisnaları penceresi açılır.
   - **Tarama istisnası açıklaması** alanındaki bağlantıya tıklayarak gereken ayarı düzenleme penceresini açın.
6. Önceki adımda **Düzenle** düğmesine tıkladıysanız **Tarama istisnası** penceresinde **Tamam**'a tıklayın.
   Bu tarama istisnasının değiştirilen ayarları **Tarama istisnası açıklaması** bölümünde görülür.
7. **Güvenilir bölge** penceresinde **Tamam**'a tıklayın.
8. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Tarama istisnasını silme

Bir tarama istisnasını silmek için:

1. Uygulama Ayarları penceresini açın.
2. Soldaki **Virüse karşı koruma** bölümünü seçin.
   Virüse karşı koruma ayarları, pencerenin sağında görüntülenir.
3. **Tarama istisnaları ve güvenilir uygulamalar** bölümünde, **Ayarlar** düğmesine tıklayın.
   Tarama istisnaları sekmesinde **Güvenilir bölge** penceresi açılır.
4. İhtiyacınız olan tarama istisnasını tarama istisnaları listesinden seçin.
5. **Kaldır** düğmesine tıklayın.
   Silinen tarama istisnası listeden kaybolur.
6. **Güvenilir bölge** penceresinde **Tamam**'a tıklayın.
7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Tarama istisnasını etkinleştirme ve devre dışı bırakma

Tarama istisnasını etkinleştirmek ve devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Soldaki **Virüse karşı koruma** bölümünü seçin.
   Virüse karşı koruma ayarları, pencerenin sağında görüntülenir.
3. **Tarama istisnaları ve güvenilir uygulamalar** bölümünde, **Ayarlar** düğmesine tıklayın.
   Tarama istisnaları sekmesinde **Güvenilir bölge** penceresi açılır.
4. Tarama istisnalarının listesinden ihtiyacınız olan istisnayı seçin.
5. Aşağıdakilerden birini yapın:
   - Tarama istisnasını etkinleştirmek için bu tarama istisnasının adının yanındaki onay kutusunu işaretleyin.
   - Tarama istisnasını devre dışı bırakmak için bu tarama istisnasının adının yanındaki onay kutusunu işaretlemeyin.
6. **Tamam**'a tıklayın.
7. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Güvenilir uygulamalar listesini düzenleme

Güvenilir uygulamalar listesini düzenlemek için:

1. Uygulama Ayarları penceresini açın.
2. Soldaki **Virüse karşı koruma** bölümünü seçin.
   Virüse karşı koruma ayarları, pencerenin sağında görüntülenir.
3. **Tarama istisnaları ve güvenilir uygulamalar** bölümünde, **Ayarlar** düğmesine tıklayın.
   Güvenilir bölge penceresi açılır.
4. **Güvenilir bölge** penceresinde, **Güvenilir uygulamalar** sekmesini seçin.
5. Güvenilir uygulamalar listesine bir uygulama eklemek için:
   a. **Ekle** düğmesine tıklayın.
   b. Açılan içerik menüsünde aşağıdakilerden birini yapın:
      - Bilgisayarda yüklü uygulamalar listesinde uygulamayı bulmak istiyorsanız menüden **Uygulamalar** öğesini seçin.
        Uygulama seç penceresi açılır.
      - İlgili uygulamanın yürütülebilir dosyasının yolunu belirtmek isterseniz **Gözat** düğmesine tıklayın.
        Microsoft Windows'ta standart **Dosyayı aç** penceresi açılır.
   c. Uygulamayı aşağıdaki yollardan birini kullanarak seçin:

- Önceki adımda **Uygulamalar**'ı seçtiyseniz bilgisayarda yüklü uygulamalar listesini seçin ve **Uygulama seç** penceresinde **Tamam**'a tıklayın.
- Önceki adımda **Gözat**'ı seçtiyseniz ilgili uygulamanın yürütülebilir dosyasını belirtin ve Microsoft Windows'un standart **Aç** penceresinde **Aç** düğmesine tıklayın.

Bu eylemler **Uygulama için tarama istisnaları** penceresini açar.

a. Seçilen uygulama için ilgili güvenilir bölge kurallarının karşısındaki onay kutularını seçin:

- **Açık dosyaları tarama**.
- **Uygulama etkinliğini izleme**.
- **Üst işlemin (uygulama) sınırlamalarını devralma**.
- **Bağlı uygulama etkinliğini izleme**.
- **Uygulama arabirimiyle etkileşime izin ver**.
- **Ağ trafiğini tarama**.

b. **Uygulama için tarama istisnaları** penceresinde **Tamam**'a tıklayın.

Eklediğiniz güvenilir uygulama, güvenilir uygulamalar listesinde görülür.

6. Güvenilir uygulamanın ayarlarını düzenlemek için:

a. Güvenilir uygulamalar listesinden bir güvenilir uygulama seçin.

b. **Düzenle** düğmesine tıklayın.

c. **Uygulama için tarama istisnaları** penceresi açılır.

d. Seçilen uygulama için ilgili güvenilir bölge kurallarının karşısındaki onay kutularını işaretleyin veya işaretini kaldırın:

> **Uygulama için tarama istisnaları** penceresinde herhangi bir güvenilir bölge kuralı seçilmezse güvenilir uygulama taramaya eklenir. Bu durumda güvenilir uygulama güvenilir uygulamalar listesinden kaldırılmaz ama onay kutusu işareti kaldırılır.

e. **Uygulama için tarama istisnaları** penceresinde **Tamam**'a tıklayın.

7. Güvenilir uygulamalar listesinden bir güvenilir uygulamayı kaldırmak için:

a. Güvenilir uygulamalar listesinden bir güvenilir uygulama seçin.

b. **Kaldır** düğmesine tıklayın.

8. **Güvenilir bölge** penceresinde **Tamam**'a tıklayın.

9. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Güvenilir uygulamalar listesindeki bir uygulamanın güvenilir bölge kurallarını etkinleştirme ve devre dışı bırakma

Güvenilir uygulamalar listesinden bir uygulamaya uygulanan güvenilir bölge kurallarının eylemini etkinleştirmek ve devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Soldaki **Virüse karşı koruma** bölümünü seçin.

   Virüse karşı koruma ayarları, pencerenin sağında görüntülenir.
3. **Tarama istisnaları ve güvenilir uygulamalar** bölümünde, **Ayarlar** düğmesine tıklayın.

   Güvenilir bölge penceresi açılır.
4. **Güvenilir bölge** penceresinde, **Güvenilir uygulamalar** sekmesini seçin.
5. Güvenilir uygulamalar listesinde, gerekli güvenilir uygulamayı seçin.
6. Aşağıdakilerden birini yapın:
   - Bir güvenilir uygulamayı Kaspersky Endpoint Security taramasının dışında tutmak için uygulamanın adının yanındaki onay kutusunu işaretleyin.
   - Bir güvenilir uygulamayı Kaspersky Endpoint Security taramasına dahil etmek için uygulamanın adının yanındaki onay kutusunu işaretlemeyin.
7. **Tamam**'a tıklayın.
8. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Güvenilir sistem sertifikası depolama alanını kullanma

Sistem sertifikası depolama alanının kullanılması, güvenilir bir dijital imza ile imzalanan uygulamaları virüs taramasından istisna tutmanıza olanak tanır. Kaspersky Endpoint Security, bu tür uygulamaları otomatik olarak *Güvenilir* gruba atar.

Güvenilir sistem sertifikası depolama alanını kullanmaya başlamak için:

1. Uygulama Ayarları penceresini açın.
2. Soldaki **Virüse karşı koruma** bölümünü seçin.

   Virüse karşı koruma ayarları, pencerenin sağında görüntülenir.
3. **Tarama istisnaları ve güvenilir uygulamalar** bölümünde, **Ayarlar** düğmesine tıklayın.

   Güvenilir bölge penceresi açılır.
4. **Güvenilir bölge** penceresinde **Güvenilir sistem sertifikası deposu** sekmesini seçin.
5. **Güvenilir sistem sertifikası deposunu kullan** onay kutusunu işaretleyin.

6. **Güvenilir sistem sertifikası deposu** açılır listesinde Kaspersky Endpoint Security tarafından hangi sistem deposunun güvenilir olarak değerlendirilmesi gerektiğini seçin.

7. **Güvenilir bölge** penceresinde **Tamam**'a tıklayın.

8. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Kaspersky Endpoint Security Kendini Koruma

Bu bölümde, Kaspersky Endpoint Security'nin kendini koruma ve uzaktan denetim koruması mekanizmaları açıklanmakta ve bu mekanizmaların ayarlarını yapılandırma talimatları sağlanmaktadır.

Kaspersky Endpoint Security Kendini Koruma Hakkında

Kaspersky Endpoint Security, bilgisayarı Kaspersky Endpoint Security'nin çalışmasını engellemeye veya hatta bilgisayardan silmeye çalışan zararlı yazılımları da kapsayan kötü amaçlı programlardan korur.

Bilgisayarın güvenlik sisteminin istikrarı, Kaspersky Endpoint Security'deki kendini koruma ve uzaktan denetim savunma mekanizmaları ile sağlanır.

Kendini Koruma mekanizması, sabit sürücüdeki uygulama dosyalarının, bellek işlemlerinin ve sistem kayıt defterindeki girişlerin değiştirilmesini veya silinmesini önler.

Uzaktan Denetim Savunması uzak bilgisayar tarafından uygulama hizmetlerini denetleme çabalarının tamamını engeller.

64 bit işletim sistemlerine sahip bilgisayarlarda sabit sürücüdeki ve sistem kayıt defteri girişlerindeki uygulama dosyalarının değiştirilmesini ve silinmesini önlemek için sadece Kaspersky Endpoint Security Kendini Koruma mevcuttur.

Kendini Korumayı etkinleştirme veya devre dışı bırakma

Kaspersky Endpoint Security'nin Kendini Koruma mekanizması varsayılan olarak etkindir. Gerekirse Kendini Koruma'yı devre dışı bırakabilirsiniz.

Kendini Korumayı etkinleştirmek veya devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol kısmında, **Gelişmiş Ayarlar** sekmesini seçin.

   Gelişmiş uygulama ayarları, pencerenin sağında görüntülenir.

3. Aşağıdakilerden birini yapın:

   - Kendini Koruma mekanizmasını etkinleştirmek için **Kendini Korumayı etkinleştir** onay kutusunu seçin.

- Kendini Koruma mekanizmasını devre dışı bırakmak için **Kendini Korumayı etkinleştir** onay kutusunun işaretini kaldırın.

4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Uzaktan Denetim Korumasını etkinleştirme veya devre dışı bırakma

Uzaktan denetim koruması mekanizması varsayılan olarak etkindir. Gerekirse uzaktan denetim koruması mekanizmasını devre dışı bırakabilirsiniz.

Uzaktan denetim koruması mekanizmasını etkinleştirmek ya da devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Gelişmiş Ayarlar** sekmesini seçin.

   Gelişmiş uygulama ayarları, pencerenin sağında görüntülenir.
3. Aşağıdakilerden birini yapın:

   - Uzaktan denetim koruması mekanizmasını etkinleştirmek için **Sistem hizmetinin harici yönetimini devre dışı bırak**'ı seçin.
   - Uzaktan denetim koruması mekanizmasını devre dışı bırakmak için **Sistem hizmetinin harici yönetimini devre dışı bırak** seçimini kaldırın.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Uzaktan yönetim uygulamalarını destekleme

Harici denetim koruması etkinken bazen uzak bir yönetim uygulaması kullanmanız gerekebilir.

Uzaktan yönetim uygulamalarının çalışmasını etkinleştirmek için:

1. Uygulama Ayarları penceresini açın.
2. Soldaki **Virüse karşı koruma** bölümünü seçin.

   Virüse karşı koruma ayarları, pencerenin sağında görüntülenir.
3. **Tarama istisnaları ve güvenilir uygulamalar** bölümünde, **Ayarlar** düğmesine tıklayın.

   Güvenilir bölge penceresi açılır.
4. **Güvenilir bölge** penceresinde, **Güvenilir uygulamalar** sekmesini seçin.
5. **Ekle** düğmesine tıklayın.
6. Açılan içerik menüsünde aşağıdakilerden birini yapın:

   - Bilgisayarda yüklü uygulamalar listesinden uzaktan yönetim uygulamasını bulmak için **Uygulamalar** öğesini seçin.

     Uygulama seç penceresi açılır.

- Uzaktan yönetim uygulamasının yürütülebilir dosya yolunu belirtmek için **Gözat**'ı seçin.

  Microsoft Windows'ta standart **Dosyayı aç** penceresi açılır.

7. Uygulamayı aşağıdaki yollardan birini kullanarak seçin:

   - Önceki adımda **Uygulamalar**'ı seçtiyseniz bilgisayarda yüklü uygulamalar listesini seçin ve **Uygulama seç** penceresinde **Tamam**'a tıklayın.

   - Önceki adımda **Gözat**'ı seçtiyseniz ilgili uygulamanın yürütülebilir dosyasını belirtin ve Microsoft Windows'un standart **Aç** penceresinde **Aç** düğmesine tıklayın.

   Bu eylemler **Uygulama için tarama istisnaları** penceresini açar.

8. **Uygulama etkinliğini izleme** onay kutusunu işaretleyin.

9. **Uygulama için tarama istisnaları** penceresinde **Tamam**'a tıklayın.

   Eklediğiniz güvenilir uygulama, güvenilir uygulamalar listesinde görülür.

10. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Kaspersky Endpoint Security'nin performansı ve diğer uygulamalarla uyumluluğu

Bu bölümde Kaspersky Endpoint Security'nin performansı ve diğer uygulamalarla uyumluluğu hakkında bilgi verilmekte ve Kaspersky Endpoint Security'nin çalışma modu ve tespit edilebilir nesne türlerinin seçilmesi kılavuzu da yer almaktadır.

Kaspersky Endpoint Security'nin performansı ve diğer uygulamalarla uyumluluğu hakkında

Kaspersky Endpoint Security'nin Performansı

Kaspersky Endpoint Security'nin performansı, tespit edilebilen bilgisayara zarar verebilecek türden nesne sayısına ve bilgisayarın kaynaklarının kullanımına ve enerji tüketimine bağlıdır.

Tespit edilebilir nesne türlerini seçme

Kaspersky Endpoint Security, bilgisayarın korumasında ince ayarlamalar yapmanıza ve çalışması sırasında uygulamanın tespit ettiği nesne türlerini seçmenize olanak tanır. Kaspersky Endpoint Security daima işletim sisteminde virüs, solucan ve Truva atlarını tarar. Bu nesne türlerinin taranmasını devre dışı bırakamazsınız. Bu zararlı yazılımlar bilgisayara büyük zarar verebilir. Bilgisayarınızda daha fazla güvenlik sağlamak amacıyla, suçlular tarafından bilgisayarınıza veya kişisel verilerinize zarar vermek için kullanılabilecek yasal yazılımların izlenmesini etkinleştirerek tespit edilebilir nesne türlerinin dizisini genişletebilirsiniz.

Enerji tasarrufu modunu kullanma

Uygulamanın enerji tüketimi, taşınabilir bilgisayarlar için önemli bir konudur. Kaspersky Endpoint Security zamanlanmış görevleri genellikle önemli ölçüde kaynak kullanır. Bilgisayar pille çalışırken daha az enerji harcamak için enerji tasarrufu modunu kullanabilirsiniz.

Enerji tasarrufu modunda aşağıdaki zamanlanmış görevler otomatik olarak ertelenir.

- Güncelleme görevi
- Tam Tarama görevi
- Kritik Alanları Tarama görevi
- Özel Tarama görevi
- Zayıf Nokta Taraması görevi
- Bütünlük Denetimi görevi

Enerji tasarrufu modunun etkin olup olmadığına bakmaksızın taşınabilir bir bilgisayar pil moduna geçtiğinde Kaspersky Endpoint Security şifreleme görevlerini duraklatır. Taşınabilir bilgisayar pil gücünden priz gücüne geçtiğinde uygulama, şifreleme görevlerini sürdürür.

Diğer uygulamalar için bilgisayar kaynağı yaratma

Kaspersky Endpoint Security tarafından bilgisayar kaynaklarının kullanılması, diğer uygulamaların performansını etkileyebilir. CPU ve sabit sürücü alt sistemlerinde yük arttığında eşzamanlı çalışma sorununu çözmek için Kaspersky Endpoint Security zamanlanmış görevleri duraklatabilir ve diğer uygulamalar için kaynak yaratabilir.

Ancak CPU kaynakları kullanılabilir olduğunda bir dizi uygulama hemen başlar ve arka plan modunda çalışmaya geçer. Taramanın diğer uygulamaların performansına bağlı olmasını önlemek için işletim sistemi kaynaklarını bunlara kullandırmamak daha iyi olacaktır.

Gerekirse bu görevleri elle başlatabilirsiniz.

Gelişmiş temizleme teknolojisini kullanma

Günümüzde kötü amaçlı programlar bir işletim sisteminin en düşük düzeylerine nüfuz edebilmekte ve bu da, bu programların ortadan kaldırılmasını neredeyse imkansız hale getirmektedir. İşletim sistemindeki kötü amaçlı etkinlikleri tespit ettikten sonra Kaspersky Endpoint Security, özel gelişmiş temizleme teknolojisini kullanan kapsamlı bir temizleme işlemi gerçekleştirmektedir. *Gelişmiş temizleme teknolojisi*, RAM'da işlem başlatmış olan ve diğer yöntemleri kullanarak Kaspersky Endpoint Security'nin bu programları kaldırmasını önleyen kötü amaçlı programların işletim sisteminden temizlenmesine yöneliktir. Sonuç olarak tehdit etkisiz duruma getirilir. Gelişmiş Virüs Temizleme devam ederken yeni işlem başlatmamanız veya işletim sistemi kayıt defterini düzenlememeniz önerilir. Gelişmiş virüs temizleme teknolojisi, oldukça fazla İşletim sistemi kaynağı kullanır ve bu da diğer uygulamaları yavaşlatabilir.

İş istasyonları için Microsoft Windows'un kurulu olduğu bir bilgisayarda Gelişmiş Virüs Temizleme işlemi tamamlandıktan sonra Kaspersky Endpoint Security, bilgisayarı yeniden başlatmak için kullanıcının iznini ister. Sistemin yeniden başlatılmasının ardından Kaspersky Endpoint Security, zararlı yazılım dosyalarını siler ve bilgisayarın "hafif" tam taramasını başlatır.

Dosya sunucularıyla ilgili Kaspersky Endpoint Security özelliklerinden dolayı Dosya sunucuları için Microsoft Windows'un kurulu olduğu bir bilgisayarda yeniden yükleme istemi mümkün değildir. Dosya sunucusunun plansız bir şekilde yeniden başlatılması, sunucu verilerinin geçici olarak kullanılamaması veya kaydedilmemiş verilerin kaybedilmesi gibi sorunlara neden olabilir. Dosya sunucusunun katı bir şekilde zamanlamaya göre yeniden başlatılması önerilir. Bu nedenle dosya sunucuları için Gelişmiş Temizleme teknolojisi varsayılan olarak devre dışıdır.

Bir dosya sunucusunda etkin bir virüs tespit edilirse Etkin Temizleme gerektiğini belirten bilgilerle olay, Kaspersky Security Center'a aktarılır. Dosya sunucusundaki etkin virüsü temizlemek için dosya sunucuları için Etkin Temizleme teknolojisini etkinleştirin ve dosya sunucusu kullanıcıları için uygun bir zamanda *Virüs taraması* grup görevini başlatın.

Tespit edilebilir nesne türlerini seçme

Tespit edilebilir nesne türlerini seçmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünü seçin.

   Virüse karşı koruma ayarları, pencerenin sağında görüntülenir.
3. **Nesneler** bölümünde **Ayarlar** düğmesine tıklayın.

   Tespit edilecek nesneler penceresi açılır.
4. Kaspersky Endpoint Security'nin tespit etmesini istediğiniz nesne türlerinin karşısındaki onay kutularını işaretleyin:
   - **Zararlı araçlar**
   - **Reklam yazılımı**
   - **Otomatik çeviriciler**
   - **Diğer**
   - **Zarar verebilecek sıkıştırılmış dosyalar**
   - **Çoklu sıkıştırılmış dosyalar**
5. **Tamam**'a tıklayın.

   Tespit için nesneler penceresi kapanır. **Nesneler** bölümünde, seçilen nesne türleri **Aşağıdaki nesne türlerinin algılanması etkinleştirildi** altında listelenir.
6. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

İş istasyonları için Gelişmiş Temizleme teknolojisini etkinleştirme veya devre dışı bırakma

İş istasyonları için Gelişmiş Temizleme teknolojisini etkinleştirmek veya devre dışı bırakmak amacıyla:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Virüse Karşı Koruma** bölümünü seçin.

Virüse karşı koruma ayarları, pencerenin sağında görüntülenir.

3. Pencerenin sağ tarafında aşağıdakilerden birini yapın:

   - Gelişmiş temizleme teknolojisini etkinleştirmek için **Gelişmiş Temizleme Teknolojisini Etkinleştir** seçeneğini seçin.

   - Gelişmiş temizleme teknolojisini devre dışı bırakmak için **Gelişmiş Temizleme Teknolojisini Etkinleştir** seçeneğinin işaretini kaldırın.

4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Kaspersky Security Center'dan Gelişmiş Virüs Temizleme görevi başlatıldığında işletim sistemi işlevlerinin büyük kısmı kullanıcı tarafından kullanılamaz. Görevler tamamlandıktan sonra iş istasyonu yeniden başlatılır.

Dosya sunucuları için Gelişmiş Temizleme teknolojisini etkinleştirme veya devre dışı bırakma

Dosya sunucuları için Gelişmiş Temizleme teknolojisini etkinleştirmek amacıyla aşağıdaki eylemlerden birini gerçekleştirin:

- Etkin Kaspersky Security Center ilkesinin özelliklerinde Gelişmiş Virüs Temizleme teknolojisini etkinleştirin. Bunun için:

  a. İlke özellikleri penceresinde **Genel Koruma Ayarları** bölümünü açın.

  b. **Gelişmiş Temizleme Teknolojisini Etkinleştir** onay kutusunu işaretleyin.

  c. Değişiklikleri kaydetmek için ilke özellikleri penceresinde **Tamam**'a tıklayın.

- Kaspersky Security Center'ın Virüs Taraması grup görevinin özelliklerinde, **Gelişmiş Temizleme işlemini derhal çalıştır** onay kutusunu işaretleyin.

Dosya sunucuları için Gelişmiş Temizleme teknolojisini devre dışı bırakmak amacıyla aşağıdaki eylemlerden birini gerçekleştirin:

- Kaspersky Security Center ilkesinin özelliklerinde Gelişmiş Temizleme teknolojisini etkinleştirin. Bunun için:

  a. İlke özellikleri penceresinde **Genel Koruma Ayarları** bölümünü açın.

  b. **Gelişmiş Temizleme Teknolojisini Etkinleştir** onay kutusunu işaretlemeyin.

  c. Değişiklikleri kaydetmek için ilke özellikleri penceresinde **Tamam**'a tıklayın.

- Kaspersky Security Center'ın Virüs Taraması grup görevinin özelliklerinde, **Gelişmiş Temizleme işlemini derhal çalıştır** onay kutusunu işaretlemeyin.

Enerji tasarrufu modunu etkinleştirme veya devre dışı bırakma

Enerji tasarruf modunu etkinleştirmek veya devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Gelişmiş Ayarlar** sekmesini seçin.

   Gelişmiş uygulama ayarları, pencerenin sağında görüntülenir.
3. **İşletim modu** bölümünde, **Ayarlar** düğmesine tıklayın.

   İşletim modu penceresi açılır.
4. **İşletim modu** penceresinde aşağıdaki eylemleri gerçekleştirin:

   - Enerji tasarruf modunu etkinleştirmek için **Pil gücüyle çalışırken zamanlanmış görevleri başlatma** onay kutusunu işaretleyin.

     Enerji tasarruf modu etkinleştirildiğinde ve bilgisayar pil gücüyle çalışırken aşağıdaki görevler zamanlanmış olsa bile çalıştırılmaz:

     - Güncelleme görevi
     - Tam Tarama görevi
     - Kritik Alanları Tarama görevi
     - Özel Tarama görevi
     - Zayıf Nokta Taraması görevi
     - Bütünlük Denetimi görevi
   - Enerji tasarruf modunu devre dışı bırakmak isterseniz **Pil gücüyle çalışırken zamanlanmış görevleri başlatma** onay kutusunu işaretlemeyin. Bu durumda Kaspersky Endpoint Security, bilgisayarın güç kaynağına bakmaksızın zamanlanmış görevleri gerçekleştirir.
5. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Diğer uygulamalar için kaynak yaratmayı etkinleştirme veya devre dışı bırakma

Diğer uygulamalar için kaynak yaratmayı etkinleştirmek veya devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Gelişmiş Ayarlar** sekmesini seçin.

   Gelişmiş uygulama ayarları, pencerenin sağında görüntülenir.
3. **İşletim modu** bölümünde, **Ayarlar** düğmesine tıklayın.

   İşletim modu penceresi açılır.
4. **İşletim modu** penceresinde aşağıdaki eylemleri gerçekleştirin:

   - Kaynakların diğer uygulamalar için kaynak yaratmakta kullanıldığı modu etkinleştirmek isterseniz, **Diğer uygulamalar için kaynak yarat** onay kutusunu işaretleyin.

Diğer uygulamalar için kaynak yaratmak için yapılandırıldığında Kaspersky Endpoint Security, diğer uygulamaları yavaşlatan zamanlanmış görevleri erteler.

- Güncelleme görevi
- Tam Tarama görevi
- Kritik Alanları Tarama görevi
- Özel Tarama görevi
- Zayıf Nokta Taraması görevi
- Bütünlük Denetimi görevi

- Kaynakların diğer uygulamalar için kaynak yaratmakta kullanıldığı modu devre dışı bırakmak isterseniz, **Diğer uygulamalar için kaynak yarat** onay kutusunun işaretini kaldırın. Bu durumda Kaspersky Endpoint Security, diğer uygulamaların işleminden bağımsız olarak zamanlanmış görevleri gerçekleştirir.

Varsayılan olarak uygulama, diğer uygulamalar için kaynak yaratacak şekilde yapılandırılmıştır.

5. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Parola koruması

Bu bölümde, Kaspersky Endpoint Security'ye erişimi parolayla kısıtlama hakkında bilgi verilmektedir.

Kaspersky Endpoint Security'ye erişimi kısıtlama hakkında

Bilgisayar okuryazarlığı düzeyi farklı kullanıcılar aynı bilgisayarı kullanabilir. Kaspersky Endpoint Security'ye ve ayarlarına sınırsız erişiminiz varsa bilgisayar korumasının genel düzeyi düşebilir.

Kaspersky Endpoint Security'ye erişimi bir kullanıcı adı ve parola ile kısıtlayabilir ve uygulamanın kullanıcıdan bu kimlik bilgilerini isteyeceği işlemleri belirleyebilirsiniz:

Uygulamanın önceki bir sürümünü Kaspersky Endpoint Security 10 Service Pack 2 for Windows'a yükseltirken (belirlendiyse) parola korunmaz. Parola koruması ayarlarını ilk kez düzenlemek için KLAdmin varsayılan kullanıcı adını kullanın.

Parola korumasını etkinleştirme ve devre dışı bırakma

Uygulamaya erişimi sınırlarken bir parola kullandığınızda dikkatli olmanızı öneririz. Parolayı unutursanız parola korumasını devre dışı bırakma talimatları için Kaspersky Teknik Destek ile irtibat kurun.

Parola korumasını etkinleştirmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Genel Ayarlar** bölümünde **Arabirim** seçeneğini belirleyin.

   Kaspersky Endpoint Security arabiriminin ayarları, pencerenin sağ kısmında görüntülenir.
3. **Parola koruması** bölümünde, **Ayarlar** düğmesine tıklayın.

   Parola koruması penceresi açılır.
4. **Parola korumasını etkinleştir** onay kutusunu seçin.
5. **Kullanıcı adı** alanına, daha sonra parola korumalı işlemler gerçekleştirildiğinde **Parola denetimi** penceresinde belirtilmesi gereken kullanıcı adını girin.
6. **Yeni parola** alanına, uygulamaya erişim parolasını yazın.
7. **Parolayı onayla** alanında parolayı onaylayın.
8. Uygulamayla tüm işlemlere erişimi sınırlamak istiyorsanız, **Parola alanı** bölümünde **Tümünü seç** düğmesine tıklayın.
9. Kullanıcı erişimini geçici olarak sınırlamak isterseniz, **Parola alanı** bölümünde, ilgili işlemlerin adlarının karşısındaki onay kutularını seçin:
   - **Uygulama ayarlarını yapılandır**.
   - **Uygulamadan çık**.
   - **Koruma bileşenlerini devre dışı bırak ve tarama görevlerini durdur**.
   - **Denetim bileşenlerini devre dışı bırak**.
   - **Anahtarı kaldır**.
   - **Uygulamayı kaldır / değiştir / geri yükle**.
   - **Şifrelenmiş sürücülerdeki verilere erişimi geri yükle**.
   - **Raporları görüntüle**.
10. **Tamam** düğmesine tıklayın.

    Uygulama, girilen parolaları doğrular. Parolalar eşleşiyorsa, uygulama parolayı uygular. Parolalar eşleşmiyorsa, uygulama **Parolayı onayla** alanında parolayı onaylamanızı ister.
11. Değişiklikleri kaydetmek için uygulama ayarları penceresinde, **Kaydet** düğmesine tıklayın.

Parola koruması etkinleştirildikten sonra, parola kapsamına dahil edilen bir işlem gerçekleştirildiğinde uygulama her seferinde parola isteyecektir. Geçerli oturum sırasında parola korumalı bir işlem gerçekleştirmeye çalıştığınız her seferde uygulamanın parola sormasını istemiyorsanız, **Parola kontrolü** pencer**Parolayı geçerli oturum için kaydet** onay kutusunu seçin.

Parolayı geçerli oturum için kaydet onay kutusunun işareti kaldırılırsa, uygulama parola korumalı işlemi gerçekleştirmeye çalıştığınız her seferde parolayı sorar.

Parola korumasını devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Genel Ayarlar** bölümünde **Arabirim** seçeneğini belirleyin.

   Kaspersky Endpoint Security arabiriminin ayarları, pencerenin sağ kısmında görüntülenir.
3. **Parola koruması** bölümünde, **Ayarlar** düğmesine tıklayın.

   Parola koruması penceresi açılır.
4. **Parola korumasını etkinleştir** onay kutusunun işaretini kaldırın.

   Sadece KLAdmin olarak oturum açtıysanız Parola korumasını devre dışı bırakabilirsiniz. Başka bir kullanıcı hesabı veya geçici parola kullanıyorsanız parola korumasını devre dışı bırakamazsınız.
5. **Tamam** düğmesine tıklayın.
6. Değişiklikleri kaydetmek için uygulama ayarları penceresinde, **Kaydet** düğmesine tıklayın.

   Parola denetimi penceresi açılır.
7. Kullanıcı adını **Kullanıcı adı** alanına girin.
8. **Parola** alanına Kaspersky Endpoint Security için erişim parolasını girin.
9. **Tamam**'a tıklayın.

Kaspersky Endpoint Security erişim parolasını değiştirme

Kaspersky Endpoint Security'nin erişim parolasını değiştirmek için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Gelişmiş Ayarlar** sekmesini seçin.
3. **Parola koruması** bölümünde, **Ayarlar** düğmesine tıklayın.

   Parola koruması penceresi açılır.
4. Kullanıcı adını **Kullanıcı adı** alanına girin.
5. **Yeni parola** alanında, uygulamaya erişim için yeni bir parola girin.
6. **Parolayı onayla** alanına yeni parolayı tekrar girin.
7. **Tamam**'a tıklayın.

   Uygulama, girilen parolaları doğrular. Parolalar eşleşiyorsa uygulama yeni parolayı uygular ve **Parola koruması** penceresini kapatır. Parolalar eşleşmiyorsa, uygulama **Parolayı onayla** alanında parolayı onaylamanızı ister.
8. Değişiklikleri kaydetmek için uygulama ayarları penceresinde, **Kaydet** düğmesine tıklayın.

Geçici bir parolanın kullanılması hakkında

Bir Kaspersky Security Center ilkesiyle yönetilen istemci bilgisayarlarda çalışırken kullanıcıların, ilke düzeyinde parola korumalı Kaspersky Endpoint Security ile işlemler yapması gerekebilir. Parola koruması etkinleştirildiğinde yalnızca Kaspersky Security Center yöneticisi parola kapsamında belirtilen işlemleri gerçekleştirebilir. Bununla birlikte Kaspersky Security Center ile bağlantı kesilmişse (kullanıcının kurumsal ağın dışında olması gibi) Kaspersky Security Center'ın yerel arabirimi ile çalışma işlevleri sınırlandırılır.

Bir kullanıcıya, ilke ayarlarında belirtilen parolayı vermeden gerekli işlemleri gerçekleştirme olanağı sağlamak için Kaspersky Security Center yöneticisi geçici bir parola oluşturabilir. Geçici bir parola, sınırlı bir geçerlilik süresine ve sınırlı bir eylem kapsamına sahiptir. Kullanıcı geçici parolayı uygulamanın yerel arabirimine girdikten sonra Kaspersky Security Center yöneticisi tarafından izin verilen işlemler yapılabilir.

Geçici parolanın süresi dolduğunda Kaspersky Endpoint Security, Kaspersky Security Center ilkesinin ayarlarına uygun olarak çalışmaya devam eder. İlke düzeyinde parola korumalı işlemler kullanıcı tarafından gerçekleştirilemez hale gelir.

Kaspersky Security Center Yönetim Konsolunu kullanarak geçici bir şifre oluşturma

Geçici bir şifre oluşturmak ve bunu bir kullanıcıya göndermek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe Geçici parola isteyen kullanıcının bilgisayarını içeren yönetim grubunun adının bulunduğu klasörü açın.
3. Çalışma alanında, **Aygıtlar** sekmesini seçin.
4. Geçici parola isteyen kullanıcıya ait bilgisayarın içerik menüsünde **Özellikler**'i seçin.

   Özellikler: <Bilgisayar adı> penceresi açılır.
5. **Özellikler:: <Bilgisayar adı>** penceresinde **Uygulamalar** bölümünü seçin.
6. Windows için Kaspersky Endpoint Security Service Pack 2'yi seçin ve aşağıdaki yöntemlerden birini kullanarak uygulama özellikleri penceresini açın.

   - Ekranında altındaki **Özellikler** düğmesine tıklayın.
   - Uygulamanın içerik menüsünde **Özellikler**'i seçin.

   Uygulama Ayarları "<Uygulama adı>" penceresi açılır.
7. **Uygulama ayarları "<Uygulama adı>"** penceresinde **Gelişmiş Ayarlar** bölümünde **Uygulama ayarları** alt bölümünü seçin.
8. **Parola koruması** bölümünde, **Ayarlar** düğmesine tıklayın.

   Parola koruması penceresi açılır.
9. **Parola koruması** penceresinde **Geçici parola** bölümünde **Ayarlar** düğmesine tıklayın.

   Bu düğme, parola koruması bilgisayarda çalışan Kaspersky Security Center ilkesindeki Kaspersky Security Center için etkinleştirilmişse kullanılabilir.

   Geçici parola oluştur penceresi açılır.

10. **Sona erme tarihi** alanında kullanıcının geçici parolayı artık kullanamayacağı tarihi belirleyin.

    Bu tarihte, geçici parola geçersiz hale gelir. Kaspersky Endpoint Security'nin yerel arabiriminde işlemlerin gerçekleştirilmesine erişim sağlamak için yeni bir geçici parola oluşturulmalıdır.

11. **Geçici parola kapsamı** tablosunda, geçici parola geçerli iken kullanıcı tarafından kullanılabilecek işlemlerin karşısındaki onay kutularını işaretleyin.

12. **Oluştur** düğmesine tıklayın.

    Şifrelenmiş bir parola içeren **Geçici parola** penceresi açılır.

13. Parolayı ve uygulanmasıyla ilgili talimatları kopyalayın ve bunları kullanıcıya gönderin.

Kaspersky Endpoint Security arabiriminde geçici bir parola uygulama

Bu talimatlar, Kaspersky Endpoint Security'nin yüklü olduğu istemci bilgisayarların kullanıcılarına yöneliktir.

Geçici parola uygulamak için:

1. Uygulama Ayarları penceresini açın.

2. Pencerenin sol kısmında, **Gelişmiş Ayarlar** sekmesini seçin.

   Uygulama ayarları, pencerenin sağında görüntülenir.

3. **Parola koruması** bölümünde, **Geçici parola** düğmesine tıklayın.

   Geçici parola penceresi açılır.

4. **Geçici parolayı etkinleştir** onay kutusunu seçin.

5. Giriş alanında, Kaspersky Security Center yöneticisinden alınan parolayı belirtin.

6. Değişiklikleri kaydetmek için **Tamam**'a tıklayın.

Geçici parola uygulandıktan sonra, Kaspersky Security Center yöneticisi tarafından belirtilen işlemler kullanılabilecektir. **Geçici parola** penceresinde geçici parolanın sona erme tarihi ve izin verilen işlemler görüntülenir.

Kaspersky Security Center vasıtasıyla uygulamanın uzaktan yönetimi

Bu bölümde, Kaspersky Security Center'dan Kaspersky Endpoint Security'nin yönetimi açıklanmaktadır.

Kaspersky Security Center'dan uygulamanın yönetimi hakkında

Kaspersky Security Center, Kaspersky Endpoint Security'yi uzaktan yüklemenizi ve kaldırmanızı, başlatmanızı ve durdurmanızı, uygulama ayarlarını yapılandırmanızı, kullanılabilir uygulama bileşenlerini değiştirmenizi, anahtar eklemenizi, güncelleme ve tarama görevlerini başlatmanızı sağlar.

Bu belgede bulunmayan Kaspersky Security Center vasıtasıyla uygulamanın uzaktan yönetimi hakkında ek bilgi için *Kaspersky Security Center Yönetici Kılavuzu*'na bakınız.

Uygulama, Kaspersky Endpoint Security yönetim eklentisini kullanarak Kaspersky Security Center aracılığıyla yönetilebilir.

Yönetim eklentisinin sürümü, istemci bilgisayarda kurulu olan Kaspersky Endpoint Security sürümünden farklı olabilir. Yönetim eklentisinin kurulu sürümü Kaspersky Endpoint Security'nin kurulu sürümünden daha az işleve sahipse eksik işlevlerin ayarları yönetim eklentisi tarafından düzenlenmez. Bu ayarlar, Kaspersky Endpoint Security'nin yerel arabiriminden kullanıcı tarafından değiştirilebilir.

Yönetim eklentilerinin farklı sürümleriyle çalışırken dikkat edilmesi gereken hususlar

Bir yönetim eklentisini aşağıdaki öğeleri değiştirmek için kullanabilirsiniz:

- İlkeler
- İlke profilleri
- Grup görevleri
- Yerel görevler
- Kaspersky Endpoint Security'nin yerel ayarları

Yalnızca Kaspersky Endpoint Security'nin yönetim eklentisine uyumluluğu ile ilgili bilgide belirtilen sürüme denk veya daha yüksek sürümde bir yönetim eklentiniz varsa Kaspersky Endpoint Security'yi Kaspersky Security Center üzerinden yönetebilirsiniz. Dağıtım kiti'nde bulunan installer.ini dosyasından yönetim eklentisinin gerekli minimum sürümünü görebilirsiniz.

Herhangi bir bileşen açılırsa yönetim eklentisi, uyumluluk bilgisini kontrol eder. Yönetim eklentisinin sürümü, uyumluluk bilgisinde belirtilen sürüme denk ya da daha yüksekse bu bileşenin ayarlarını değiştirebilirsiniz. Değilse seçilen bileşenin ayarlarını değiştirmek için yönetim eklentisini kullanamazsınız. Yönetim eklentisinin sürümünü yükseltmeniz önerilir.

Yönetim eklentisinin daha yüksek bir sürümünü kullanarak önceden tanımlanan ayarları değiştirme

Yönetim eklentisinin daha yüksek bir sürümünü kullanarak önceden tanımlanan bütün ayarları değiştirebilir ve yönetim eklentisinin önceki kullandığınız sürümünde bulunmayan yeni ayarları yapılandırabilirsiniz.

Yeni ayarlar için yönetim eklentisinin daha üst sürümü; bir ilke, ilke profili veya görev ilk kez kaydedildiğinde varsayılan değerleri atar.

Yönetim eklentisinin daha üst sürümünü kullanarak bir ilke, ilke profili veya grubun ayarlarını değiştirdikten sonra, bu bileşenler yönetim eklentisinin önceki sürümlerinde mevcut olmayacaktır. Kaspersky Endpoint Security'nin yerel ayarları ve yerel görevlerin ayarları, önceki sürümlerin yönetim eklentileri için hala kullanılabilir.

İstemci bilgisayarda Kaspersky Endpoint Security'nin başlatılması ve durdurulması

İstemci bilgisayarda uygulamayı başlatmak veya durdurmak için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen cihazlar** klasöründe, ilgili istemci bilgisayarın ait olduğu yönetim grubu adının bulunduğu klasörü açın.
3. Çalışma alanında, **Aygıtlar** sekmesini seçin.
4. Uygulamayı başlatmak veya durdurmak istediğiniz bilgisayarı seçin.
5. İstemci bilgisayarın içerik menüsünü görüntülemek için sağ tıklayın ve **Özellikler**'i seçin.

   İstemci bilgisayar özellikleri penceresi açılır.
6. İstemci bilgisayar özellikleri penceresinde **Uygulamalar** bölümünü seçin.

   İstemci bilgisayarda yüklü Kaspersky uygulamalarının listesi, istemci bilgisayar özellikleri penceresinin sağında görülür.
7. Kaspersky Endpoint Security'yi seçin.
8. Aşağıdakileri uygulayın:

   - Uygulamayı başlatmak için Kaspersky uygulamalarının listesinin sağındaki düğmesine tıklayın veya aşağıdakileri uygulayın:

     a. Kaspersky Endpoint Security'nin içerik menüsünden **Özellikler**'i seçin veya Kaspersky uygulamalarının listesinin altında yer alan **Özellikler** düğmesine tıklayın.

     Kaspersky Endpoint Security for Windows ayarları penceresi açılır.

     b. **Genel** bölümünde, pencerenin sağındaki **Başlat** düğmesine tıklayın.

   - Uygulamayı durdurmak için Kaspersky uygulamalarının listesinin sağındaki düğmesine tıklayın veya aşağıdakileri uygulayın:

     a. Kaspersky Endpoint Security'nin içerik menüsünden **Özellikler**'i seçin veya Kaspersky uygulamalarının listesinin altında yer alan **Özellikler** düğmesine tıklayın.

     Kaspersky Endpoint Security for Windows ayarları penceresi açılır.

     b. **Genel** bölümünde, pencerenin sağındaki **Durdur** düğmesine tıklayın.

Kaspersky Endpoint Security ayarlarını yapılandırma

Kaspersky Endpoint Security ayarlarını yapılandırmak için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen cihazlar** klasöründe, ilgili istemci bilgisayarın ait olduğu yönetim grubu adının bulunduğu klasörü açın.
3. Çalışma alanında, **Aygıtlar** sekmesini seçin.
4. Kaspersky Endpoint Security ayarlarını yapılandırmak istediğiniz bilgisayarı seçin.
5. İstemci bilgisayarın içerik menüsünden **Özellikler**'i seçin.

   İstemci bilgisayar özellikleri penceresi açılır.
6. İstemci bilgisayar özellikleri penceresinde **Uygulamalar** bölümünü seçin.

   İstemci bilgisayarda yüklü Kaspersky uygulamalarının listesi, istemci bilgisayar özellikleri penceresinin sağında görülür.
7. Kaspersky Endpoint Security 10 for Windows uygulamasını seçin.
8. Aşağıdakilerden birini yapın:

   - Kaspersky Endpoint Security 10 for Windows'un içerik menüsünden **Özellikler**'i seçin.
   - Kaspersky uygulamalarının listesinden **Özellikler** düğmesine tıklayın.

   Kaspersky Endpoint Security 10 for Windows uygulama ayarları penceresi açılır.
9. **Gelişmiş Ayarlar** bölümünde, Kaspersky Endpoint Security'nin ayarlarını ve rapor ve depolama ayarlarını yapılandırın.

   Kaspersky Endpoint Security 10 for Windows uygulama ayarları penceresinin diğer bölümleri Kaspersky Security Center'ın standart uygulama bölümleriyle aynıdır. Bu bölümlerin açıklaması *Kaspersky Security Center Yönetici Kılavuzu*'nda bulunmaktadır.

   > Uygulama, belirli ayarlarda değişiklik yapılmasını yasaklayan bir ilkeye tabi ise **Gelişmiş ayarlar** bölümünde uygulama ayarlarını yapılandırırken bunları düzenleyemezsiniz.
10. Değişiklikleri kaydetmek için **Kaspersky Endpoint Security 10 for Windows uygulama ayarları** penceresinde **Tamam**'a tıklayın.

Görevleri yönetme

Bu bölümde Kaspersky Endpoint Security için görevlerin nasıl yönetileceği açıklanmaktadır. Kaspersky Security Center aracılığıyla görev yönetimiyle ilgili ayrıntılar için *Kaspersky Security Center Yönetici Kılavuzu*'na bakınız.

Kaspersky Endpoint Security görevleri hakkında

Kaspersky Security Center, istemci bilgisayarlarda Kaspersky uygulamalarının etkinliğini denetler. Görevler; anahtar yükleme, bilgisayar tarama ve veritabanı ve uygulama yazılım modülü güncellemeleri gibi ana yönetim işlevlerini uygular.

Kaspersky Security Center vasıtasıyla Kaspersky Endpoint Security'yi uygulamak için aşağıdaki görev türlerini oluşturabilirsiniz:

- Tek bir istemci bilgisayar için yapılandırılan yerel görevler.
- Yönetim gruplarındaki istemci bilgisayarlar için yapılandırılan grup görevleri.
- Yönetim gruplarına ait olmayan bilgisayar setlerinin görevleri.

  Yönetim gruplarının dışındaki bilgisayar setlerinin görevleri sadece görev ayarlarında belirtilen istemci bilgisayarlar için geçerlidir. Bir görevin yapılandırıldığı bilgisayarlar setine yeni istemci bilgisayarlar eklenirse bu görev yeni bilgisayarlar için geçerli değildir. Görevi bu bilgisayarlara uygulamak için yeni bir görev oluşturun veya mevcut görevin ayarlarını düzenleyin.

Kaspersky Endpoint Security'yi uzaktan yönetmek için listelenen türdeki aşağıdaki görevlerden herhangi birini kullanabilirsiniz:

- **Anahtar ekle**. Kaspersky Endpoint Security ek anahtar dahil olmak üzere uygulamanın etkinleştirilmesi için bir anahtar ekler.
- **Uygulama bileşenlerini değiştir**. Kaspersky Endpoint Security, görev ayarlarında belirtilen bileşenlerin listesine göre istemci bilgisayarlara bileşenleri yükler veya kaldırır.
- **Envanter**. Kaspersky Endpoint Security, bilgisayarlarda depolanan uygulamalara ait tüm yürütülebilir dosyalarla ilgili bilgi alır.

  DLL modülü ve komut dizisi dosyalarının envanterini etkinleştirebilirsiniz. Bu durumda Kaspersky Security Center, Kaspersky Endpoint Security'nin kurulu olduğu bilgisayara yüklenen DLL modülleri hakkında ve komut dizilerini içeren dosyalar hakkında bilgi alır.

  DLL modülü ve komut dizisi dosyalarının envanterinin etkinleştirilmesi, envanter görevi süresini ve veritabanı boyutunu önemli ölçüde artırır.

  Uygulama Denetimi bileşeni Kaspersky Endpoint Security yüklü bir bilgisayara yüklenmemişse bu bilgisayardaki envanter görevi hata verir.
- **Güncelleme**. Kaspersky Endpoint Security, veritabanlarını ve uygulama modüllerini yapılandırılan güncelleme ayarlarına göre günceller.
- **Son güncellemeyi geri alma**. Kaspersky Endpoint Security, veritabanları ve modüllerin son güncellemesini geri alır.
- **Dosya koruması**. Kaspersky Endpoint Security, görev ayarlarında belirtilen bilgisayar alanlarında virüs ve diğer tehditleri tarar.

- **Bütünlük Denetimi**. Kaspersky Endpoint Security, istemci bilgisayarda kurulu uygulama modülleri hakkında bilgi alır ve her bir modülün dijital imzasını tarar.

- **Kimlik Doğrulama Aracısı hesaplarını yönet**. Bu görevi gerçekleştirirken Kaspersky Endpoint Security, Kimlik Doğrulama Aracısı hesaplarının kaldırılması, eklenmesi veya değiştirilmesi için komutlar üretir.

Görevlerle aşağıdaki eylemleri gerçekleştirebilirsiniz:

- Görevi başlatabilir, durdurabilir, askıya alabilir ve sürdürebilirsiniz.

- Yeni görevler oluşturabilirsiniz.

- Görev ayarlarını düzenleyebilirsiniz.

Kaspersky Endpoint Security görevlerine erişim hakları (okuma, yazma, uygulama) Kaspersky Security Center Yönetim Sunucusu'na erişimi olan her bir kullanıcı için Kaspersky Endpoint Security'nin işlevsel alanlarına erişim ayarlarıyla belirlenmektedir. Kaspersky Endpoint Security'nin işlev alanlarına erişimi yapılandırmak için Kaspersky Security Center Yönetim Sunucusu'nun özellikler penceresinin **Güvenlik** bölümüne girin.

Görev yönetimi modunu yapılandırma

Kaspersky Endpoint Security'nin yerel arabirimindeki görevlerle çalışma modunu yapılandırmak için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, Kaspersky Endpoint Security'nin yerel arabirimindeki görevlerle çalışma modunu yapılandırmak istediğiniz yönetim grubunun adının bulunduğu klasörü açın.

3. Çalışma alanında, **İlkeler** sekmesini seçin.

4. Gereken ilkeyi seçin.

5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:

   - İlkenin içerik menüsünde **Özellikler**'i seçin.

   - Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.

6. **Gelişmiş ayarlar** bölümünde, **Uygulama ayarları** alt bölümünü seçin.

7. **İşletim modu** bölümünde:

   - Kaspersky Endpoint Security'nin arabiriminde ve komut satırında kullanıcıların yerel görevlerle çalışmasına izin vermek istiyorsanız **Yerel görevlerin kullanımına izin ver** onay kutusunu açın.

     Onay kutusu işaretlenmezse yerel görevlerin işlevleri durdurulur. Bu modda, yerel görevler zamanlamaya göre çalışmaz. Ayrıca yerel görevler, Kaspersky Endpoint Security'nin yerel arabiriminde ve komut satırı ile çalışırken başlatma ve düzeltme için kullanılamaz.

   - Kullanıcıların grup görevlerinin listesini görmesine izin vermek isterseniz **Grup görevlerinin gösterilmesine izin ver** onay kutusunu işaretleyin.

- Kullanıcıların grup görevlerinin ayarlarını değiştirmesine izin vermek isterseniz **Grup görevlerinin yönetimine izin ver** onay kutusunu işaretleyin.

8. Değişiklikleri kaydetmek için **Tamam** düğmesine tıklayın.

9. İlkeyi uygulayın.

   Kaspersky Security Center ilkesinin uygulanmasıyla ilgili ayrıntılar için *Kaspersky Security Center Yönetici Kılavuzu*'na bakınız.

Yerel görev oluşturma

Bir yerel görev oluşturmak için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacındaki **Yönetilen cihazlar** klasöründe, ilgili istemci bilgisayarın ait olduğu yönetim grubu adının bulunduğu klasörü açın.

3. Çalışma alanında, **Aygıtlar** sekmesini seçin.

4. Yerel görevi oluşturmak istediğiniz bilgisayarı seçin.

5. Aşağıdakilerden birini yapın:

   - İstemci bilgisayarın içerik menüsünde **Tüm görevler** Görev oluştur seçeneğini seçin.

   - İstemci bilgisayarın içerik menüsünden **Özellikler**'i seçin ve açılan **Özellikler: <Bilgisayar adı>** penceresinde, **Görevler** sekmesinde, **Ekle** düğmesine tıklayın.

   - **Eylemi gerçekleştir** açılır listesinden **Görev oluştur**'u seçin.

   Görev Sihirbazı başlatılır.

6. Görev Sihirbazı talimatlarını uygulayın.

Grup görevi oluşturma

Bir grup görevi oluşturmak için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.

2. Aşağıdakilerden birini yapın:

   - Kaspersky Security Center tarafından yönetilen bütün bilgisayarlar için bir grup görevi oluşturmak için Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasörünü seçin.

   - Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, ilgili istemci bilgisayarların ait olduğu yönetim grubu adının bulunduğu klasörü seçin.

3. Çalışma alanında **Görevler** sekmesini seçin.

4. **Görev oluştur** düğmesine tıklayın.
   Görev Sihirbazı başlatılır.
5. Görev Sihirbazı talimatlarını uygulayın.

Aygıt seçimi için bir görev oluşturma

Aygıt seçimi için bir görev oluşturmak için aşağıdakileri gerçekleştirin:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Görevler** klasörünü seçin.
3. **Görev oluştur** düğmesine tıklayın.
   Görev Sihirbazı başlatılır.
4. Görev Sihirbazı talimatlarını uygulayın.
5. Sihirbazın **Görevin atanacağı aygıtı seçin** penceresinde **Aygıtların seçimi için görev ata** düğmesine tıklayın.
6. Sihirbazın sonraki penceresinde **Seç** düğmesine tıklayın.
   Aygıt seçimi penceresi açılır.
7. Gereken uygulamayı seçin.
8. **Aygıt seçimi** penceresinde **Tamam**'a tıklayın.
9. Görev Sihirbazı talimatlarını uygulayın.

Görevi başlatma, durdurma, askıya alma ve sürdürme

Bir istemci bilgisayarda Kaspersky Endpoint Security uygulaması çalışıyorsa bu istemci bilgisayarda Kaspersky Security Center üzerinden bir görevi başlatabilir, durdurabilir, askıya alabilir ve sürdürebilirsiniz. Kaspersky Endpoint Security askıya alındığında, çalışan işlemler askıya alınır ve bir görevi Kaspersky Security Center'dan başlatmak, durdurmak, askıya almak veya sürdürmek imkansız hale gelir.

Bir yerel görevi başlatmak, durdurmak, askıya almak veya sürdürmek için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen cihazlar** klasöründe, ilgili istemci bilgisayarın ait olduğu yönetim grubu adının bulunduğu klasörü açın.
3. Çalışma alanında, **Aygıtlar** sekmesini seçin.
4. Bir yerel görevi başlatmak, durdurmak, duraklatmak veya sürdürmek istediğiniz bilgisayarı seçin.
5. İstemci bilgisayarın içerik menüsünü görüntülemek için sağ tıklayın ve **Özellikler**'i seçin.

İstemci bilgisayar özellikleri penceresi açılır.

6. **Görevler** bölümünü seçin.

   Pencerenin sağ tarafında yerel görevlerin listesi açılır.

7. Başlatmak, durdurmak, askıya almak veya sürdürmek istediğiniz yerel görevi seçin.

8. Aşağıdaki yöntemlerden birini kullanarak görevde gereken işlemi gerçekleştirin:

   - Yerel görevin içerik menüsünü açmak için sağ tıklayın ve **Çalıştır** / **Durdur** / **Duraklat** / **Sürdür**'ü seçin.
   - Bir yerel görevi başlatmak veya durdurmak için yerel görevler listesinin sağındaki / düğmesine tıklayın.
   - Aşağıdakileri uygulayın:

     a. Yerel görevler listesinin altındaki **Özellikler** düğmesine tıklayın veya görev içerik menüsünde **Özellikler**'i seçin.

     Özellikler: <Görev adı> penceresi açılır.

     b. **Genel** sekmesinde, **Çalıştır** / **Durdur** / **Duraklat** / **Sürdür** düğmesine tıklayın.

Bir grup görevini başlatmak, durdurmak, duraklatmak veya sürdürmek için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacındaki **Yönetilen cihazlar** klasöründe, başlatmak, durdurmak, duraklatmak veya sürdürmek istediğiniz grup görevinin yönetim grubunun adına sahip klasörü açın.

3. Çalışma alanında **Görevler** sekmesini seçin.

   Grup görevleri, pencerenin sağında görüntülenir.

4. Başlatmak, durdurmak, duraklatmak veya sürdürmek istediğiniz grup görevini seçin.

5. Aşağıdaki yöntemlerden birini kullanarak görevde gereken işlemi gerçekleştirin:

   - Grup görevinin içerik menüsünde, **Çalıştır** / **Durdur** / **Duraklat** / **Sürdür**'ü seçin.
   - Bir grup görevini başlatmak veya durdurmak için penceresinin sağ kısmındaki / düğmesine tıklayın.
   - Aşağıdakileri uygulayın:

     a. Yönetim Konsolu çalışma alanının sağındaki **Görev Ayarları** bağlantısına tıklayın veya görev içerik menüsünden **Özellikler**'i seçin.

     Özellikler: <Görev adı> penceresi açılır.

     b. **Genel** sekmesinde, **Çalıştır** / **Durdur** / **Duraklat** / **Sürdür** düğmesine tıklayın.

Bilgisayarları seçmek amacıyla bir görevi başlatmak, durdurmak, duraklatmak veya sürdürmek için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacının **Görevler** klasöründe, seçtiğiniz bilgisayarlar için başlatma, durdurma, duraklatma veya sürdürme görevlerini seçin.

3. Aşağıdakilerden birini yapın:

- Görev içerik menüsünde, **Çalıştır** / **Durdur** / **Duraklat** / **Sürdür**'ü seçin.
- Belirli bilgisayarların görevini başlatmak veya durdurmak için penceresinin sağ kısmındaki / düğmesine tıklayın.
- Aşağıdakileri uygulayın:

  a. Yönetim Konsolu çalışma alanının sağındaki **Görev Ayarları** bağlantısına tıklayın veya görev içerik menüsünden **Özellikler**'i seçin.

  Özellikler: <Görev adı> penceresi açılır.

  b. **Genel** sekmesinde, **Çalıştır** / **Durdur** / **Duraklat** / **Sürdür** düğmesine tıklayın.

Görev ayarlarını düzenleme

Bir yerel görevin ayarlarını düzenlemek için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacındaki **Yönetilen cihazlar** klasöründe, ilgili istemci bilgisayarın ait olduğu yönetim grubu adının bulunduğu klasörü açın.
3. Çalışma alanında, **Aygıtlar** sekmesini seçin.
4. Uygulama ayarlarını yapılandırmak istediğiniz bilgisayarı seçin.
5. İstemci bilgisayarın içerik menüsünü görüntülemek için sağ tıklayın ve **Özellikler**'i seçin.

   İstemci bilgisayar özellikleri penceresi açılır.
6. **Görevler** bölümünü seçin.

   Pencerenin sağ tarafında yerel görevlerin listesi açılır.
7. Yerel görevler listesinde gereken yerel görevi seçin.
8. **Özellikler** düğmesine tıklayın.

   Özellikler: <Yerel görev adı> penceresi açılır.
9. **Özellikler: <Yerel görev adı>** penceresinde **Ayarlar** bölümünü seçin.
10. Yerel görev ayarlarını düzenleyin.
11. Değişiklikleri kaydetmek için **Özellikler: <Yerel görev adı>** penceresinde **Tamam**'a tıklayın.
12. Değişiklikleri kaydetmek için **Özellikler: <Bilgisayar adı>** penceresinde **Tamam**'a tıklayın.

Bir grup görevinin ayarlarını düzenlemek için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. **Yönetilen cihazlar** klasöründe, ilgili yönetim grubunun adının bulunduğu klasörü seçin.
3. Çalışma alanında **Görevler** sekmesini seçin.

   Grup görevleri, Yönetim konsolu çalışma alanında görüntülenir.

4. Gereken grup görevini seçin.
5. Grup görevinin içerik menüsünü görüntülemek için sağ tıklayın ve **Özellikler**'i seçin.
   Özellikler: <Grup görevi adı> penceresi açılır.
6. **Özellikler: <Grup görevi adı>** penceresinde **Ayarlar** bölümünü seçin.
7. Grup görevi ayarlarını düzenleyin.
8. Değişiklikleri kaydetmek için **Özellikler: <Grup görevi adı>** penceresinde **Tamam**'a tıklayın.

Bilgisayarları seçme görevinin ayarlarını düzenlemek için:

1. Kaspersky Security Center Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacının **Görevler** klasöründe, ayarlarını düzenlemek istediğiniz bilgisayarları seçme görevini seçin.
3. Bilgisayar seçimi amacıyla görevin içerik menüsünü görüntülemek için sağ tıklayın ve **Özellikler**'i seçin.
   Özellikler: **<Bilgisayar seçimi için görev adı>** penceresi açılır.
4. **Özellikler: <Bilgisayar seçimi için görev adı>** penceresinde **Ayarlar** bölümünü seçin.
5. Bilgisayarı seçme görevinin ayarlarını düzenleyin.
6. Değişiklikleri kaydetmek için **Özellikler: <Bilgisayar seçimi için görev adı>** penceresinde **Tamam**'a tıklayın.

Ayarlar bölümü haricinde görev özellikleri penceresindeki tüm bölümler Kaspersky Security Center'da kullanılanlar ile aynıdır. Ayrıntılı açıklamaları için Kaspersky Security Center Yardım içeriğine bakın. **Ayarlar** bölümü, Kaspersky Endpoint Security for Windows'un belirli ayarlarını içermektedir. İçeriği, seçilen göreve ya da görev türüne bağlıdır.

İlkeleri yönetme

Bu bölümde, Kaspersky Endpoint Security için ilkelerin oluşturulması ve yapılandırılması açıklanmaktadır. Kaspersky Security Center ilkelerini kullanarak Kaspersky Endpoint Security'yi yönetmekle ilgili ayrıntılı bilgi için lütfen *Kaspersky Security Center Yönetici Kılavuzu*'na başvurun.

İlkeler hakkında

Bir yönetim grubundaki bütün istemci bilgisayarlara aynı Kaspersky Endpoint Security ayarlarını uygulamak için ilkeleri kullanabilirsiniz.

Kaspersky Endpoint Security kullanan bir yönetim grubundaki bazı bilgisayarlar için bir ilke tarafından belirlenen ayarların değerlerini yerel olarak değiştirebilirsiniz. Yalnızca ilkenin değiştirilmesini yasaklamadığı ayarları yerel olarak değiştirebilirsiniz.

İstemci bilgisayarda uygulama ayarlarını değiştirme kabiliyeti, bu ayarların ilke özelliklerindeki "kilit" durumuna göre belirlenir:

- Kapalı "kilit" () aşağıdaki anlama gelir:

- Kaspersky Security Center, istemci bilgisayarlarda Kaspersky Endpoint Security arabiriminden bu kilitle ilgili ayarları değiştirmeyi engeller. Kaspersky Endpoint Security, tüm istemci bilgisayarlarda bu ayarlarla aynı değerleri örn. ilke özelliklerinde tanımlanan değerleri kullanır.

- Kaspersky Security Center, **Üst düzey ilkenin ayarlarını devral** işlevinin etkin olduğu iç içe geçmiş yönetim grupları ve bağımlı Yönetim Sunucuları için bu ilkelerin özelliklerindeki bu kilit ile ilgili ayarların değiştirilmesini engeller. Bu ayarların değerleri, üst düzey ilke özelliklerinde belirtilen değerleri kullanır.

- Açık "kilit" ( ) aşağıdaki anlama gelir:

  - Kaspersky Security Center, istemci bilgisayarlarda Kaspersky Endpoint Security arabiriminden bu kilitle ilgili ayarları değiştirmeye izin verir. Bileşen etkinleştirilmişse Kaspersky Endpoint Security, her istemci bilgisayarda bu ayarların yerel değerlerine göre çalışır.

  - Kaspersky Security Center, **Üst düzey ilkenin ayarlarını devral** işlevinin etkin olduğu iç içe geçmiş yönetim grupları ve bağımlı Yönetim Sunucuları için bu ilkelerin özelliklerindeki bu kilit ile ilgili ayarların değiştirilmesine izin verir. Bu ayarların değerleri, üst düzey ilke özelliklerinde belirtilenlere bağlı değildir.

İlke ilk kez uygulandıktan sonra, yerel uygulama ayarları ilke ayarlarına göre değişir.

İlke ayarlarına erişim hakları (okuma, yazma, uygulama) Kaspersky Security Center Yönetim Sunucusu'na erişimi olan her bir kullanıcı için ve Kaspersky Endpoint Security'nin her bir işlev kapsamı için ayrıca belirtilir. İlke ayarlarına erişim haklarını yapılandırmak için Kaspersky Security Center Yönetim Sunucusu'nun özellikler penceresinin **Güvenlik** bölümüne gidin.

Kaspersky Endpoint Security'nin aşağıdaki işlev kapsamları belirlenebilir:

- Temel Tehdit Koruması. İşlev kapsamı; Dosya Tehdidi Koruması, Posta Tehdidi Koruması, Web Tehdidi Koruması, Ağ Tehdidi Koruması, Güvenlik Duvarı ve Tarama Görevi bileşenlerini içerir.

- Uygulama Denetimi. İşlev kapsamı Uygulama Denetimi bileşenini içerir.

- Aygıt Denetimi. İşlev kapsamı Aygıt Denetimi bileşenini içerir.

- Şifreleme. İşlev kapsamı Tam Disk Şifreleme ve Dosya Düzeyinde Şifreleme bileşenlerini içerir.

- Güvenilir bölge. İşlev kapsamı Güvenilir Bölge'yi içerir.

- İnternet Denetimi. İşlev kapsamı İnternet Denetimi bileşenini içerir.

- Gelişmiş Tehdit Koruması. İşlev kapsamı KSN ayarları ve Davranış Tespiti, Exploit Önleme, Sunucu Yetkisiz Erişim Önleme ve Düzeltme Altyapısı bileşenlerini içerir.

- Temel işlev. Bu işlev kapsamı, aşağıdakiler dahil olmak üzere diğer işlev kapsamlarında belirtilmeyen genel uygulama ayarlarını içerir: lisanslama, envanter görevleri, uygulama veritabanı ve modül güncelleme görevleri, Kendini Koruma, gelişmiş uygulama ayarları, raporlar ve depolama alanları, parola koruması ve uygulama arabirim ayarları.

Aşağıdaki işlemleri bir ilkeyle gerçekleştirebilirsiniz:

- Bir ilke oluşturabilirsiniz.

- İlke ayarlarını düzenleyebilirsiniz.

Yönetim Sunucusu'na eriştiğiniz kullanıcı hesabı belirli işlev kapsamlarının ayarlarını düzenleme haklarına sahip değilse bu işlev kapsamlarının ayarları düzenlemeye açık değildir.

- İlkeyi silebilirsiniz.
- İlke durumunu değiştirebilirsiniz.

Kaspersky Endpoint Security ile etkileşimle ilgili olmayan ilkeleri kullanma hakkında bilgi için Kaspersky Security Center Yardım içeriğine başvurun.

İlke oluşturma

Bir ilke oluşturmak için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Aşağıdakilerden birini yapın:
   - Kaspersky Security Center tarafından yönetilen bütün bilgisayarlar için bir ilke oluşturmak istiyorsanız Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasörünü seçin.
   - Yönetim Konsolu ağacındaki **Yönetilen aygıtlar** klasöründe, ilgili istemci bilgisayarların ait olduğu yönetim grubu adının bulunduğu klasörü seçin.
3. Çalışma alanında, **İlkeler** sekmesini seçin.
4. Aşağıdakilerden birini yapın:
   - **İlke oluştur** düğmesine tıklayın.
   - İçerik menüsünü açmak için sağ tıklayın ve **İlke** Oluştur'u seçin.

   İlke Sihirbazı başlatılır.
5. Etkinleştirme Sihirbazı talimatlarını uygulayın.

İlke ayarlarını düzenleme

İlke ayarlarını düzenlemek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. Yönetim Konsolu ağacının **Yönetilen aygıtlar** klasöründe, ilke ayarlarını düzenlemek istediğiniz ilgili yönetim grubunun adının bulunduğu klasörü açın.
3. Çalışma alanında, **İlkeler** sekmesini seçin.
4. Gereken ilkeyi seçin.
5. Aşağıdaki yöntemlerden birini kullanarak **Özellikler: <İlke adı>** penceresini açın:

- İlkenin içerik menüsünde **Özellikler**'i seçin.
- Yönetim Konsolu çalışma alanının sağ kısmında yer alan **İlkeyi yapılandır** bağlantısına tıklayın.

Kaspersky Endpoint Security 10 for Windows ilke ayarları, bileşenlerin ayarlarını ve uygulama ayarları'nı içerir. **Özellikler: <İlke adı>** penceresinin **Virüse karşı koruma** ve **Uç nokta denetimi** bölümlerinde koruma ve denetim bileşenlerinin ayarları görüntülenir, **Veri Şifreleme** bölümünde dosyalar ve klasörler için şifreleme ayarları görüntülenir ve **Gelişmiş Ayarlar** bölümünde uygulama ayarları görüntülenir.

Veri şifreleme ayarlarının ve denetim bileşeni ayarlarının ilke ayarlarında görüntülenmesini etkinleştirmek için Kaspersky Security Center'ın **Arabirim ayarları** penceresinde ilgili onay kutularını seçmelisiniz.

6. İlke ayarlarını düzenleyin.
7. Değişikliklerinizi kaydetmek için **Özellikler: <İlke adı>** penceresinde **Tamam**'a tıklayın.

Kaspersky Security Center ilkesinde görüntülenecek ayarları seçme

Kaspersky Security Center ilkesinde görüntülenecek ayarları seçmek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.
2. **Yönetim Sunucusu**'nun içerik menüsünde Yönetim Konsolu ağacının **– <Bilgisayar adı>** düğümünde Göster → **Arabirim ayarları**'nı seçin.

   Arabirim ayarları penceresi açılır.
3. **Arabirim ayarları** penceresinde, Kaspersky Security Center ilke oluşturma ayarları ve ilke özelliklerinde görüntülenmesi gereken ayarların karşısındaki onay kutularını işaretleyin.
   - Kaspersky Security Center'ın Yeni İlke Sihirbazı penceresinde ve ilke özelliklerinde denetimi bileşenleri ayarlarının görüntülenmesini etkinleştirmek için **Uç nokta denetimi bileşenlerini göster** onay kutusunu işaretleyin.
   - Kaspersky Security Center'ın Yeni İlke Sihirbazı'nda ve ilke özelliklerinde veri şifreleme ayarlarının görüntülenmesini etkinleştirmek için **Şifreleme ve veri korumasını göster** onay kutusunu işaretleyin.
4. **Tamam**'a tıklayın.

Kaspersky Security Center sunucusuna kullanıcı mesajlarını gönderme

Bir kullanıcının aşağıdaki durumlarda yerel kurumsal ağ yöneticisine bir mesaj göndermesi gerekebilir:

- Aygıt Denetimi aygıta erişimi engellemiştir.

  Kaspersky Endpoint Security arabiriminde Aygıt Denetimi bölümünde engellenen bir aygıta erişim isteği için mesaj şablonu bulunmaktadır.
- Uygulama Başlatma Denetimi bir uygulamanın başlatılmasını engellemiştir.

  Engellenen bir uygulamanın başlatılması izni isteği için mesaj şablonu Kaspersky Endpoint Security arabiriminde Uygulama Başlatma Denetimi bölümünde mevcuttur.
- İnternet Denetimi bir İnternet kaynağına erişimi engellemiştir.

Kaspersky Endpoint Security arabiriminde İnternet Denetimi bölümünde engellenen bir İnternet kaynağına erişim isteği için mesaj şablonu bulunmaktadır.

Mesaj göndermek için kullanılan yöntem ve kullanılan şablon, Kaspersky Endpoint Security'nin yüklü olduğu bilgisayarda çalışmakta olan etkin bir Kaspersky Security Center ilkesinin olup olmadığına ve Kaspersky Security Center Yönetim Sunucusu ile bir bağlantı olup olmadığına bağlıdır. Aşağıdaki senaryolar olasıdır:

- Kaspersky Security Center yüklü bilgisayarda bir Kaspersky Security Center ilkesi çalışmıyorsa yerel ağ yöneticisine e-posta ile bir kullanıcı mesajı gönderilir.

  Mesaj alanları, Kaspersky Endpoint Security'nin yerel arabiriminde tanımlanan şablondaki alanların değerleri ile doldurulmuştur.

- Kaspersky Security Center yüklü bilgisayarda bir Kaspersky Security Center ilkesi çalışıyorsa Kaspersky Security Center Yönetim Sunucusu'na standart mesaj gönderilir.

  Bu durumda, Kaspersky Security Center olay deposunda kullanıcı mesajları görüntülenebilir. Mesaj alanları Kaspersky Security Center ilkesinde tanımlanan şablondaki alanların değerleri ile doldurulmuştur.

- Kaspersky Endpoint Security yüklü bilgisayarda bir Kaspersky Security Center ofis dışı ilkesi çalışıyorsa mesajları göndermek için kullanılan yöntem Kaspersky Security Center ile bir bağlantı olup olmadığına bağlıdır.

  - Kaspersky Security Center ile bir bağlantı kurulduysa Kaspersky Endpoint Security, Kaspersky Security Center Yönetim Sunucusu'na standart mesaj gönderir.

  - Kaspersky Security Center ile bağlantı yoksa yerel ağ yöneticisine e-posta ile bir kullanıcı mesajı gönderilir.

  Her iki durumda da, mesaj alanları Kaspersky Security Center ilkesinde tanımlanan şablondaki alanların değerleri ile doldurulur.

Kaspersky Security Center olay depolama alanında kullanıcı mesajlarını görüntüleme

Uygulama Başlatma Denetimi, Aygıt Denetimi ve İnternet Denetimi bileşenleri, Kaspersky Endpoint Security kurulu bilgisayarları olan LAN kullanıcılarının yöneticiye mesaj göndermesine olanak tanır.

Kullanıcı, iki yöntemle yöneticiye mesaj gönderebilir:

- Kaspersky Security Center olay depolama alanında bir olay olarak.

  Kullanıcının bilgisayarında kurulu Kaspersky Security Center uygulaması etkin bir ilke altında çalışıyorsa kullanıcının olayı Kaspersky Security Center olay depolama alanına gönderilir.

- E-posta mesajı olarak.

  Kullanıcının bilgisayarında kurulu Kaspersky Endpoint Security uygulaması bir ilkeyle çalışmıyorsa ya da ofis dışı ilkesiyle çalışıyorsa kullanıcı bilgisi e-postayla gönderilir.

Kaspersky Security Center olay depolama alanındaki bir kullanıcı mesajını görüntülemek için:

1. Kaspersky Security Center'ın Yönetim Konsolu'nu açın.

2. Yönetim Konsolu ağacının **Yönetim Sunucusu** düğümünde **Olaylar** sekmesini seçin.

   Kaspersky Security Center çalışma alanı, Kaspersky Endpoint Security'nin çalışması sırasında meydana gelen bütün olayları, LAN kullanıcılarından yöneticiye gönderilen mesajlarla birlikte görüntüler.

3. Olay filtresini yapılandırmak için **Seçim olayları** açılır listesinden **Kullanıcı istekleri**'ni seçin.

4. Yöneticiye gönderilecek mesajı seçin.

5. **Olay ayarları** penceresini aşağıdaki yöntemlerden biriyle açın:

   - Olaya sağ tıklayın. Açılan içerik menüsünde **Özellikler**'i seçin.
   - Yönetim Konsolu çalışma alanının sağ tarafındaki **Olay özelliklerini aç penceresi** düğmesine tıklayın.

Kaspersky Security Network'e katılım

Bu bölümde, Kaspersky Security Network'e katılım hakkında bilgiler ve Kaspersky Security Network'ün kullanımını etkinleştirme ve devre dışı bırakma talimatları bulunmaktadır.

Kaspersky Security Network'e katılım hakkında

Bilgisayarınızı daha etkili bir şekilde korumak için Kaspersky Endpoint Security, dünyanın her yerindeki kullanıcılardan alınan verileri kullanır. *Kaspersky Security Network*, bu tür verileri almak için tasarlanmıştır.

Kaspersky Security Network (KSN); dosyaların, İnternet kaynaklarının ve yazılımın tanınırlığı hakkında bilgiler içeren çevrimiçi Kaspersky Bilgi Bankasına erişim sağlayan bir bulut hizmetleri altyapısıdır. Kaspersky Security Network'ten verilerin kullanılması, Kaspersky Endpoint Security'nin yeni tehditlere daha hızlı yanıt vermesini sağlar, bazı koruma bileşenlerinin performansını arttırır ve hatalı pozitif olasılığını azaltır.

Altyapının konumuna bağlı olarak bir Global KSN hizmeti (altyapı Kaspersky sunucuları tarafından barındırılır) ve bir Özel KSN hizmeti vardır.

Lisansı değiştirdikten sonra Özel KSN'yi kullanabilmek için hizmet sağlayıcıya yeni anahtarın bilgilerini gönderin. Aksi halde, Özel KSN ile veri alışverişi mümkün olmayacaktır.

KSN'ye katılan kullanıcılar sayesinde Kaspersky, tehditlerin türleri ve kaynakları hakkında anında bilgi alabilmekte, bunları etkisiz hale getirmek için çözümler geliştirebilmekte ve uygulama bileşenlerinin görüntülediği yanlış alarmların sayısını en aza indirebilmektedir.

Genişletilmiş KSN modu kullanılırken uygulama sonuç istatistiklerini otomatik olarak KSN'ye gönderir. Uygulama ayrıca bilgisayar korsanlarının bilgisayara ya da verilere zarar vermek için kullanabileceği bazı dosyaları (veya dosyaların parçalarını) da ek tarama için Kaspersky'ye gönderebilir.

KSN kullanırken oluşturulan istatistiksel bilgiler, bu bilgilerin Kaspersky'ye gönderilmesi ve bu bilgilerin depolanması ve imhasıyla ilgili ayrıntılar için lütfen Kaspersky Security Network Statement'a ve Kaspersky İnternet sitesine bakın. Kaspersky Security Network Bildirimi'nin metnini içeren ksn_<dil kodu>.txt dosyası dağıtım kitinde mevcuttur.

KSN sunucularındaki yükü azaltmak için Kaspersky, Kaspersky Security Network'e talepleri geçici olarak devre dışı bırakan veya kısmen kısıtlayan uygulama anti-virüs veritabanları çıkarabilir. Bu durumda KSN bağlantısının durumu *Kısıtlı olarak etkin* görülür.

Kaspersky Security Center Yönetim Sunucusu tarafından yönetilen kullanıcı bilgisayarları, KSN ile KSN Proxy hizmeti aracılığıyla etkileşimde bulunabilir.

KSN Proxy hizmeti, aşağıdaki özellikleri sağlar:

- Kullanıcının bilgisayarı, doğrudan İnternet erişimi olmadan bile KSN'ye soru sorabilir ve KSN'ye bilgi gönderebilir.
- KSN Proxy işlenmiş verileri önbelleğe alır, böylece dış ağ bağlantısı üzerindeki yükü azaltır ve kullanıcının bilgisayarı tarafından istenen bilginin alınmasını hızlandırır.

KSN Proxy hizmeti hakkında daha ayrıntılı bilgi için lütfen *Kaspersky Security Center Yardım Kılavuzu'na başvurun.*

KSN Proxy hizmeti ayarları, *Kaspersky Security Center* ilkesinin özelliklerinden yapılandırılabilir.

Kaspersky Security Network kullanımı isteğe bağlıdır. Uygulama, uygulamanın ilk yapılandırması sırasında KSN'yi kullanmanızı ister. Kullanıcılar istedikleri zaman KSN'ye katılabilir ya da katılımlarına son verebilir.

Kaspersky Security Network'ün kullanımını etkinleştirme ve devre dışı bırakma

Kaspersky Security Network'ün kullanımını etkinleştirmek ve devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Gelişmiş ayarlar** bölümünde, **KSN Ayarları** alt bölümünü seçin.

   Kaspersky Security Network ayarları, pencerenin sağında görüntülenir.
3. Aşağıdakilerden birini yapın:
   - Kaspersky Security Network'ün kullanımını etkinleştirmek istiyorsanız **KSN Bildirimi'ni ve katılım koşullarını kabul ediyorum** onay kutusunu işaretleyin.
   - Kaspersky Security Network'ün kullanımını devre dışı bırakmak istiyorsanız **KSN Bildirimi'ni ve katılım koşullarını kabul ediyorum** onay kutusunun işaretini kaldırın.
4. Değişiklikleri kaydetmek için **Kaydet** düğmesine tıklayın.

Kaspersky Security Network bağlantısını denetleme

Kaspersky Security Network bağlantısını denetlemek için:

1. Ana uygulama penceresini açın.
2. Pencerenin üst kısmında, **Kaspersky Security Network** düğmesine tıklayın.

   Kaspersky Security Network penceresi açılır.

   Kaspersky Security Network penceresinin solunda, Kaspersky Security Network'e bağlantı modu yuvarlak bir **KSN** düğmesi şeklinde görülür:
   - Kaspersky Endpoint Security, Kaspersky Security Network'e bağlanmazsa **KSN** düğmesi gri olur. **KSN** düğmesinin altında görüntülenen durum *Devre dışı bırakıldı* olur.
   - Kaspersky Endpoint Security, Kaspersky Security Network'e bağlandıysa ve KSN sunucuları kullanılabilirse, **KSN** düğmesi yeşil olur. **KSN** düğmesinin altında aşağıdaki bilgiler görülür: *Etkin* durumu, kullanılan KSN türü; **Özel KSN** veya **Global KSN** ve KSN sunucularıyla son senkronizasyonun tarihi ve saati. Pencerenin sağında dosya, İnternet kaynakları ve yazılım saygınlığı ile ilgili istatistikler görüntülenir.

   > **Kaspersky Security Network** penceresini açtığınızda Kaspersky Endpoint Security, KSN kullanımıyla ilgili istatistiksel veriler toplar. İstatistikler gerçek zamanlı olarak güncellenmez.

   - Kaspersky Endpoint Security, Kaspersky Security Network'e bağlandıysa ama KSN sunucuları kullanılabilir değilse, **KSN** düğmesi kırmızı olur. **KSN** düğmesinin altında görüntülenen durum *Etkin* olur.

KSN sunucularıyla son senkronizasyonun süresi 15 dakikayı aşarsa veya *Bilinmiyor* durumundaysa KSN sunucuları kullanılamaz. Bu durumda Teknik Destek veya hizmet sağlayıcınız ile irtibat kurmanız önerilir.

Aşağıdaki nedenlerle Kaspersky Security Network sunucularıyla bağlantı kurulmamış olabilir:

- Bilgisayar İnternet'e bağlı değildir.
- Uygulama etkinleştirilmemiştir veya lisansın süresi sona ermiştir.
- Anahtarla ilgili sorunlar algılanmıştır (örneğin anahtar kara listeye alınmıştır).

Kaspersky Security Network'den bir dosyanın saygınlığını kontrol etme

KSN hizmeti, Kaspersky saygınlık veritabanlarında yer alan uygulamalar hakkında bilgi almanıza olanak tanır. Bu, bilgisayarınıza veya kişisel verilerinize zarar vermek isteyen suçlular tarafından kullanılabilecek reklam yazılımlarının ve programların başlatılmasını önlemek suretiyle şirket düzeyinde uygulama başlatma ilkelerinin esnek yönetimini sağlar.

Kaspersky Security Network'den bir dosyanın saygınlığını kontrol etmek için:

1. Sağ tıklayarak saygınlığını kontrol etmek istediğiniz dosyanın içerik menüsünü açın.
2. **KSN içindeki itibarı kontrol et** seçeneğini seçin.

   Bu seçenek, Kaspersky Security Network Bildirimi şartları kabul edilirse etkinleşir.

Bu, **<Dosya adı> - KSN içindeki tanınırlık** penceresini açar. **<Dosya adı> - KSN** içindeki itibar penceresi kontrol edilen dosya hakkında aşağıdaki bilgileri görüntüler:

- **Yol**. Dosyanın sürücüde kaydedildiği yoldur.
- **Sürüm**. Uygulama sürümüdür (bilgi yalnızca yürütülebilir dosyalar için görüntülenir).
- **Dijital imza**. Dosya ile birlikte bir dijital imzanın bulunmasıdır.
- **İmzalanma tarihi**. Sertifikanın bir dijital imza ile imzalandığı tarihtir.
- **Oluşturulma tarihi**. Dosyanın oluşturulma tarihidir.
- **Değiştirilme tarihi**. Dosyanın en son değiştirildiği tarihtir.
- **Boyut**. Dosyanın kapladığı disk alanıdır.
- Dosyaya kaç kullanıcının güvendiği veya engellediği hakkındaki bilgidir.

Kaspersky Security Network ile gelişmiş koruma

Kaspersky, Kaspersky Security Network aracılığıyla kullanıcılara ekstra bir koruma katmanı sunar. Bu koruma yöntemi, gelişmiş kalıcı tehditler ve sıfır gün saldırıları ile mücadele etmek üzere tasarlanmıştır. Tümleşik bulut teknolojileri ve Kaspersky virüs analistlerinin uzmanlığı, Kaspersky Endpoint Security'yi en karmaşık ağ tehditlerine karşı en üstün koruma seçeneği haline getirmektedir.

Kaspersky Endpoint Security'de gelişmiş korumanın ayrıntılarını Kaspersky web sitesinden bulabilirsiniz.

Uygulama hakkında bilgi kaynakları

Kaspersky web sitesinde Kaspersky Endpoint Security sayfası

Kaspersky Endpoint Security sayfasında, uygulama hakkında genel bilgileri ve işlevleri ve özelliklerini görebilirsiniz.

Kaspersky Endpoint Security sayfası, çevrimiçi mağazaya bir bağlantı içermektedir. Bu mağazadan uygulamayı satın alabilir ya da yenileyebilirsiniz.

Bilgi Bankasında Kaspersky Endpoint Security sayfası

Bilgi Bankası, Teknik Destek web sitesinin bir bölümüdür.

Bilgi Bankasındaki Kaspersky Endpoint Security sayfasında, faydalı bilgiler, tavsiyeler ve uygulamanın nasıl satın alınacağı, yükleneceği ve kullanılacağına dair sık sorulan sorulara cevaplar sağlayan makaleler okuyabilirsiniz.

Bilgi Bankası makalelerinden, hem Kaspersky Endpoint Security hem de diğer Kaspersky uygulamaları ile ilgili soruların yanıtlarını bulabilirsiniz. Bilgi Bankasındaki makaleler ayrıca Teknik Destek'ten haberler de içerebilir.

Kaspersky uygulamalarının kullanıcı topluluğunda tartışılması

Sorunuza acil bir yanıt gerekmiyorsa Topluluğumuzda Kaspersky uzmanlarıyla ve diğer kullanıcılarla tartışabilirsiniz.

Bu toplulukta mevcut konuları görebilir, yorumlarınızı bırakabilir ve yeni tartışma konuları oluşturabilirsiniz.

Teknik Destek ile irtibat kurma

Bu bölümde, teknik destek alma yolları ve sunulduğu koşullar açıklanmaktadır.

Teknik destek nasıl alınır

Uygulama belgelerinde veya uygulama hakkındaki bilgi kaynaklarından birinde sorununuza bir çözüm bulamazsanız Teknik Destek ile iletişim kurmanızı öneririz. Teknik Destek uzmanları, uygulamayı yükleme ve kullanmayla ilgili sorularınızı yanıtlayacaktır.

Teknik Destek ile irtibat kurmadan önce lütfen destek kurallarını okuyun.

Teknik Destek ile aşağıdaki yollardan biriyle irtibat kurabilirsiniz:

- Teknik Desteği telefonla arayarak
- Kaspersky Teknik Destek'e Kaspersky CompanyAccount portalından bir talep göndererek

Telefonla teknik destek

Dünya çapında çoğu bölgeden Teknik Destek temsilcilerini arayabilirsiniz. Kaspersky Teknik Destek web sitesinden bölgenizde teknik destek alma yolları ve Teknik Destek iletişim kişileri hakkında bilgi bulabilirsiniz.

Teknik Destek ile irtibat kurmadan önce lütfen destek kurallarını okuyun.

Kaspersky CompanyAccount üzerinden Teknik Destek

Kaspersky CompanyAccount, Kaspersky uygulamalarını kullanan şirketlere yönelik bir portaldır. Kaspersky CompanyAccount portalı, kullanıcılar ile Kaspersky uzmanları arasında elektronik taleplerle etkileşimi kolaylaştırmak üzere tasarlanmıştır. Kaspersky CompanyAccount portalını elektronik taleplerinizin durumunu takip etmek ve bu taleplerin geçmişini depolamak için kullanabilirsiniz.

Şirketinizin bütün çalışanlarını Kaspersky CompanyAccount'ta tek bir hesap altına kaydedebilirsiniz. Tek bir hesap, kayıtlı çalışanlardan Kaspersky'ye giden bütün elektronik talepleri bir merkezden yönetmenize ve ayrıca Kaspersky CompanyAccount aracılığıyla bu çalışanların ayrıcalıklarını yönetmenize olanak tanır.

Kaspersky CompanyAccount portalı aşağıdaki dillerde sunulmaktadır:

- İngilizce
- İspanyolca
- İtalyanca
- Almanca

- Polonyaca
- Portekizce
- Rusça
- Fransızca
- Japonca

Kaspersky CompanyAccount hakkında daha fazla bilgi edinmek için Teknik Destek web sitesini ziyaret edin.

Teknik Destek için bilgi toplama

Kaspersky Teknik Destek uzmanlarına sorununuzu bildirdikten sonra bir *iz dosyası* oluşturmanızı isteyebilirler. İz dosyası, uygulama komutlarının gerçekleştirilme işlemini adım adım izlemenize ve uygulamanın çalışmasının hangi aşamasında hata oluştuğunu belirlemenize olanak tanır.

Teknik Destek uzmanları ayrıca işletim sistemi, bilgisayarda çalışan işlemler, uygulama bileşenlerinin çalışması hakkında ayrıntılı raporlar ve uygulamanın çökme raporları hakkında ek bilgi isteyebilir.

Kaspersky Endpoint Security'nin yardımıyla gerekli bilgileri toplayabilirsiniz. Toplanan bilgiler sabit sürücüye kaydedilebilir ve daha sonra uygun bir zamanda yüklenebilir.

Tanılama yaparken Teknik Destek uzmanları aşağıdakileri yaparak uygulama ayarlarını değiştirmenizi isteyebilirler:

- Genişletilmiş tanılama bilgileri toplayan işlevi etkinleştirerek.
- Ayrı ayrı uygulama bileşenlerinin standart kullanıcı arabirim öğelerinde mevcut olmayan ayarlarına ince ayar yaparak.
- Toplanan tanılama bilgilerinin depolama ve iletim ayarlarını değiştirerek.
- Ağ trafiğinin yakalanmasını ve kaydedilmesini yapılandırarak.

Teknik Destek uzmanları, bu işlemleri gerçekleştirmek için gerekli bütün bilgileri (adımların sıralamasının açıklaması, değiştirilecek ayarlar, yapılandırma dosyaları, komut dizileri, ek komut satırı işlevi, hata ayıklama modülleri, özel amaçlı yardımcı programlar vs.) sağlayacak ve hata ayıklama amaçlı toplanan verilerin kapsamı hakkında sizi bilgilendirecektir. Toplanan genişletilmiş tanılama bilgileri, kullanıcının bilgisayarına kaydedilir. Toplanan veriler otomatik olarak Kaspersky'ye iletilmez.

Kaspersky'ye döküm dosyalarını göndermek için döküm sunucusunun adresini belirlemede kullanılan ayarlar kullanıcının bilgisayarında depolanır. Gerekirse bu ayarların değerleri işletim sisteminin `"DumpServerConfigUrl"="https://dmpcfg.kaspersky-labs.com/dumpserver/config.xml”` kayıt defteri anahtarında düzenlenebilir.

Yukarıda sıralanan işlemler yalnızca Teknik Destek uzmanlarının gözetimi altında, onların talimatlarını izleyerek yapılmalıdır. Yönetici Kılavuzu'nda açıklananların ya da Teknik Destek uzmanlarının talimatlarının dışında başka şekillerde uygulama ayarlarında gözetimsiz değişiklik yapılması, işletim sistemini yavaşlatabilir ya da çökmesine neden olabilir, bilgisayar güvenliğini etkileyebilir veya işlenen verinin erişilebilirliğini ya da bütünlüğünü tehlikeye atabilir.

Uygulama izi dosyası oluşturma

Uygulama izleri, uygulama tarafından gerçekleştirilen işlemlerin ayrıntılı kayıtları ve uygulamanın çalışması sırasındaki olaylar hakkındaki mesajlardır.

Uygulama izi dosyası oluşturmak için:

1. Ana uygulama penceresinde **Destek** düğmesine tıklayın.

   Destek penceresi açılır.

2. **Destek** penceresinde **Sistem izleri** düğmesine tıklayın.

   Teknik Destek Bilgileri penceresi açılır.

3. İzleme işlemini başlatmak için **Uygulama izleri** açılır listesinde aşağıdaki öğelerden birini seçin:

   - **etkin**

     İzlemeyi etkinleştirmek için bu öğeyi seçin.

   - **dönüşlü**.

     İzlemeyi etkinleştirmek ve iz dosyalarının maksimum sayısını ve her iz dosyasının maksimum boyutunu sınırlamak için bu öğeyi seçin. Maksimum boyutta maksimum iz dosyası sayısı yazılırsa yeni bir iz dosyası yazılabilmesi için en eski iz dosyası silinir.

     Bu öğe işaretlenirse aşağıdaki alanlar için bir değer belirleyebilirsiniz:

     - **Dönüş için en fazla dosya sayısı**

       Bu alanda, yazılan iz dosyalarının maksimum sayısını belirleyebilirsiniz.

     - **Her dosya için maksimum boyut**

       Bu alanda, yazılan her iz dosyasının maksimum boyutunu belirleyebilirsiniz.

4. **Düzey** açılır listesinde izleme düzeyini seçin.

   Gerekli izleme düzeyini bir Teknik Destek uzmanına danışmanız önerilir. Teknik Destek'e danışamazsanız izleme düzeyini **Normal (500)**'e ayarlayın.

5. Kaspersky Endpoint Security'yi yeniden başlatın.

6. İzleme işlemini durdurmak için **Teknik Destek Bilgileri** penceresine dönün ve **Uygulama izleri** açılır listesinde **Devre dışı bırakıldı** öğesini seçin.

setup.ini dosyasını kullanarak veya uygulamayı komut satırından yüklerken de iz dosyaları oluşturabilirsiniz.

İz dosyalarının içeriği ve depolanması

Kullanıcılar, bilgisayarlarında yer alan bilgilerin güvenliğinden bizzat sorumludur. Özellikle verilerin Kaspersky'ye gönderilmeden önce izlenmesine ve sınırlandırılmasına daha dikkat edilmelidir.

İz dosyaları, uygulama kullanımda olduğu sürece bilgisayarda saklanır ve uygulama kaldırıldığında kalıcı olarak silinir.

İz dosyaları ProgramData\Kaspersky Lab klasörüne kaydedilir.

İz dosyası aşağıdaki ad biçimindedir: `KES<sürüm numarası_tarihXX.XX_süreXX.XX_pidXXX.><iz dosyası türü>.log`.

Kimlik Doğrulama Aracısı iz dosyası, Sistem Birim Bilgisi klasörüne kaydedilir ve aşağıdaki ada sahiptir: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

İz dosyalarına kaydedilen verileri görüntüleyebilirsiniz.

Tüm iz dosyaları aşağıdaki ortak bilgileri içerir:

- Olay zamanı.
- Yürütülen iş parçacığı sayısı.

  Kimlik Doğrulama Aracısı iz dosyası bu bilgiyi içermez.

- Olaya neden olan uygulama bileşeni.
- Olayın önem düzeyi (bilgilendirici olay, uyarı, kritik olay, hata).
- Uygulamanın bir bileşeni tarafından komutun yürütülmesini ve bu komutun yürütülmesinin sonucunu içeren olayın açıklamasıdır.

Kaspersky Endpoint Security, kullanıcı parolalarını yalnızca şifrelenmiş biçimde bir iz dosyasına kaydeder.

SRV.log, GUI.log ve ALL.log iz dosyalarının içeriği

SRV.log, GUI.log ve ALL.log iz dosyaları genel bilgilere ek olarak aşağıdaki bilgileri depolayabilir:

- Yerel bilgisayardaki dosyaların yolunda bu bilgiler bulunuyorsa soyadı, ad ve ikinci ad dahil kişisel veriler.
- Açık olarak iletildiyse kullanıcı adı ve parola. Bu veriler, İnternet trafiği taraması sırasında iz dosyalarına kaydedilebilir. Trafik sadece trafmon2.ppl'den iz dosyalarına kaydedilir.
- HTTP başlıklarında yer alıyorsa kullanıcı adı ve parola.
- Hesap adı dosya adında yer alıyorsa Microsoft Windows hesabının adı.
- Tespit edilen nesnenin adında yer alıyorsa hesabınızın adını ve parolanızı içeren e-posta adresiniz veya web adresiniz.
- Ziyaret ettiğiniz web siteleri ve bu web sitelerinden yeniden yönlendirmeler. Uygulama, web sitelerini taradığı zaman bu bilgiler iz dosyalarına yazılır.
- Proxy sunucusunda oturum açmak için kullanılan proxy sunucusu adresi, bilgisayar adı, bağlantı noktası, IP adresi ve kullanıcı adı. Uygulama bir proxy sunucusu kullanıyorsa bu bilgiler iz dosyalarına yazılır.
- Bilgisayarınızın bağlantı kurduğu uzak IP adresleri.

- Mesaj konusu, ID, gönderenin adı ve mesaj gönderenin sosyal ağdaki İnternet sayfasının adresi. İnternet Denetimi bileşeni etkinse bu bilgiler iz dosyalarına yazılır.

HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log iz dosyalarının içeriği

Genel verilere ek olarak HST.log iz dosyası, bir veritabanının ve uygulama modülü güncelleme görevinin yürütülmesi hakkında bilgi içerir.

Genel verilere ek olarak BL.log iz dosyası, uygulamanın çalışması sırasında oluşan olaylar hakkında bilgi ve uygulama hatalarının çözülmesi için gerekli verileri içerir. Uygulama, avp.exe –bl parametresi ile başlatılırsa bu dosya oluşturulur.

Genel verilere ek olarak Dumpwriter.log iz dosyası, uygulama bellek dökümü dosyası yazıldığında oluşan sorun giderme hataları için gereken servis bilgilerini içerir.

Genel verilere ek olarak WD.log iz dosyası, uygulama modülü güncelleme olayları dahil olmak üzere avpsus hizmetinin çalışması sırasında oluşan olaylar hakkında bilgi içerir.

Genel verilere ek olarak AVPCon.dll.log iz dosyası, Kaspersky Security Center bağlantı modülünün çalışması sırasında oluşan olaylar hakkında bilgi içerir.

AMSI Koruma Sağlayıcısı iz dosyalarının içeriği

Genel verilere ek olarak AMSI.log iz dosyası, üçüncü taraf uygulamalardan gelen talep üzerine gerçekleştirilen taramaların sonuçları hakkında bilgi içerir.

Posta Tehdidi Koruması bileşeninin iz dosyalarının içeriği

mcou.OUTLOOK.EXE.log iz dosyası, e-posta mesajlarının genel verilere ek olarak e-posta adreslerinin de bulunduğu kısımlarını içerebilir.

Bağlam Menüsünden Tarama bileşeninin iz dosyalarının içerikleri

shellex.dll.log iz dosyası, genel bilgilere ek olarak tarama görevinin tamamlanması hakkında bilgileri ve uygulamanın hatalarını ayıklamak için gereken verileri içerir.

Uygulama web eklentisinin iz dosyalarının içeriği

İz dosyaları, Kaspersky Security Center 11 Web Console'un dağıtıldığı bilgisayarda, Program Files\Kaspersky Lab\Kaspersky Security Center Web Console 11\logs dizininde depolanır. Web Console, kurulumdan sonra verileri yazmaya başlar ve Web Console kaldırıldıktan sonra iz dosyalarını siler.

Kaspersky Endpoint Security iz dosyaları şu şekilde adlandırılır: `logs-kes_windows-<iz dosyasının türü>.DESKTOP-<dosyanın güncellendiği tarih>.log`.

Uygulama web eklentisinin iz dosyaları, genel verilere ek olarak aşağıdaki bilgileri içerir:

- Kaspersky Endpoint Security arabiriminin kilidini kaldırmak için KLAdmin kullanıcı parolası (Parola koruması).
- Kaspersky Endpoint Security arabiriminin kilidini kaldırmak için geçici parola (Parola koruması).

- SMTP posta sunucusu için kullanıcı adı ve parola (E-posta bildirimleri).
- İnternet proxy sunucusu için kullanıcı adı ve parola (Proxy sunucusu).
- *Uygulama bileşenlerini değiştirme* görevi için kullanıcı adı ve parola.
- Kaspersky Endpoint Security görevleri ve ilke özelliklerinde belirtilen hesap kimlik bilgileri ve yolları.

Kimlik Doğrulama Aracısı iz dosyasının içeriği

Genel verilere ek olarak Kimlik Doğrulama Aracısı iz dosyası, Kimlik Doğrulama Aracısı'nın çalışması ve kullanıcı tarafından Kimlik Doğrulama Aracısı ile gerçekleştirilen eylemler hakkında bilgi içerir.

Döküm dosyalarının ve iz dosyalarının Kaspersky'ye aktarılmasını etkinleştirme veya devre dışı bırakma

Döküm ve izleme dosyalarının Kaspersky'ye aktarılmasını etkinleştirmek veya devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Pencerenin sol kısmında, **Gelişmiş Ayarlar** sekmesini seçin.
   Gelişmiş uygulama ayarları, pencerenin sağında görüntülenir.
3. **İşletim modu** bölümünde, **Ayarlar** düğmesine tıklayın.
   İşletim modu penceresi açılır.
4. **İşletim modu** penceresinde uygulamanın uygulama döküm dosyalarına yazmasını etkinleştirmek için **Döküm yazımını etkinleştir** onay kutusunu işaretleyin.
5. Aşağıdakilerden birini yapın:
   - Uygulamanın sonraki çalıştırılmasında başarısız olması durumunda döküm ve izleme dosyalarını analiz edilmesi için Kaspersky'ye göndermek üzere uygulamanın **Teknik Destek bilgilerini sunucuya yükle** penceresinde bir istem görüntülemesini isterseniz **Döküm ve iz dosyalarını Kaspersky'ye analiz edilmesi için gönder** onay kutusunu işaretleyin.
   - İstemezseniz **Döküm ve iz dosyalarını Kaspersky'ye analiz edilmesi için gönder** onay kutusunu işaretlemeyin.
6. **İşletim modu** penceresinde **Tamam**'a tıklayın.
7. Değişiklikleri kaydetmek için ana uygulama penceresinde **Kaydet** düğmesine tıklayın.

Teknik Destek sunucusuna dosya gönderme

İşletim sistemi hakkında bilgileri içeren dosyalar, izleme dosyaları ve döküm dosyaları Kaspersky Teknik Destek uzmanlarına gönderilmelidir.

Teknik Destek sunucusuna dosya göndermek için:

1. Çalışırken herhangi bir arıza verdiğinde Kaspersky Endpoint Security'yi yeniden başlatın.

   Önceki uygulamayı başlatma başarısız penceresi açılır.

   > **Önceki uygulamayı başlatma başarısız** penceresi, döküm dosyalarını ve izleme dosyalarını Teknik Destek'e gönderene veya **Gönderme** düğmesine basana kadar Kaspersky Endpoint Security her başlatıldığında (bilgisayarı yeniden başlattıktan sonrası dahil) açılır.

2. **Önceki uygulamayı başlatma başarısız** penceresinde, **buraya** tıklayarak oluşturulan dosyaların listesini açın.
3. Teknik Destek'e göndermek istediğiniz dosyaların yanındaki onay kutularını seçin.
4. **Bildirim metnini göster** düğmesine tıklayın.

   Veri Sağlama Bildirimi penceresi açılır.

5. Veri Sağlama Bildirimi metnini okuyun ve **Kapat** düğmesine tıklayın.
6. **Önceki uygulamayı başlatma başarısız** penceresinde, **Veri Sağlama Bildirimini kabul ediyorum** onay kutusunu işaretleyin.
7. **Gönder** düğmesine tıklayın.

   İstek numarası penceresi açılır.

8. **İstek numarası** penceresinde, Kaspersky CompanyAccount üzerinden Teknik Destek ile iletişim kurduğunuzda isteğinize atanan numarayı belirtin.
9. **Tamam**'a tıklayın.

Seçilen veri dosyaları sıkıştırılır ve Teknik Destek sunucusuna gönderilir.

Döküm dosyalarının ve iz dosyalarının korumasını etkinleştirme veya devre dışı bırakma

Döküm dosyaları ve izleme dosyaları işletim sistemi hakkında bilgiler ile birlikte kullanıcının gizli verilerini içerir. Bu tür verilere yetkisiz erişimin engellenmesi için döküm dosyaları ve izleme dosyalarının korunmasını etkinleştirebilirsiniz.

Döküm dosyaları ve iz dosyalarının koruması etkinleştirilirse dosyalara aşağıdaki kullanıcılar tarafından erişilebilir.

- Döküm dosyalarına sistem yöneticisi ve yerel yönetici ile döküm dosyaları ve izleme dosyalarının yazılmasına izin veren kullanıcı tarafından erişilebilir.
- İzleme dosyalarına sadece sistem yöneticisi ve yerel yönetici tarafından erişilebilir.

Döküm dosyalarının ve izleme dosyalarının korumasını etkinleştirmek veya devre dışı bırakmak için:

1. Uygulama Ayarları penceresini açın.
2. Soldaki **Gelişmiş Ayarlar** bölümünü seçin.

   Uygulama ayarları, pencerenin sağında görüntülenir.

3. **İşletim modu** bölümünde, **Ayarlar** düğmesine tıklayın.

   İşletim modu penceresi açılır.

4. Aşağıdakilerden birini yapın:

   - Korumayı etkinleştirmek isterseniz **Döküm ve izleme dosyaları korumasını etkinleştir** onay kutusunu işaretleyin.

   - Korumayı devre dışı bırakmak isterseniz **Döküm ve izleme dosyaları korumasını etkinleştir** onay kutusunu işaretlemeyin.

5. **İşletim modu** penceresinde **Tamam**'a tıklayın.

6. Değişiklikleri kaydetmek için ana uygulama penceresinde **Kaydet** düğmesine tıklayın.

Koruma etkinken yazılan döküm dosyaları ve izleme dosyaları bu işlev devre dışı bırakıldıktan sonra bile korunur.

Sözlük

Açık bırakıcılar

Sistem veya yazılım içindeki bir tür güvenlik açığını kullanan program kodu. Sömürü yazılımları genellikle kullanıcının bilgisi olmadan bilgisayara kötü amaçlı yazılım yüklemek için kullanılır.

Adres kara listesi

Kaspersky uygulaması tarafından mesajın içeriğinden bağımsız olarak gelen bütün mesajların engellendiği bir e-posta adresleri listesi.

Ağ Aracısı

Belirli bir ağ düğümünde (iş istasyonu veya sunucu) yüklü Yönetim Sunucusu ve Kaspersky uygulamaları arasındaki etkileşimi etkinleştiren bir Kaspersky Security Center bileşenidir. Bu bileşen Windows altında çalışan tüm Kaspersky uygulamaları için ortaktır. Ağ Aracısı'nın özel sürümleri, diğer işletim sistemlerinde çalışan uygulamalar için tasarlanmıştır.

Ağ Aracısı Bağlayıcısı

Uygulamayı Ağ Aracısına bağlayan uygulama işlevi. Ağ Aracısı, uygulamanın Kaspersky Security Center üzerinden uzaktan yönetilmesine olanak tanır.

Ağ hizmeti

Ağ etkinliğini tanımlayan parametreler kümesi. Bu ağ etkinliği için Güvenlik Duvarı çalışmasını düzenleyen bir ağ kuralı oluşturabilirsiniz.

Aktif anahtar

Uygulama tarafından kullanılmakta olan bir anahtar.

Anti-virüs veritabanları

Kaspersky'nin anti-virüs veritabanı sürüm tarihi itibarıyla bildiği bilgisayar güvenliği tehditleri hakkında bilgi içeren veritabanları. Anti-virüs veritabanı imzaları, taranan nesnelerdeki kötü amaçlı kodların algılanmasına yardımcı olur. Anti-virüs veritabanları Kaspersky uzmanları tarafından oluşturulur ve her saat güncellenir.

Arşiv

Bir veya daha fazla dosya tek bir sıkıştırılmış dosyaya paketlendi. Verileri paketlemek ve açmak için arşivleyici olarak adlandırılan özel bir uygulama gereklidir.

Bir web kaynağının adresinin normalleştirilmiş biçimi

Bir İnternet kaynağının normalleştirilmiş adres biçimi, normalleştirme yoluyla elde edilen bir İnternet kaynağı adresinin metinsel gösterimidir. Normalleştirme, belirli kurallara göre bir İnternet kaynağı adresinin metinsel gösterimi vasıtasıyla değişmesi işlemidir (örneğin, HTTP, kullanıcı adı, parola ve bağlantı noktasının İnternet kaynağı adresinin metin gösteriminin dışında tutulması; ayrıca, İnternet kaynağı adresinin büyük harflerden küçük harflere değiştirilmesi.)

Virüse karşı koruma bağlamında, İnternet kaynağı adreslerinin normalleştirme amacı fiziksel olarak eşitken söz diziminde farklı İnternet sitesi adreslerinin bir defadan fazla taranmasını engellemektir.

Örnek:

Bir adresin normalleştirilmemiş biçimi: www.Example.com\.

Bir adresin normalleştirilmiş biçimi: www.example.com.

Büyük olasılıkla virüslü dosya

Bilinen bir virüsün değiştirilmiş kodunu ya da bir virüse benzeyen ancak henüz Kaspersky'nın bilmediği bir kodu içeren bir dosyadır . Büyük olasılıkla virüslü dosyalar Sezgisel analiz tarafından algılanır.

Doğrulama Aracısı

Şifrelenmiş sabit sürücülere erişim sağlamak ve sistem sabit sürücüsü şifrelendikten sonra işletim sistemini yüklemek için kimlik doğrulama işlemini geçmenizi sağlayan bir arabirimdir.

Dosya maskesi

Joker karakterler kullanarak bir dosya adının ve uzantısının temsilidir.

Dosya maskeleri, joker karakterler de dahil olmak üzere dosya adlarında izin verilen tüm karakterleri içerebilir:

- ***** – Herhangi bir sıfırı veya daha fazla karakteri değiştirir.
- **?** – Herhangi bir karakteri değiştirir.

Dosya adının ve uzantısının daima bir nokta ile ayrıldığına dikkat edin.

Dosyaları Karantinaya Taşıma.

Dosyaya erişimi engelleyerek ve dosyayı orijinal konumundan, virüs bulaşması tehdidini ortadan kaldırmak için şifrelenmiş biçimde tutulduğu Karantina klasörüne taşıyarak Büyük olasılıkla virüslü bir dosyayı işleme yöntemi.

E-dolandırıcılık

Genellikle finansal veriler olan gizli verileri çalmak amacıyla e-posta mesajlarının gönderildiği bir İnternet dolandırıcılığı türüdür.

E-dolandırıcılık web adreslerinin veritabanı

Kaspersky uzmanlarının e-dolandırıcılıkla ilgili olduğunu tespit ettiği web adreslerinin bir listesi. Veritabanı düzenli olarak güncellenir ve Kaspersky uygulama dağıtım kitinin bir parçasıdır.

Ek anahtar

Uygulamayı kullanma hakkını onaylayan ancak kullanımda olmayan bir anahtar.

Görev

Kaspersky uygulaması tarafından görev olarak gerçekleştirilen işlevler, örneğin: Gerçek Zamanlı Dosya Koruma, Tam Aygıt Tarama, Veritabanı Güncellemesi.

Görev Ayarları

Her görev türüne özgü uygulama ayarları.

Güncelleme

Kaspersky güncelleme sunucularından alınan dosyaları değiştirme veya yeni dosyalar (veritabanları veya uygulama modülleri) ekleme işlemi.

Güvenilir Platform Modülü

Güvenlikle ilgili (örneğin, şifreleme anahtarlarını saklamak için) basit işlevleri sağlamak için bir mikroçip geliştirilmiştir. Bir Güvenilir Platform Modülü genellikle bilgisayarın ana kartına yüklenmiştir ve donanım veri yolu aracılığıyla tüm diğer sistem bileşenleri ile etkileşim halindedir.

İmza Analizi

Kaspersky Endpoint Security veritabanlarını kullanan, bilinen tehditlerin ve ortadan kaldırma yöntemlerinin açıklamalarını içeren bir tehdit algılama teknolojisi. İmza analizi kullanan koruma, minimum seviyede kabul edilebilir bir güvenlik düzeyi sağlar. Kaspersky uzmanlarının önerdiği şekilde bu yöntem her zaman etkindir.

Karantina

Kaspersky Endpoint Security, büyük olasılıkla virüslü dosyaları bu klasöre yerleştirir. Karantinaya alınmış dosyalar şifrelenmiş biçimde depolanır.

Koruma kapsamı

Çalıştığında virüsten koruma tarafından sürekli olarak taranan nesneler. Farklı bileşenlerin koruma kapsamları farklı özelliklere sahiptir.

Lisans Sertifikası

Kaspersky'nin anahtar dosyası veya etkinleştirme kodu ile birlikte kullanıcıya aktardığı bir belge. Kullanıcıya verilen lisans hakkında bilgi içerir.

OLE nesnesi

Ekli bir dosya veya başka bir dosyaya katıştırılmış bir dosya. Kaspersky uygulamaları, OLE nesnelerinin virüs taramasına izin verir. Örneğin, Microsoft Office Excel® tablosunu bir Microsoft Office Word dosyasına eklerseniz tablo bir OLE nesnesi olarak taranır.

Sertifika

Özel anahtar, anahtar sahibi ve anahtar kapsamı hakkında bilgi içeren ve genel anahtarın sahibine ait olduğunu onaylayan elektronik belge. Sertifika, sertifikayı düzenleyen sertifikalandırma merkezi tarafından imzalanmalıdır.

Sertifika konusu

Sertifikayla bağlantılı özel anahtarın sahibi. Bu bir kullanıcı, uygulama, herhangi bir sanal nesne, bilgisayar veya hizmet olabilir.

Sertifika veren

Sertifikayı düzenleyen sertifikalandırma merkezi.

Sezgisel Analiz

Bu teknoloji, Kaspersky uygulama veritabanlarının güncel sürümünü kullanarak tespit edilemeyen tehditleri tespit etmek için geliştirilmiştir. Bilinmeyen bir virüs veya bilinen bir virüsün yeni bir çeşidinin bulaşmış olabileceği dosyaları tespit eder.

Tarama kapsamı

Bir tarama görevi yürütülürken Kaspersky Endpoint Security tarafından taranan nesneler.

Taşınabilir Dosya Yöneticisi

Bu, bilgisayarda herhangi bir şifreleme işlevi bulunmadığında çıkarılabilir sürücüler üzerinde şifrelenmiş dosyalarla çalışmak için bir arabirim sağlayan bir uygulamadır.

Temizlik

Virüslü nesneleri, verileri tam ya da kısmen kurtarabilecek şekilde işleme yöntemi. Bütün virüslü nesneler temizlenemez.

Thumbprint sertifikası

Bir sertifika anahtarını belirlemek için kullanılan bilgiler. Thumbprint, anahtar değerine kriptografik karma kod işlevini uygulayarak oluşturulur.

Uygulama Ayarları

Uygulama performans ayarları, rapor ayarları ve yedekleme ayarları gibi her tür görevde ortak olan ve uygulamanın genel çalışmasını yöneten uygulama ayarları.

Uygulama modülleri

Uygulamanın temel işlevlerini gerçekleştiren, uygulamanın kurulum dosyasına dahil dosyalar. Uygulama tarafından gerçekleştirilen her görev türüne ayrı bir yürütülebilir modül karşılık gelir (Gerçek Zamanlı Koruma, İsteğe Bağlı Tarama ve Güncelleme). Ana uygulama penceresinden bilgisayarın tam bir taramasına başlarken, bu görevin modülünü başlatırsınız.

Virüs bulaşabilecek dosya

Yapısı veya biçimi nedeniyle saldırganlar tarafından kötü amaçlı kod saklamak ve yaymak için "taşıyıcı" olarak kullanılabilen bir dosyadır. Kural olarak bunlar .com, .exe ve .dll gibi dosya uzantılarına sahip yürütülebilir dosyalardır. Bu tür dosyalarda kötü amaçlı kodlarla saldırma riski oldukça yüksektir.

Virüslü dosya

Kötü amaçlı kod içeren bir dosya (dosya taranırken bilinen kötü amaçlı kodlar tespit edildi). Kaspersky bu tip dosyaları kullanmanızı önermez çünkü bilgisayarınıza virüs bulaştırabilirler.

Yama

Uygulamaya, uygulamanın çalışması sırasında keşfedilen hataları düzelten ya da güncellemeleri yükleyen küçük bir ek.

Yanlış alarm

Kaspersky uygulaması bir dosyanın imzası bir virüsünkine benzediği için virüslü olmayan bir dosyayı virüslü olarak rapor ettiğinde yanlış alarm oluşur.

Yedekleme

Temizlik veya silmeye çalışmadan önce oluşturulan dosyaların yedek kopyaları için özel bir depolama.

Yönetim grubu

Ortak fonksiyonları paylaşan bir aygıtlar kümesi ve bunlara yüklü olan bir Kaspersky uygulamalarının kümesi. Aygıtlar tek bir ünite olarak rahatça yönetilebilecek şekilde gruplanır. Bir grup diğer grupları içerebilir. Grupta yüklü her bir uygulama için grup ilkeleri ve grup görevleri oluşturulabilir.

Yönetim Sunucusu

Kaspersky Security Center'ın kurumsal bir ağda yüklenmiş bütün Kaspersky uygulamaları hakkında merkezi olarak bilgi depolayan bir bileşeni. Bu uygulamaları yönetmek için de kullanılabilir.

Zararlı web adreslerinin veritabanı

İçeriği tehlikeli görülebilecek web adreslerinin bir listesi. Liste, Kaspersky uzmanları tarafından oluşturulur. Düzenli olarak güncellenir ve Kaspersky uygulama dağıtım kitine dahildir.

Üçüncü taraf kod hakkında bilgi

Üçüncü taraf kod hakkındaki bilgiler, uygulamanın yükleme klasöründe legal_notices.txt dosyasında bulunur.

Ticari marka bildirimleri

Tescilli ticari markalar ve hizmet markaları, ilgili sahiplerinin mülkiyetindedir.

Adobe, Acrobat ve Shockwave, Adobe Systems Incorporated'in ABD'deki ve / veya başka yerlerdeki ticari markaları veya tescilli ticari markalarıdır.

Mac ve FireWire Apple Inc.'in Amerika Birleşik Devletleri'nde ve başka yerlerde kayıtlı olan ticari markalarıdır.

AutoCAD, Autodesk, Inc.'nin ve/veya yan kuruluşlarının/bağlı kuruluşlarının Amerika Birleşik Devletleri'ndeki ve başka yerlerdeki ticari markası veya tescilli ticari markasıdır.

Bluetooth markası ve logosu Bluetooth SIG, Inc.'e aittir.

Borland, Borland Software Corporation'ın, Amerika Birleşik Devletleri'ndeki ve başka yerlerdeki ticari markası veya tescilli ticari markasıdır.

Citrix ve Citrix Provisioning Services, Citrix Systems, Inc.'nin ve/veya yan kuruluşlarının, Amerika Birleşik Devletleri ve diğer ülkelerdeki patent bürosuna kayıtlı ticari markalarıdır.

dBase, dataBased Intelligence, Inc.'in ticari markasıdır.

EMC ve SecurID EMC Corporation'ın ABD ve başka yerlerdeki ticari markalarıdır veya tescilli EMC Corporation markalarıdır.

ICQ, ICQ LLC'nin ticari markası ve / veya hizmet markasıdır.

Intel, Pentium, Intel Corporation'ın Amerika Birleşik Devletleri'nde ve başka yerde kayıtlı olan ticari markalarıdır.

Logitech, Logitech Company'nin ABD ve başka yerlerdeki tescilli ticari markası veya ticari markasıdır.

Mail.ru, Mail.Ru LLC'nin tescilli ticari markasıdır.

Microsoft, Windows, Internet Explorer, Access, Excel, PowerPoint, Outlook, Outlook Express, Windows Server, Visual Basic, Visual FoxPro, BitLocker, LifeCam Cinema, PowerShell ve Surface, Microsoft Corporation'ın Amerika Birleşik Devletleri'nde ve başka yerlerde kayıtlı olan ticari markalardır.

Mozilla ve Thunderbird, Mozilla Foundation'ın ticari markalarıdır.

Novell, Novell Inc.'in ABD'de ve başka yerlerde kayıtlı olan ticari markasıdır.

Java ve JavaScript, Oracle Corporation'ın ve/veya yan kuruluşlarının tescilli ticari markalarıdır.

SafeNet, SafeNet, Inc'nin tescilli ticari markasıdır.

UNIX, Birleşik Devletler ve diğer yerlerde tescilli bir ticari markadır ve X/Open Company Limited lisansı kapsamında kullanılmaktadır.